jamk.fi

Tietoturvatyökalujen tuominen osaksi testausprosessia

Vesse Saastamoinen

Opinnäytetyö
Lokakuu 2016
Tekniikan ja liikenteen ala
Insinööri (AMK), tietotekniikan tutkinto-ohjelma
Tietoturva

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päivämäärä
Saastamoinen, Vesse	Opinnäytetyö, AMK	Lokakuu 2016
	Sivumäärä 87	Julkaisun kieli Suomi
		Verkkojulkaisulupa myönnetty: x

Työn nimi
Tietoturvatyökalujen tuominen osaksi Codematen testausprosessia

Tutkinto-ohjelma
Insinööri (AMK), tietotekniikan tukinto-ohjelma

Työn ohjaaja(t)
Antti Häkkinen, Karo Saharinen

Toimeksiantaja(t)
Jukka Katajaharju, Codemate Oy

Tiivistelmä

Opinnäytetyö tehtiin Codemate-nimiselle suomalaiselle ohjelmistoyritykselle, joka tarvitsi hyvää vertailua nykyisistä tietoturvatestaukseen suunnitelluista työkaluista. Vertailun tavoitteena oli löytää ja valita sopivat työkalut, joita voidaan hyödyntää Codematen testausprosessissa. Vertailua oli tarkoituksena tehdä lähinnä web-sovelluksiin suunnattuihin työkaluihin, mutta lisäksi mukaan otettiin myös muutamia verkko- ja palvelinskannereita ja Content Management System –skannereita.

Vertailtavien työkalujen valintaan käytettiin muutamia kriteerejä. Tärkeimpinä kriteereinä olivat työkalun haavoittuvuuksien löytökyky, työkalun käytettävyys, raporttien laatu ja selkeys sekä jatkuva kehitys tasaisilla päivityksillä. Kaikista työhön valituista työkaluista kirjoitettiin selkeät ja laajat teoriaosuudet joissa tuotiin esille työkalujen perustiedot, tarkat tekniset ominaisuudet, käyttöliittymät sekä skannereiden tekemät haavoittuvuustestit.

Toteutusosuudessa vertailtiin valittuja web-sovelluksiin suunnattuja työkaluja tarkemmin. Jokaisesta työkalusta vertailtiin hintaa, WAVSEP-tuloksia, OWASP top 10 kattavuutta, käytettävyyttä/ominaisuuksia ja päivityksiä. Tulososuudessa valittiin vertailluista työkaluista Codematelle sopivat ja maksullisille työkaluille valittiin myös ilmainen vaihtoehto. Valitut web-sovelluten automaattiset skannerit olivat Arachni, Acuentix, Tinfoil Security ja CMSmap. Valitut web-sovellusten manuaaliset testityökalut olivat Burp Suite ja OWASP ZAP. Web-sovellusten exploit-työkaluiksi valittiin SQLmap ja W3AF. Palvelin- ja verkkoskannereiksi valittiin OpenVAS sekä NMAP.

Työtä tehdessä selvisi, että web-sovellusskannereille on todella vaikea tehdä luotettavia vertailutestejä johtuen haavoittuviksi tehtyjen web-sovellusten ja oikeiden web-sovellusten eroavaisuuksista. Yhdellä työkalulla ei myöskään tietoturvatestauksessa usein pärjää vaan parhaat tulokset saa, kun joka osa-alueeseen käyttää siihen suunniteltua työkalua.

Avainsanat (asiasanat)
Tietoturva, tietoturvaskannerit, web-sovellukset, tietoturvatestaus

Muut tiedot

jamk.fi

Description

Author(s)	Type of publication	Date
Saastamoinen, Vesse	Bachelor's thesis	October 2016
		Language of publication: Finnish
	Number of pages: 87	Permission for web publication: x

Title of publication

Bringing security-tools to Codemate's testing process

Degree programme

Bachelor of Engineering, Information Technology

Supervisor(s)

Antti Häkkinen, Karo Saharinen

Assigned by

Jukka Katajaharju, Codemate Ltd.

Abstract

The Bachelor's thesis was assigned by a Finnish software company named Codemate. Codemate needed a good comparison of web application security-testing tools. The goal with the comparison was to find the right tools for Codemate's testing process. The comparison was to be done mostly between the web application security-testing tools and also some network scanners and Content Management System scanners were to be included.

Few criteria were used to choose the tools for comparison. The most important criteria were the vulnerability detection ability and usability of the tool, the quality of reports and continuous development including updates. An extensive theory section was written on every tool which includes the basic info, technical features, available user interfaces and the security tests executed by the scanner.

In the comparison section the web application testing tools were compared in more detail. Every tool was compared regarding its price, WAVSEP score, OWASP top 10 coverage, usability, features and updates. In the results section the suitable tools were chosen for Codemate and for every commercial tool there was also a free option. The chosen automatic scanners for web applications were Arachni, Acuentix, Tinfoil Security and CMSmap. The chosen manual tools for web applications were Burp Suite and OWAPS ZAP. The tools chosen for exploiting were SQLmap and W3AF. OpenVAS and NMAP were chosen for network scanning.

During the thesis it became clear that a reliable comparison of web application security-scanners is not that easy because of the differences in designed to be vulnerable web applications and real world web applications. Also, one tool is rarely enough for security testing and often the best results are achieved by using the right tool for the part it is mostly designed for.

Keywords/tags (subjects)

Cybersecurity, security scanners, web-applications, security testing

Miscellaneous

Sisältö

Kuviot

1 Työn lähtökohdat

Tietoturva on ajankohtainen aihe, ja sitä kohti on alkanut kääntymään jatkuvasti enemmän katseita. Maailmassa, jossa hyökkäykset tietoverkkoihin ja palvelimiin ovat jo jokapäiväinen uhka, pitää järjestelmien tietoturvallisuus nostaa korkealle prioriteettilistalla. Tätä onkin alkanut jo tapahtumaan, ja yhä useampi yritys budjetoi nykyään kohtuullisia summia rahaa tietoturvaan. Tietoturvatestauksen kysyntä on kasvanut jatkuvasti, mikä johtaa myös tarjonnan kasvuun ja tarpeeseen.

Codemate on suomalainen ohjelmistoyritys, jolla on toimipisteitä suomen lisäksi myös Aasiassa. Heidän yksi osaamisalueistaan on testaus, jota he tekevätkin jatkuvasti enemmän. Tavallisesta testauksesta heillä on jo pitkät kokemukset, mutta tietoturvatestausta on tehty vasta suhteellisen vähän. Tietoa tästä osa-alueesta he haluavatkin kasvattaa. Suurimpana tarpeena on sopivien tietoturvatyökalujen ja skannereiden löytäminen.

Tämän työn tarkoituksena olikin testata ja vertailla erilaisia tietoturvatestaukseen suunniteltuja skannereita ja työkaluja sekä valita niistä sopivat Codematen käyttöön sulautettavaksi heidän testausprosessiin. Työssä keskitytään pääasiassa web-sovellusten testaukseen suunniteltuihin työkaluihin ja skannereihin. Mukaan on myös otettu joitakin verkko– ja palvelinskannereita sekä skannereita hieman erikoisempiin tarkoituksiin.

Valintakriteereinä olivat työkalujen kyky löytää haavoittuvuuksia sekä niiden käytettävyys ja raporttien laatu. Tärkeänä kriteerinä oli myös työkalujen kehityksen jatkuvuus sekä jatkuvat päivitykset, jotka sisältävät tarvittaessa myös uusia haavoittuvuustestejä. Työssä käsiteltävät työkalut valittiin näitä kriteerejä silmällä pitäen ja vertailtavista työkaluista valittiin sopivimmat Codematen käyttöön.

2 Web-sovellusskannereiden teoria

2.1 Arachni

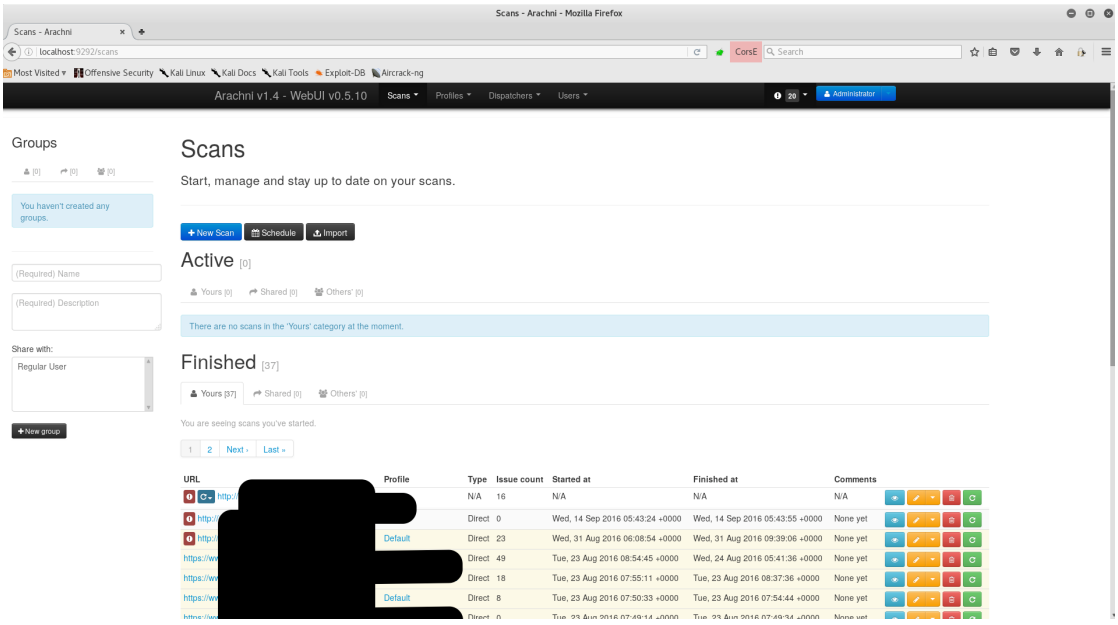
Arachni (ks. Kuvio 1) on ilmainen ja avoimelle lähdekoodille rakennettu web-sovellusten tietoturvaskanneri, jonka ensimmäinen versio julkaistiin vuonna 2010. Arachnin luoja on Anastasios ”Zapotek” Laskos niminen kreikkalainen kehittäjä, joka on rakentanut koko projektin lähes kokonaan itse. Tämä skanneri ei ole niin tunnettu kuin monet muut web-sovelluksiin keskittyvät skannerit, mutta se on alkanut saamaan lähivuosina enemmän näkyvyyttä tehokkuutensa ja haavoittuvuuksien löytökykynsä vuoksi.

Kuvio 1. Arachnin logo

Arachni on rakennettu Ruby Frameworkin päälle ja se on saatavilla Windowsille, Linuxille ja Mac OS X:lle. Se ei vaadi minkäänlaista asennusta vaan toimii suoraan käynnistämällä tarvittavat osat latauskansiostaan. Arachni on suhteellisen automatisoitu skanneri joka konfiguroidaan ympäristöön sopivaksi, minkä jälkeen skannaus aloitetaan napin painalluksella. Skannausprosessin aikana ei ole mahdollista tehdä lisäkonfigurointeja vaan sitä varten pitää tehdä uusi skannaus.

Arachni sisältää myös monipuolisesti käyttäjien tekemiä lisäosia, jotka lisäävät monia hyödyllisiä ominaisuuksia. Arachnia voi käyttää joko komentoriviltä cli-versionsa kautta tai sitä voi käyttää graafisella käyttöliittymällä. Cli-pohjainen versio on todella

monipuolinen sallien myös omien Ruby-skriptien sisällyttämisen todella monimutkaisten ympäristöjen varalle, mutta vaihtoehtoinen web-käyttöliittymä on rakennettu helpottamaan koko prosessia niin paljon, että cli-versiota tarvitsee käyttää vain erityistapauksissa. Graafinen web-käyttöliittymä toimii selaimen kautta ja se mahdollistaa Arachnin helpon käytön myös etänä. Siinä on keskitytty useampien eri tietokoneilla sijaitsevien Arachni-prosessien (dispatcher) helppoon yhdistämiseen. Tällä ominaisuudella on mahdollista skannausprosessin jakamisen monelle tietokoneelle yhtäaikaisesti, mikä nopeuttaa skannausta huomattavasti. Web-käyttöliittymä sisältää myös monipuoliset lisäosat ja konfiguraatiomahdollisuudet, jotka riittävät todella hyvin suurimpaan osaan käyttöympäristöistä. Arachnin web-käyttöliittymä näkyy kuviossa 2. Näiden lisäksi Arachni sisältää myös REST API:n, joka mahdollistaa skannerin sulauttamisen omiin olemassa oleviin järjestelmiin.



Kuvio 2. Arachnin web-käyttöliittymän scans-ikkuna (osoitteet peitetty)

Web-käyttöliittymälle voi myös luoda käyttäjiä joilla on pääsy ohjelmistoon eri oikeuksilla. Jos käyttäjä on ylläpitäjä, hän pystyy lisäämään uusia käyttäjiä ja hänellä on pääsy kaikkiin edellisiin skannauksiin. Tavallinen käyttäjä pystyy luomaan uusia skannauksia, mutta hän näkee vaan ne skannaukset, jotka hänelle on jaettu. Edellisten skannausten tiedot ja tulokset säilyvät vakiona ohjelmistopakettiin sisäänrakennetussa SQLite3 tietokannassa. Tämä tietokanta toimii hyvin pienempien skannausten

kanssa, mutta kun dataa alkaa tulla enemmän, Arachni suosittelee tietokannan vaihtamista ulkoiseen PostgreSQL tietokantaan. PostgreSQL toimii paljon paremmin isompien tietomäärien kanssa.

Arachnin päämääränä on suorittaa black box -skannausta, eli se etsii uusia haavoittuvuuksia web-sovelluksista, eikä se esimerkiksi skannaa versionumeroita ja etsi tunnettuja haavoittuvuuksia niiden perusteella. Sen skannaushaarukkaan kuuluvat muun muassa SQL-injektiot, NoSQL-injektiot, Cross Site Request Forgery –haavoittuvuudet, koodi-injektiot, erilaiset tiedostojen lisäykset (file inclusion), käyttöjärjestelmän komento-injektiot, Cross Site Scripting (XSS) –haavoittuvuudet jne. Kattava lista Arachnin skannaushaarukasta löytyy liitteestä 1. Näiden lisäksi jotkut saatavilla olevat lisäosat tuovat lisää tarkistuksia (check) skanneriin.

Skannausten parantamiseksi Arachniin on lisätty ominaisuuksia, jotka auttavat sitä käyttämään keräämänsä tietoa oppiakseen lisää web-sovelluksesta kesken skannauksen ja sulautumaan näin paremmin ympäristöön. Se analysoi jokaista sovelluksen resurssia erikseen, minkä avulla se räätälöi jokaisen http-pyynnön sovelluksen teknologioita silmällä pitäen. Tämän avulla Arachni räätälöi vain sovellukseen sopivia hyökkäyksiä eikä käytä aikaa ja kaistaa sovelluksen teknologioihin sopimattomien hyökkäyksen toimittamiseen. Arachni oppii myös HTTP-vastauksista (HTTP-response), joista se etsii uusia kenttiä ja vektoreita skannattavaksi. Lisäksi web-sovelluksen käyttäytymistä monitoroidaan jatkuvasti, minkä avulla esimerkiksi tietoa sovelluksen error 404 –viesteistä ja palvelimen terveydestä pystytään käyttämään skannausstrategian muuttamiseen kesken kaiken. Tämä lisää skannausten tarkkuutta sekä vakautta ja estää palvelimen tukkimisen liiallisella pyyntömäärällä.

Löydetyt haavoittuvuudet näkyvät web-käyttöliittymässä skannauksen sivulla ja niissä on tarkat selitykset siitä, millä keinoilla ja injektiolla haavoittuvuus löydettiin. Kuvauksessa näkyvät kokonaiset lähetetyt pyynnöt, vastaukset sekä lähdekoodi ja haavoittuvuuden vakavuus ja toimintatapa on selitetty. Kuvauksessa annetaan myös suhteellisen tarkat ohjeet haavoittuvuuden korjaamiseen. Löydettyihin haavoittuvuuksiin voi myös lisätä korjausohjeita ja ne voi merkitä tarkastettaviksi tai vääriksi hälytyksiksi. Tämän avulla muut käyttäjät voivat esimerkiksi käydä tuloksia läpi ja käyttää toisen käyttäjän syöttämiä ohjeita korjatakseen ongelmia. Näillä ominaisuuksilla ohjelmisto on rakennettu isompiin organisaatioihin sopivaksi. Itse raportin saa

ohjelmistosta ulos esimerkiksi interaktiivisena HTML-raporttina. Muita tuettuja raporttimuotoja ovat teksti, JSON, XML, YAML, Marshal ja AFR, joka on Arachnin oma raporttiformaatti. (Arachni 2016.)

Koko ohjelmiston lähdekoodi löytyy Github-sivustolta. Siellä ohjelmistolla on aktiivinen yhteisö ehdottamassa jatkuvasti uusia ominaisuuksia.

2.2 Burp Suite

2.2.1 Yleistä

Burp Suite (ks. Kuvio 3) on yksi suosituimmista web-sovellusten tietoturvatestaus-ohjelmistoista. Isoimpia syitä sen suosioon on sen monipuolisuus, se onkin suunniteltu nopeuttamaan ja helpottamaan monia tavallisesti manuaalisesti tehtäviä testejä. Burp Suite onkin enemmän kokoelma erilaisia työkaluja eikä niinkään yksi työkalu.

Kuvio 3. Burp Suiten logo

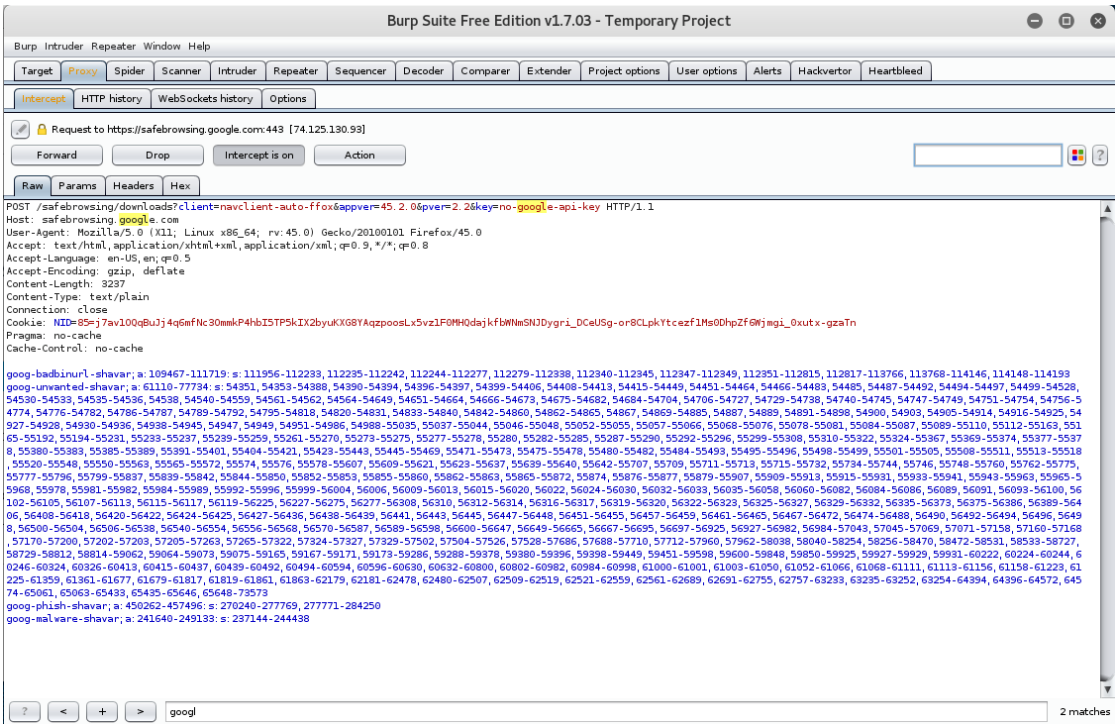
Burp Suiten ensimmäinen versio v1.0 julkaistiin vuonna 2003. Tämän jälkeen ohjelmistoa on kehitetty tasaista tahtia ja tämänhetkinen versio on v1.7 (2016). Burp Suiten kehittäjä on PortSwigger Ltd. -niminen yhtiö joka on Englannista lähtöisin.

Ohjelmisto koostuu kahdeksasta pääasiallisesta työkalusta. Työkalut ovat Proxy, Scanner, Intruder, Repeater, Sequencer, Decoder ja Comparer. Näiden lisäksi Burp

sisältää vielä yhden työkalun Extender. Extender sisältää lisäosakirjaston sekä työkalut omien lisäosien tekemiseen, kuten API-dokumentoinnin. (Portswigger 2012.)

2.2.2 Proxy

Proxy on työkalu, jota käytetään usein testauksen alkuvaiheessa. Sen avulla pystyy ohjaamaan kaiken selaimesta lähtevän ja selaimeen tulevan liikenteen Burp Suiten kautta. Tämä mahdollistaa sen, että kaikki vieraillut linkit ja selaimen pyynnöt tallentuvat Burp Suiten ”site-map” sivulistalle, josta niihin on helppo ajaa myöhemmin lisätestejä. Proxyn yksi käyttötarkoitus onkin sivun vähän varovaisempi kartoittaminen. Jotta selaimen liikenteen pystyy ongelmitta reitittämään Burpin kautta, pitää selaimeen ensin asentaa Burp Suiten oma sertifikaatti. Sertifikaatin avulla selain saadaan luottamaan Burp Suiteen, ja Burp Suite pystyy purkamaan pyyntöjen SSL-salauksen. Proxyn toinen ja ehkä isompi käyttötarkoitus on HTTP-pyyntöjen reaaliaikainen muokkaus ja pysäyttäminen (Break). Tämä ”intercept” funktio on Proxyssa vakiona päällä. Joka kerta kun web-palvelimelta tulee pyyntö selaimelle tai selaimesta lähtee pyyntö web-palvelimelle, Proxy pysäyttää pyynnön tutkittavaksi ja muokattavaksi. Pyynnön voi joko lähettää samatien eteenpäin, muokata sitä tai poistaa (drop) se kokonaan. Mikä tekee tästä työkalusta tehokkaan, on mahdollisuus tehdä automaattisia sääntöjä erilaisten pyyntöjen varalle. Joitakin tiettyjä pyyntöjä voidaan muuttaa automaattisesti ja joitain toisia voidaan poistaa automaattisesti. Proxyn käyttöliittymä ja intercept-ominaisuus näkyy kuviossa 4.



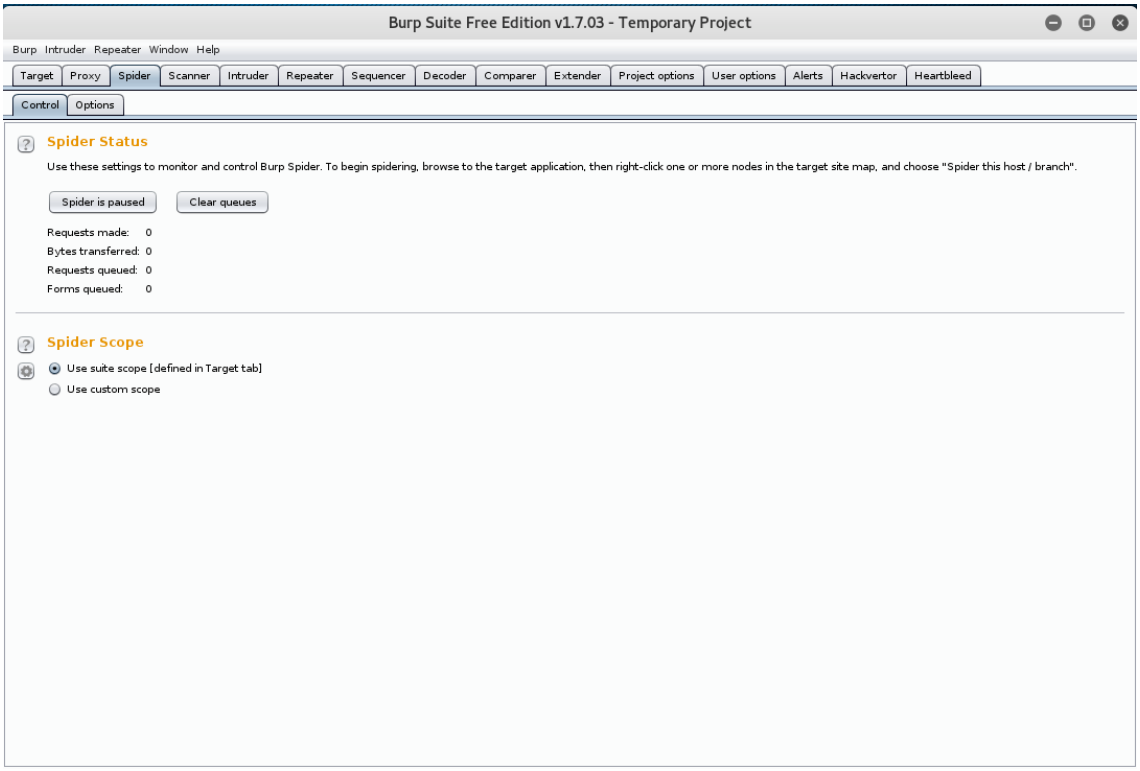
Kuvio 4. Burp Suite proxy

2.2.3 Spider

Spider on Burpin tärkein työkalu web-sovelluksen kartoittamiseen. Spider-työkalu skannaa automaattisesti koko web-sovelluksen läpi ja etsii kaikki mahdolliset linkit ja pyynnöt, joita se löytää. Se myös täyttää vastaantulevia kenttiä saadakseen niiden pyyntöjen tiedot. Sen lisäksi Spider kokeilee myös monia tunnettuja ja usein käytettyjä polkuja ja tarkistaa löytyykö niitä kyseisestä web-sovelluksesta. Spider hoitaa myös kaikki passiiviset sivustojen tallennukset site-map listalle Proxya käytettäessä. Näistä kaikista löydetyistä sivuista ja pyynnöistä Spider kasaa site-map listalle helposti luettavan sivupuun (site-tree). Spider analysoi myös sivuston ”robots.txt”-tiedoston, josta se poimii kaikki löydetyt polut.

