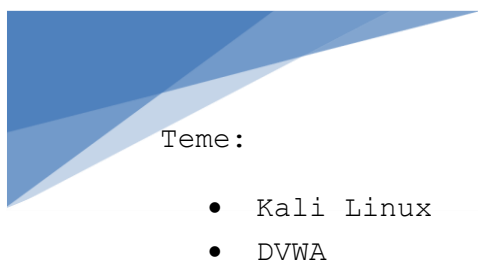


KOLEGIJ

Sigurnost informacijskih sustava

Laboratorijska vježba br.5 – Web Application Penetration Testing



U ovoj laboratorijskoj vježbi ćemo nakon vježbi u kojima smo radili iskorištavanje ranjivosti na operacijske sustave, raditi s alatom koji je namijenjen za iskorištavanje ranjivosti na web aplikacijama. Koristiti ćemo DVWA, tj. *Damn Vulnerable Web Application*.

DVWA – Damn Vulnerable Web Application

DNWA je jedna od poznatih PHP/MySQL web aplikacija koje se koriste za demonstriranje prilikom provođenja penetracijskog testiranja na web aplikacije.

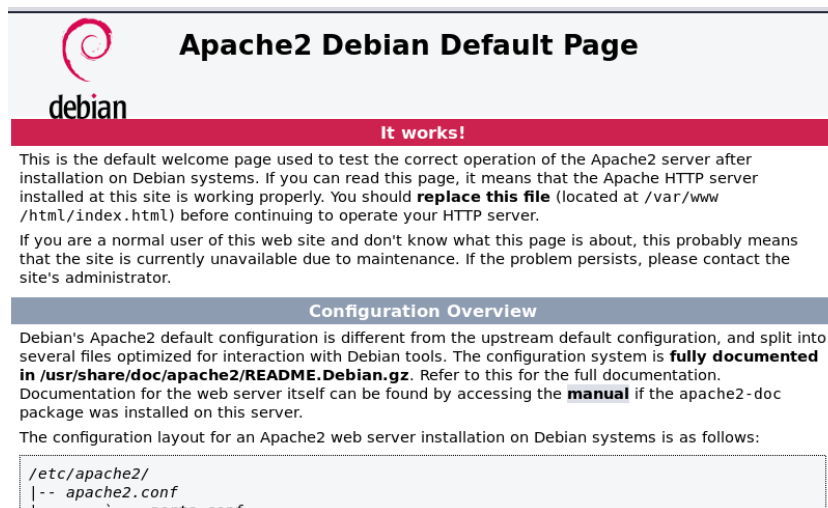
Da bi konfigurirali DVWA na Kali Linuxu slijedite sljedeće korake:

1. Instalacija Apache2

Instalirajte Apache2 ili ga pokrenite ukoliko je već instaliran.

```
root@kali:/var/www/html# apt install apache2
Reading package lists... Done
Building dependency tree
Reading state information... Done
apache2 is already the newest version (2.4.41-1).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
root@kali:/var/www/html# /etc/init.d/apache2 start
Starting apache2 (via systemctl): apache2.service.
root@kali:/var/www/html#
root@kali:/var/www/html#
```

Na localhost morate dobiti sljedeći landing page:



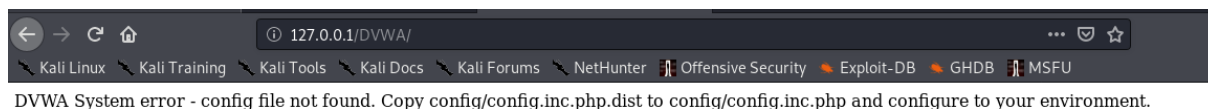
Sljedeće je potrebno maknuti standardni landing page s sljedećom naredbom: `rm /var/www/html/index.html`

2. Download DNWA


```
root@kali:/var/www/html# cd /var/www/html/
root@kali:/var/www/html# git clone https://github.com/ethicalhack3r/DVWA.git
Cloning into 'DVWA'...
remote: Enumerating objects: 2995, done.
remote: Total 2995 (delta 0), reused 0 (delta 0), pack-reused 2995
Receiving objects: 100% (2995/2995), 1.52 MiB | 2.25 MiB/s, done.
Resolving deltas: 100% (1318/1318), done.
root@kali:/var/www/html# ls
DVWA
root@kali:/var/www/html# cd DVWA/
root@kali:/var/www/html/DVWA# ls
about.php      dvwa          index.php      php.ini        vulnerabilities
CHANGELOG.md  external     instructions.php README.md
config         favicon.ico  login.php      robots.txt
COPYING.txt   hackable    logout.php     security.php
docs          ids_log.php phpinfo.php    setup.php
root@kali:/var/www/html/DVWA# cd ..
root@kali:/var/www/html# chmod -R 755 DVWA/
root@kali:/var/www/html# /etc/init.d/apache2 restart
Restarting apache2 (via systemctl): apache2.service.
root@kali:/var/www/html#
```

Probajte otvoriti <http://127.0.0.1/DVWA/>.

