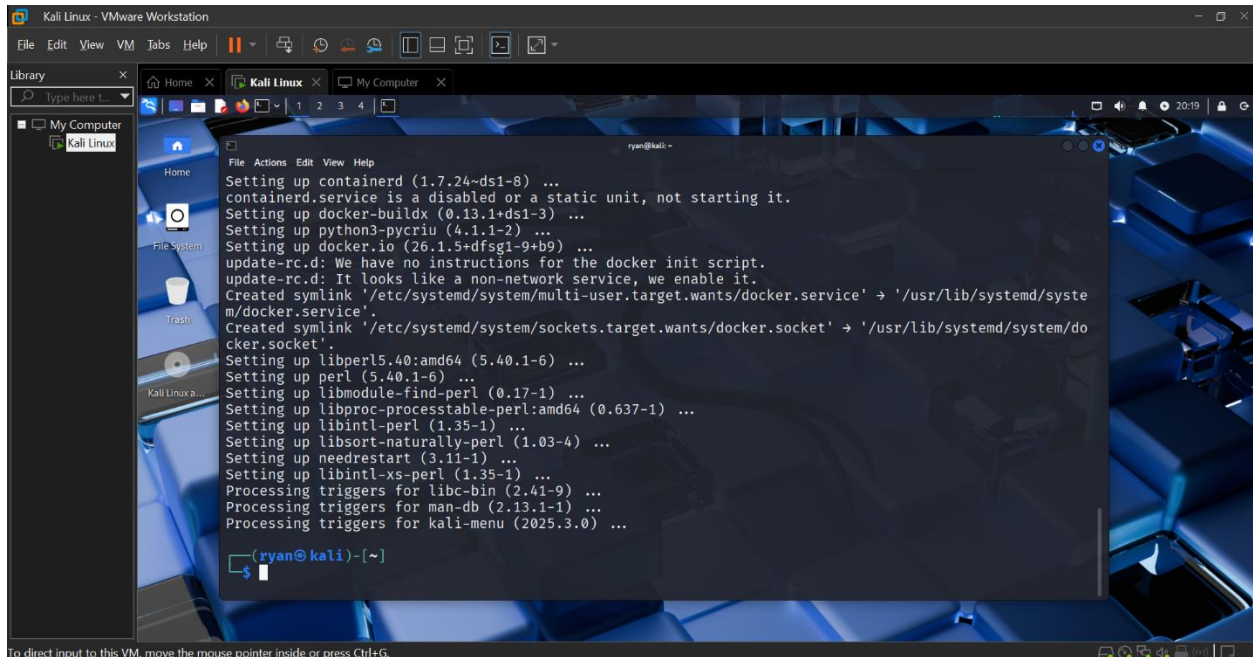


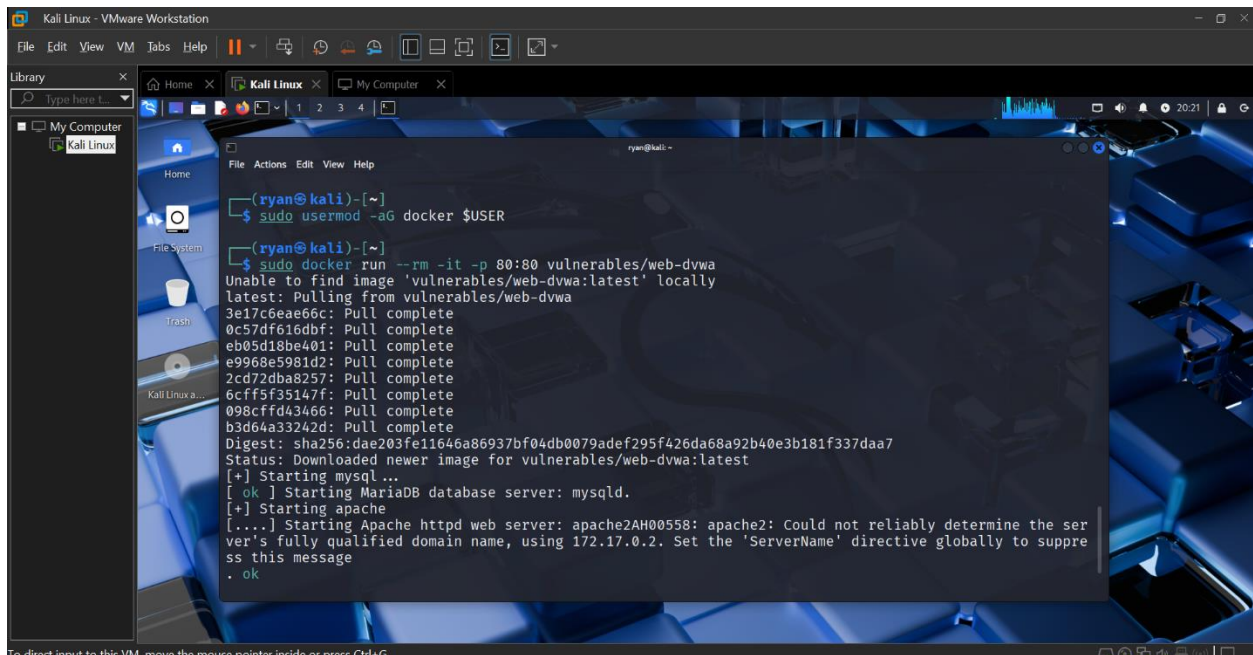
# Laporan Audit Keamanan Konfigurasi Aplikasi Dummy dan Usulkan Mitigasi