Spider sisältää monipuoliset säätövalikot joiden avulla sen toimintaa pystyy määrittelemään todella tarkasti. Säätää voi esimerkiksi tietoja, joita syötetään vastaan tuleviin kenttiin tai lähetettävien pyyntöjen odotusväliä. Myös kirjautumiskenttiä voi määrittää asetuksista, joiden avulla Spider pääsee kartoittamaan myös kirjautumisfunktioiden takana olevia sivuja. Kirjautumisen voi hoitaa kahdella tavalla, antamalla asetuksissa käyttäjätunnukset, joiden avulla Spider hoitaa kirjautumisen itse tai antamalla

asetuksissa selaimen istunto-keksin (session cookie), jonka Spider lisää jokaiseen tekemäänsä pyyntöön. Kirjautumisoptio on varmempi, koska selaimesta otettava keksi vanhenee silloin, kun selain kirjautuu sovelluksesta ulos. Kuviossa 5 on Spider-työkalun käyttöliittymä.



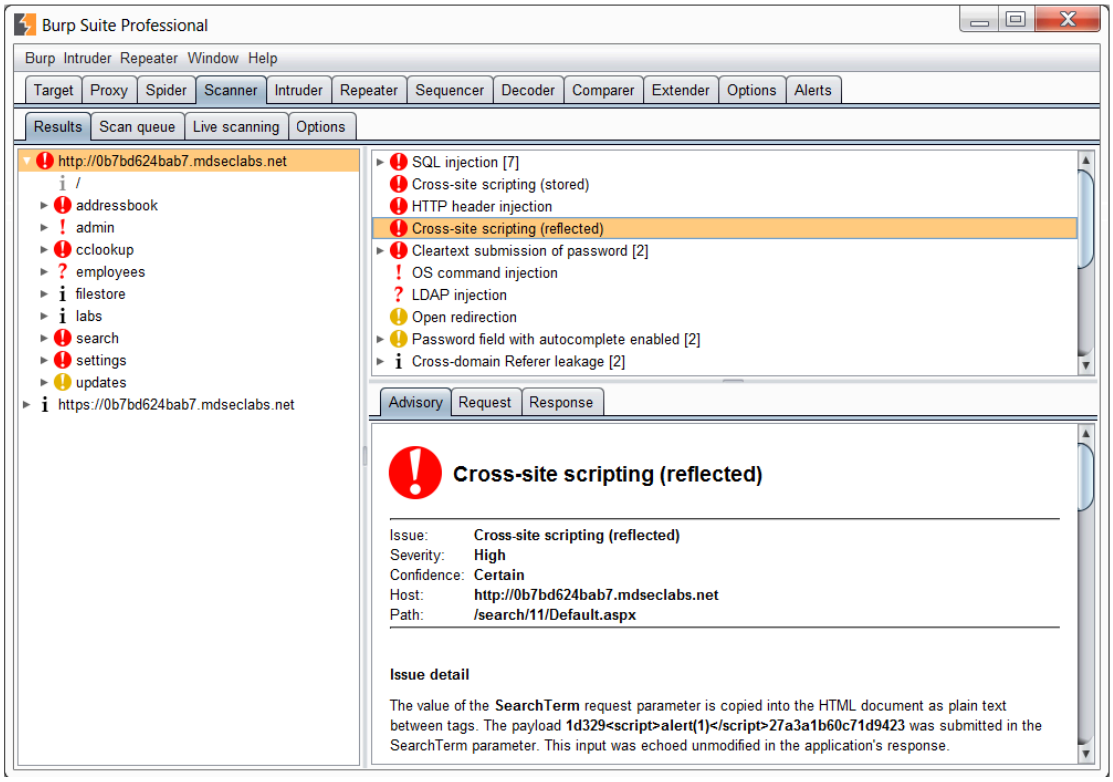
Kuvio 5. Spider-työkalun käyttöliittymä

2.2.4 Scanner

Scanner on työkalu, joka hoitaa haavoittuvuuksien automaattisen skannauksen. Se ottaa kohteensa site-mapista, jonka Spider on luonut. Skanneri voidaan määritellä skannaamaan joko tiettyjä osia site-mapista tai se voidaan määrittää skannaamaan e kokonaisuudessaan. Skanneri tekee myös passiivista skannausta silloin kun Proxy on käytössä. Passiivinen skannaus tehdään jokaiselle sivulle, jonka Spider lisää sivupuuhun. Passiivinen skannaustapa löytää haavoittuvuuksia ja ongelmia, jotka voi nähdä suoraan pyyntöjen header-osiosta tai itse pyynnöstä. Passiivinen skannaus ei siis synnytä mitään ylimääräistä liikennettä. Kolmas Scanner-työkalun vaihtoehto on aktiivinen skannaus. Kun aktiivinen skannaus otetaan käyttöön, Burp ajaa kaikki skannaus-

skenaariot niille sivuille, missä käyttäjä selaimellaan vierailee. Aktiivinen skannaus synnyttää paljon liikennettä, johtuen kaikista injektioista, joita se kokeilee.

Burp Suiten skanneri kattaa myös kaikki yleisimmät haavoittuvuudet ja sen lisäksi vielä monia muita. Liitteessä 2 on lueteltuna kaikki Burp Suiten Scanner-työkalun haavoittuvuustarkistukset. Skannauksen jälkeen kaikki tulokset näkyvät kuvion 6 mukaisesti käyttöliittymässä. Löydetyt haavoittuvuudet on luokiteltu eri vakavuusasteisiin ja ne on selitetty hyvin auki. Tulokset saa sisällytettyä interaktiiviseen HTML-pohjaiseen raporttiin, jossa ne näkyvät selkeästi ja ovat hyvin lueteltu.

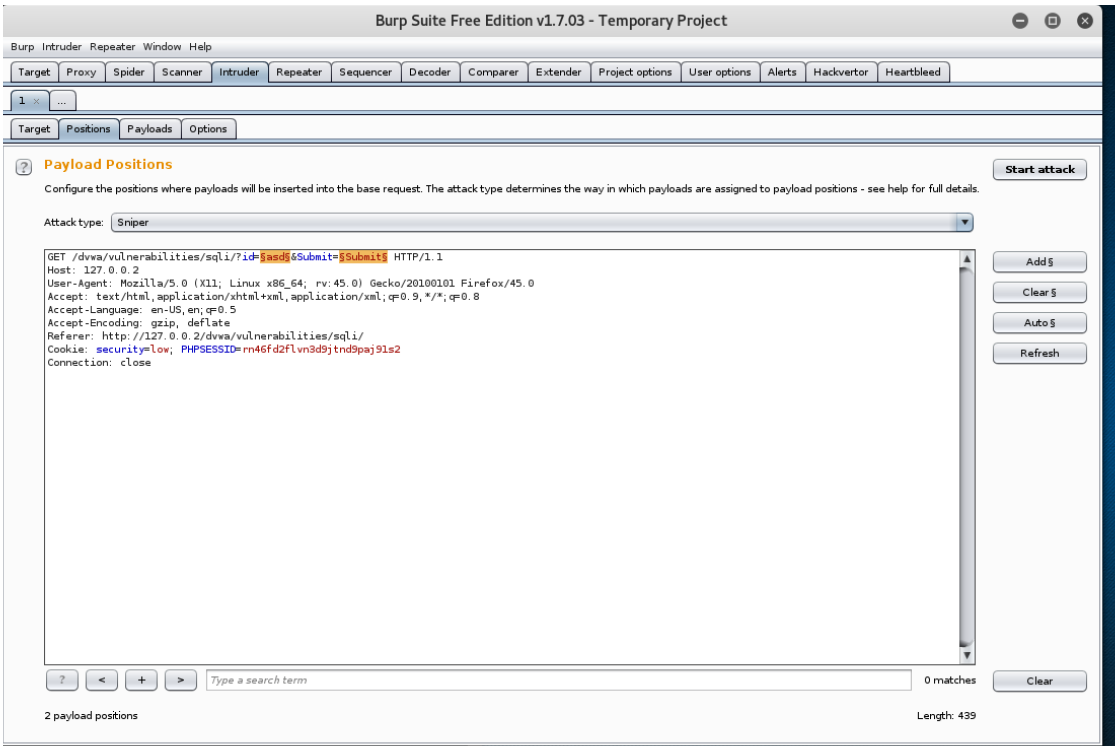


Kuvio 6. Scanner-työkalun tulos-sivu

2.2.5 Intruder

Intruder on yksi tärkein työkalu Burp Suitessa, joka erottaa sen myös hyvin muista kilpailijoista. Intruder-työkalulla on todella monia käyttötarkoituksia ja tapoja. Sillä voi valita pyynnöstä tiettyjä kohtia, joihin on tarvetta kokeilla eri arvoja tai injektioita. Sen jälkeen määritellään lista, mistä Intruder ottaa nämä syötteet. Kun nämä on määritelty, Intruder kokeilee jokaisen listassa löytyvän syötteen pyynnössä määritel-

tyihin kohtiin ja monitoroi mitä vastauksia palvelimelta tulee. Jos esimerkiksi joku injektio toimii ja palvelimelta tulee erilainen vastaus kuin normaalisti, Intruder huomaa tämän ja merkitsee sen ylös. Mahdollista on myös määrittää erilaisia hyökkäystapoja, joilla Intruder kokeilee syötteitä määriteltyihin kohtiin. Jos määriteltyjä kohtia on monta, se voidaan esimerkiksi määrittää kokeilemaan jokaiseen kohtaan samaa syötettä tai jokaiseen kohtaan täysin satunnaista syötettä. Nämä mukautumismahdollisuudet antavat tälle työkalulle lukemattomia käyttömahdollisuuksia, kuten käyttäjätunnuksiin kohdistuvia brute-force hyökkäyksiä tai vaikka denial of service -hyökkäyksiä. Burp Suiten ilmaisessa versiossa Intruder-työkalun nopeutta on rajoitettu. Kuviossa 7 näkyy GET-pyyntö, jossa on määritelty kaksi kohtaa, joihin Intruder kokeilee määriteltyjä syötteitä. Hyökkäykset kohdistetaan ”§”-merkkien väliin.

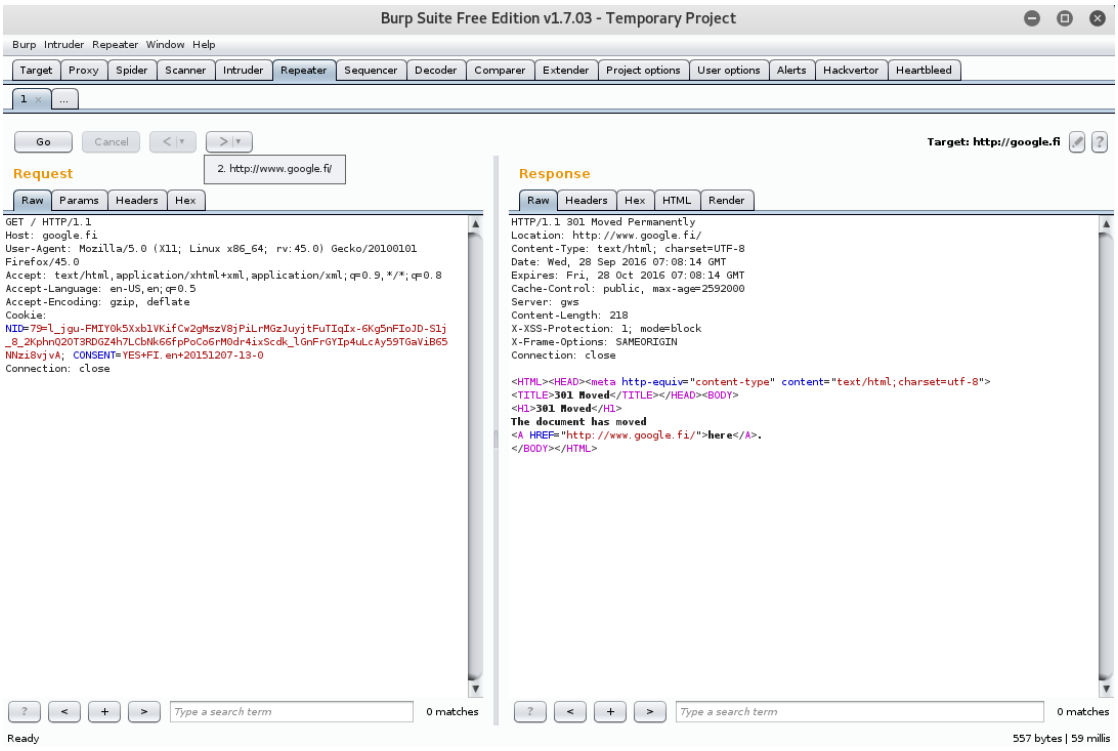


Kuvio 7. Intruder-työkalu

2.2.6 Repeater

Repeater on työkalu, jonka avulla pystytään lähettämään samaa pyyntöä moneen kertaan uudestaan ja lähetysten välissä muokkaamaan sitä tarpeen mukaan. Sillä testataan miten palvelin vastaa erilaisiin variaatioihin samasta pyynnöstä. Sen käyttöliit-

tymässä on kaksi osiota: lähetettävä pyyntö ja palvelimen vastaus. Molempia pyyntöjä pystyy myös tarkastelemaan hex-muodossa sekä erottelemaan niistä vain header- tai parametriosion. Vastaus on myös mahdollista renderoida, jolloin se näkyy samanlaisena kuin selaimessa. Ominaisuutena on myös mahdollisuus palata historiassa taaksepäin ja tarkastella edellisiä lähetettyjä pyyntöjä ja vastauksia. Historiassa olevia pyyntöjä voi myös etsiä hakusanoilla. Pyynnön ja vastauksen eroavaisuuksien etsimiselle löytyy myös automatisoitu mahdollisuus tai itse syötetty Regular Expression (regex). Repeater-työkaluun voi myös syöttää useita pyyntöjä, jotka kaikki aukeavat eri välilehdissä. Kuviossa 8 on Repeater-työkalun käyttöliittymä.

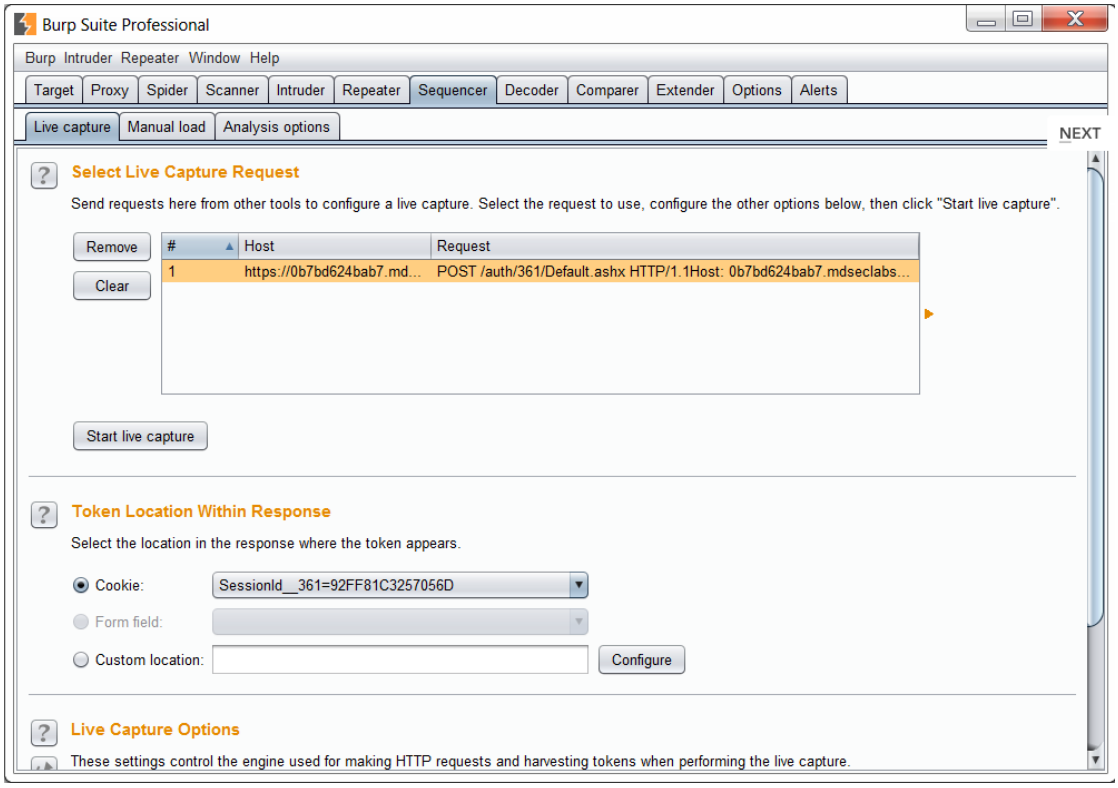


Kuvio 8. Repeater-työkalu

2.2.7 Sequencer

Sequencer on tehty erilaisten satunnaisten arvojen kuten session token tai CSRF-token satunnaisuuden testaamiseen. Tämä työkalu lähettää token-arvon saavan pyynnön useita kertoja uudestaan, kunnes se saa vähintään 100 eri token-arvoa joita vertailemalla se pystyy testaamaan niiden satunnaisuuden ja turvallisuuden. Sequencer-työkaluun on sisällytetty monia erilaisia testejä, millä se testaa näitä arvoja. Federal Information Processing Standard (FIPS)-testien ajamiseen on suositeltu vähintään

20000 tokenin lista, jotta tulos on luotettava. Testit ajettua Sequencer piirtää tuloksista graafiset kaaviot, jotka on myös selitetty hyvin auki. Kuviossa 9 näkyy Sequencer-työkalun live capture -sivu.



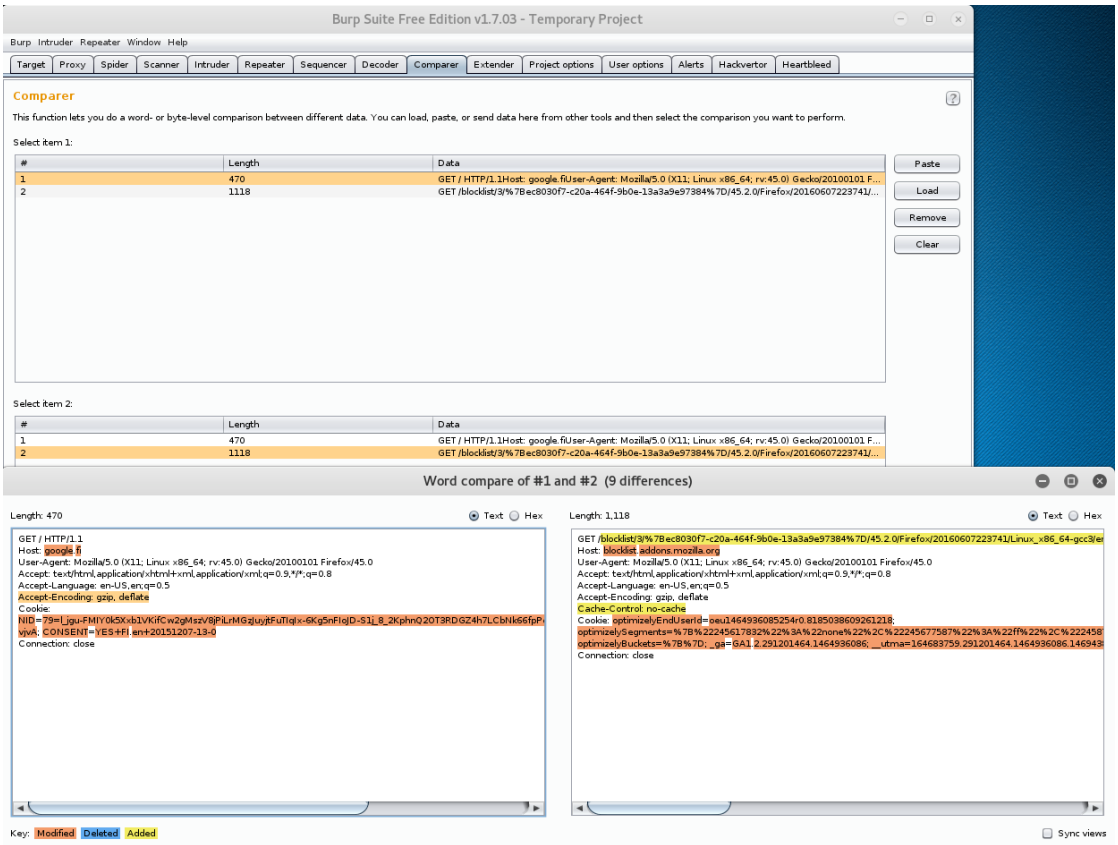
Kuvio 9. Sequencer-työkalu

2.2.8 Decoder ja Comparer

Decoder on yksinkertainen työkalu, jolla pystyy joko dekoodaamaan tai koodaamaan erilaisia merkkijonoja. Decoder tukee monia erilaisia formaatteja kuten URL, HTML, Base64, ASCII Hex, Hex, Octal, Binary ja Gzip. Näiden lisäksi Decoder pystyy myös muuntamaan merkkijonoja erilaisiksi hash-arvoiksi. Tuettuja hash-funktioita ovat SHA-384, SHA-224, SHA-256, MD2, SHA, SHA-512 ja MD5.

Comparer on myös yksinkertainen ja kätevä työkalu jolla voi vertailla kahta erilaista pyyntöä keskenään. Comparer värittää pyynnöistä eroavat ja muutetut kohdat eri väreillä.

Pyyntöjen siirto on tehty helpoksi kaikkien näiden työkalujen välillä. Suurimmassa osassa työkaluista pyyntöä hiiren oikeaa näppäintä klikkaamalla, pyynnön voi lähettää valitsemaansa toiseen työkaluun. Esimerkiksi Proxy-työkalussa voidaan valita kaksi pyyntöä listalta ja lähettää ne molemmat Comparer-työkaluun. Kuviossa 10 Comparer-työkalussa vertaillaan kahta sille lähetettyä pyyntöä. (Burp Suite 2016.)



Kuvio 10. Comparer-työkalu

2.3 OWASP Zed Attack Proxy (ZAP)

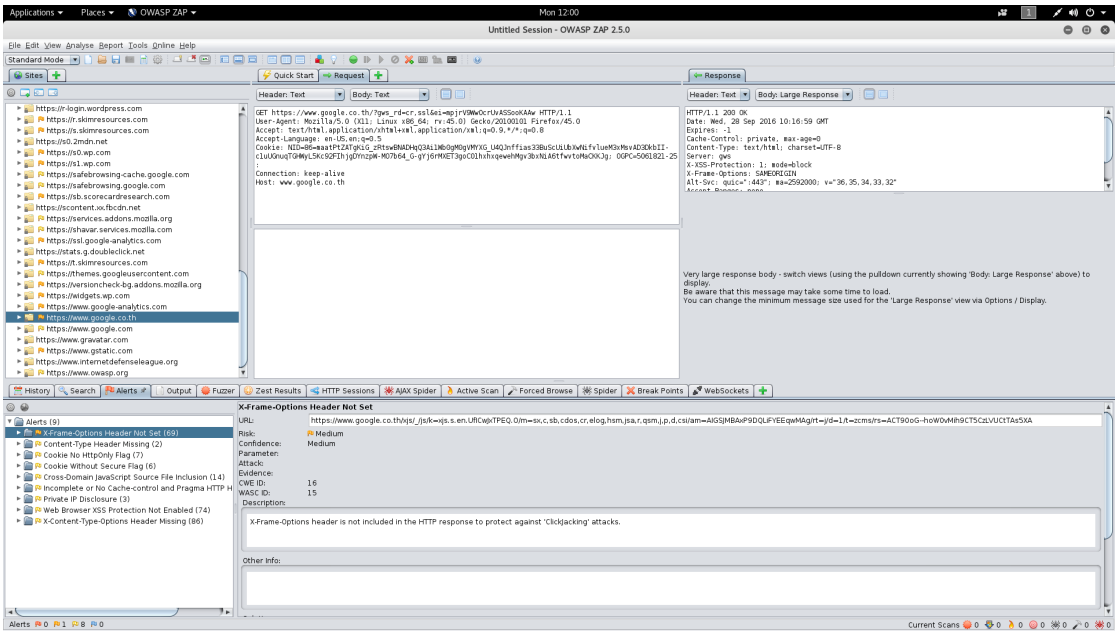
2.3.1 Yleistä

OWASP ZAP (ks. Kuvio 11) on saman tyyppinen ohjelmisto kuin Burp Suite ja siinä on monia samoja toiminnallisuuksia sisältäviä työkaluja. Myös ZAP toimii Proxy-palvelimena selaimelle eli sen kautta pystyy ohjaamaan kaikki selaimen liikenteen. ZAP on täysin ilmainen ja avoimen lähdekoodin ohjelmisto, sen lähdekoodi löytyy Github-sivustolta. ZAP 1.0.0 julkaistiin vuonna 2010 ja se on kehitetty Paros Proxyn pohjalta.

ZAP:lla on aktiivinen tukijoukko kehittämässä sitä jatkuvasti. Sille on tehty paljon erilaisia lisäosia, joista löytyy monia hyödyllisiä ominaisuuksia. Lisäosat ovatkin yksi tärkeä osa ohjelmistoa.