Ukoliko se pojavi poruka niža potrebno je još napraviti promjenu config file-a (s **cp** naredbom i ispravno konfigurirati.)



Nakon setup-a treba se pojaviti sljedeća stranica nakon refresha:



Setup DVWA

Instructions

About

Database Setup

Click on the 'Create / Reset Database' button below to create or reset your database.
If you get an error make sure you have the correct user credentials in: `/var/www/html/DVWA/config/config.inc.php`

If the database already exists, **it will be cleared and the data will be reset.**
You can also use this to reset the administrator credentials ("**admin** // **password**") at any stage.

Setup Check

Operating system: ***nix**
Backend database: **MySQL**
PHP version: **7.3.12-1**

Web Server SERVER_NAME: **127.0.0.1**

PHP function display_errors: **Disabled**
PHP function safe_mode: **Disabled**
PHP function allow_url_include: **Disabled**
PHP function allow_url_fopen: **Enabled**
PHP function magic_quotes_gpc: **Disabled**
PHP module gd: **Missing - Only an issue if you want to play with captchas**
PHP module mysql: **Installed**
PHP module pdo_mysql: **Installed**

3. Install/setup MySQL

```
root@kali:~# service mysql start
root@kali:~# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 51
Server version: 10.3.20-MariaDB-1 Debian buildd-unstable

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> create database dvwa;
Query OK, 1 row affected (0.000 sec)

MariaDB [(none)]> grant all on dvwa.* to dvwa@localhost identified by 'aprojic';
Query OK, 0 rows affected (0.008 sec)

MariaDB [(none)]> flush privileges
-> ;
Query OK, 0 rows affected (0.000 sec)

MariaDB [(none)]>
```

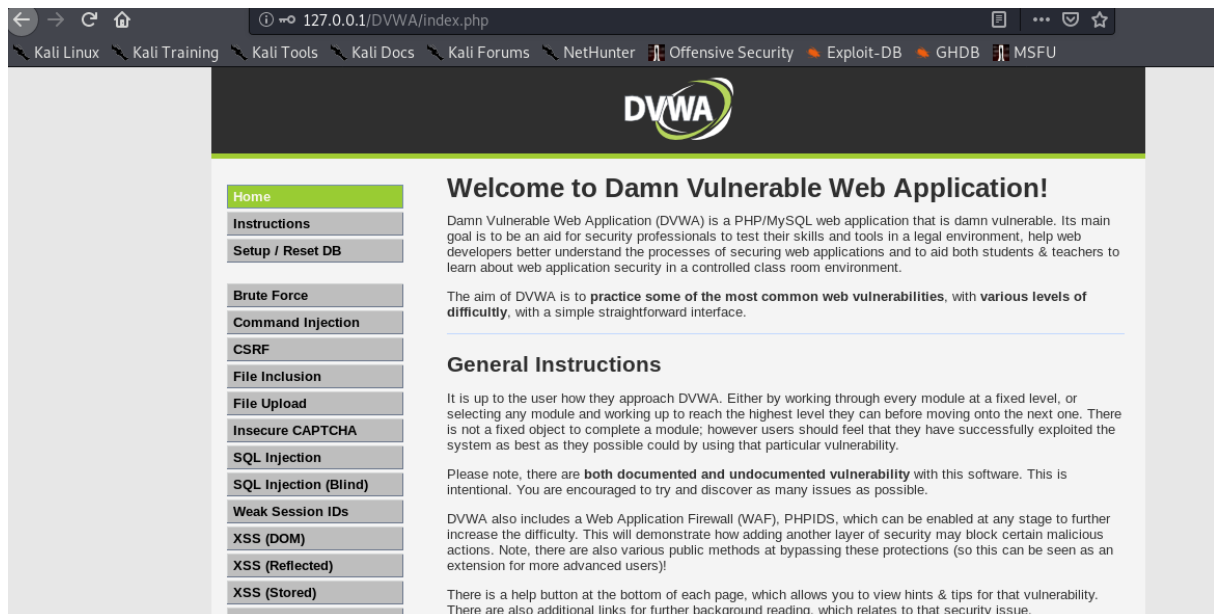
4. Configure DVWA

Podesite config file s novo kreiranom userom i passwordom u /var/www/html/DVWA/config i ponovno pokrenite setup na web stranici od DVWA. Morate kreirati i reCaptcha prema uputama.