Disusun: Ryan Hanif Dwihandoyo

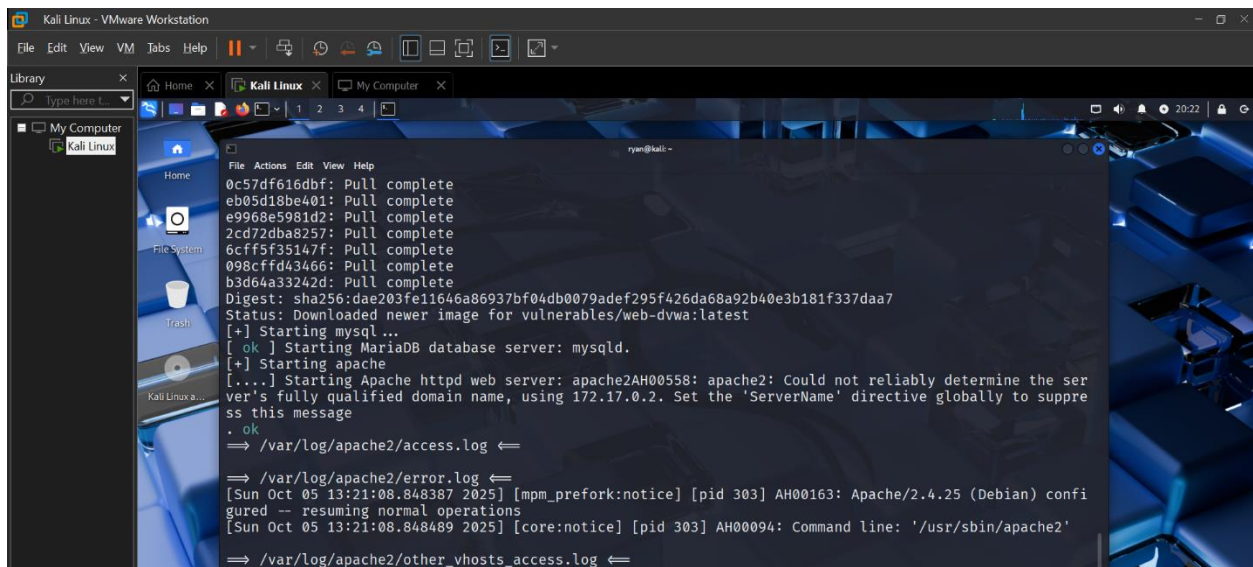
## Damn Vulnerable Web Application (DVWA)



```
Kali Linux - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Kali Linux
Home
File System
Trash
Kali Linux a...
ryan@kali:~$
Setting up containerd (1.7.24~ds1-8) ...
containerd.service is a disabled or a static unit, not starting it.
Setting up docker-buildx (0.13.1~ds1-3) ...
Setting up python3-pycrui (4.1.1-2) ...
Setting up docker.io (26.1.5+dfsg1-9+b9) ...
update-rc.d: We have no instructions for the docker init script.
update-rc.d: It looks like a non-network service, we enable it.
Created symlink '/etc/systemd/system/multi-user.target.wants/docker.service' -> '/usr/lib/systemd/system/docker.service'.
Created symlink '/etc/systemd/system/sockets.target.wants/docker.socket' -> '/usr/lib/systemd/system/docker.socket'.
Setting up libperl5.40:amd64 (5.40.1-6) ...
Setting up perl (5.40.1-6) ...
Setting up libmodule-find-perl (0.17-1) ...
Setting up libproc-processtable-perl:amd64 (0.637-1) ...
Setting up libintl-perl (1.35-1) ...
Setting up libsort-naturally-perl (1.03-4) ...
Setting up needrestart (3.11-1) ...
Setting up libintl-xs-perl (1.35-1) ...
Processing triggers for libc-bin (2.41-9) ...
Processing triggers for man-db (2.13.1-1) ...
Processing triggers for kali-menu (2025.3.0) ...
(ryan@kali)-[~]
$
```