Kuvio 11. OWASP ZAP:n logo

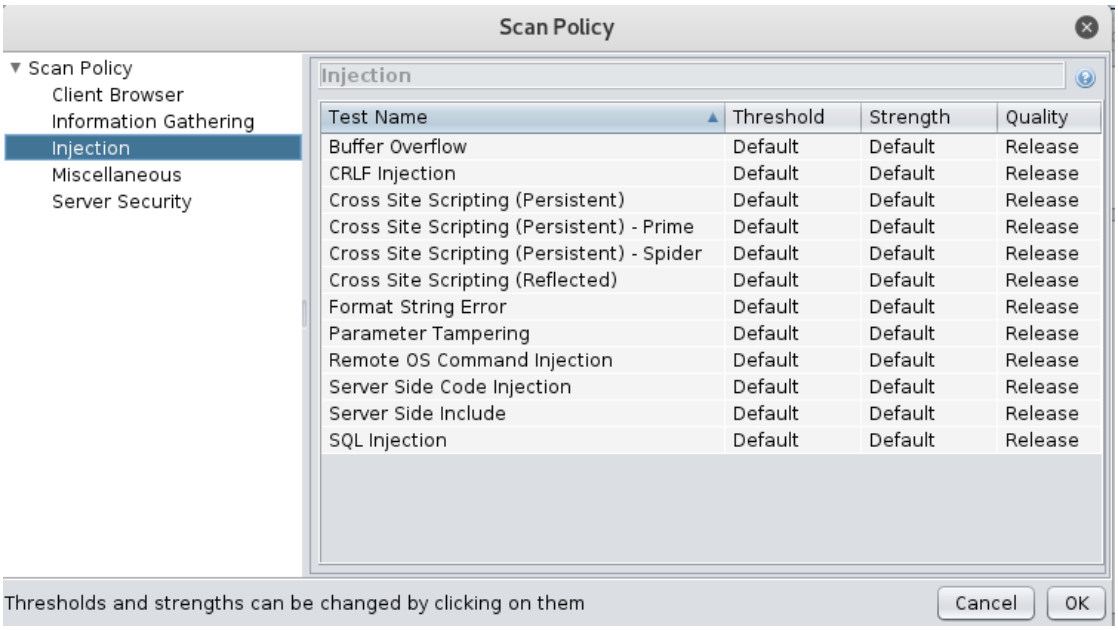
OWASP ZAP on myös yksi suosituimmista web-sovellusten tietoturva-auditointityökaluista. Siinä on mahdollista tehdä joko täysin automaattisia skannauksia tai sitten käyttää mukana tulevia työkaluja manuaaliseen testaukseen. Käyttöliittymässä vasemmalla puolella näkyvät proxyn sekä crawler-työkalun keräämät ja löytämät sivut ja pyynnöt. Alhaalla näkyvät lähetettyjen pyyntöjen historia, skannaustulokset ja kaikki muut eri työkalujen ulostulot. Keskellä ja oikealla näkyy valittu pyyntö ja sen vastaus. Kuviossa 12 näkyy Zed Attack Proxyn pääikkuna.



Kuvio 12. OWASP ZAP:n pääikkuna

2.3.2 Add-On mekanismi

Kaikki OWASP ZAP:n testit ja tarkistukset on lisätty ohjelmistoon lisäosien kautta. Kun ohjelmisto ladataan, mukana tulee jo iso osa luotettuja ja laadukkaita lisäosia, jotka sisältävät kaikki perus testit. Nämä perustestit sisältävät kaikki yleiset SQL-injektiot, XSS-testit jne. Mukana olevien lisäosien testit on lueteltu kuviossa 13, näiden lisäksi ”Server Security”-osiossa on vielä ”Path traversal” ja ”remote file inclusion” -testit. Perus lisäosien lisäksi tarjolla on paljon muita lisäosia joiden kaikkien testit eivät ole välttämättä niin laadukkaita tai sitten ne ovat vaan niin spesifejä, että niitä ei ole lisätty perus kokoonpanoon.



Kuvio 13. OWASP ZAP:n testit

Kuviossa 13 näkyy myös jokaisen testin kohdalla kolme kohtaa; Threshold, Strength ja Quality. Threshold tarkoittaa kynnystä hälytysten antamiseksi ja sen Default-arvo on määritelty medium-tasolle. Jos kynnystä suurennetaan, niin hälytyksiä tulee vähemmän ja väärät hälytykset vähenevät. Samalla joitakin oikeita haavoittuvuuksia saatetaan jättää hälyttämättä. Jos kynnystä pienennetään, niin kaikista vähänkin

epäilyä herättävistä asioista tulee hälytys. Monet näistä saattavat olla vääriä hälytyksiä. Tätä kynnystä säätämällä voi kuitenkin vaikuttaa skannausprosessiin tarpeen tullessa.

Strength eli voimakkuus on toinen arvo, jonka avulla testien määrää voidaan rajoittaa. Valmiina tulevissa asetuksissa voimakkuus on määritelty myös medium-tasolle, mutta sitä voi pienentää tai kasvattaa tarpeen mukaisesti. Vaihtoehtoina ovat Low, Medium, High ja Insane. Matala voimakkuus rajaa jokaiselle testille tietyn määrän pyyntöjä, mitä ne voivat lähettää. Medium-tasolla pyyntöjen määrä on rajoitettu noin 12 pyyntöön per testi. Insane –taso on tilanteita varten joissa pyyntöjen määrää ei ole tarvetta rajoittaa. Siinä tilassa ZAP lähettää niin paljon pyyntöjä kun on tarpeellista haavoittuvuuden varmistamiseksi. Tämä tietenkin lisää palvelimelle menevää liikennettä paljon ja pidentää skannauksen aikaa huomattavasti.

Quality eli laatu on viimeinen kohta, joka määrittelee jokaisen testin laadun. Ohjelmiston mukana tulevien lisäosien valmiissa testeissä on laaduksi määritelty Release. Lisäosia itse lisää ladatessa niiden laatu vaihtelee ja tämän takia niihin onkin lisätty quality-arvo, josta laadun näkee helposti.

2.3.3 ZAP:n tilat

Pääikkunan vasemmassa yläkulmassa on valikko josta voi valita ohjelman aggressiivisuustason jossa vaihtoehtoina ovat Safe mode, Protected mode, Standard mode ja Attack mode. Safe mode on taso, joka estää kaikki aktiiviset skannaukset niin, että niitä ei voi tehdä edes manuaalisesti. Aktiivisiin skannauksiin kuuluvat kaikki testit, jotka vaativat, että ZAP lähettää joitain dataa web-sovellukseen. Safe mode tilassa ZAP tekee siis vain passiivista skannausta.

Protected mode on taso, jossa ZAP estää kaikki aktiiviset skannaukset kohteisiin, jotka eivät ole määritelty kohdelistalle (scope). ZAP sallii kuitenkin aktiivisen skannauksen kohteisiin jotka ovat kohdelistalla tilanteissa, joissa käyttäjä manuaalisesti toteuttaa aktiivisen skannauksen. Myös Protected tilassa passiivinen skannaus toteutetaan automaattisesti.

Standard mode –tilassa ZAP sallii aktiivisen skannauksen myös kohteisiin jotka eivät ole määritelty kohdelistalle. Tämäkin tapahtuu vain, jos käyttäjä manuaalisesti toteuttaa aktiivisen skannauksen näihin kohteisiin. Muuten Standard mode on vastaava kuin Protected mode. Se on automaattisesti käytössä, kun ZAP käynnistetään.

Attack mode on viimeinen tila, joka on selvästi aggressiivisempi kuin muut. Se toteuttaa aktiivisen skannauksen automaattisesti kaikkiin sivuihin ja pyyntöihin mitä pääikkunan vasemmalla olevaan sivulistaan ilmestyy. Esimerkiksi jos Proxy on käytössä, niin aktiivinen skannaus toteutetaan automaattisesti kaikille sivuille, joissa käyttäjä selaimellaan vierailee. (Cornell 2015.)

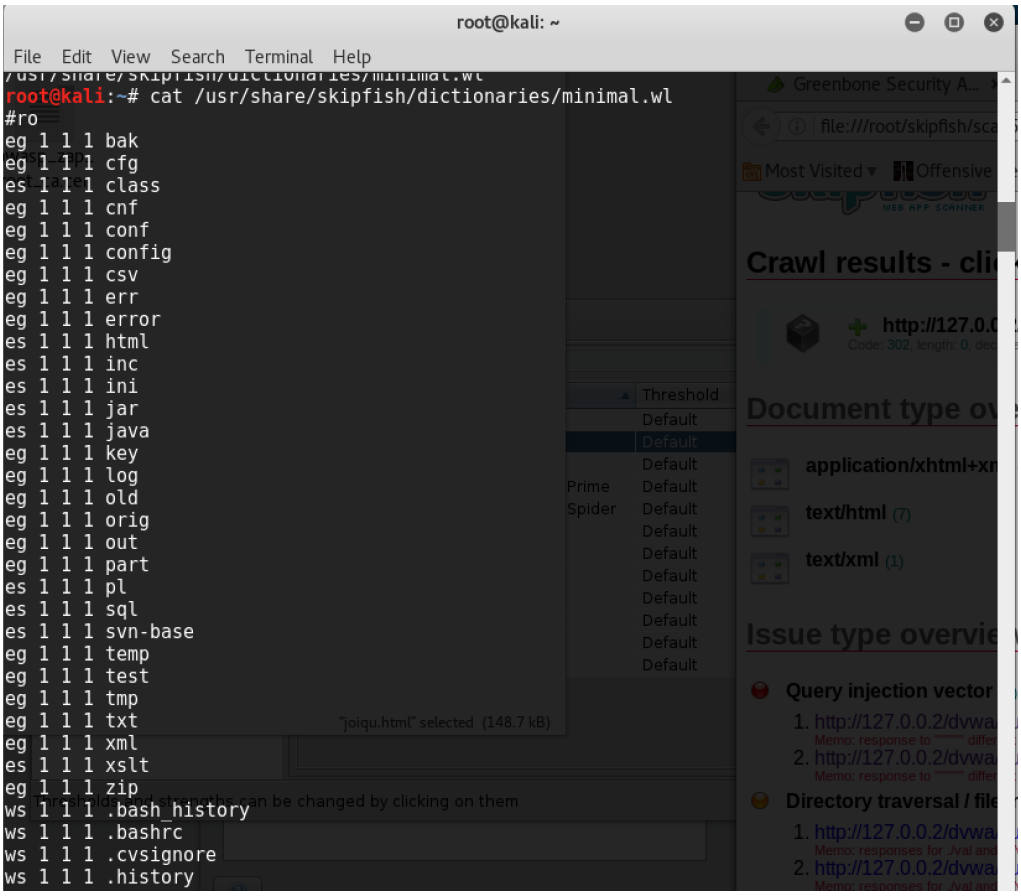
2.4 SkipFish

SkipFish (ks. Kuvio 14) on Arachnin tapaan automaattinen web-sovellusten haavoittuvuusskanneri. Se on Googlen oma projekti ja sen kehittäjinä ovat olleet Michael Zawelski, Niels Heinen ja Sebastian Roschke. Skipfish-projekti alkoi vuonna 2009 ja sen versio 1.00 julkaistiin maaliskuussa 2010. Tätä skanneria ei enää kehitetä ja sen viimeinen versio on vuodelta 2012. SkipFish on myös täysin ilmainen ja avoimen lähdekoodin ohjelmisto.

Kuvio 14. SkipFishin logo

Skipfish toimii komentoriviltä eikä sille ole tehty ollenkaan graafista käyttöliittymää. Se on ohjelmoitu kokonaan käyttäen C ohjelmointikieltä. Kehittäjien tavoitteena olikin tehdä siitä kevyt ja todella nopea skanneri, joka tekee mahdollisimman vähän turhia testejä. Skipfish-skannerin kehittäjien päämääränä oli myös tehdä skanneri helppokäyttöiseksi ja sopeutuvaksi. Se on suunniteltu sopeutumaan moniin erilaisiin ja monimutkaisiin web-sovelluksiin ja hyödyntääkin monia tekniikoita tämän toteuttamiseksi.

Jokaisen skannauksen konfiguraatioissa skannerille pitää määrittää sanalista (wordlist) johon se kerää skannauksen aikana hyödyllisiä polkuja ja nimiä. Skannausta varten voi joko luoda uuden sanalistan tai sitten käyttää sanalistaa joistain edellisistä skannauksista. Sanalistan hyötynä onkin se, että sitä voi kasvattaa erilaisia kohteita skannaamalla, jolloin se kehittyy jatkuvasti. Isosta sanalistasta hyötyy Crawler-osa, joka käy läpi web-sovelluksen polkuja sekä sivuja ja etsii aktiivisesti uusia kohteita sanalistan avulla. Kuviossa 15 näkyy osa mukana tulevan sanalistan ”minimal.wl” sisällöstä.



Kuvio 15. SkipFishin sanalista

SkipFish sisältää myös monia muita konfiguraatiomahdollisuuksia kuten erilaisia autentikaatiomekanismeja sekä erilaisia tehokkuuden opitmointisääntöjä. Myös Crawler-osalle ja tulosten ilmoittamiselle on monipuolisesti säätömahdollisuuksia. Minimikonfiguraatioihin pitää sanalistan lisäksi määritellä kansio, mihin ulostulot tallennetaan sekä skannauksen aloitusosoite.

Kun SkipFish käynnistetään konfiguraatioineen, tekee se ensimmäisenä annetusta kohteesta interaktiivisen sivukartan. Sivukartan se rakentaa tekemällä rekursiivisen crawl-skannauksen mihin se käyttää myös yllämainittua ja konfiguroitua sanalistaa. Sivukartan pohjalta SkipFish tekee kaikki tarvittavat haavoittuvuustestit kartalla oleviin kohteisiin. Kaikkien kohteiden testauksen jälkeen työkalu merkitsee löytämänsä haavoittuvuuden sivukartalle ja tallentaa raportin määriteltyyn kansioon html-muodossa tai muissa määritellyissä muodoissa.

SkipFish-skannerin mukana tulee valmiit allekirjoitus-listat (signature-list), jotka sisältävät kaikki tehtävät haavoittuvuustestit. Alun perin nämä eivät olleet muokattavissa, mutta uusimmissa versioissa tämä on muutettu. Nykyään jokainen voi tehdä listoihin omia uusia tarkistus-sääntöjä. Säännöt tehty saman tyyppisiksi kuin esimerkiksi tunnetussa Snort Intrusion Detection System –ohjelmistossa. Lista mukana tulevista haavottuvuustesteistä näkyy liitteessä 3. (Zalewski 2016.)

2.5 Tinfoil Security

2.5.1 Yleistä

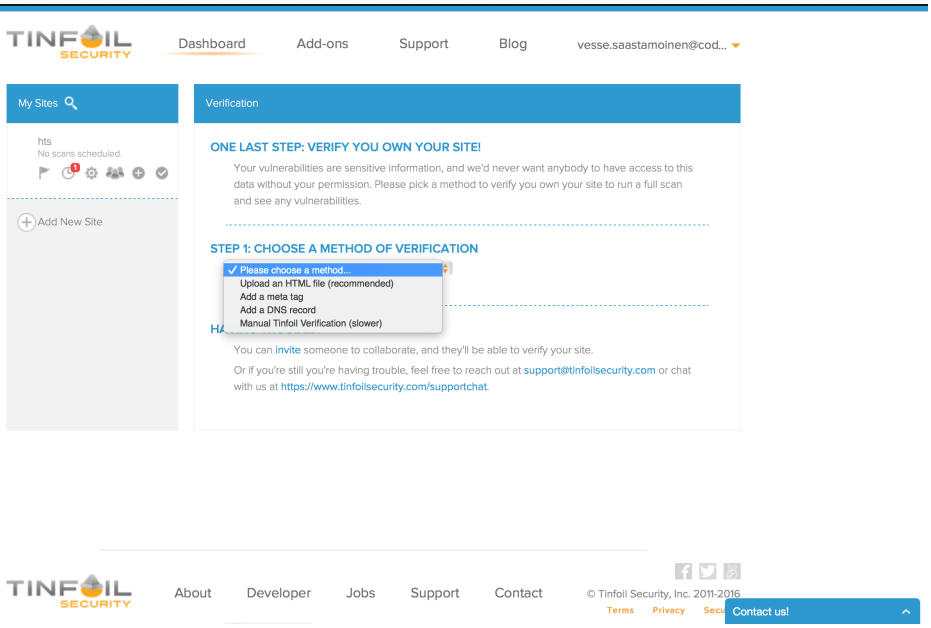
Tinfoil security (ks. Kuvio 16) on suhteellisen uusi Software as a Service (SaaS) projektina toteutettu haavoittuvuusskanneri. Projektin aloittivat kaksi MIT-yliopiston opiskelijaa Ainsley Braun ja Michael Borohovski vuonna 2011. Tinfoil security on maksullinen palvelu, joka on lähinnä suunnattu yrityksille. Se yrittää edistää DevOps-liikettä, jonka tavoitteena on helpottaa kehittäjien (Developers) ja palvelinylläpidon (Operations) välistä yhteistyötä. DevOps-integraatio näkyy palvelussa monina ominaisuuksina, joiden tarkoitus on helpottaa koko prosessia. Palvelu onkin suunniteltu myös

kehittäjien käyttöön, jotka voivat ohjeiden mukaan helposti korjata ilmeneviä haavoittuvuuksia. Tinfoil Security skannaa web-sovelluksia sekä myös pavelinpuolen haavoittuvuuksia.

Kuvio 16. Tinfoil securityn logo

2.5.2 Skannausprosessi

Tinfoil security –palvelun skannausprosessi alkaa sivuston määrittelystä ja tunnistamisesta. Skannattava sivu syötetään palveluun, jonka jälkeen palvelu pyytää käyttäjää varmistamaan sivun omakseen. Varmistuksen voi tehdä muutamalla eri tapaa, joista suositeltu tapa on Tinfoil Securityn antaman html-tiedoston lataaminen palvelimelle. Tämä osoittaa palvelulle sen, että käyttäjä on sivuston ylläpitäjä. Muita tapoja ovat mm. palvelun antaman meta tagin lisääminen sivuston ”<head>”-otsakkeeseen tai erityisen DNS rekisterin lisääminen sivuston DNS-palveluun. Varmennuksen voi tehdä myös manuaalisesti ottamalla yhteyttä palvelun asiakaspalveluun, mutta muut vaihtoehdot ovat tätä nopeampia. Kuviossa 17 näkyy varmennusvaihe.



Kuvio 17. Sivuston varmennus Tinfoil Security –palvelussa

Kuten Arachni-skannerin web-käyttöliittymässä, myös tässä palvelussa skannaukseen voi lisätä muita käyttäjiä, joilla on pääsy skannauksen tuloksiin. Eri käyttäjät (kehittäjät) voivat tulosten perusteella aloittaa haavoittuvuuksien korjaukset. Kun haavoittuvuus saadaan korjattua, skannauksen voi ajaa uudestaan vain tälle yhdelle löydetylle haavoittuvuudelle varmistaen täten, että korjaus oli toimiva. Tämän jälkeen palvelussa kyseinen haavoittuvuus voidaan merkitä korjatuksi. Skannauksen voi myös helposti uusia koko sivustolle, kun löydetyt haavoittuvuudet on korjattu. Skannauksen tulokset on esitetty selkeässä muodossa ja niihin on lisätty monipuoliset selitykset ja korjausohjeet. Tuloksista on myös piirretty monia kuvaavia graafisia kaavioita, jotka antavat kokonaiskuvan järjestelmän haavoittuvuuksista.

Tinfoil Security sisältää ominaisuuden, jonka avulla sen voi integroida myös tehtävänhallintaohjelmistojen kanssa kuten JIRA. Jos integrointi suoritetaan, niin kaikki skannauksen haavoittuvuudet lisätään tähän valittuun tehtävänhallintaohjelmistoon ja korjaustyön voi jakaa helposti tällä tavalla. Tämä on yksi ominaisuuksista, joka integroi palvelua DevOps-prosessiin. Jos integrointia halutaan lisätä vielä enemmän, Tinfoil Security tarjoaa myös API:n joka mahdollistaa vielä monipuolisempaa automatisointia. Näin automaattisen skannauksen voi esimerkiksi suorittaa aina, kun sivustosta ja web-sovelluksesta julkaistaan uusi versio.

Kuten suurin osa muista skannereista, Tinfoil Security tukee monia erilaisia autentikaatiotapoja web-sovelluksiin. HTTP-autentikaatio ja form-pohjainen autentikaatio on helppo konfiguroida palveluun. Näiden lisäksi mahdollisuutena on myös tunnistautua SAML / Single Sing-On -autentikaatioilla, joita usein löytyy uudemmista ja isommista web-sovelluksista.

2.5.3 Haavoittuvuustestit

Tinfoil Securityn skanneri on rakennettu monista open source –työkaluista ja heidän omista itse kehittämistään työkaluista. He eivät ole ilmoittaneet, mitä vapaan lähdekoodin työkaluja he ovat käyttäneet. Skanneri testaa kohdetta kehittäjän sanojen mukaan ”yleisimmiltä haavoittuvuuksilta mitä hakkerit tavallisesti sivustoilta etsivät”. Täydessä skannaukessa haavoittuvuuksia etsitään myös palvelinpuolelta, josta etsitään esimerkiksi vanhoja ohjelmistoversioita ja tunnettuja haavoittuvuuksia. Ilmoitetut web-sovelluksista etsittävät haavoittuvuudet ovat mm.

- Erilaiset SQL injektiot
- Cross Site Scripting (XSS) -haavoittuvuudet ja HTML-injektiot
- Cross Site Request Forgrery (CSRF) -haavoittuvuudet
- OS komentoinjektiot
- Validoimattomat uudelleenohjaukset (unvalidated redirects)
- LDAP injektiot
- XPath injektiot
- Muut koodi-injektiot
- HTTP Response splitting -haavoittuvuudet
- Cross site Tracing (XST) -haavoittuvuudet
- Path traversal –haavoittuvuudet
- Remote file inclusion (RFI) –haavoittuvuudet

Näiden lisäksi skanneri etsii monia muita haavoittuvuuksia joita ei ole ilmoitettu. Skanneri etsii myös yleisiä kansiopolkuja, takaovia, tiedostoja jne. Lisäksi etsintähaarukkaan kuuluvat mahdollisesti valonarat löydetyt tiedot, kuten ip-osoitteet, sähköpostit, pankkikorttinumerot ja muut vastaavat ilmoitetaan tulosten yhteydessä. (Tinfoil Security 2016.)

2.6 Acuentix

2.6.1 Yleistä

Acuentix (ks. Kuvio 18) on maksullinen haavoittuvuusskanneri, joka toimii joko SaaS web-palveluna tai vaihtoehtoisesti sen voi myös pystyttää omaan verkkoon. Acuentix skanneri julkaistiin vuonna 2005 ja nykyään se on käytössä monissa suurissa yrityksissä ja valtiollisilla tekijöillä. Skanneri on pääosin automaattinen eli se konfiguroidaan vain ennen skannausta, mutta mahdollista on myös tehdä joitain testejä manuaalisemmin. Tämä palvelu ei toimi täysin blackbox-ideologialla vaan se etsii haavoittuvuuksia web-sovelluksen ja palvelin/verkkopuolen lisäksi myös koodista. Acuentix-palvelu koostuukin kolmesta eri tyyppisestä skannerista, jotka ovat web-sovellusskanneri, palvelin/verkkoskanneri sekä wordpress-skanneri.

Kuvio 18. Acuentixin logo

2.6.2 Web-sovellusskanneri ja AcuSensor

Acuentix-palvelun pääpaino on web-sovellusten haavoittuvuusskannauksessa ja sen käyttämä DeepScan teknologia löytää tarkasti ”Asynchronous Javascript and XML” (AJAX)-tekniikkaa painottavien sivujen haavoittuvuusherkkiä osia. DeepScan-teknolo-

gia tukee myös monimutkaisempia tekniikoita kuten SOAP, JSON, Google Web Toolkit (GWT), CRUD yms. Skannerissa on panostettu nopeuteen ja se hyödyntää skannauksessa moniytimisiä prosessoriarkkitehtuureja.

Acuentix-palvelu sisältää ”Login Sequence Recorder”-työkalun jonka avulla skanneri pystyy kirjautumaan sisälle myös monimutkaisten autentikaatiomekanismien takana oleviin web-sovelluksiin. Tämä työkalu seuraa ja tallentaa kaikki kirjautumiseen tarvittavat vaiheet ja pystyy myöhemmin replikoimaan tämän prosessin. ”Login Sequence Recorder”-työkalun avulla skanneri pystyy toteuttamaan monivaiheisia autentikaatioita, SSO-autentikaatioita, CAPTCHA-mekanismeja sekä monia muita erikoisia kirjautumisia.

AcuSensor on yksi isoin Acuentix-palvelun ominaisuus, joka erottaa sen tavallisista Blackbox-haavoittuvuusskannereista. AcuSensor on pieni agenttisovellus, joka asennetaan skannattavalle palvelimelle ennen skannausta. Kun skanneri käynnistetään, AcuSensor on sen kanssa jatkuvassa yhteydessä ja lähettää skannerille tietoja myös palvelimen sisältä. Agentti seuraa mitkä osat web-sovelluksen koodista reagoivat tiettyihin haavoittuvuustesteihin ja miten ne reagoivat niihin. Jos haavoittuvuus löydetään, niin agentti lähettää skannerille sen osan koodista, mikä on haavoittuvuudesta vastuussa. Acusensor parantaa myös monien SQL-injektioiden löytämistä, koska se pystyy seuraamaan sql-kyselyitä myös suoraan palvelimella. Näiden lisäksi palvelimella oleva agentti etsii crawl-vaiheessa palvelimelta kaikki tiedostot, joihin web-palvelimen kautta on mahdollista päästä käsiksi, vaikka ne eivät ole mitenkään mainostettu web-sovelluksessa. Näistä tiedostoista agentti lähettää listan skannerille. Tämä antaa web-sovelluksesta 100% kattavan hyökkäyskartan, jota on täysin blackbox-skannereilla vaikea saavuttaa. Lopuksi Acusensor vähentää myös väärien positiivisten (false-positive) tulosten määrää, koska palvelimella oleva agentti pystyy tekemään skannauksen aikana vielä erillisiä testejä lähdekoodiin. Valmistajan mukaan Acuentix saavuttaakin lähes 0% väärissä positiivisissa.

Haavoittuvuustestejä Acuentix tekee kaikista yleisimmistä haavoittuvuuksista, joista se väittää löytävänsä XSS ja SQLi –haavoittuvuudet erittäin tarkasti. Yleisimpien haavoittuvuuksien lisäksi Acuentix-skanneri löytää myös muutamia vähän harvinaisempia haavoittuvuuksia, kuten

- Blind XSS-haavoittuvuuksia
- XML External Entity (XXE)-haavoittuvuuksia
- Server Side Request Forgery (SSRF)-haavoittuvuuksia
- Host Header -hyökkäyksiä
- Email Header –hyökkäyksiä
- Password Reset Poisoning -hyökkäyksiä

2.6.3 Palvelin/verkkoskanneri

Web-sovellusten lisäksi Acuentix skannaa myös palvelin- ja verkkopuolta, josta se etsii haavoittuvuuksia ja vääriä konfiguraatioita. Verkkopuolen skanneri on toteutettu integroimalla OpenVAS-skanneri palveluun. OpenVAS on vapaan lähdekoodin projekti ja se on yksi suosituimmista ilmaisista verkkoskannereista.