Ove dvije postavke u ovom file-u moraju biti omogućene - /etc/php/7.3/apache2/php.ini:

```
; Whether to allow the treatment of URLs (like http:// or ftp://) as files.
; http://php.net/allow-url-fopen warning (0.01 sec)
allow_url_fopen = On
mysql> flush privileges;
; Whether to allow include/require to open URLs (like http:// or ftp://) as files.
; http://php.net/allow-url-include
allow_url_include = On
to update the config file, the new entries will look like
```

Napravite restart mysql i apache2 servisa s `service ime_servisa restart` i pokrenite DVWA i pristupite istom s admin/password.



Dodatno još instalirajte ovaj paket i napravite reset apache2 i mysql servisa. ***apt-get install php7.3-gd***

Priložite screenshot aplikacije koja radi i config file-a.

ROOT pristup na web server

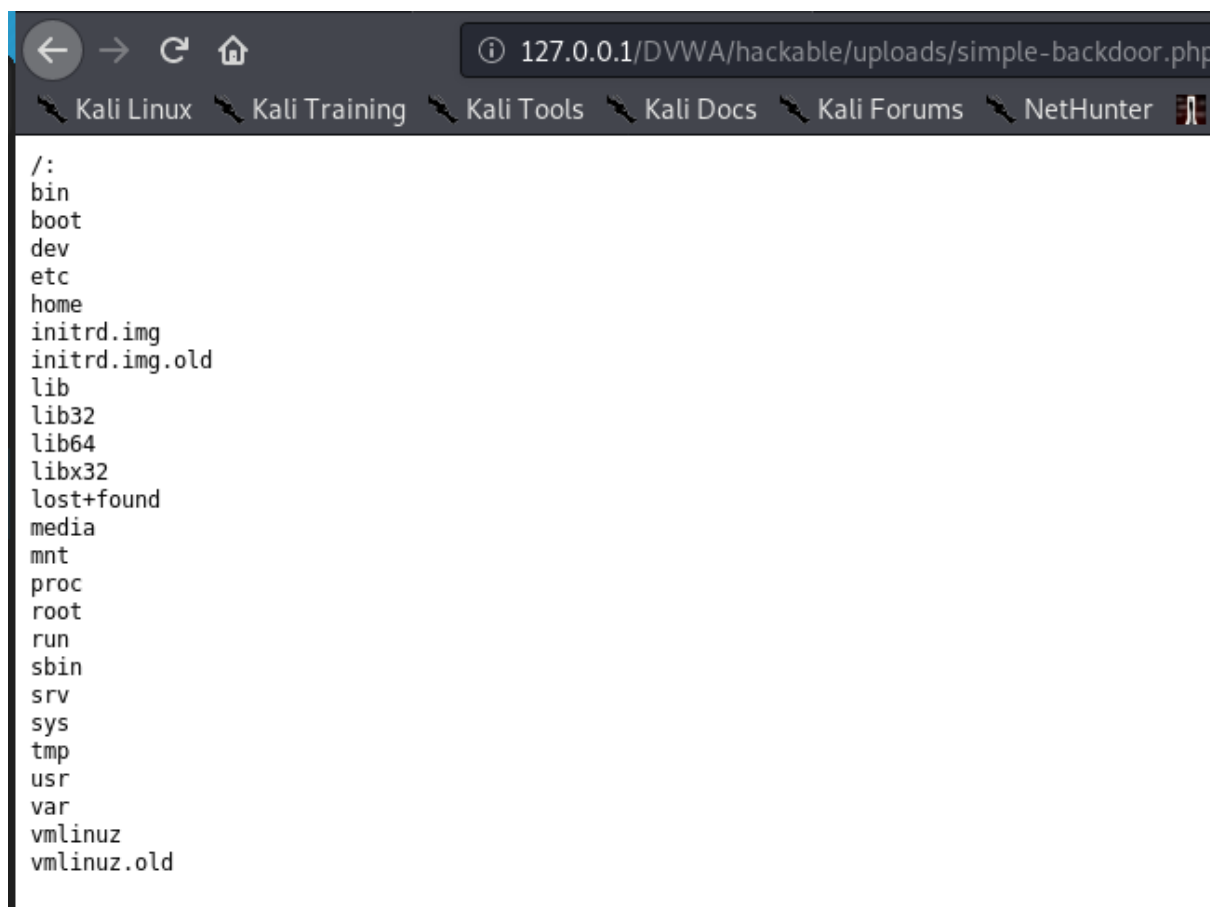
Hakiranje poslužitelja nije jednostavno, postoji mnogo načina da to učinite. U ovoj vježbi ćemo ostvariti pristup na server tako da ćemo uploadati shell preko učitavanja slike na web server. Postoji mnogo načina i web stranica koje omogućuju učitavanje slika avatar-a i omogućuju vam uređivanje profila.

