Installasjon av DVWA på Debian

Contents

[Debian 2](#_Toc104460004)

[LAMP 2](#_Toc104460005)

[DVWA 3](#_Toc104460006)

[DVWA Setup 4](#_Toc104460007)

[PHP 5](#_Toc104460008)

[Mapperettigheter 5](#_Toc104460009)

[Captcha 6](#_Toc104460010)

[MariaDB 7](#_Toc104460011)

[Konklusjon! 8](#_Toc104460012)

Installasjon av DVWA. Damn Vulnerable Web Application.

# Debian

Start med samme Debian installasjon som vi brukte under Linux faget.

Graphical user interface, application

Description automatically generated

Eneste å bemerke seg under installasjonen kan være default domain. Det kan være greit å notere seg hvilket default domain du skriver inn, som f.eks frank.local.

Når det er installert anbefaler jeg å installere noen av de samme verktøyene vi brukte under Linux Fun, som sudo og tree, for å forenkle prosessen litt.

Husk å bruke kommandoen ip addr hvis du har brukt DHCP, så vi finner ut hva adressen er.

# LAMP

Når vi er fornøyd med Linux distroen våres skal vi installere resten av LAMP stacken for å ha alle programmene vi trenger. Vi kjører:

apt install -y apache2 mariadb-server mariadb-client php php-mysqli php-gd libapache2-mod-php git

Når den er ferdig har vi installert en full LAMP stack. Linux, Apache, Mariadb, PHP. Grunnen til at vi velger MariaDB istedenfor MySQL er enkelt og greit for det er bedre integrert i Debian.

# DVWA

Nå trenger vi selve webapplikasjonen. Vi manøvrer til mappen vi ønsker å intallere den i. Jeg valgte /var/www/.

cd /var/www/

sudo git clone <https://github.com/digininja/DVWA.git>

Dette vil lage en kopi av gitfilene rett til din harddisk, og lage en egen DVWA mappe i den working directory du stod i.

Hvis du kjører

ls -l

vil du se at vi har fått DVWA mappen. Nå må vi gjøre noen småendringer!

Personlig erfaring sier at den raskeste måten til målet er at vi bruker default config, og setter opp DVWA som default website i apache.

Først: ta i bruk default config filen til DVWA. Vi manøvrer til config mappen.

cd /var/www/DVWA/config

Deretter renamer vi default config filen ved å fjerne alt bak det siste punktum. Hvis du kjører ls i denne mappen vil du se navnet config.inc.php.dist

For å rename kjører vi kommandoen

sudo mv config.inc.php.dist config.inc.php

Så setter vi DVWA som default webpage for Apache2.

sudo nano /etc/apache2/sites-enabled/000-default.conf

Text

Description automatically generated

Vi finner frem til DocumentRoot mappen og bytter ut html med DVWA.

# DVWA Setup

Vi burde nå kunne åpne websiden og starte førstegangssetup ved å manøvrere til http://(Din IP Adresse Her)/setup.php

Graphical user interface, text, application

Description automatically generated

Her skal vi fikse alle de røde punktene 😊

Vi starter med den første, den er ganske simpel!

# PHP

Manøvrer til php config filen ved å skrive

sudo nano /etc/php/8.2/apache2/php.ini

Så kan du bruke søk funksjonen ved å trykke Ctrl + W og søke på f.eks «allow\_url\_include» Da vil du bli tatt direkte til riktig linje, og kan endre den til «On» - iht til «Setup Check» siden.

Text

Description automatically generated

# Mapperettigheter

Her trenger vi å gi apache skrivetilganger til de mappene og filene som er nevnt. Det går selfvølgelig an å løse det ved å gi global write, men da senker vi sikkerheten unødvendig mye.

Vi manøverer til DVWA mappen.

cd /var/www/DVWA

Vi starter med å endre eierskap.

sudo chown -R root:www-data hackable/uploads

sudo chown root:www-data external/phpids/0.6/lib/IDS/tmp/phpids\_log.txt

sudo chown -R root:www-data config

Så må vi endre tilganger så gruppen også kan skrive.

sudo chmod -R 775 hackable/uploads/

sudo chmod 775 external/phpids/0.6/lib/IDS/tmp/phpids\_log.txt

sudo chmod -R 775 config

Etter vi har gjort disse endringer kan vi restarte Apache2 prosessen

sudo systemctl restart apache2

Da kan vi refreshe websiden, og VIPPS så skal alt det røde være borte. Nesten 😊

# Captcha

Hvis du ønsker å registre siden for en Captcha kan du gjøre det nå. Da må vi første gå inn til Google og regge en captcha, og deretter sette inn nøklene i config filen til DVWA.Gå til [**https://www.google.com/recaptcha/admin/create**](https://www.google.com/recaptcha/admin/create) Her må du nok logge inn med google konto.Graphical user interface, text, application, email

Description automatically generated



Lag noe som ser sånn ca sånn ut, men bytt ut info med din egen. Hvis du ikke har et domenenavn kan du putte inn ipadressen til webserveren.



Du vil da få 2 nøkler, som må settes inn i config filen.

Graphical user interface, text, application, email

Description automatically generated

Manøvrer til dvwa config;

sudo nano /var/www/DVWA/config/config.inc.php

Scroll ned til Captcha settings. Sett inn Site Key mellom fnuttene på «Public key», og secret key på «Private key»

Graphical user interface

Description automatically generated with low confidence

# MariaDB

Til slutt skal vi lage en database for brukerne. Vi logger inn på MariaDB(MySQL) ved å skrive:

sudo mysql

Kommandlinen vil skifte til MariaDB input, så vi kan skrive alle kommandoene våre. For de som allerede kan litt SQL er denne en walk in the park. Jeg bruker default values på databasen, men man kan også kalle den hva man vil og så gjøre endringer i DVWA konfig.

Når vi skriver SQL til Maria skriver vi hele linjen og skiller med ;. Så skriv inn eksemplene under, og trykk enter, så vil du få en kvittering.

Vi lager en database.

create database dvwa;

Vi lager en bruker for DVWA

create user dvwa@localhost identified by 'p@ssw0rd';

*Merk her at det er 0 «null», ikke «STOR O»!*

Vi gir DVWA brukeren alle rettigheter i dvwa databasen.

grant all on dvwa.\* to ‘dvwa’@’localhost’;

Og til slutt resetter rettighetene

flush privileges;

Hvis alt fungerte som det skal kan du gå tilbake til startsiden i nettleseren, og trykke på «create database» i bunnen av siden.

A picture containing shape

Description automatically generated

# Konklusjon!

Nå burde alt være i orden, og når du trykker «Create /Reset Database» skal websiden ta deg rett til login.

Default login her vil være admin og password

Og så er det opp til deg og dine crackeferdigheter å finne flere/resten av brukerne som eksisterer 😉

Når du logger inn på websiden kan du trykke litt nede på ventre side «DVWA Security» knappen.

Her kan du velge forskjellig vanskelighetsgrad på alle modulene, fra low til impossible.

Happy cracking!