Verkkoskannauksen alussa kaikki palvelimen portit skannataan läpi ja niistä etsitään avoimet ja suodatetut portit. Skanneri pyrkii selvittämään mitä palveluja avoimissa porteissa ajetaan ja tämän jälkeen portit käydään läpi 35000 tunnetun haavoittuvuuden ja väärien konfiguraatioiden varalta. Haavoittuvuuksia etsitään myös löydetyistä verkkolaitteista kuten reitittimistä, kytkimistä, palomuureista ja kuormantasaajista (load balancer). Näiden lisäksi kirjautumista vaativat palvelut tarkistetaan heikkojen salasanojan varalta. Tällaisia palveluita ovat muun muassa FTP, IMAP, tietokannat, POP3, Socks, SSH ja Telnet. Skannauslistalla ovat myös DNS, SNMP, TLS/SLL sekä monia muita kohteita.

2.6.4 Wordpress-skanneri

Worpressin suuren suosion vuoksi Acuentix on sisältänyt palveluunsa myös erikseen Wordpress-sivustojen skannerin. Tämä skanneri käy läpi kaikki web-sovelluksesta löydetyt wordpress-kofiguraatiot sekä lisäosat konfiguraatioineen ja tarkistaa ne haavoittuvuuksien varalta. Skanneri tunnistaa yli 1200 yleistä wordpress-lisäosaa ja se etsii lisäosien joukosta mahdollisia pahansuopia lisäosia, joita hakkerit ovat ujuttaneet nettiin. Konfiguraatio tarkistetaan myös heikkojen salasanojen tunnettujen käyttäjänimien varalta.

Worpressin wp-config.php tiedostoon ei ole mahdollista päästä käsiksi web-sovelluksen kautta, ellei käyttäjällä ole ylläpito-oikeuksia. Usein ylläpitäjät kuitenkin ottavat

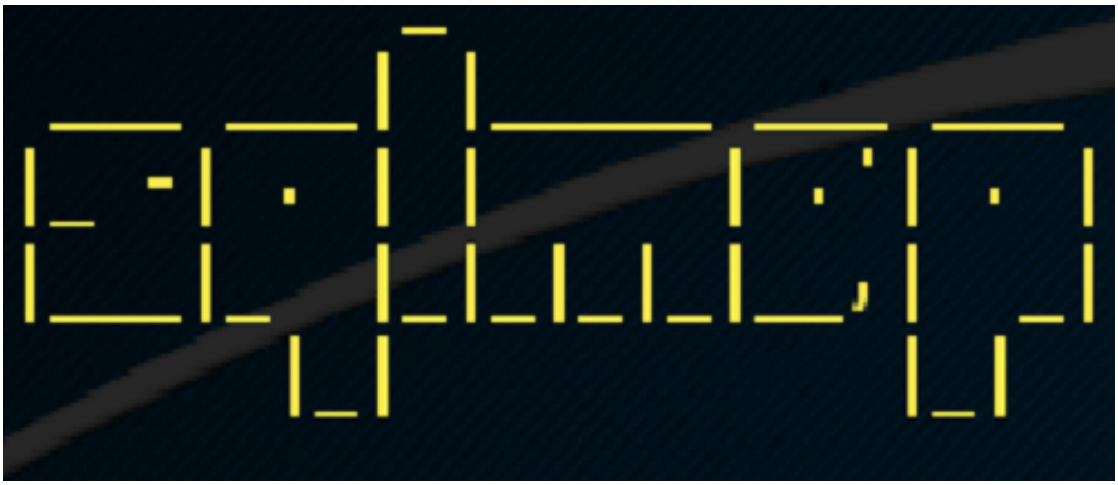
varmuuskopion tästä kyseisestä konfiguraatiotiedostosta ja jättävät sen samaan kansioon muuttamatta sen oikeuksia. Tähän varmuuskopioon voi jokainen päästä websovelluksen käyttäjä päästä käsiksi, jos pystyy vain arvaamaan varmuuskopiotiedoston nimen. Wp-config.php –tiedostosta löytyy paljon tärkeää tietoa, josta voi olla hyökkääjälle hyötyä. Wordpress-skanneri etsii myös tällaisia varmuuskopiotiedostoja kokeilemalla monia yleisiä tiedostonimiä mitä varmuuskopioille annetaan.

Skannauksen tulokset ilmoitetaan Acuentix-palvelun tulos-osiossa, jossa on koottuna myös kaikkien muiden skannereiden löydetyt haavoittuvuudet ja ilmoitukset. Tulokset saa myös helposti järjestelmästä ulos raporttina erilaisissa muodoissa.

Uusimpaan versioon Acuentix on lisännyt myös vastaavat skannerit Joomla- ja Drupal järjestelmille. (Acuentix vulnerability scanner 2016.)

2.7 SQLmap

SQLmap (ks. Kuvio 19) on SQL-injektioiden haavoittuvuusskanneri, joka on keskittynyt vain SQL-pohjaisten haavoittuvuuksien etsimiseen ja hyödyntämiseen. SQLmap on vapaan lähdekoodin työkalu, joka on käyttäjille täysin ilmainen. Sen ensimmäinen versio julkaistiin vuonna 2006 ja nyt vuonna 2016 julkaistiin versio 1.0. SQLmap toimii vain komentoriviltä eikä sen mukana tule graafista käyttöliittymää.



Kuvio 19. SQLmapin logo

SQLmap eroaa muista haavoittuvuusskannereista siinä, ettei se lopeta siinä vaiheessa, kun haavoittuvuus on löydetty. Haavoittuvuuden löytämisen jälkeen se kokeilee myös erilaisia keinoja haavoittuvuuden hyödyntämiseksi. Tämän option voi tietenkin laittaa pois päältä, mutta se on yksi tärkeä keino todistaa haavoittuvuus oikeaksi. SQLmap-työkalua käytetäänkin usein sellaisten SQL-haavoittuvuuksien varmistamiseen, jotka on löydetty jollain toisella skannerilla. Haavoittuvuusskannereiden ongelma on yleensä se, että joskus ne löytävät haavoittuvuuksia, joita ei ole olemassa. Näitä löytöjä kutsutaan vääriksi positiivisiksi (false positive) ja ainoa keino todistaa haavoittuvuus oikeaksi, on sen hyödyntäminen (exploit). Esimerkiksi SQL-injektion voi todistaa oikeaksi pyrkimällä sen kautta tietokantaan sisälle ja yrittämällä ladata koko tietokanta kyseisen haavoittuvuuden kautta. SQLmap kykenee tekemään kaiken tämän, sekä lisäksi se sisältää myös monia muita hyödyllisiä optioita. SQLmap pystyy esimerkiksi etsimään tietokannasta salasanatiivisteet ja testaamaan niiden vahvuuden. Tämän se toteuttaa suorittamalla sanakirja-pohjaisen brute-force hyökkäyksen, jossa se vertaa löydettyjä salasanatiivisteitä yleisiin salasanoihin. Jos salasanat löydetään, niin SQLmap kirjoittaa ne näytölle.

SQLmap –työkalussa tuettuja tietokantoja ovat,

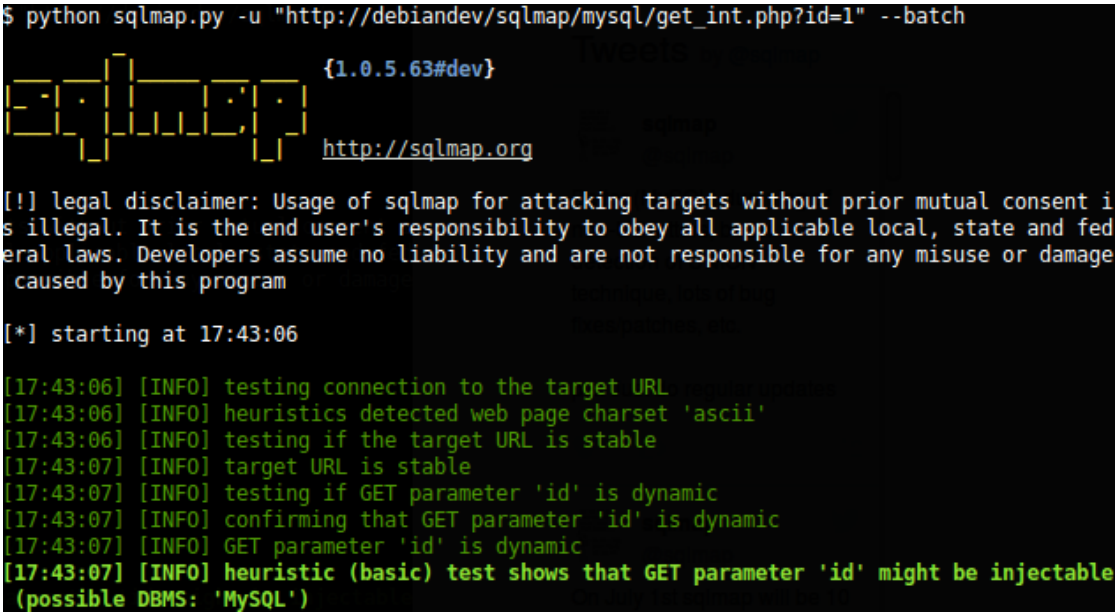
- Oracle
- MySQL
- PostgreSQL
- Microsoft SQL Server
- Microsoft Access, IBM DB2
- SQLite
- Firebird
- Sybase
- SAP MaxDB
- HSQLDB
- Informix

SQLmap ei ole täysin automaattinen työkalu vaan siinä tehdään säätöjä myös skannauksen aikana. Työkalu sisältää todella monipuolisesti optioita, joilla sen voi konfiguroida tilanteeseen kuin tilanteeseen sopivaksi. Konfiguraatiot on luokiteltu 15 kategoriaan, joita ovat

- Target
- Request
- Optimization

- Injection
- Detection
- Techniques
- Fingerprint
- Enumeration
- Brute-force
- User-defined function injection
- File system access
- Operating system access
- Windows registry access
- General
- Miscellaneous

Näistä kategorioista saa hyvän kuvan siitä, mihin kaikkeen SQLmap kykenee. Se voi muun muassa huonosti konfiguroidun tietokannan kautta saada shellin palvelimelle tai päästä käsiksi windowsin rekisteriin. (SQLmap 2016.) Kuviossa 20 näkyy juuri käynnistetty SQLmap.



Kuvio 20. SQLmap toiminnassa

2.8 W3AF

2.8.1 Yleistä

W3AF (ks. Kuvio 21) on web-sovellusten hyökkäys ja auditointityökalu, joka on ilmainen ja rakennettu vapaalle lähdekoodille. W3AF luokitellaan samaan työkalukategoriaan kuin Burp Suite ja ZAP. W3AF sisältää monia manuaalisia työkaluja, mutta myös

mahdollisuuden automaattiseen skannaukseen. Sen erottaa muista vastaavista ohjelmistoista se, että sillä voi edetä haavoittuvuuksien löytämisen jälkeen myös exploit-vaiheeseen varmistaen näin haavoittuvuuksien vakavuudet. Ohjelmisto tarjoaa selkeän graafisen käyttöliittymän, mutta se on mahdollista ajaa myös komentoriviltä. Ensimmäinen W3AF:n täysversio 1.0-rc1 julkaistiin vuonna 2009, kehittäjänä Andres Riancho.

Kuvio 21. W3AF:n logo

2.8.2 Lisäosat

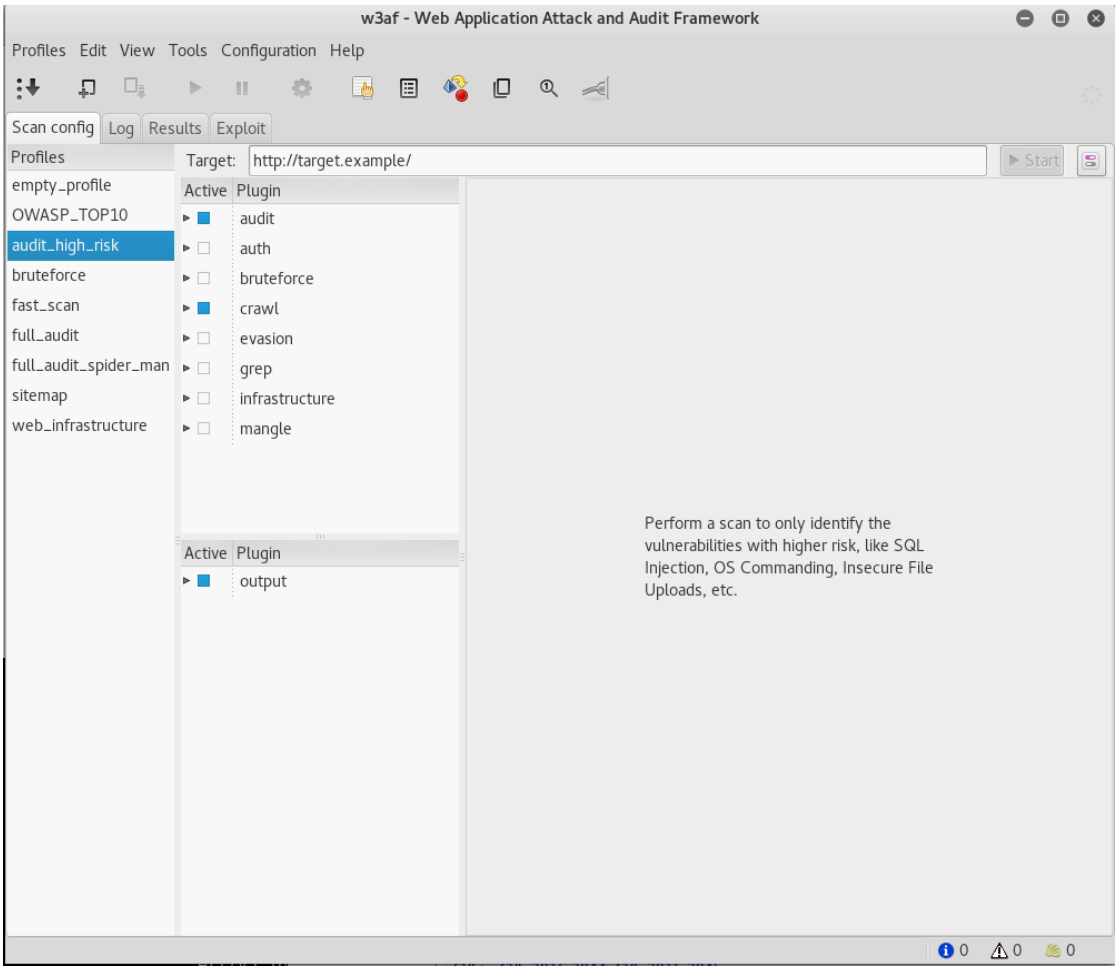
W3AF on rakennettu lisäosa-arkkitehtuurilla, missä itse pohjaohjelmisto tarjoaa vain kehykset ja kaikki haavoittuvuustestit yms. on lisätty ohjelmistoon lisäosina. Tämä arkkitehtuuri tekee uusien ominaisuuksien ja testien lisäämisen helpoksi, koska jokainen voi koodata Python-kielellä oman lisäosan ja jakaa sen muille. Tätä tapahtuukin W3AF-ohjelmistossa paljon, missä aktiivinen yhteisö on jatkuvasti luomassa uusia lisäosia ohjelmistoon.

Lisäosat ovat jaoteltu yhdeksään eri kategoriaan, kategorioita ovat

- Audit
- Auth
- Bruteforce
- Crawl
- Evasion
- Grep
- Infrastructure
- Mangle
- Output

Näistä kategorioista eniten lisäosia sisältävät Audit, Crawl, Grep ja Infrastructure. Audit-kategoria sisältää kaikki haavoittuvuuksien etsimiseen ja hyödyntämiseen tarkoitetut lisäosat. Siellä on lisäosia kaikkien yleisimpien haavoittuvuuksien löytämiseen ja myös paljon lisäosia erikoisempien haavoittuvuuksien etsimiseen. Auth-kategoriassa ovat autentikointi-lisäosat, jotka hoitavat web-sovellusten kirjautumiset skannauksen aikana. Brute-force -kategoriassa ovat lisäosat, joilla näitä web-sovellusten autentikaatioita yritetään murtaa arvaamalla salasanoja ja käyttäjänimiä. Crawl-kategoria sisältää erilaisia etsintälisäosia, jotka etsivät yleisiä tiedostoja, takaovia, wordpress-käyttäjiä, erilaisia kansiorakenteita ja monia muita kohteita. Evasion-kategoriaan kuuluvat lisäosat pyrkivät muuttamaan hyökkäyksiä niin, etteivät ne jäisi Intrusion Preventio System (IPS) –järjestelmien tai web-sovelluspalomuurien (WAF) haarukkaan kiinni, vaan pystyvät ohittamaan ne. Usein nämä lisäosat pyrkivät koodaamaan hyökkäyksiä eri keinoin.

Grep-kategoria sisältää hakulisäosia, jotka etsivät tiettyjä tietoja löydetystä datasta. Etsittyjä tietoja ovat esimerkiksi sähköpostit, ip:t , keksit, pankkikorttinumerot yms. Jotkut näistä lisäosista tekevät myös syvempää profilointia etsityillä tiedoilla. Infrastructure-kategoria pyrkii keräämään tietoa palvelimesta ja verkkopuolesta. Tämän kategorian lisäosat pyrkivät muun muassa tunnistamaan ja löytämään web-sovelluspalomuureja, välityspalvelimia, DNS-tietoja yms. Mangle-kategorian lisäosat muuttavat erilaisten pyyntöjen tietoja ja osia lennosta. Niiden tarkoituksena on automatisoida joitain haluttuja muutoksia. Viimeisenä output-kategorian lisäosat tarjoavat erilaisia keinoja tulosten muuttamiseen raporttimuotoon tai automatisoivat niiden sähköpostituksen yms. Kuviossa 22 on W3AF:n käyttöliittymä, jossa vasemmalla on profiililista ja lisäosalista. (Introduction 2016).



Kuvio 22. W3AF:n graafinen käyttöliittymä

2.8.3 Profiilit ja Exploit-osio

W3AF:ssä skannausprosessi aloitetaan valitsemalla listasta kaikki halutut lisäosat ja tarvittaessa konfiguroimaan ne. Tämän jälkeen valitut lisäosat konfigurointeineen tallennetaan profiiliksi, joka ilmestyy käyttöliittymän vasempaan laitaan. Skannaus aloitetaan valitsemalla haluttu profiili listasta. Ohjelmistossa on jo monia erilaisia profiileita valmiina jotka ovat tarkoitettu erilaisiin tilanteisiin. Valmiissa profiileissa on muun muassa nopea skannaus, hidas/täysskannaus, web-infrastruktuurin skannaus ja esimerkiksi brute-force, joka keskittyy vain autentikaatiomekanismien hyökkäämiseen.

Jotkut exploit-lisäosat eivät ole sisällytettävissä skannaukseen ja niille on tehty oma ”Exploit”-välilehti W3AF:ssä. Näihin lisäosiin kuuluu muun muassa SQLmap-lisäosa, joka hyödyntää SQLmap-ohjelmistoa löydettyjen SQL-injektioiden hyödyntämiseen.

Mukana on myös erilaisia file inclusion –lisäosia sekä hyökkäyksiä, jotka pyrkivät saamaan pääsyn käyttöjärjestelmän komentoriville (OS Shell).

2.8.4 Manuaaliset työkalut

W3AF:ssä on mukana joitain syvempää testausta ja vertailua varten tarkoitettuja työkaluja, jotka sisältävät samoja toiminnallisuuksia esimerkiksi Burp Suiten työkalujen kanssa. Manual request -työkalulla pystyy muokkaamaan ja luomaan pyyntöjä ja lähettämään niitä. Työkalu näyttää myös palvelimen lähettämän vastauksen. Työkalu mahdollistaa myös audit-kategorian lisäosatestien ajamisen suoraan kyseiseen pyyntöön. Tästä työkalusta pystyy pyynnön myös lähettämään eteenpäin muille työkaluille.

Fuzzy-request työkalu toimii vähän niin kuin Burp Suiten Intruder-työkalu. Sillä pystyy automaattisesti muuttamaan tiettyjä osia pyynnöstä ja monitoroimaan palvelimen vastausta muutosten varalta. Työkalulla pystyy generoimaan lukuja tai merkkejä tiettyyn kohtaan pyyntöä, sekä sillä pystyy myös kokeilemaan samaan kohtaan koko sanalistan sisällön, sana kerrallaan.

Encode/decode-työkalu on yksinkertainen työkalu koodausta ja dekoodausta varten. Myös siitä voi helposti siirtää käsiteltyä sisältöä eteenpäin. Export request –työkalulla pyyntöjä voi muuntaa erilaisille ohjelmille ja kielille ymmärrettävään muotoon. Tuettuna ovat HTML, Ajax, Python ja ruby. Compare request -työkalu on tehty pyyntöjen vertailua varten. Sillä saa kaksi pyyntöä auki vierekkäin ja se myös merkitsee pyynnöistä eroavaisuudet.

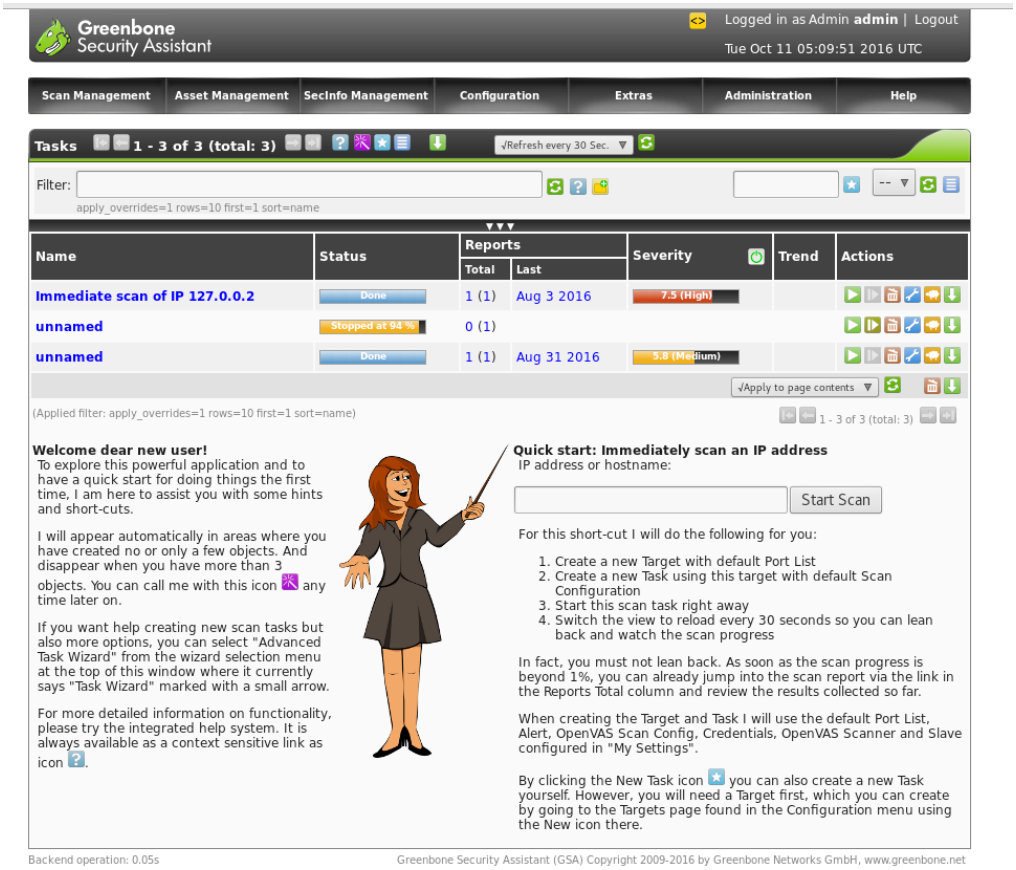
Proxy-työkalu toimii kuten muiden skannereiden proxyt. Selaimen liikenne määritellään kulkemaan sen kautta, jotta kaikki pyynnöt ja vastaukset saadaan näkyviin ohjelmaan. Myös W3AF:n proxy-työkalussa on intercept-ominaisuus, jolla jokaisen pyynnön voi pysäyttää ja tarvittaessa muuttaa ennen sen edelleen lähetystä. (Take a Tour 2016.)

3 Verkkoskannerit ja muut työkalut

3.1 OpenVAS

OpenVAS (ks. Kuvio 23) on ilmainen verkkopuolen haavoittuvuusskanneri, joka pohjautuu viimeiseen ilmaiseen versioon Nessus-verkkoskannerista, joka muuttui maksulliseksi vuonna 2005. OpenVAS-skanneria on kehittänyt joukko IT ja tietoturva-asiantuntijoita sekä myös aktiivinen yhteisö. Ohjelmisto on pääosin rakennettu vapaalle lähdekoodille ja se on selvästi suosituin ilmainen oman kategoriansa skanneri. Muita yhtä monipuolisia ja ilmaisia graafisella käyttöliittymällä toimivia verkkoskannereita ei olekaan. Lähin vaihtoehto on Nmap, joka on enemmän suunniteltu porttiskannaukseen. OpenVAS-skanneria voi käyttää cli-pohjaisesti, GTK-pohjaisella graafisella käyttöliittymällä tai uudella web-käyttöliittymällä. Kuviossa 24 on OpenVAS:n web-käyttöliittymä Greenbone Security Assistant (GSA). (OpenVAS 2016.)