Za početak podesite security level na DVWA na **low**.

Uploadajte file `simple-backdoor.php` koji se nalazi na `/usr/share/webshells/`.

Demonstrirajte korištenje ovog jednostavnog shella na dva primjera.

Moj primjer: izlist direktorija na root FS-u



The screenshot shows a web browser window with the address bar displaying `127.0.0.1/DVWA/hackable/uploads/simple-backdoor.php`. Below the address bar, there is a navigation bar with links to `Kali Linux`, `Kali Training`, `Kali Tools`, `Kali Docs`, `Kali Forums`, and `NetHunter`. The main content area of the browser displays the output of a shell command, which is a list of directories and files in the root filesystem:

```
/:
bin
boot
dev
etc
home
initrd.img
initrd.img.old
lib
lib32
lib64
libx32
lost+found
media
mnt
proc
root
run
sbin
srv
sys
tmp
usr
var
vmlinuz
vmlinuz.old
```

Objasnite moguće implikacije ovakvog propusta.

Uploadajte `qsd-php-backdoor.php` i demonstrirajte korištenje, te objasnite ovaj backdoor.

Uploadajte `php-reverse-shell.php` i demonstrirajte korištenje, te objasnite ovaj backdoor (nap.a. prije pokretanja pokrenite netcat listening na web serveru s `nc -lvp broj_porta`)).

Priložiti screenshotove za sve.

NASTAVAK:

Pobrišite sve uploadove koje ste napravili u ../uploads/

Promijenite security level na NVWA na medium i probajte uploadati simple-backdoor.php.

Vulnerability: File Upload

Choose an image to upload:

No file selected.

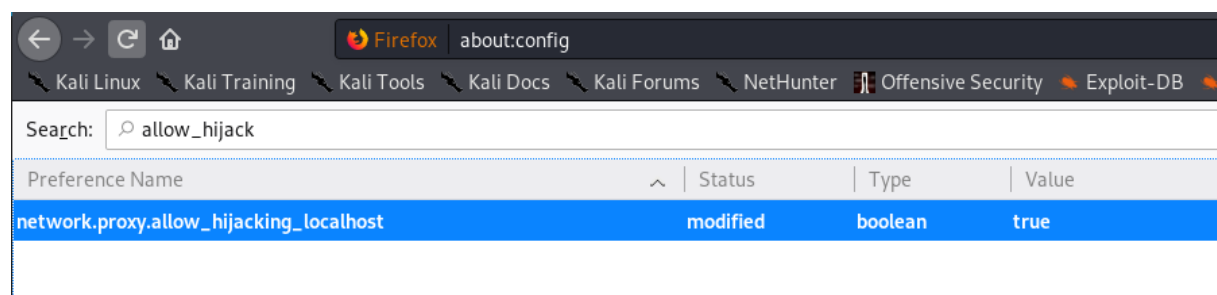
Your image was not uploaded. We can only accept JPEG or PNG images.

Kao što vidite, ne može se napraviti upload ničega osim image file-a. Znači, web aplikacija provjerava da li je upload ispravan. Međutim, to možemo zaobići na način da presretnemo HTTP POST nedtodu i promijenimo ovo:

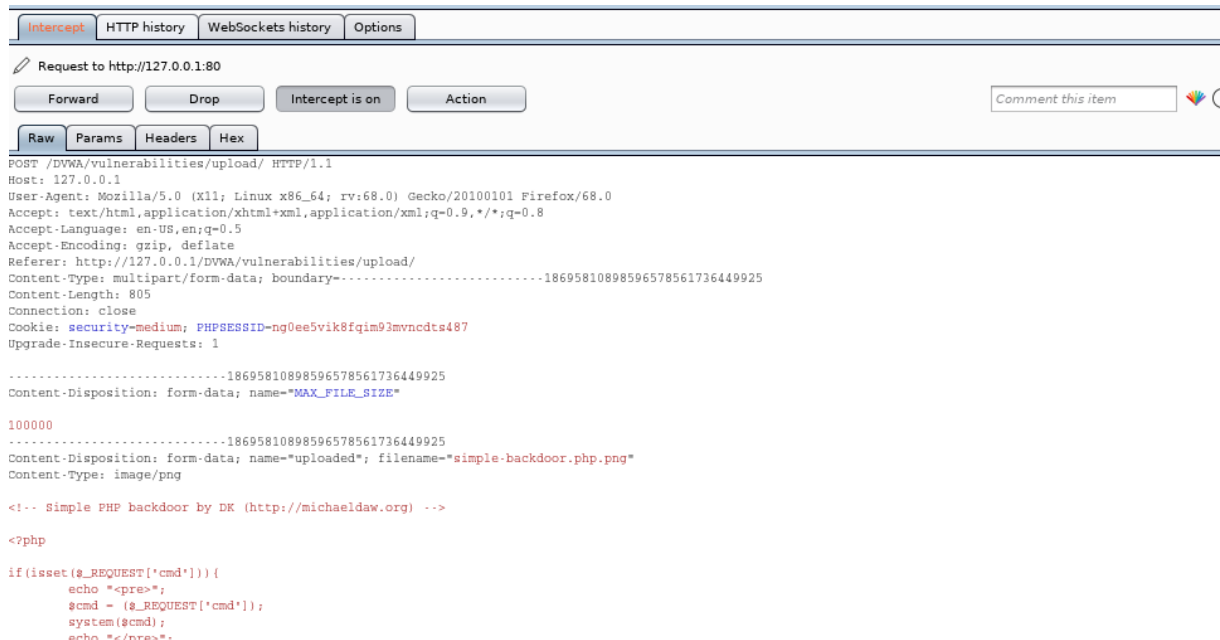
```
if( ( $uploaded_type == "image/jpeg" || $uploaded_type == "image/png" ) &&
    ( $uploaded_size < 100000 ) )
```

Kopirajte simple-backdoor.php u novi file imena simple-backdoor.php.png.

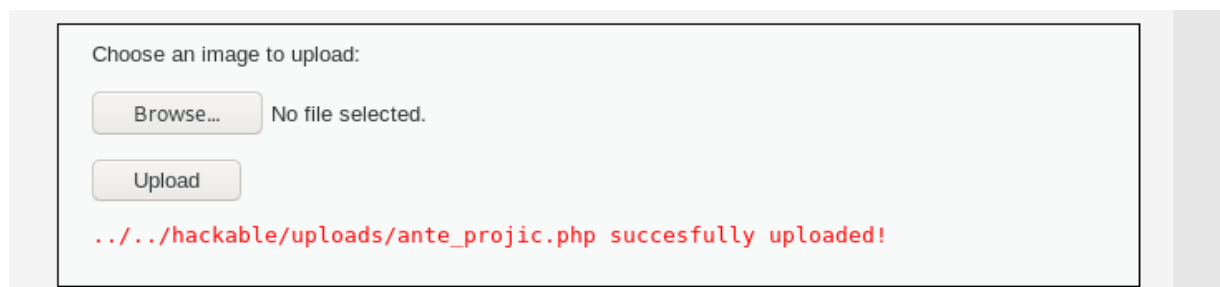
Upalite Burp Suite aplikaciju koja je sastavni dio Kali Linuxa. Postavite se u proxy mod rada. Konfigurirajte proxy na Firefoxu na 127.0.0.1:8080. Također postavite sljedeći parametar.



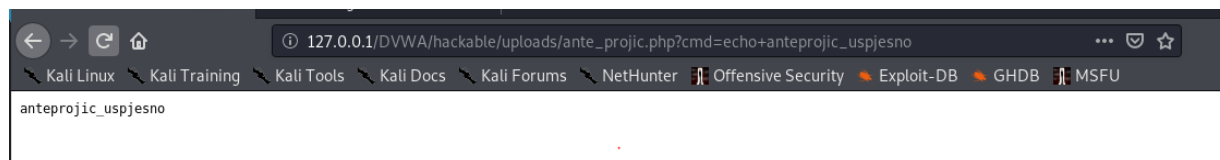
Probajte ponovno uploadati simple-backdoor.php.png s intercept postavkom uključenom:



Promijenite ime file-a u HTTP request-u u ime_prezime.php i prosljedite zahtjev. **PRILOŽITI SCREENSHOT**



Pokrenite naredbu echo s kojom će te ispisati ime i prezime, a preko web aplikacije. **PRILOŽITI SCREENSHOT**



VLASTITIM RIJEČIMA OBRAZLOŽITE POSTUPAK i TIP NAPADA KOJI SE OVDJE IZVEO.