Kuvio 23. OpenVASin logo



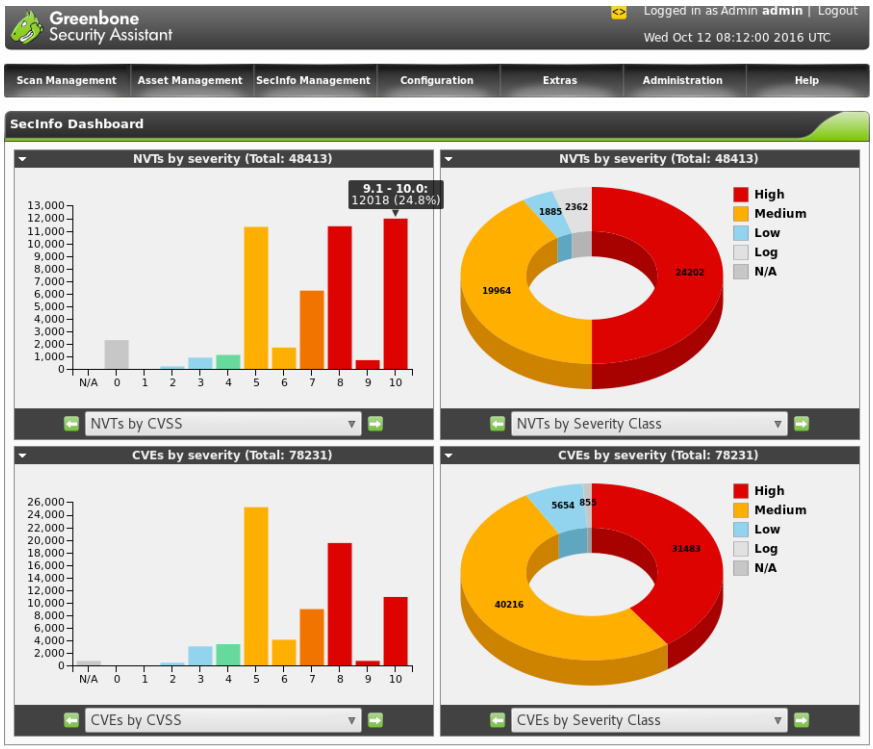
Kuvio 24. OpenVAS:n web-käyttöliittymä

OpenVAS etsii pääasiassa haavoittuvuuksia palvelimen avoimissa porteissa ajettavista palveluista sekä verkkolaitteista. Haavoittuvuustietokanta sisältää yli 48000 verkon haavoittuvuustestiä (NVT), joilla se etsii löydetyistä palveluista tunnettuja haavoittuvuuksia ja vääriä konfiguraatioita. Kuviossa 25 näkyvät OpenVAS:n NVT- ja CVE diagrammit. Common Vulnerabilities and Exposures (CVE) on järjestelmä, millä ilmoitetaan ja listataan kaikki tunnetut tietoturva-haavoittuvuudet.

NVT-haavoittuvuustestejä sekä tunnettuja haavoittuvuuksia päivitetään jatkuvasti. Myös uusia testejä tehdään usein ja niitä pystyy päivittämään web-käyttöliittymän kautta.

OpenVAS-ohjelmistoon on myös integroitu muita tunnettuja työkaluja skannauspinta-alan suurentamiseksi. Integroituina lisäosina ovat muun muassa Nmap ja W3AF. W3AF-lisäosa mahdollistaa myös web-sovellusten haavoittuvuusskannauksen ja Nmap parantaa OpenVAS:n porttiskannaustekniikoita. Integraatioiden joukossa on

vielä kymmeniä muita lisäosia, joilla on pyritty tekemään OpenVAS-skannerista mahdollisimman monipuolinen.



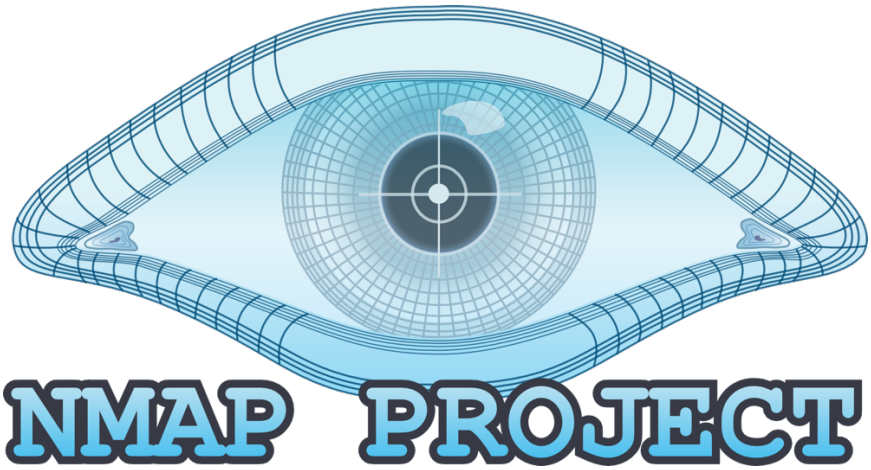
Kuvio 25. NVT/CVE diagrammit

OpenVAS ei ole suunniteltu vain kertaskannaukseen vaan sen yksi iso tavoite on myös jatkuva ylläpito. Kaikki suoritetut skannaukset ja kohteet tallentuvat tietokantaan ja niille pystyy tarvittaessa tekemään uusia skannauksia. Skannaukset voi myös automatisoida ja ajoittaa tietyin väliajoin tapahtuviksi. OpenVAS:n web-käyttöliittymässä on myös mahdollista luoda monia käyttäjiä, käyttäjäryhmiä ja rooleja. Näin eri kohteita ja skannaustuloksia voi jakaa vain tietyille henkilöille sekä toisille käyttäjille voi antaa skannausoikeuksia ja toisille ei.

Tarvittaessa OpenVAS:n voi rakentaa myös master/slave tyyppisesti, jossa slave-instansseja voi sijoittaa eri paikkoihin ja verkkoihin. Master-instanssilla voi sen jälkeen määrätä slave-instansseille skannaustehtäviä ja slave-instanssit lähettävät tulokset takaisin master-instanssille. (OpenVAS Vulnerability Scan 2016.)

3.2 NMAP

Nmap (ks. Kuvio 26) on ilmainen vapaan lähdekoodin porttiskanneri ja nykyään myös haavoittuvuusskanneri monien skriptien ansiosta. Se julkaistiin vuonna 1997 ilman versionumeroa, koska sitä ei ollut tarkoitus kehittää eteenpäin. Suosionsa vuoksi kuitenkin kehitys jatkui ja muun muassa Nessus-haavoittuvuusskanneri kehitettiin Nmap:n lähdekoodin pohjalta vuonna 1998. Tämän jälkeen Nmap:iin on tullut vuosittain useita päivityksiä ja uusia ominaisuuksia sekä kehitys jatkuu edelleen. (Introduction 2016.)



Kuvio 26. Nmap:n logo

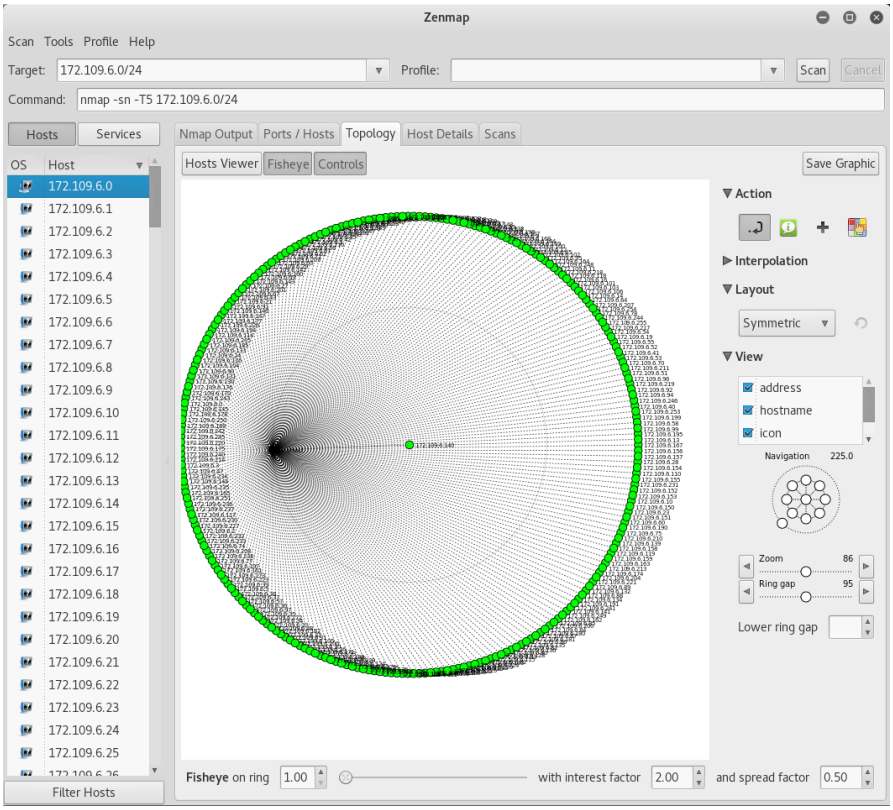
Nmap käyttää raakoja IP-paketteja skannausten tekemiseen ja kykeneekin näin todella monipuolisiin skannauksiin. Skannaustapoja on kymmeniä, joista suosituimpia ovat muun muassa SYN SCAN -skannaus, joka lähettää portteihin SYN-paketteja CONNECT-pakettien sijaan. Palomuurit eivät tunnista SYN SCAN -skannausta yhtä helposti kuin tavallista CONNECT SCAN -skannausta. Vaihtoehtoina on myös paljon erikoisempia tapoja suorittaa skannaus, joista suurin osa keskittyy palomuurien ja IDS-järjestelmien ohittamiseen ja skannauksen huomaamattomuuteen. Nmap on suunniteltu suurten verkkojen skannaukseen ja sitä onkin käytetty mm. koko internetin skannaukseen tietyn portin osalta. Se toimii kuitenkin hyvin myös yksittäisten isäntälaitteiden skannauksessa. Skannauksen aikana Nmap etsii verkosta kaikki aktiivisena olevat isäntälaitteet ja lisäksi

- Avoimissa porteissa ajetut palvelut versionumeroineen
- Käyttöjärjestelmät versioineen

- Reitittimet
- Pakettisuotimet, palomuurit ja muut esteet
- Lisäksi paljon muuta Nmap Scripting Engine (NSE):n tuomilla lisäominaisuuksilla

Nmap Scripting Engine (NSE) on tuonut Nmap:iin monia lisäominaisuuksia ja mukana tulevia skriptejä onkin jo 541 (versio 7.30). Skriptejä on laidasta laitaan, jotkut etsivät ja hyödyntävät tiettyjä haavoittuvuuksia, toiset parantavat palomuurin ohitustekniikoita. Mukana on myös paljon http-skriptejä, jotka tuovat web-sovellusten skannausominaisuuksia Nmap:iin. NSE onkin nykyään yksi tärkein osa Nmap-työkalua ja se antaa suurelle yhteisölle mahdollisuuden laajentaa työkalua haluamaansa suuntaan.

Nmap-työkalu on cli-pohjainen ohjelma, jota yleensä käytetään komentoriviltä. Nykyään sille on tehty myös graafinen käyttöliittymä Zenmap, joka sisältää kaikki Nmap:n ominaisuudet ja myös muutaman lisäominaisuuden. Esimerkiksi Zenmap piirtää löydetyistä isäntälaitteista topologian ja muutenkin jäsentelee tulokset selkeämmin kuin Nmap. Myös löydetyt palvelut listataan sivupalkkiin, josta näkee helposti mitä palveluita on eniten käytössä. Kuviossa 27 näkyy Zenmapin käyttöliittymä sekä topologia satunnaisesta verkosta. (The History and Future of Nmap 2016.)



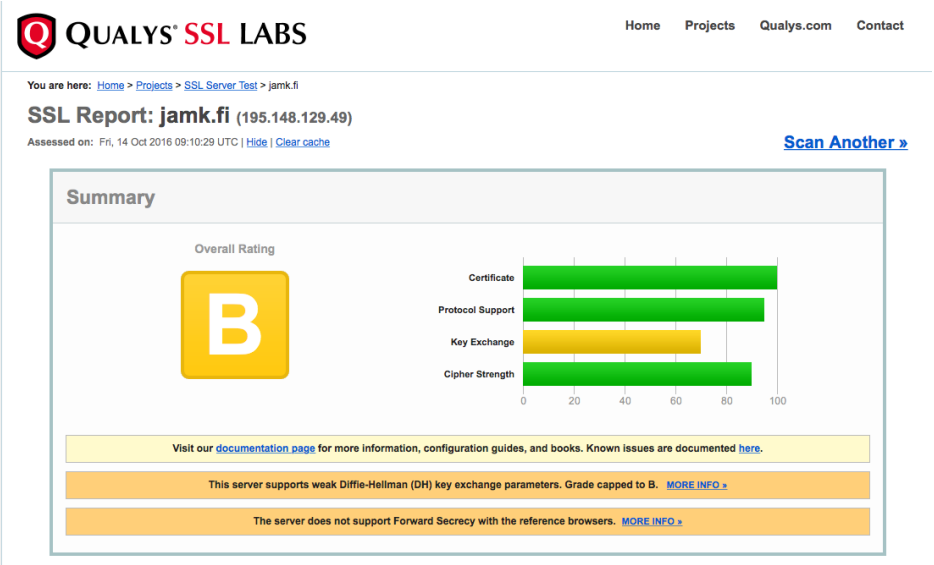
Kuvio 27. Zenmap

3.3 Qualsys SSL Labs palvelinskanneri

Qualsys SSL Labs (ks. Kuvio 28) on kokoelma dokumentteja, työkaluja ja SSL-protokollaan liittyviä keskusteluja ja ehdotuksia. Se on ei-kaupallinen tutkimusprojekti, jonka tarkoituksena on tutkia ja kehittää SSL-protokollaa. Yksi SSL Labs-projektin hyödyllisistä työkaluista on Server Scan, joka skannaa kohdeserverin SSL-protokollaa sekä testaa sen turvallisuuden. Server Scan toimii SaaS-tyyppisesti selaimesta, kuten kaikki SSL Labs:n muutkin työkalut.

Kuvio 28. Qualsys SSL Labs:n logo

Skannauksen tulokset on jaettu kolmeen osaan jotka ovat yhteenveto, autentikaatio ja konfiguraatio. Yhteenvedossa SSL Labs antaa SSL:lle yleisarvosanan sekä erittelee sertifikaatin, protokollatuen, avaimen vaihdon (key exchange) ja salausavaimen vahvuuden arvosanat. Kuviossa 29 näkyy esimerkkinä jamk.fi sivuston yhteenveto, täysi raportti on liitteessä 4. Autentikaation alla skanneri kuvaa tarkat tiedot ja käytetyt saalaukset palvelimen pääsertifikaatista ja lisäsertifikaateista. Lisäksi autentikaation alla on myös tiedot sertifikaattien luotetuista poluista.



Kuvio 29. Qualsys SSL Labs:n skannaustulos

Konfiguraation alla ovat eriteltynä hyväksytyt SSL-protokollat, salausavaintyypit (cipher suite), handshake-simulaation tulokset, protokollan yksityiskohdat ja muut sekalaiset tiedot. SSL-protokollista skanneri hyväksyy TLS 1.0-1.2 versiot joista suositeltu on TLS 1.2. SSLv2 ja SSLv3-versiot sisältävät haavoittuvuuksia ja ne näkyvät tuloksissa heti punaisina. Handshake-simulaatiossa skanneri imitoi yhdistämistä eri selaintyypeillä ja käyttöjärjestelmillä, tuloksissa näkyy mitä salaustapoja ja avaimia näille tarjotaan.

Protokollan yksityiskohdissa skanneri on testannut protokollaan tunnettuja hyökkäyksiä kuten DROWN, BEAST, POODLE, Heartbleed sekä muutamia muita. Testien tulokset on kerrottu ja niiden lisäksi tässä osiossa on paljon muutakin tietoa SSL-protokollan turvallisuudesta ja suojauksista.

SSL Labs:n palvelinskanneri on nopea keino saada kuva palvelimen SSL:n turvallisuustasosta ja hyväksytyistä salaustyypeistä yms. Tulokset ovat yksityiskohtaisia ja sisältävät paljon hyödyllistä tietoa. Palvelu on jatkuvan kehityksen alla ja uusista SSL-haavoittuvuuksista luodaan testit nopeasti.

3.4 WPScan, Joomscan, Droopescan ja CMSmap

3.4.1 Yleistä

Suurin osa web-sivustoista on rakennettu nykyään jonkun Content Management System (CMS):n avulla. Suosituimpia CMS-ympäristöjä ovat Wordpress, Joomla ja Drupal. Yleensä jokainen näistä CMS:stä on itse rakennettu turvalliseksi, suurin osa tietoturva-aukoista löytyykin näiden ympäristöjen lisäosista. Useimmat web-sovellusten haavoittuvuusskannereista eivät etsi tunnettuja haavoittuvuuksia CMS-ympäristöistä. Tätä varten löytyy kuitenkin muutamia vapaan lähdekoodin skannereita, jotka lataavat kaikki haavoittuvuustiedot julkisesta haavoittuvuustietokannasta ja vertaavat näitä web-sivustolla käytössä oleviin CMS:iin ja niiden lisäosiin.

3.4.2 WPScan

WPScan (ks. Kuvio 30) on yksi tunnetuimmista tämän käyttötarkoituksen skannereista ja se nimensä mukaisesti etsii tunnettuja haavoittuvuuksia Wordpress-sivustoilta. Sen kehittäminen alkoi vuonna 2011 ja siitä lähtien se on ollut jatkuvan kehityksen alla. WPScan toimii täysin cli-pohjaisesti, eikä sille löydy graafista käyttöliittymää (Alam 2016.)

Skannerin ominaisuuksiin kuuluu

- Käytettyjen lisäosien listaaminen
- Käytettyjen teemojen listaaminen
- Brute-force hyökkäykset heikkojen salasanojen löytämiseksi
- Brute-force hyökkäykset käyttäjänimien löytämiseksi
- Kansiorakenteen listaaminen
- Versiotietojen listaaminen
- Mahdollisten haavoittuvuuksien listaaminen
- Helpot haavoittuvuuspäivitykset

(WPScan 2016.)

Kuvio 30. WPScan:n logo

3.4.3 Joomscan

Joomscan on saman tyyppinen skanneri kuin WPScan, mutta sen kohteena ovat Joomla-ympäristöllä rakennetut web-sivustot. Joomscan-työkalun kehittäminen alkoi vuonna 2009 ja sen kehittäjänä on OWASP. Myös tämä työkalu toimii täysin cli-ympäristössä. Sen ominaisuuksiin kuuluu

- Tarkka versiontunnistus
- Yleisten Joomla-pohjaisten websovelluspalomuurien tunnistaminen
- Tunnettujen haavoittuvuuksien etsiminen Joomlasta ja sen lisäosista
- Tulokset teksti/html-raportteina
- Helpot haavoittuvuuspäivitykset

(OWASP Joomla Vulnerability Scanner Project 2016.)

3.4.4 Droopescan

Droopescan kehitettiin alun perin Drupal ja SilverStripe ympäristöjen haavoittuvuusskannaukseen, mutta nyt siihen on myös lisätty tuki Wordpressille ja osittain Joomlalle. Droopescan julkaistiin vuonna 2014 ja on ollut jatkuvassa kehityksessä siitä lähtien. Github-sivustolla siitä on tehty 102 julkaisua ja lähes 900 muutosta (commit). Ohjelma toimii cli-ympäristössä.

Droopescan ei itse tunnista skannattavaa ympäristöä vaan se pitää syöttää alkukonfiguraatioissa. Täysin tuetuista ympäristöistä skanneri etsii lisäosia, teemoja, CMS-versioita sekä mielenkiintoisia URL-polkuja. Droopescan tukee myös yksinkertaista http-autentikaatiota, jonka tunnukset sille voi syöttää ”.netrc” –tiedostossa. Monimutkaisempiin autentikaatioihin skannerin voi määrittää käyttämään esimerkiksi Burp Suitea tai ZAP:a välityspalvelimena.

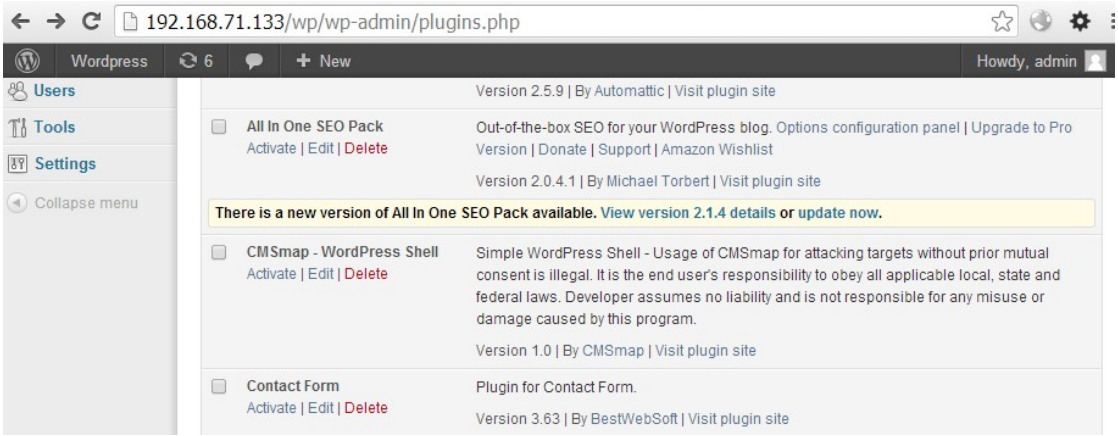
Joomla-ympäristöstä, joka ei ole vielä täysin tuettu, Droopescan etsii vain versiotiedot sekä mielenkiintoiset URL-polut.

3.4.5 CMSmap

CMSmap on ohjelmisto, jossa on pyritty yhdistämään kaikkien tunnettujen CMS:n haavoittuvuudet samaan skanneriin. CMSmap julkaistiin vuonna 2015 ja se tukee tällä hetkellä Wordpress-, Joomla- ja Drupal-ympäristöjä. Skannauksen aikana CMSmap tekee monia erilaisia testejä, joilla se pyrkii löytämään CMS-ympäristössä olevia haavoittuvuuksia ja vääriä konfiguraatioita. Skannerille ei tarvitse kertoa käytössä olevaa CMS-ympäristöä vaan se tunnistaa sen omilla testeillään. CMSmap etsii

- Versiotietoja
- Käytössä olevia teemoja
- Yleisiä tiedostoja
- Lisäosia

CMSmap tukee multithread-skannausta, jossa samalle prosessorille annetaan useita tehtäviä samanaikaisesti. Oletusarvona säikeiden määrä on 5. Ominaisuutena ovat myös brute-force hyökkäykset heikkojen salasanojen testaamiseen. Brute-force hyökkäyksiä voi ohjelman kautta tehdä myös löydetyille salasanatiivisteille, tähän CMSmap käyttää tehokasta HashCAT ohjelmistoa. Jos CMSmap löytää joidenkin haavoittuvuuksien kautta sivustolta käyttäjätunnuksia, niin niihin ajetaan automaattisesti brute-force hyökkäys kokeillen viittä yleisintä salasanaa. Jos toimivat tunnukset löydetään, niin CMSmap lataa sivustolle shell-lisäosan, jonka kautta pystyy palvelimelle syöttämään komentoja. Kuviossa 31 näkyy asennettu lisäosa.



Kuvio 31. CMSmapin shell-lisäosa

Kaikki etsityt haavoittuvuudet ladataan www.exploit-db.com haavoittuvuustietokannasta. Tämä tietokanta sisältää ajankohtaisimmat haavoittuvuustiedot kaikista CMS-ympäristöistä ja niiden lisäosista. (Michele 2014.)

4 Web-sovellusskannereiden vertailu

4.1 OWASP top 10

Open Web Application Security Project (OWASP) on voittoa tavoittelematon säätiö, joka perustettiin vuonna 2001. Se on kansainvälinen organisaatio sekä myös avoin yhteisö, jonka tavoitteena on kehittää ja ylläpitää luotettavia ohjelmia sekä tietoa tietoturvan kehittämisestä. Kaikki OWASP:n työkalut, foorumit ja dokumentit ovat ilmaisia ja kaikkien vapaassa käytössä. OWASP:n tavoitteena onkin kehittää ihmisten ja organisaatioiden tietoisuutta tietoturvasta ja tarjota sitä varten luotettavia työkaluja. (The OWASP Foundation 2016.)

OWASP top 10 lista sisältää listan kymmenestä kriittisimmästä web-sovellusten tietoturvariskistä. Jokainen riski sisältää kuvauksen, esimerkkihaavoittuvuuden, esimerkkihyökkäyksen, neuvoja hyökkäykseltä suojautumiseen ja referenssejä OWASP:n dokumentaatioon sekä muihin hyödyllisiin lähteisiin. Listaa on ollut kehittämässä monia tietoturva-asiantuntijoita ympäri maailmaa.

OWASP suosittelee kaikkia yrityksiä ottamaan tämän listan käyttöön organisaatioissaan ja varmistamaan, etteivät heidän web-sovelluksensa sisällä näitä haavoittuvuuksia. Listaa on pyritty kääntämään mahdollisimman monelle kielelle. (OWASP Top Ten Project 2016.)

4.2 Web Application Vulnerability Scanner Evaluation Project (WAVSEP)

WAVSEP on web-sovellusten haavoittuvuusskannereiden testaamiseen tehty projekti. Se on web-sovellus, joka sisältää paljon tunnettuja ja dokumentoituja haavoittuvuuksia. WAVSEP-projektin kehittäjä on Shay Chen ja projektin ensimmäinen versio julkaistiin vuonna 2010. Tämän jälkeen projektia on käytetty moniin erilaisiin haavoittuvuustyökalujen benchmark-testeihin. (wavsep 2016.)

Sectoolsmarket-sivuston tekemä web-sovellusskannereiden benchmark-testi käyttää WAVSEP-projektia. Tämän sivuston tekemässä skannerivertailussa on otettu WAVSEP-tulosten lisäksi myös huomioon työkalujen hintatiedot, auditointiominaisuuksien määrä sekä input-vektorit. Skannereiden Crawler-ominaisuutta testataan myös erikseen Web Input Vector Extractor Teaser (WIVET)-projektilla. Tämä projekti testaa kuinka hyvin skanneri löytää kaikki web-sovelluksen polut, tiedostot ja muut input-vektorit. Tulos ilmoitetaan prosentuaalisena tuloksena skannerin löytämistä input-vektoreista verrattuna niiden todelliseen määrään. (Web Input Vector Extractor Teaser 2016.)

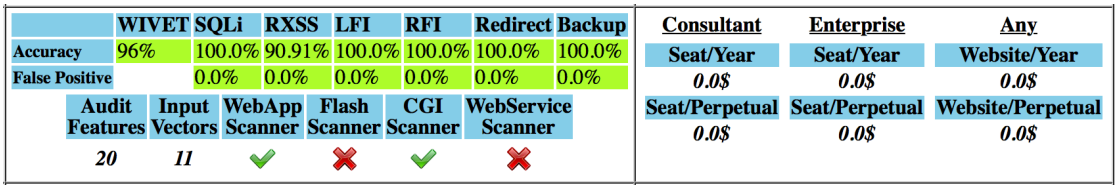
Sectoolsmarket on tehnyt ensimmäiset testit vuonna 2011 ja sen jälkeen uusintatestejä vuosina 2012, 2014 ja 2016. Kaikkien työkalujen testejä ei ole uusittu, joten jotkut tuloksista saattavat olla jo hieman vanhaa tietoa ja ohjelmistojen uudemmat versiot saattavat pärjätä testeissä paremmin. Muutenkaan testi ei välttämättä kerro täyttä totuutta ja on tarkoitettu enemmänkin suuntaa antavaksi. (Price and Feature Comparison of Web Application Scanners 2016.)

4.3 Arachni

Hinta ja Lisenssi

Arachni on lisensoitu Arachni Public Source License v1.0 alle. Tämä tarkoittaa sitä, että lähdekoodi on vapaa ja ohjelma on ilmainen, kunhan siitä ei tehdä kaupallista tuotetta tai palvelua. Tähän tarkoitukseen tarvitsee maksullisen lisenssin. Tietoturvatestaajat ja yritykset voivat siis käyttää tuotetta ilmaiseksi asiakkaiden tai omien järjestelmien testaukseen.

WAVSEP tulokset



	WIVET	SQLi	RXSS	LFI	RFI	Redirect	Backup
Accuracy	96%	100.0%	90.91%	100.0%	100.0%	100.0%	100.0%
False Positive		0.0%	0.0%	0.0%	0.0%	0.0%	0.0%

Audit Features	Input Vectors	WebApp Scanner	Flash Scanner	CGI Scanner	WebService Scanner
20	11	✓	✗	✓	✗

Consultant	Enterprise	Any
Seat/Year	Seat/Year	Website/Year
0.0$	0.0$	0.0$
Seat/Perpetual	Seat/Perpetual	Website/Perpetual
0.0$	0.0$	0.0$

Kuvio 32. Arachnin WAVSEP-testin tulokset

Kuten kuviosta 32 näkee, Arachni on löytänyt kaikki yleisimmät haavoittuvuudet lähes sataprosenttisesti. RXSS tulos ei ole täydellinen, koska Arachni ei tue testissä sisältyvää jo yleisestä käytöstä poistettua VBScript ohjelmointikieltä. False-postive –tuloksia ei ole, mikä onkin Arachnin yksi suurimmista vahvuuksista. 96% WIVET tulos on WAVSEP-testin paras ja osoittaa Arachnin crawler-ominaisuuden kyvykkyyden. Input-vektoreita Arachnilla on 11 ja auditointikeinoja 20. Flash- ja palvelinpuolta Arachni ei skannaa.

OWASP top 10

Arachni kattaa OWASP top 10 listasta seitsemän haavoittuvuutta. Katetut haavoittuvuudet ovat

- A1 – Injection
- A2 – Broken Authentication and Session Management
- A3 – Cross-Site Scripting (XSS)
- A5 – Security Misconfiguration
- A6 – Sensitive Data Exposure
- A8 – Cross Site Request Forgery (CSRF)
- A10 – Unvalidated Redirects and Forwards

Arachni kehittäjä Tasos Laskos on sitä mieltä, että A4 – Broken Authentication and Session Management ja A7 – Missing Function Level Access Control –haavoittuvuuksia ei voi skannata automaattisella skannerilla johtuen automatiikan kyvyttömyydestä erottaa arkaluonteisia resursseja tavallisista resursseista.

A9 – Using Components With Known Vulnerabilities –kohtaa Arachni ei testaa, koska Arachni fokusoi vain Black-Box testaukseen. (Arachni Detection Coverage versus OWASP top-10 2015.)

Ominaisuudet, käytettävyys ja alustat

Yksi tärkeä ominaisuus Arachnissa, mikä erottaa sen monista muista skannereista, on hajautettu rakenne. Sen avulla skannauskuormaa pystyy jakamaan monelle isäntälaitteelle samanaikaisesti skannauksen nopeuttamiseksi. Toinen hyödyllinen ominaisuus on käyttäjä- ja roolipohjainen käyttöliittymä, joka mahdollistaa vaivattomasti skannauksen jälkeisen työn jakamisen monelle käyttäjälle. Arachni on täysin automaattinen skanneri, joten se ei muilta ominaisuuksiltaan ole yhtä monipuolinen kuin esimerkiksi Burp Suite tai ZAP.

Arachnin web-käyttöliittymä on nykyaikainen ja helppokäyttöinen, eikä se tarvitse paljoa opettelua. Kaikki tarvittavat konfiguraatiot tehdään profiileihin, joihin määritellään muun muassa kirjautumiset, skannattavat polut, tehtävät testit, optimoinnit ja muut tarpeelliset säädöt. Kaikki mahdolliset säädöt ovat selvästi eriteltynä ja selitettynä profiiliasetuksissa. Skannaus aloitetaan ilmoittamalla skannattava osoite, käytettävä profiili ja käytettävien prosessori-instanssien määrä. Arachni toimii Windows, Linux ja Mac OS X käyttöjärjestelmissä.

Päivitykset

Arachnin tekijä Tasos Laskos on alusta asti kehittänyt skanneria jatkuvalla tahdilla, päivityksiä ja uusia ominaisuuksia tulee joskus jopa päivittäin. Haavoittuvuustestejä päivitetään myös jatkuvasti ja myös yhteisö ehdottelee päivityksiä aktiivisesti. Kaikista uusimmat ominaisuudet päivitetään heti nigthly-versioon, joka on ladattavissa Arachnin nettisivun kautta. Stable-versioon päivitykset tulevat silloin, kun ne ovat luotettavia.

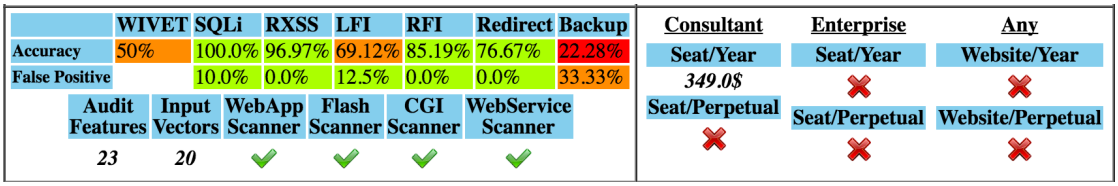
4.4 Burp Suite

Hinta ja Lisenssi

Burp suitella on kaksi versiota, ilmainen ja pro-versio. Ilmaisversiossa toimivat kaikki perustyökalut, lukuun ottamatta automaattista skanneria. Intruder-työkalua on myös hidastettu ilmaisversiossa ja iso osa lisäosista on vain pro-versiolle. Ilmaisversiossa ei myöskään pysty tallentamaan työsessiota. Pro-versioon tulee jatkuvia päivityksiä ja ominaisuuksia, ilmaisversioon päivitykset tulevat harvoin ja isoina kokonaisuuksina.

Pro-version lisenssi maksaa 349$ vuodessa käyttäjää kohden. Käyttäjä pystyy asentamaan ohjelmiston muutamalle koneelle samalla lisenssillä, samalla lisenssillä tehtyjen asennusten määrää kuitenkin seurataan ja liiallisissa määrissä tehtynä lisenssi voidaan evätä.

WAVSEP tulokset



Kuvio 33. Burp Suiten WAVSEP-testin tulokset

Kuviossa 33 näkyy, miten Burp Suiten automaattinen skanneri löysi SQL-injektiot ja RXSS-haavoittuvuudet lähes täydellisesti ja myös RFI- ja Redirect –haavoittuvuudet löysi suhteellisen hyvin. WIVET-tulos jäi 50 % ja backup-tiedostojen löytäminen 22.28 %. Input-vektoreissa Burp Suite on testin kärjessä 20 vektorilla ja myös auditointikeinoissa se on kärkiluokassa. Burp Suite tukee myös web-sovellus ja CGI-skannerin lisäksi palvelin- ja flash-puolta.

Testistä huomaa, että Burp Suiten vahvin osa ei ole automaattinen skanneri, vaikka se perushaavoittuvuudet löytääkin suhteellisen hyvin. Burp Suiten vahvuus on sen puolimanuaalisissa työkaluissa, monipuolisuudessa ja monenlaisissa input-vektoreissa, jotka erottavat sen selvästi muista ohjelmistoista.

OWASP top 10

Burp Suite kattaa OWASP top 10 listasta kaikki haavoittuvuudet ja lisäksi vielä joitain muita haavoittuvuuksia, joita lista ei sisällä. Automaattisesti Burp Suite skannaa kohdat

- A1 – Injection
- A2 – Broken Authentication and Session Management
- A3 – Cross-Site Scripting (XSS)
- A5 – Security Misconfiguration
- A6 – Sensitive Data Exposure
- A8 – Cross Site Request Forgery (CSRF)
- A9 – Using Components with Known Vulnerabilities
- A10 – Unvalidated Redirects and Forwards

Kohdat A4 ja A7 vaativat jossain väärin manuaalista työtä, joskin ne on automatisoitu mahdollisimman pitkälle.

Ominaisuudet, käytettävyys ja alustat

Burp Suite sisältää kymmeniä erilaisia ominaisuuksia ja työkaluja jotka helpottavat web-sovellusten haavoittuvuustestausta. Lisäosat tuovat monia näitä ominaisuuksia vielä lisää. Burp Suiten työkalut ovat laadukkaita ja hyvin toimivia sekä yleensä toimivat paremmin kuin muiden ohjelmistojen vastaavien työkalut.

Burp Suite ei ole kovin helppokäyttöinen aloittajalle, ja työkalusetin opetteluun meneekin hetki ennen kuin se muuttuu hyödylliseksi. Ohjelman käyttö vaatii monipuolista tietämystä web-sovellusten ja http-protokollan toiminnasta. Kun ohjelmistoa oppii käyttämään ja sen loogisuuden tajuaa, monet työt nopeutuvat kymmenkertaisesti. Burp Suite vaatii pyöriäkseen Java Runtime Environment (JRE) –ympäristön eli se toimii kaikissa käytetyimmissä käyttöjärjestelmissä kuten Windows, Mac OS X ja Linux.

Päivitykset

Burp Suiten Pro-versioon tulee jatkuvasti päivityksiä ja uusia ominaisuuksia. Uusien hyökkäysten löytyessä testit rakennetaan pikaisesti ja julkaistaan päivityksillä.

Ilmaisversioon päivityksiä tulee paljon harvemmin ja ne ovat tullessaan isoja kokonaisuuksia.

4.5 OWASP ZAP

Hinta ja Lisenssi

OWASP ZAP on täysin ilmainen vapaanlähdekoodin ohjelmisto, joka on julkaistu Apache 2 lisenssin alla. Apache 2 lisenssi sallii ohjelman kokonaisvaltaisen ilmaisen käytön.

WAVSEP tulokset

	WIVET	SQLi	RXSS	LFI	RFI	Redirect	Backup
Accuracy	73%	100.0%	100.0%	75.0%	100.0%	16.67%	38.04%
False Positive		30.0%	0.0%	0.0%	16.67%	0.0%	33.33%

Audit Features	Input Vectors	WebApp Scanner	Flash Scanner	CGI Scanner	WebService Scanner
17	11	✔	✖	✔	✖

Consultant	Enterprise	Any
Seat/Year	Seat/Year	Website/Year
0.0$	0.0$	0.0$
Seat/Perpetual	Seat/Perpetual	Website/Perpetual
0.0$	0.0$	0.0$

Kuvio 34. ZAP:n WAVSEP-testin tulokset

Kuviossa 34 näkyvässä WAVSEP-testissä ZAP pärjäsi perushaavoittuvuuksien osalta suhteellisen hyvin, joista SQL-injektiot, RXXS-haavoittuvuudet ja RFI-haavoittuvuudet se löysi kaikki. Joitakin false-positive tuloksia tuli myös. Redirect- ja Backup-testeissä ZAP pärjäsi suhteellisen huonosti. WIVET-tulos on 73%, parempi kuin Burp Suitella. Input-vektoreita ja auditointikeinoja on taas selvästi vähemmän kuin Burp Suitella.

ZAP on kovin kilpailija Burp Suitelle ja skanneriominaisuuksilta se päihittääkin Burp Suiten suhteellisen hyvin, ainakin tässä testissä. Redirect-haavoittuvuuksien löytämisessä ZAP jää selvästi taka-alalle.

OWASP top 10

ZAP-ohjelmisto pystyy testaamaan kaikkia OWASP top 10 listan haavoittuvuuksia ja niistä seitsemää se testaa automaattisen skannauksen aikana. Automaattinen skanneri testaa

- A1 – Injection
- A3 – Cross-Site Scripting (XSS)
- A5 – Security Misconfiguration
- A6 – Sensitive Data Exposure
- A8 – Cross Site Request Forgery (CSRF)
- A9 – Using Components with Known Vulnerabilities
- A10 – Unvalidated Redirects and Forwards

A2, A4 ja A7 –haavoittuvuuksia pystyy ZAP:ssa testaamaan manuaalisilla työkaluilla.

Ominaisuudet, käytettävyys ja alustat

Ominaisuuksiltaan ZAP lähentelee Burp Suitea, vaikka ainakaan vielä siinä ei kaikkia samoja ominaisuuksia ole. ZAP:n lisäosakirjasto sisältää myös monia lisäosia, jotka tuovat ohjelmistoon paljon spesifejä ominaisuuksia lisää. Lisäosakirjasto ei sisällä yhtä monipuolisesti lisäosia kuin Burp Suiten kirjasto.

ZAP on suhteellisen helppokäyttöinen, jos sillä tekee vain tavallista automaattista skannausta. Käyttöliittymä onkin suunniteltu enemmän automaattiskannausta silmällä pitäen. Manuaaliset työkalut eivät ole tavallisessa näkymässä kovin esillä, mutta ne voi tuoda näkyviin tarvittaessa. Kuten Burp Suite, myös ZAP pyörii Javalla ja toimii näin Windowsilla, Linuxilla ja Mac OS X:llä.

Päivitykset

ZAP:n weekly-versioon päivityksiä uusine ominaisuuksineen tulee viikoittain. Full/stable-versioon uudet ominaisuudet tulevat silloin kun te ovat todettu toimiviksi ja vakaiksi. Myös full/stable-versioon voi kuitenkin ottaa uusia ominaisuuksia käyttöön lisäosakirjaston kautta. Kaikki kehitteillä olevat ominaisuudet ovat lisätty lisäosakirjastoon Alpha tai Beta-tageilla.

4.6 SkipFish

Hinta ja Lisenssi

SkipFish on täysin ilmainen ja vapaan lähdekoodin ohjelmisto. Se on lisensoitu Apache 2 lisenssin alle.

WAVSEP tulokset

	WIVET	SQLi	RXSS	LFI	RFI	Redirect	Backup
Accuracy	73%	100.0%	100.0%	75.0%	100.0%	16.67%	38.04%
False Positive		30.0%	0.0%	0.0%	16.67%	0.0%	33.33%

Audit Features	Input Vectors	WebApp Scanner	Flash Scanner	CGI Scanner	WebService Scanner
17	11	✓	✗	✓	✗

Consultant	Enterprise	Any
Seat/Year	Seat/Year	Website/Year
0.0$	0.0$	0.0$
Seat/Perpetual	Seat/Perpetual	Website/Perpetual
0.0$	0.0$	0.0$

Kuvio 35. SkipFishin WAVSEP-testin tulokset

Kuviossa 35 näkyy, kuinka SkipFish löysi sataprosenttisesti SQL-injektiot, RXSS-haavoittuvuudet ja RFI-haavoittuvuudet. Redirect- ja backup –haavoittuvuuksia SkipFish löysi heikosti. Skanneri antoi myös jonkun verran false-positive tuloksia SQLi, RFI ja Backup-haavoittuvuuksista. WIVET-tulos on sama kuin OWASP ZAP:lla.

SkipFishin kehittäjän mukaan monet web-sovellusskannerit kehitetään pärjäämään hyvin tällaisia haavoittuvia web-sovellusprojekteja vastaan. SkipFish on ilmainen voittoa tavoittelematon projekti ja tämän takia kehittäjänsä sanoin sitä ei ole luotu pärjäämään tämmöisissä testisovelluksissa, joissa haavoittuvuudet eivät usein vastaa oikean maailman tilanteita.

OWASP top 10

SkipFish ei mainitse dokumentaatiossaan tarkalleen sitä, mitä haavoittuvuuksia se OWASP top 10 listalta testaa. Sen kaikki tekemät testit ovat kuitenkin dokumentoitu ja ne ovat näkyvissä liitteessä 3.

Ominaisuudet, käytettävyys ja alustat

SkipFish on suhteellisen yksinkertainen työkalu, eikä siinä ole lisäominaisuuksia automaattisen skannerin lisäksi. Sen tärkein ominaisuus onkin sen nopeus, jossa selvästi päihittää muut vertailtavat skannerit. SkipFish yltää samalla koneella olevaa web-sovellusta skannatessa helposti 2000 pyyntöön sekunnissa, välillä jopa 6000 pyyntöön sekunnissa. SkipFish kokoaa myös löydettyjä polkuja, tiedostonimiä ja muita merkkijonoja sanalistaan, jota voi käyttää uudestaan seuraavissa skannauksissa crawl-pinta-alan suurentamiseksi.

Skipfish toimii komentorivikäyttöliittymällä, joten se ei välttämättä kaikille ole kovin helppo käyttää. Jos komentoriviympäristö on kuitenkin tuttu, niin SkipFish on yksinkertainen ohjelma, jolle pitää vain syöttää alkukonfiguraatiot ja antaa sen hoitaa loput. Tulokset tulevat ulos html-muodossa, josta ne ovat suhteellisen helposti luettavissa. SkipFish toimii tunnetuimmilla alustoilla kuten Mac OS X, Windows ja Linux.

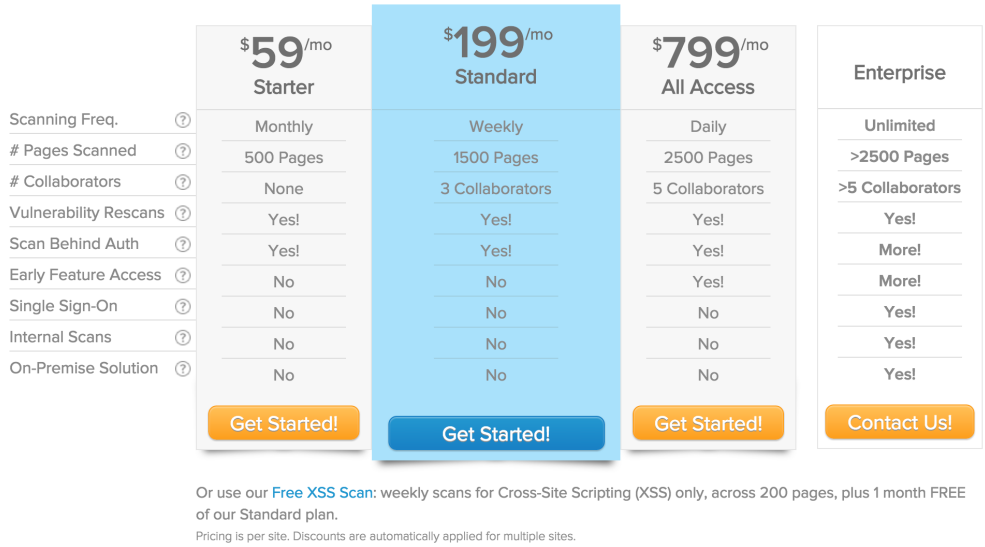
Päivitykset

Itse SkipFish ohjelmistoa ei ole päivitetty vuoden 2014 jälkeen eikä siihen tule automaattisesti mitään muitakaan päivityksiä. Ohjelmisto on kuitenkin rakennettu niin, että haavoittuvuustestejä voi lisätä ja tehdä itse signature-listaan. Näin myös muiden tekemiä testejä voi ottaa käyttöön.

4.7 Tinfoil Security

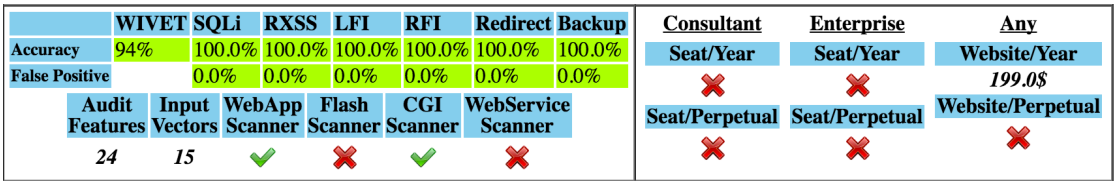
Hinta ja Lisenssi

Tinfoil security tarjoaa hinnoittelupaketteja, joissa laskutetaan kuukausittain per sivusto. Tarjolla on kolme valmista pakettia jotka maksavat 59$/kk, 199$/kk ja 799$/kk. Paketit eroavat toisistaan lähinnä sivuston maksimikoossa, skannausten tiheydessä, käyttäjien määrässä sekä lisäominaisuuksissa. Tarjolla on myös Enterprise-paketti, jonka hinnoittelu on sovittava erikseen. Tinfoil Security tarjoaa myös ilmaisen viikoittaisen XSS-skannauksen. Kuviossa 36 näkyvät hinnoittelupaketit kuvauksineen.



Kuvio 36. Tinfoil Securityn hinnoittelu

WAVSEP tulokset



Kuvio 37. Tinfoil Securityn WAVSEP-testin tulokset

Kuviossa 37 näkyvät Tinfoil Securityn tulokset. Tinfoil Security löysi kaikki haavoittuvuudet sataprosenttisesti ilman false-positive –tuloksia. Näillä tuloksilla se asettuu testin parhaimmistoon muun muassa Arachnin kanssa. WIVET-tulos on Tinfoil Securityllä 94%, joka on myös testin yläpäätä. WAVSEP-tuloksissa on Tinfoil security –palvelusta myös jonkin verran väärää tietoa muun muassa hinnasta. Tinfoil Security sisältää myös verkko/palvelin-skannerin, jota näissä tuloksissa ei ole ilmoitettu. Input-vektoreita skannerissa on 15, enemmän kuin esimerkiksi Arachnissa ja ZAP:ssa, joissa niitä on vain 11.

OWASP top 10

Tinfoil Security skannaa kaikkia OWASP top 10 listan haavoittuvuuksia, sekä vielä joitakin sellaisia haavoittuvuuksia, mitä listassa ei ole. Tarkempaa tietoa Tinfoil Security ei ole antanut siitä, miten A4 – Broken Authentication and Session Management ja A7 – Missing Function Level Access Control –haavoittuvuuksia skannataan. Monet muut skannerit eivät skannaa näitä haavoittuvuuksia automaattisesti, koska kehittäjiensä mukaan näiden haavoittuvuuksien skannausta ei ole täysin mahdollista automatisoida. (What vulnerabilities do you scan for? 2016.)

Ominaisuudet, käytettävyys ja alustat

Tinfoil Security ei sisällä oikeastaan mitään manuaalisempia työkaluja, mutta siinä on muutama muu todella hyödyllinen lisäominaisuus. Mahdollisuus integroida skanneri tehtävänhallintaohjelmistojen kanssa on hyödyllinen ja työtä vähentävä ominaisuus. Myös yksittäisten haavoittuvuuksien uudelleenskannaus on hyödyllinen ominaisuus automaattiskannerissa, esimerkiksi Arachnissa tätä ei ole ja se hidastuttaa tarkastusprosessia.

Palvelu on todella helppokäyttöinen ja se onkin suunniteltu myös kehittäjien käyttöön. Kaikki asiat on ohjeistettu käyttöliittymässä selkeästi. Tulokset on myös avattu hyvin ja jokaiselle löydetylle haavoittuvuudelle on korjausohjeet.

Palvelu toimii pääasiassa SaaS-tyyppisesti, eikä sitä asenneta omalle tietokoneelle tai palvelimelle. Enterprise-versio tarjoaa myös On-Premise omille palvelimille asennettavan version, mutta tuettuja käyttöjärjestelmiä ei ole ilmoitettu.

Päivitykset

Tinfoil Security-palveluun tulee tasaisin väliajoin uusia haavoittuvuustestejä ja päivityksiä. Sivustolla on myös blogi, joissa kehittäjät kertovat uusista haavoittuvuuksista ja kertovat, miten nämä skannataan Tinfoil Securityn skannerissa.

4.8 Acuentix

Hinta ja Lisenssi

Acuentix on maksullinen palvelu ja se tarjoaa kolme erilaista hinnoittelutapaa. Ohjelmiston voi ostaa kertahinnalla ja maksaa siitä ylläpitomaksua vuosittain, siitä voi maksaa vuosittaista lisenssimaksua tai sitä voi käyttää SaaS-tyyppisesti Acuentixin sivuilta. Ensimmäisen paketin halvin versio maksaa 4500 € ja vuosittain 1013 € ylläpitokuluja. Sen ohjelmisto asennetaan omille palvelimille ja sillä voi suorittaa kahta skannausta yhtäaikaisesti. Toisen paketin halvin vuosittainen lisenssimaksu on 2250 € vuodessa ja silläkin voi tehdä kaksi yhtäaikaista skannausta.

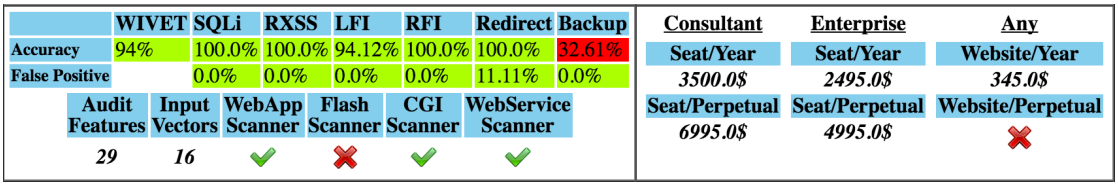
SaaS-hinnoittelu määritellään skannattavien kohteiden määrän mukaan. Hinnoittelu vain yhdelle web-sovellukselle on 295 € vuodessa ja sen mukana tulee kolme ilmaista verkkopuolen kohdetta. Tarkemmat hinnoittelutiedot näkyvät kuviossa 38.

License	USD ($)	EUR (€)	Buy	Maintenance (MA)
Acunetix WVS Perpetual Licenses (On-Premise)				
Enterprise 2 Concurrent Scans	$ 4,995	€ 4,500		$ 1,124 / € 1,013 per year Renew
Consultant 5 Concurrent Scans	$ 6,995	€ 5,995		$ 1,574 / € 1,349 per year Renew
Consultant 10 Concurrent Scans	$ 10,995	€ 9,995		$ 2,474 / € 2,249 per year Renew
Acunetix WVS 1 Year Subscription (On-Premise)				
Enterprise 2 Concurrent Scans	$ 2,495	€ 2,250		*Included*
Consultant 5 Concurrent Scans	$ 3,500	€ 2,995		*Included*
Consultant 10 Concurrent Scans	$ 5,495	€ 4,995		*Included*
Acunetix OVS 1 Year Subscription (Online)				
1 Target + 3 FREE Network Targets	$ 345	€ 295		*Included*
3 Targets + 3 FREE Network Targets	$ 685	€ 595		*Included*
5 Targets + 5 FREE Network Targets	$ 1,150	€ 995		*Included*
10 Targets + 10 FREE Network Targets	$ 2,200	€ 1,895		*Included*
15 Targets + 15 FREE Network Targets	$ 3,200	€ 2,795		*Included*
25 Targets + 25 FREE Network Targets	$ 5,310	€ 4,595		*Included*
50 Targets + 50 FREE Network Targets	$ 10,275	€ 8,950		*Included*

Contact sales@acunetix.com for volume pricing of over 50 targets

Kuvio 38. Acuentix-palvelun hinnoittelu

WAVSEP tulokset



	WIVET	SQLi	RXSS	LFI	RFI	Redirect	Backup
Accuracy	94%	100.0%	100.0%	94.12%	100.0%	100.0%	32.61%
False Positive		0.0%	0.0%	0.0%	0.0%	11.11%	0.0%

Audit Features	Input Vectors	WebApp Scanner	Flash Scanner	CGI Scanner	WebService Scanner
29	16	✓	✗	✓	✓

Consultant	Enterprise	Any
Seat/Year	Seat/Year	Website/Year
3500.0$	2495.0$	345.0$
Seat/Perpetual	Seat/Perpetual	Website/Perpetual
6995.0$	4995.0$	✗

Kuvio 39. Acuentix-palvelun WAVSEP-testin tulokset

Kuvion 39 tulokset sijoittavat Acuentix-palvelun myös tuloslistan yläpäähän. SQL-injektiot, RXSS-haavoittuvuudet, RFI-haavoittuvuudet ja Redirect-haavoittuvuudet Acuentix löysi sataprosenttisesti. Ainoastaan Redirect-haavoittuvuuksissa tuli hieman false-positive –tuloksia. Backup-haavoittuvuuksia skanneri löysi suhteellisen heikosti. WIVET-tulos on myös tuloslistan yläluokkaa.

Auditointiominaisuuksia palvelussa on 29 joka tuo sen listan kakkoseksi. Ainoastaan IBM Appscan-ohjelmistossa on enemmän auditointiominaisuuksia (30). Acuentix sisältää myös keskiarvoa enemmän input-vektoreita, niitä on 16. Palvelu skannaa myös verkko/palvelinpuolta, mutta flash-skanneria se ei sisällä.

OWASP top 10

Acuentixin web-sovellusskanneri etsii kaikkia haavoittuvuuksia OWASP top 10 listalta. Tarkemmin he eivät ole sivustoillaan kertonut, miten kaikki osat tältä listalta skannataan. Palvelussa on valmiina OWASP top 10 raporttipohja johon tulokset voi laittaa.

Ominaisuudet, käytettävyys ja alustat

Ominaisuuksiltaan Acuentix on todella monipuolinen. Wordpress-, Drupal- ja Joomla-skannerit erottavat sen kilpailijoistaan hyvin ja myös Acusensor-tekniikka on hyvä kilpailuetu. Näiden lisäksi palvelussa on myös manuaalisia työkaluja, joilla voi tehdä yksityiskohtaisempaa testausta.

Acuentixin web-käyttöliittymä on selkeä ja suhteellisen helppokäyttöinen. Ominaisuudet on ohjeistettu hyvin ja tulokset ovat myös selkeässä muodossa. Tuloksissa on

myös jonkun verran diagrammeja, joista saa hyvää yleiskuvaa. On-premise versio vaikuttaa kuvien perusteella hieman vanhanaikaiselta ja myös hieman vaikeakäyttöisemmältä. On-Premise ohjelmisto toimii vain Windows-käyttöjärjestelmissä. (Acuentix 2016.)

Päivitykset

Acuentixin on-premise versioiden ylläpito-paketti sisältää jatkuvia päivityksiä ja uusia haavoittuvuustestejä. SaaS-versioon nämä päivitykset tulevat myös automaattisesti.

4.9 SQLmap

Hinta ja Lisenssi

SQLmap on ilmainen vapaan lähdekoodin ohjelmisto, joka on lisensoitu GNU v2 General Public License –lisenssin alle. Tämä lisenssi oikeuttaa ohjelmiston ilmaisen käytön suurimmassa osassa tapauksista. Jos ohjelmistoa alkaa kaupallistamaan palveluna yms. niin silloin lisenssistä joutuu maksamaan.

WAVSEP tulokset

	WIVET	SQLi	RXSS	LFI	RFI	Redirect	Backup
Accuracy	✗	100.0%	✗	✗	✗	✗	✗
False Positive		0.0%	✗	✗	✗	✗	✗

Audit Features	Input Vectors	WebApp Scanner	Flash Scanner	CGI Scanner	WebService Scanner
2	4	✓	✗	✗	✗

Consultant	Enterprise	Any
Seat/Year	Seat/Year	Website/Year
0.0$	*0.0$*	*0.0$*
Seat/Perpetual	Seat/Perpetual	Website/Perpetual
0.0$	*0.0$*	*0.0$*

Kuvio 40. SQLmapin WAVSEP-testin tulokset

SQLmap nimensä mukaisesti skannaa vain SQL-injektioita (Ks. Kuvio 40) ja testissä se löysikin ne sataprosenttisesti ilman false-positive –tuloksia. SQLmap etsii SQLi-haavoittuvuuksia neljästä eri input-vektorista. Auditointiominaisuuksia on kaksi.

OWASP top 10

OWASP top 10 listasta SQLmap etsii vain injektiohaavoittuvuuksia. Se ei kata mitään muuta osaa listasta.

Ominaisuudet, käytettävyys ja alustat

SQLmap sisältää paljon spesifejä ominaisuuksia SQLi-hyökkäyksiin. Monet näistä ominaisuuksista ovat löydettyjen haavoittuvuuksien hyödyntämistä varten. Näitä ominaisuuksia löytyy todella vähän muista skannereista ja se tekeekin SQLmapista suhteellisen uniikin työkalun löydettyjen haavoittuvuuksien testaamiseen ja varmistamiseen.

SQLmap toimii cli-ympäristössä ja sen käyttö vaatii hyvää ymmärrystä http-protokollasta sekä muutenkin web-sovellusten rakenteesta. SQLmap tarvitsee myös jonkin verran opettelua ennen kuin sen kaikkia ominaisuuksia oppii hyödyntämään. Jos cli-ympäristöstä on kokemusta, niin ohjelmisto on selkeä ja mukava käyttää. SQLmap toimii Windowsilla, Mac OS X:llä ja Linuxilla.

Päivitykset

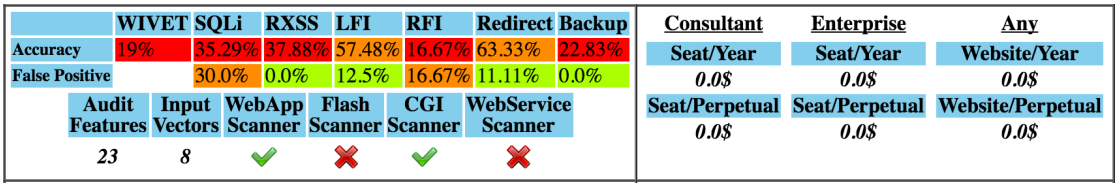
SQLmap on jatkuvan kehityksen alla ja uusia päivityksiä tulee kuukausittain. Open-source –yhteisö on jatkuvasti aktiivisena ehdottamassa uusia ominaisuuksia.

4.10 W3AF

Hinta ja Lisenssi

W3AF on ilmainen ja vapaalle lähdekoodille rakennettu ohjelmisto. Se on lisensoitu GNU v2 General Public License –lisenssillä, samalla lisenssillä kuin SQLmap. Käyttö on siis ilmaista, ellei ohjelmistosta tehdä kaupallista palvelua.

WAVSEP tulokset



	WIVET	SQLi	RXSS	LFI	RFI	Redirect	Backup
Accuracy	19%	35.29%	37.88%	57.48%	16.67%	63.33%	22.83%
False Positive		30.0%	0.0%	12.5%	16.67%	11.11%	0.0%

Audit Features	Input Vectors	WebApp Scanner	Flash Scanner	CGI Scanner	WebService Scanner
23	8	✓	✗	✓	✗

Consultant	Enterprise	Any
Seat/Year	Seat/Year	Website/Year
0.0$	0.0$	0.0$
Seat/Perpetual	Seat/Perpetual	Website/Perpetual
0.0$	0.0$	0.0$

Kuvio 41. W3AF:n WAVSEP-testin tulokset

W3AF ei selvästi pärjännyt kovin hyvin WAVSEP-testissä, ainakaan testissä käytetyillä vakiolisäosilla. Kuviossa 41 näkyy, kuinka vain LFI- ja RFI-haavoittuvuudet skanneri löysi kohtalaisesti. Muita haavoittuvuuksia W3AF löysi vielä huonommin ja myös false-positive –tuloksia löytyy. WIVET-tulos on 19 %, joka on myös aika alhainen.

Auditointiominaisuuksia W3AF:llä on 23, keskiarvoa enemmän. Skanneri tukee kahdeksaa input-vektoria.

OWASP top 10

W3AF:n mukana tulevissa valmiissa profiileissa on myös OWASP top 10 –profiili, johon on sisällytetty kaikki tarvittavat lisäosat OWASP top 10 –listan haavoittuvuuksien skannaamiseen.

Ominaisuudet, käytettävyys ja alustat

W3AF on ominaisuuksiltaan hieman erilainen, kun monet muut kilpailevat ohjelmistot. Iso osa sille tehdyistä lisäosista keskittyy haavoittuvuuksien hyödyntämiseen vastaavalla tavalla mitä SQLmap tekee. Tämä tekeekin W3AF:stä hyödyllisen ohjelmiston löydettyjen haavoittuvuuksien varmistamiseen ja testaamiseen. Kuten WAVSEP tuloksesta näkyy, itse skanneri ei ole kovin hyvä löytämään kaikkia haavoittuvuuksia, mutta sen exploit-mahdollisuudet tekevät siitä hyödyllisen.

Ohjelmisto sisältää selkeän käyttöliittymän joka on itsessään helppokäyttöinen. Lisäosakirjasto on W3AF:llä laaja ja lisäosien opettelu vie aikaa. Lisäosista tarvitsee hyvän yleiskuvan ennen kuin niitä pystyy hyödyntämään hyvin. Lisäosien käyttö vaatii myös

syvempää tuntemusta skannattavasta web-sovelluksesta. Mukana tulevien valmiiden profiileiden käyttö on kuitenkin helppoa, eikä vaadi syvempää tuntemusta. W3AF toimii Linux- ja Mac OS X –käyttöjärjestelmissä.

Päivitykset

W3AF-ohjelmisto on jatkuvan kehityksen alla ja github-sivustolla oleviin develop- ja feature –haaroihin uusia ominaisuuksia ja testejä tulee usein. Master-haaraan päivityksiä ei tule niin usein ja vasta toimivaksi todetut testit lisätään master-haaraan isommissa kokonaisuuksissa. Edellinen täysi stable-versio julkaistiin 2015.

5 Tulokset

Codemate tarvitsee tietoturvatyökaluja asiakasprojekteihin sekä myös omiin projekteihinsa. Vertailussa on ollut monia työkaluja ja jokaisella on omat vahvuutensa sekä omat heikkoutensa. Mikään työkaluista ei yksinään kata kaikkia Codematen tarpeita, erilaisiin käyttötarkoituksiin pitääkin valita sopiva työkalu. Moniin projekteihin tarvitaan automaattista skanneria, jolla saa hyvän yleiskuvan web-sovelluksen turvallisuustasosta ja tarvittaessa testausta jatketaan manuaalisemmin ja yksityiskohtaisemmin. Tähän käyttötarkoitukseen soveltuu taas toisenlainen työkalu. Useissa projekteissa verkko- ja palvelinpuoli vaatii myös testausta, johon tarkoitukseen on omat työkalut.

Tuloksissa on tarjottu maksullisia sekä ilmaisia vaihtoehtoja samoihin käyttötarkoituksiin. Maksulliset palvelut sisältävät ”kokonaisemman paketin”, joka vastaa montaa ilmaista työkalua. Imaiset työkalut ovat paljon spesialisoituneempia ja niitä tarvitsee usein monta yhden kokonaisuuden testaamiseen.

5.1 Automaattiset skannerit

Automaattisista skannereista Codematen testausprosessiin soveltuvat hyvin Arachni, Acuentix sekä mahdollisesti Tinfoil Security. Arachni on ilmainen sekä todella kykenevä ja helppokäyttöinen automaattinen web-sovellusskanneri, joka pärjää todella hyvin maksullisille kilpailijoilleen. Sillä on nykyaikainen käyttäjä- ja roolipohjainen Web-käyttöliittymä ja skanneri on jatkuvan kehityksen alla. Hajautettu rakenne mahdollistaa nopeat skannaukset, joiden työn voi ulkoistaa omille palvelimille. Arachni ei sisällä verkko- ja palvelinpuolen skanneria eikä myöskään CMS-skanneria. Sen kanssa tarvitsee siis myös muita työkaluja.

Acuentix on maksullinen palvelu, joka sisältää web-sovellusskannerin, verkko- ja palvelinskannerin sekä myös CMS-skannerin. Se on sopiva esimerkiksi asiakasprojekteihin, jotka vaativat jatkuvaa ylläpitoa. Acuentixin Acusensor-tekniikka on myös työtä paljon helpottava ominaisuus ja hoitaa myös osittain koodiskannerin virkaa. Palvelu on helppokäyttöinen, eikä tarvitse paljoa opettelua.

Tinfoil Security on toinen, paljon kalliimpi vaihtoehto Acuentix-palvelulle, joka on hyödyllinen ylläpitoa vaativiin asiakasprojekteihin. Palvelu sisältää JIRA-integraation, jota muissa täällä vertailluissa palveluissa ei automaattisesti ole. Tämä on myös työtä vähentävä ja helpottava ominaisuus. Tinfoil Security on myös suunniteltu DevOps-kulttuuria silmällä pitäen ja soveltuu tästä syystä hyvin Codematen testausprosessiin.

CMSmap-skanneria on hyvä käyttää Arachnin rinnalla. Se löytää kaikki Wordpressin, Drupalin ja Joomlan tunnetut haavoittuvuudet, sekä pyrkii myös hyödyntämään niitä varmistaakseen niiden toimivuuden.

5.2 Manuaaliset työkalut

Manuaaliseen testaukseen soveltuvat hyvin Burp Suite ja vaihtoehtoisesti Zed Attack Proxy, joka ei sisällä kuitenkaan yhtä monipuolisesti ominaisuuksia. Maksullinen Burp Suite sisältää monipuolisesti työkaluja, joilla voi testata kaikkia web-sovelluksen osia ja toimintoja. Sille tulee nopealla tahdilla päivityksiä ja lisäosia sekä uusista löyde-

tyistä haavoittuvuuksista tehdään Burp Suitelle pikaisesti haavoittuvuustestit. Yleisesti Burp Suiten rakenne on parempi verraten muihin vastaaviin ohjelmistoihin ja se on paras vaihtoehto Codematelle manuaaliseksi web-sovellusten testaustyökaluksi.

OWASP Zed Attack Proxy on ilmainen vaihtoehto Burp Suitelle ja se kykenee myös suhteellisen monipuoliseen manuaaliseen testaukseen. Sen työkalut eivät ole yhtä monipuoliset ja tehokkaat kuin Burp Suitessa, mutta se tuo kuitenkin paljon lisämahdollisuuksia automaattisen skannerin rinnalle.

5.3 Exploit-työkalut

Haavoittuvuuksien varmistamiseen ja hyödyntämiseen sopivat vertailluista työkaluista hyvin SQLmap ja W3AF. Haavoittuvuuksia voi varmistaa manuaalisesti, mutta näillä työkaluilla osaa niistä voi varmistaa myös automaattisemmin. SQLmap on todella hyvä työkalu SQL-injektioiden varmentamiseen. Sillä on hyvä testata kaikki esimerkiksi Arachnilla löytämät SQLi-haavoittuvuudet.

W3AF sisältää paljon erilaatuisia lisäosia joilla voi hyödyntää ja varmistaa myös muita haavoittuvuuksia SQL-injektioiden lisäksi. Kaikki näistä lisäosista eivät ole laadultaan saman tasoisia kuin SQLmap, mutta hyviäkin löytyy ja ne helpottavat kyseistä työtä paljon.

5.4 Verkko- ja palvelinskannerit

Maksullisen Acuentix-palvelun lisäksi verkko- ja palvelinskannereiksi Codematen testausprosessiin soveltuvat hyvin ilmaiset OpanVAS, Nmap sekä Qualsys:n SSL-skanneri. Näitä skannereita voi käyttää Arachnin rinnalla tai yksistään tunnettujen haavoittuvuuksien ja väärien konfiguraatioiden löytämiseen. OpenVAS tekee syvän ja monipuolisen skannauksen testaten palveluja monien haavoittuvuuksien varalta. Arachnin ja CMSmapin kanssa se kattaa kaikki tarvittavat hyökkäyspinta-alat kohteesta.

Nmap on hyvä työkalu nopean yleiskuvan saamiseksi ja yksittäisten haavoittuvuuksien testaamiseen. Sillä selviää nopeasti palvelimen avoimet portit, sekä niitä kuuntelevat palvelut.

Qualsys:n SSL-skanneri antaa tarkan ja nopean kuvan palvelimen SSL-protokollan turvallisuustasosta. Se on hyödyllinen työkalu nopeaan testaukseen ja sen tulosraportti on yksityiskohtainen, selkeä sekä hyvä sisällyttää valmiiseen haavoittuvuusraporttiin.

6 Pohdinta

Työn tavoitteena oli löytää sopivat tietoturvatyökalut Codematen käyttöön ja siihen tavoitteeseen päästiin. Hyviä työkaluja löytyikin monia ja kaikista valituista työkaluista on hyötyä joihinkin testauksen osa-alueisiin. Muutamat valituista työkaluista tulevat luultavasti olemaan isommassa käytössä kuin toiset, mutta kaikki työkalut ovat kuitenkin hyödyllisiä ja ne ovat olemassa sekä testattu toimivaksi tarpeen tullessa.

Isoin vaihe työstä oli vertailtavien työkalujen etsiminen ja testaaminen, jota tulikin tehtyä paljon. Monet ennen suosituista tietoturvatyökaluista eivät enää nykyään ole kovin kilpailukykyisiä, joten paljon sellaisia jäi vertailusta kokonaan pois. Tietoturva-alan työkalut vaativat jaktuvaa muutosta ja kehitystä pärjätäkseen, koska uusia tulee koko ajan lisää. Jotkut työkalut jäivät myös pois vertailusta todella huonon käyttömukavuutensa ja raporttiensa takia, joista esimerkiksi raporttien laatu on todella tärkeä vertailukriteeri.

Huomattua tuli myös, että tietoturvatestaukseen suunniteltuja työkaluja on todella vaikea vertailla. Täysin tasapuolisia testejä ei ole olemassa. Usein vertailut pohjautuvat johonkin valmiiksi rakennettuun haavoittuvaan web-sovellukseen ja se kertookin sannereiden kyvykkyyden tämän kyseisen sovelluksen kohdalla. Monet työkalut saattavatkin pärjätä paljon paremmin joissain toisissa haavottuvissa web-sovelluksissa. Haavoittuviksi rakennetut web-sovellukset eivät myöskään vastaa täysin oikean maailman haavoittuvia web-sovelluksia, joka muuttaa tuloksia vielä lisää. Näistä syistä testituloksiin ei voi luottaa sokeasti vaan vertailua pitää myös tehdä itse kokeilemalla työkaluja erilaisiin kohteisiin.

Tällaista vertailua on tässäkin työssä dokumentoimattomana mukana ja sitä tulee myös varmasti tehtyä jatkossa vertailutulosten parantamiseksi. Jatkossa työssä

tehtyä vertailua voi myös lähteä laajentamaan koodiskannereiden suuntaan, jotka etsivät haavoittuvuuksia suoraan kirjoitetusta koodista. Koodiskannereden vertailu jäi tästä työstä pois työn jo ison laajuuden vuoksi. Tulevaisuudessa vertailua voi myös parantaa kokeilemalla kaikkia kyseisiä skannereita esimerkiksi moneen oikeaan web-sovellukseen ja vertailla kaikkia näitä tuloksia keskenään skannereiden paremman kokonaiskyvykkyyden kartoittamiseksi.

7 Lähteet

Acuentix. Download 14 Day trial. Viitattu 22.10.2016. https://www.acunetix.com/vulnerability-scanner/download/

Acuentix vulnerability scanner. Viitattu 5.10.2016. https://www.acunetix.com/vulnerability-scanner/

Alam, S. WPScan – WordPress Security Scanner. Viitattu 14.10.2016. http://www.hackersgarage.com/wpscan-wordpress-security-scanner.html

Arachni. 2016. Arachnin infosivu. Viitattu 22.9.2016 http://www.arachni-scanner.com/

Arachni Detection Coverage versus OWASP Top-10. 2015. Viitattu 16.10.2016. http://support.arachni-scanner.com/discussions/questions/12627-arachni-detection-coverage-versus-owasp-top-10

Burp suite. 2016. Burp Suiten infosivu. Viitattu 23.9.2016. https://portswigger.net/burp/

Cornell, D. 2015. Getting Started with ZAP and the OWASP Top 10: Common Questions. Viitattu 1.10.2016. http://www.denimgroup.com/blog/denim_group/2015/07/getting-started-questions.html

Introduction. NMAP:n infosivu. Viitattu 12.10.2016. https://nmap.org

Michele. 2014. CMSMAP – Simple CMS Vulnerability Scanner. Viitattu 15.10.2016. https://www.dionach.com/blog/cmsmap-–-a-simple-cms-vulnerability-scanner

OpenVAS. OpenVASin infosivu. Viitattu 10.10.2016. http://sectools.org/tool/openvas/

OpenVAS Vulnerability Scan. Viitattu 11.10.2016. https://hackertarget.com/openvas-scan/

Ortega, M. 2014. Acuentix Web Vulnerability Scanner. Viitattu 6.10.2016. https://hakin9.org/acunetix-web-vulnerability-scanner/

OWASP Joomla Vulnerability Scanner Project. Viitattu 14.10.2016. https://www.owasp.org/index.php/Category:OWASP_Joomla_Vulnerability_Scanner_Project

OWASP Top Ten Project. Viitattu 15.10.2016. https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

Portswigger. 2012. Viitattu 23.9.2016. http://blog.portswigger.net/2013/10/burp-through-ages.html

Price and Feature Comparison of Web Application Scanners. Viitattu 22.10.2016. http://www.sectoolmarket.com/price-and-feature-comparison-of-web-application-scanners-unified-list.html

SQLmap. SQLmapin infosivu. Viitattu 8.10.2016. http://sqlmap.org

Tinfoil Security. Tinfoil Securityn infosivu. Viitattu 4.10.2016. https://www.tinfoilsecurity.com/

Tinfoil Security. Tinfoil Securityn support-sivu. Viitattu 5.10.2016. https://support.tinfoilsecurity.com/

The History and Future of Nmap. Viitattu 13.10.2016. https://nmap.org/book/history-future.html

The OWASP Foundation. Viitattu 15.10.2016. https://www.owasp.org/index.php/About_OWASP#The_OWASP_Foundation

wavsep. Viitattu 23.10.2016. https://code.google.com/archive/p/wavsep/

Web Input Vector Extractor Teaser. Viitattu 23.10.2016. https://github.com/bedirhan/wivet

What vulnerabilities do you scan for?. 2016. FAQ. Viitattu 21.10.2016. http://support.tinfoilsecurity.com/article/67-what-vulnerabilities-do-you-scan-for

WPScan. WPScanin readme-sivu. Viitattu 14.10.2016. https://github.com/wpscanteam/wpscan

W3AF. Introduction. Viitattu 10.10.2016. http://docs.w3af.org/en/latest/phases.html

W3AF. Take a Tour. Viitattu 10.10.2016. http://w3af.org/take-a-tour

Zalewski, M. Skipfish - web application security scanner. Viitattu 3.10.2016 https://code.google.com/archive/p/skipfish/wikis/SkipfishDoc.wiki

8 Liitteet

8.1 Liite 1. Arachni-skannerin haavoittuvuustarkastuslista (Check list)

Checks
Checks are system components which perform security checks and log issues.
Active
Active checks engage the web application via its inputs.

- SQL injection (sql_injection) — Error based detection.
- Oracle
- InterBase
- PostgreSQL
- MySQL
- MSSQL
- EMC
- SQLite
- DB2
- Informix
- Firebird
- SaP Max DB
- Sybase
- Frontbase
- Ingres
- HSQLDB
- MS Access
- Blind SQL injection using differential analysis (sql_injection_differential).
- Blind SQL injection using timing attacks (sql_injection_timing).
- MySQL
- PostgreSQL
- MSSQL
- NoSQL injection (no_sql_injection) — Error based vulnerability detection.
- MongoDB
- Blind NoSQL injection using differential analysis (no_sql_injection_differential).
- CSRF detection (csrf).
- Code injection (code_injection).
- PHP
- Ruby
- Python
- Java
- ASP
- Blind code injection using timing attacks (code_injection_timing).
- PHP
- Ruby
- Python
- Java
- ASP
- LDAP injection (ldap_injection).
- Path traversal (path_traversal).
- *nix
- Windows
- Java
- File inclusion (file_inclusion).
- *nix

- Windows
- Java
- PHP
- Perl
- Response splitting (response_splitting).
- OS command injection (os_cmd_injection).
- *nix
- *BSD
- IBM AIX
- Windows
- Blind OS command injection using timing attacks (os_cmd_injection_timing).
- Linux
- *BSD
- Solaris
- Windows
- Remote file inclusion (rfi).
- Unvalidated redirects (unvalidated_redirect).
- Unvalidated DOM redirects (unvalidated_redirect_dom).
- XPath injection (xpath_injection).
- Generic
- PHP
- Java
- dotNET
- libXML2
- XSS (xss).
- Path XSS (xss_path).
- XSS in event attributes of HTML elements (xss_event).
- XSS in HTML tags (xss_tag).
- XSS in script context (xss_script_context).
- DOM XSS (xss_dom).
- DOM XSS script context (xss_dom_script_context).
- Source code disclosure (source_code_disclosure)
- XML External Entity (xxe).
- Linux
- *BSD
- Solaris
- Windows

Passive

Passive checks look for the existence of files, folders and signatures.

- Allowed HTTP methods (allowed_methods).
- Back-up files (backup_files).
- Backup directories (backup_directories)
- Common administration interfaces (common_admin_interfaces).
- Common directories (common_directories).
- Common files (common_files).
- HTTP PUT (http_put).
- Insufficient Transport Layer Protection for password forms (unencrypted_password_form).
- WebDAV detection (webdav).
- HTTP TRACE detection (xst).
- Credit Card number disclosure (credit_card).
- CVS/SVN user disclosure (cvs_svn_users).
- Private IP address disclosure (private_ip).
- Common backdoors (backdoors).
- .htaccess LIMIT misconfiguration (htaccess_limit).
- Interesting responses (interesting_responses).
- HTML object grepper (html_objects).
- E-mail address disclosure (emails).
- US Social Security Number disclosure (ssn).
- Forceful directory listing (directory_listing).

- Mixed Resource/Scripting (mixed_resource).
- Insecure cookies (insecure_cookies).
- HttpOnly cookies (http_only_cookies).
- Auto-complete for password form fields (password_autocomplete).
- Origin Spoof Access Restriction Bypass (origin_spoof_access_restriction_bypass)
- Form-based upload (form_upload)
- localstart.asp (localstart_asp)
- Cookie set for parent domain (cookie_set_for_parent_domain)
- Missing Strict-Transport-Security headers for HTTPS sites (hsts).
- Missing X-Frame-Options headers (x_frame_options).
- Insecure CORS policy (insecure_cors_policy).
- Insecure cross-domain policy (allow-access-from) (insecure_cross_domain_policy_access)
- Insecure cross-domain policy (allow-http-request-headers-from) (insecure_cross_domain_policy_headers)
- Insecure client-access policy (insecure_client_access_policy)

8.2 Liite 2. Burp Suite -ohjelmiston haavoittuvuustarkastuslista

Name	Typical severity	Type index
OS command injection	High	0x00100100
SQL injection	High	0x00100200
SQL injection (second order)	High	0x00100210
ASP.NET tracing enabled	High	0x00100280
File path traversal	High	0x00100300
XML external entity injection	High	0x00100400
LDAP injection	High	0x00100500
XPath injection	High	0x00100600
XML injection	Medium	0x00100700
ASP.NET debugging enabled	Medium	0x00100800
HTTP PUT method is enabled	High	0x00100900
Out-of-band resource load (HTTP)	High	0x00100a00
File path manipulation	High	0x00100b00
PHP code injection	High	0x00100c00
Server-side JavaScript code injection	High	0x00100d00
Perl code injection	High	0x00100e00
Ruby code injection	High	0x00100f00
Python code injection	High	0x00100f10
Expression Language injection	High	0x00100f20
Unidentified code injection	High	0x00101000
Server-side template injection	High	0x00101080
SSI injection	High	0x00101100
Cross-site scripting (stored)	High	0x00200100
HTTP response header injection	High	0x00200200
Cross-site scripting (reflected)	High	0x00200300
Client-side template injection	High	0x00200308
Cross-site scripting (DOM-based)	High	0x00200310
Cross-site scripting (reflected DOM-based)	High	0x00200311
Cross-site scripting (stored DOM-based)	High	0x00200312
JavaScript injection (DOM-based)	High	0x00200320
JavaScript injection (reflected DOM-based)	High	0x00200321
JavaScript injection (stored DOM-based)	High	0x00200322
Path-relative style sheet import	Information	0x00200328
Client-side SQL injection (DOM-based)	High	0x00200330
Client-side SQL injection (reflected DOM-based)	High	0x00200331
Client-side SQL injection (stored DOM-based)	High	0x00200332
WebSocket hijacking (DOM-based)	High	0x00200340
WebSocket hijacking (reflected DOM-based)	High	0x00200341

WebSocket hijacking (stored DOM-based)	High	0x00200342
Local file path manipulation (DOM-based)	High	0x00200350
Local file path manipulation (reflected DOM-based)	High	0x00200351
Local file path manipulation (stored DOM-based)	High	0x00200352
Client-side XPath injection (DOM-based)	Low	0x00200360
Client-side XPath injection (reflected DOM-based)	Low	0x00200361
Client-side XPath injection (stored DOM-based)	Low	0x00200362
Client-side JSON injection (DOM-based)	Low	0x00200370
Client-side JSON injection (reflected DOM-based)	Low	0x00200371
Client-side JSON injection (stored DOM-based)	Low	0x00200372
Flash cross-domain policy	High	0x00200400
Silverlight cross-domain policy	High	0x00200500
HTML5 cross-origin resource sharing	Information	0x00200600
Cross Origin Resource Sharing: Arbitrary Origin Trusted	High	0x00200601
Cross Origin Resource Sharing: Insecure Origin Trusted	Low	0x00200602
Cross Origin Resource Sharing: All Subdomains Trusted	Low	0x00200603
Cross-site request forgery	Medium	0x00200700
Cleartext submission of password	High	0x00300100
External service interaction (DNS)	High	0x00300200
External service interaction (HTTP)	High	0x00300210
Referer-dependent response	Information	0x00400100
X-Forwarded-For dependent response	Information	0x00400110
User agent-dependent response	Information	0x00400120
Password returned in later response	Medium	0x00400200
Password submitted using GET method	Low	0x00400300
Password returned in URL query string	Low	0x00400400
SQL statement in request parameter	Medium	0x00400480
Cross-domain POST	Information	0x00400500
ASP.NET ViewState without MAC enabled	Low	0x00400600
XML entity expansion	Medium	0x00400700
Long redirection response	Information	0x00400800
Serialized object in HTTP message	High	0x00400900
Duplicate cookies set	Information	0x00400a00
Input returned in response (stored)	Information	0x00400b00
Input returned in response (reflected)	Information	0x00400c00
Open redirection	Low	0x00500100
Open redirection (DOM-based)	Low	0x00500110
Open redirection (reflected DOM-based)	Low	0x00500111
Open redirection (stored DOM-based)	Medium	0x00500112
SSL cookie without secure flag set	Medium	0x00500200
Cookie scoped to parent domain	Low	0x00500300
Cross-domain Referer leakage	Information	0x00500400
Cross-domain script include	Information	0x00500500
Cookie without HttpOnly flag set	Low	0x00500600

Session token in URL	Medium	0x00500700
Password field with autocomplete enabled	Low	0x00500800
Password value set in cookie	Medium	0x00500900
File upload functionality	Information	0x00500980
Frameable response (potential Clickjacking)	Information	0x005009a0
Browser cross-site scripting filter disabled	Information	0x005009b0
HTTP TRACE method is enabled I	nformation	0x00500a00
Cookie manipulation (DOM-based)	Low	0x00500b00
Cookie manipulation (reflected DOM-based)	Low	0x00500b01
Cookie manipulation (stored DOM-based)	Low	0x00500b02
Ajax request header manipulation (DOM-based)	Low	0x00500c00
Ajax request header manipulation (reflected DOM-based)	Low	0x00500c01
Ajax request header manipulation (stored DOM-based)	Low	0x00500c02
Denial of service (DOM-based)	Information	0x00500d00
Denial of service (reflected DOM-based)	Information	0x00500d01
Denial of service (stored DOM-based)	Low	0x00500d02
HTML5 web message manipulation (DOM-based)	Information	0x00500e00
HTML5 web message manipulation (reflected DOM-based)	Information	0x00500e01
HTML5 web message manipulation (stored DOM-based)	Information	0x00500e02
HTML5 storage manipulation (DOM-based)	Information	0x00500f00
HTML5 storage manipulation (reflected DOM-based)	Information	0x00500f01
HTML5 storage manipulation (stored DOM-based)	Information	0x00500f02
Link manipulation (DOM-based)	Low	0x00501000
Link manipulation (reflected DOM-based)	Low	0x00501001
Link manipulation (stored DOM-based)	Low	0x00501002
Document domain manipulation (DOM-based)	Medium	0x00501100
Document domain manipulation (reflected DOM-based)	Medium	0x00501101
Document domain manipulation (stored DOM-based)	Medium	0x00501102
DOM data manipulation (DOM-based)	Information	0x00501200
DOM data manipulation (reflected DOM-based)	Information	0x00501201
DOM data manipulation (stored DOM-based)	Information	0x00501202
Database connection string disclosed	Medium	0x00600080
Source code disclosure	Low	0x006000b0
Directory listing	Information	0x00600100
Email addresses disclosed	Information	0x00600200
Private IP addresses disclosed	Information	0x00600300
Social security numbers disclosed	Information	0x00600400
Credit card numbers disclosed	Information	0x00600500
Private key disclosed	Information	0x00600550
Robots.txt file	Information	0x00600600
Cacheable HTTPS response	Information	0x00700100
Base64-encoded data in parameter	Information	0x00700200
Multiple content types specified	Information	0x00800100
HTML does not specify charset	Information	0x00800200

HTML uses unrecognized charset	Information	0x00800300
Content type incorrectly stated	Low	0x00800400
Content type is not specified	Information	0x00800500
SSL certificate	Medium	0x01000100
Unencrypted communications	Low	0x01000200
Strict transport security not enforced	Low	0x01000300
Mixed content	Information	0x01000400
Extension generated issue	Information	0x08000000

8.3 Liite 3. SkipFish-skannerin haavoittuvuustarkastuslista

- High risk flaws (potentially leading to system compromise):
- Server-side SQL / PHP injection (including blind vectors, numerical parameters).
- Explicit SQL-like syntax in GET or POST parameters.
- Server-side shell command injection (including blind vectors).
- Server-side XML / XPath injection (including blind vectors).
- Format string vulnerabilities.
- Integer overflow vulnerabilities.
- Locations accepting HTTP PUT.
-
- Medium risk flaws (potentially leading to data compromise):
  Stored and reflected XSS vectors in document body (minimal JS XSS support present).
  Stored and reflected XSS vectors via HTTP redirects.
  Stored and reflected XSS vectors via HTTP header splitting.
  Directory traversal / file inclusion (including constrained vectors).
  Assorted file POIs (server-side sources, configs, etc).
  Attacker-supplied script and CSS inclusion vectors (stored and reflected).
  External untrusted script and CSS inclusion vectors.
  Mixed content problems on script and CSS resources (optional).
  Password forms submitting from or to non-SSL pages (optional).
  Incorrect or missing MIME types on renderables.
  Generic MIME types on renderables.
  Incorrect or missing charsets on renderables.
  Conflicting MIME / charset info on renderables.
  Bad caching directives on cookie setting responses.
-
- Low risk issues (limited impact or low specificity):
  - Directory listing bypass vectors.
  - Redirection to attacker-supplied URLs (stored and reflected).
  - Attacker-supplied embedded content (stored and reflected).
  - External untrusted embedded content.
  - Mixed content on non-scriptable subresources (optional).
  - HTTPS -> HTTP submission of HTML forms (optional).
  - HTTP credentials in URLs.
  - Expired or not-yet-valid SSL certificates.
  - HTML forms with no XSRF protection.
  - Self-signed SSL certificates.
  - SSL certificate host name mismatches.
  - Bad caching directives on less sensitive content.
-
- Internal warnings:
  - Failed resource fetch attempts.
  - Exceeded crawl limits.
  - Failed 404 behavior checks.
  - IPS filtering detected.
  - Unexpected response variations.
  - Seemingly misclassified crawl nodes.
-
- Non-specific informational entries:
  - General SSL certificate information.
  - Significantly changing HTTP cookies.
  - Changing Server, Via, or X-... headers.
  - New 404 signatures.

- Resources that cannot be accessed.
- Resources requiring HTTP authentication.
- Broken links.
- Server errors.
- All external links not classified otherwise (optional).
- All external e-mails (optional).
- All external URL redirectors (optional).
- Links to unknown protocols.
- Form fields that could not be autocompleted.
- Password entry forms (for external brute-force).
- File upload forms.
- Other HTML forms (not classified otherwise).
- Numerical file names (for external brute-force).
- User-supplied links otherwise rendered on a page.
- Incorrect or missing MIME type on less significant content.
- Generic MIME type on less significant content.
- Incorrect or missing charset on less significant content.
- Conflicting MIME / charset information on less significant content.

OGNL-like parameter passing conventions.

8.4 Liite 4. Qualsys SSL Labs SSL-testin tulokset

QUALYS® SSL LABS

Home Projects Qualys.com Contact

You are here: Home > Projects > SSL Server Test > jamk.fi

SSL Report: jamk.fi (195.148.129.49)

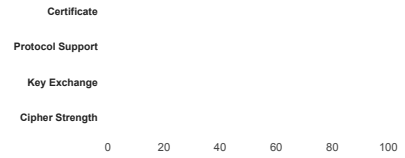
Assessed on: Fri, 14 Oct 2016 09:10:29 UTC | Hide | Clear cache

Scan Another »

Summary

Overall Rating

B



Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server supports weak Diffie-Hellman (DH) key exchange parameters. Grade capped to B. MORE INFO »

The server does not support Forward Secrecy with the reference browsers. MORE INFO »

Authentication

Server Key and Certificate #1

Subject	*.jamk.fi Fingerprint SHA1: 329d396f2cc9440ba71df03ebefc38eadce7df50 Pin SHA256: W9fGbFV3Hu70xVNnoNKb7BvntEfmCbYE37uLFwqrqBY=
Common names	*.jamk.fi
Alternative names	*.jamk.fi jamk.fi
Valid from	Mon, 15 Aug 2016 00:00:00 UTC
Valid until	Tue, 20 Aug 2019 12:00:00 UTC (expires in 2 years and 10 months)
Key	RSA 4096 bits (e 65537)
Weak key (Debian)	No
Issuer	TERENA SSL CA 3 AIA: http://cacerts.digicert.com/TERENASSLCA3.crt
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	No
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://crl3.digicert.com/TERENASSLCA3.crl OCSP: http://ocsp.digicert.com
Revocation status	Good (not revoked)
Trusted	Yes

Additional Certificates (if supplied)

Certificates provided	3 (3844 bytes)
Chain issues	Contains anchor

#2

Subject	TERENA SSL CA 3 Fingerprint SHA1: 77b99bb2bd7522e17ec099ea7177516f27787cad Pin SHA256: 8651wEkMkH5ftiaLp57oqmx3KHTFzDgp7ZeJXR0ToBs=
Valid until	Mon, 18 Nov 2024 12:00:00 UTC (expires in 8 years and 1 month)
Key	RSA 2048 bits (e 65537)
Issuer	DigiCert Assured ID Root CA
Signature algorithm	SHA256withRSA

#3

Subject	DigiCert Assured ID Root CA In trust store Fingerprint SHA1: 0563b8630d62d75abbc8ab1e4bdfb5a899b24d43 Pin SHA256: l/Lt/z7ekCWanjD0Cvj5EqXls2lOaThEA0H2Bg4BT/o=
Valid until	Mon, 10 Nov 2031 00:00:00 UTC (expires in 15 years)
Key	RSA 2048 bits (e 65537)
Issuer	DigiCert Assured ID Root CA Self-signed
Signature algorithm	SHA1withRSA Weak, but no impact on root certificate

Certification Paths

Path #1: Trusted

1	Sent by server	*.jamk.fi Fingerprint SHA1: 329d396f2cc9440ba71df03ebefc38eadce7df50 Pin SHA256: W9fGbFV3Hu70xVNnoNKb7BvntEfmCbYE37uLFwqrqBY= RSA 4096 bits (e 65537) / SHA256withRSA
2	Sent by server	TERENA SSL CA 3 Fingerprint SHA1: 77b99bb2bd7522e17ec099ea7177516f27787cad Pin SHA256: 8651wEkMkH5ftiaLp57oqmx3KHTFzDgp7ZeJXR0ToBs= RSA 2048 bits (e 65537) / SHA256withRSA
3	Sent by server In trust store	DigiCert Assured ID Root CA Self-signed Fingerprint SHA1: 0563b8630d62d75abbc8ab1e4bdfb5a899b24d43 Pin SHA256: l/Lt/z7ekCWanjD0Cvj5EqXls2lOaThEA0H2Bg4BT/o= RSA 2048 bits (e 65537) / SHA1withRSA Weak or insecure signature, but no impact on root certificate

Configuration

Protocols

TLS 1.2	Yes
TLS 1.1	Yes
TLS 1.0	Yes
SSL 3	No
SSL 2	No

Cipher Suites (SSL 3+ suites in server-preferred order; deprecated and SSL 2 suites at the end)

TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) DH 1024 bits FS **WEAK**	256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e) DH 1024 bits FS **WEAK**	128
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b) DH 1024 bits FS **WEAK**	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) DH 1024 bits FS **WEAK**	256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67) DH 1024 bits FS **WEAK**	128
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) DH 1024 bits FS **WEAK**	128
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16) DH 1024 bits FS **WEAK**	112
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d)	256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c)	128
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)	256
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	256

TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)	128
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	128
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)	112
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH secp384r1 (eq. 7680 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH secp384r1 (eq. 7680 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ECDH secp384r1 (eq. 7680 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH secp384r1 (eq. 7680 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ECDH secp384r1 (eq. 7680 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH secp384r1 (eq. 7680 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012) ECDH secp384r1 (eq. 7680 bits RSA) FS	112

Handshake Simulation

Android 2.3.7 No SNI [2]	RSA 4096 (SHA256)	TLS 1.0	TLS_DHE_RSA_WITH_AES_128_CBC_SHA DH 1024 FS
Android 4.0.4	RSA 4096 (SHA256)	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA DH 1024 FS
Android 4.1.1	RSA 4096 (SHA256)	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA DH 1024 FS
Android 4.2.2	RSA 4096 (SHA256)	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA DH 1024 FS
Android 4.3	RSA 4096 (SHA256)	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA DH 1024 FS
Android 4.4.2	RSA 4096 (SHA256)	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 DH 1024 FS
Android 5.0.0	RSA 4096 (SHA256)	TLS 1.2	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 DH 1024 FS
Android 6.0	RSA 4096 (SHA256)	TLS 1.2	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 DH 1024 FS
Baidu Jan 2015	RSA 4096 (SHA256)	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA DH 1024 FS
BingPreview Jan 2015	RSA 4096 (SHA256)	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 DH 1024 FS
Chrome 51 / Win 7 R	RSA 4096 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_GCM_SHA384 No FS
Firefox 31.3.0 ESR / Win 7	RSA 4096 (SHA256)	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_CBC_SHA DH 1024 FS
Firefox 46 / Win 7 R	RSA 4096 (SHA256)	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_CBC_SHA DH 1024 FS
Firefox 47 / Win 7 R	RSA 4096 (SHA256)	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_CBC_SHA DH 1024 FS
Googlebot Feb 2015	RSA 4096 (SHA256)	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_CBC_SHA DH 1024 FS
IE 6 / XP No FS [1] No SNI [2]	Server sent fatal alert: handshake_failure		
IE 7 / Vista	RSA 4096 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
IE 8 / XP No FS [1] No SNI [2]	RSA 4096 (SHA256)	TLS 1.0	TLS_RSA_WITH_3DES_EDE_CBC_SHA
IE 8-10 / Win 7 R	RSA 4096 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
IE 11 / Win 7 R	RSA 4096 (SHA256)	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 DH 1024 FS
IE 11 / Win 8.1 R	RSA 4096 (SHA256)	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 DH 1024 FS
IE 10 / Win Phone 8.0	RSA 4096 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_256_CBC_SHA No FS
IE 11 / Win Phone 8.1 R	RSA 4096 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_CBC_SHA256 No FS
IE 11 / Win Phone 8.1 Update R	RSA 4096 (SHA256)	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 DH 1024 FS
IE 11 / Win 10 R	RSA 4096 (SHA256)	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 DH 1024 FS
Edge 13 / Win 10 R	RSA 4096 (SHA256)	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 DH 1024 FS
Edge 13 / Win Phone 10 R	RSA 4096 (SHA256)	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 DH 1024 FS
Java 6u45 No SNI [2]	RSA 4096 (SHA256)	TLS 1.0	TLS_DHE_RSA_WITH_AES_128_CBC_SHA DH 1024 FS
Java 7u25	RSA 4096 (SHA256)	TLS 1.0	TLS_DHE_RSA_WITH_AES_128_CBC_SHA DH 1024 FS
Java 8u31	RSA 4096 (SHA256)	TLS 1.2	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 DH 1024 FS
OpenSSL 0.9.8y	RSA 4096 (SHA256)	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA DH 1024 FS
OpenSSL 1.0.1l R	RSA 4096 (SHA256)	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 DH 1024 FS
OpenSSL 1.0.2e R	RSA 4096 (SHA256)	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 DH 1024 FS
Safari 5.1.9 / OS X 10.6.8	RSA 4096 (SHA256)	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA DH 1024 FS
Safari 6 / iOS 6.0.1 R	RSA 4096 (SHA256)	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 DH 1024 FS
Safari 6.0.4 / OS X 10.8.4 R	RSA 4096 (SHA256)	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA DH 1024 FS
Safari 7 / iOS 7.1 R	RSA 4096 (SHA256)	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 DH 1024 FS
Safari 7 / OS X 10.9 R	RSA 4096 (SHA256)	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 DH 1024 FS
Safari 8 / iOS 8.4 R	RSA 4096 (SHA256)	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 DH 1024 FS

Safari 8 / OS X 10.10 R	RSA 4096 (SHA256)	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 DH 1024 FS
Safari 9 / iOS 9 R	RSA 4096 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_GCM_SHA384 No FS
Safari 9 / OS X 10.11 R	RSA 4096 (SHA256)	TLS 1.2	TLS_RSA_WITH_AES_256_GCM_SHA384 No FS
Apple ATS 9 / iOS 9 R	RSA 4096 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1 FS
Yahoo Slurp Jan 2015	RSA 4096 (SHA256)	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 DH 1024 FS
YandexBot Jan 2015	RSA 4096 (SHA256)	TLS 1.2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 DH 1024 FS

(1) Clients that do not support Forward Secrecy (FS) are excluded when determining support for it.
(2) No support for virtual SSL hosting (SNI). Connects to the default site if the server uses SNI.
(3) Only first connection attempt simulated. Browsers sometimes retry with a lower protocol version.
(R) Denotes a reference browser or client, with which we expect better effective security.
(All) We use defaults, but some platforms do not use their best protocols and features (e.g., Java 6 & 7, older IE).

Protocol Details

DROWN (experimental)	No, server keys and hostname not seen elsewhere with SSLv2 **(1) For a better understanding of this test, please read this longer explanation** (2) Key usage data kindly provided by the Censys network search engine; original DROWN test here (3) Censys data is only indicative of possible key and certificate reuse; possibly out-of-date and not complete
Secure Renegotiation	**Supported**
Secure Client-Initiated Renegotiation	Yes
Insecure Client-Initiated Renegotiation	No
BEAST attack	Not mitigated server-side (more info) TLS 1.0: 0x39
POODLE (SSLv3)	No, SSL 3 not supported (more info)
POODLE (TLS)	No (more info)
Downgrade attack prevention	**Yes, TLS_FALLBACK_SCSV supported** (more info)
SSL/TLS compression	No
RC4	No
Heartbeat (extension)	No
Heartbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No (more info)
OpenSSL Padding Oracle vuln. (CVE-2016-2107)	No (more info)
Forward Secrecy	**Weak key exchange WEAK**
ALPN	No
NPN	No
Session resumption (caching)	Yes
Session resumption (tickets)	No
OCSP stapling	No
Strict Transport Security (HSTS)	No
HSTS Preloading	**Not in: Chrome Edge Firefox IE Tor**
Public Key Pinning (HPKP)	No
Public Key Pinning Report-Only	No
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	No
Incorrect SNI alerts	No
Uses common DH primes	No
DH public server param (Ys) reuse	**Yes**
SSL 2 handshake compatibility	Yes

Miscellaneous

Test date	Fri, 14 Oct 2016 09:08:16 UTC
Test duration	133.256 seconds
HTTP status code	301
HTTP forwarding	**http://www.jamk.fi PLAINTEXT**
HTTP server signature	Microsoft-IIS/8.0

Server hostname	host49.guest.jamk.fi

SSL Report v1.24.0