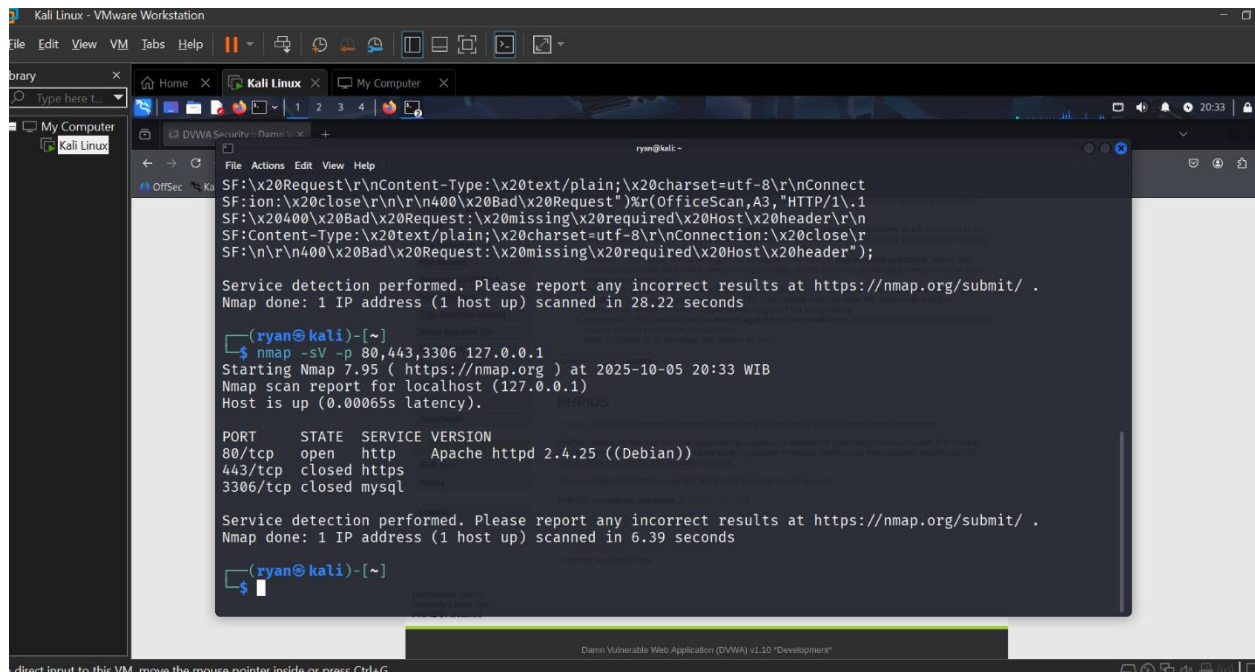
```
Kali Linux - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Kali Linux
Home
File System
Trash
Kali Linux a...
ryan@kali:~$
(ryan@kali)-[~]
$ sudo usermod -aG docker $USER
(ryan@kali)-[~]
$ sudo docker run --rm -it -p 80:80 vulnerables/web-dvwa
Unable to find image 'vulnerables/web-dvwa:latest' locally
latest: Pulling from vulnerables/web-dvwa
3e17c6eae66c: Pull complete
0c57df616dbf: Pull complete
eb05d18be401: Pull complete
e9968e5981d2: Pull complete
2cd72dba8257: Pull complete
6cff5f35147f: Pull complete
098cffd43466: Pull complete
b3d64a33242d: Pull complete
Digest: sha256:dae203fe11646a86937bf04db0079adef295f426da68a92b40e3b181f337daa7
Status: Downloaded newer image for vulnerables/web-dvwa:latest
[+] Starting mysql ...
[ ok ] Starting MariaDB database server: mysqld.
[+] Starting apache
[....] Starting Apache httpd web server: apache2AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 172.17.0.2. Set the 'ServerName' directive globally to suppress this message
. ok
```



## 1. Pengungkapan Informasi Server (Banner Grabbing)

Ini didapat dari hasil pemindaian Nmap Anda:

- **Kerentanan:** Information Disclosure (Pengungkapan Informasi) melalui Banner Grabbing.
- **Bukti (Nmap):** Server mengungkapkan nama perangkat lunak dan versi spesifiknya: Apache httpd 2.4.25 (Debian).
- **Dampak:** Informasi ini memberikan titik awal yang spesifik bagi penyerang. Mereka dapat langsung mencari exploit publik (kerentanan yang sudah diketahui) yang menargetkan versi Apache 2.4.25 atau versi Debian spesifik yang digunakan.
- **Rekomendasi Perbaikan:** Nonaktifkan ServerSignature dan ServerTokens di konfigurasi Apache untuk menyembunyikan versi dan jenis server (banner hiding).



```
ryan@kali:~$ nmap -sV -p 80,443,3306 127.0.0.1
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-05 20:33 WIB
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00065s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.25 ((Debian))
443/tcp   closed https
3306/tcp  closed mysql

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.22 seconds
```

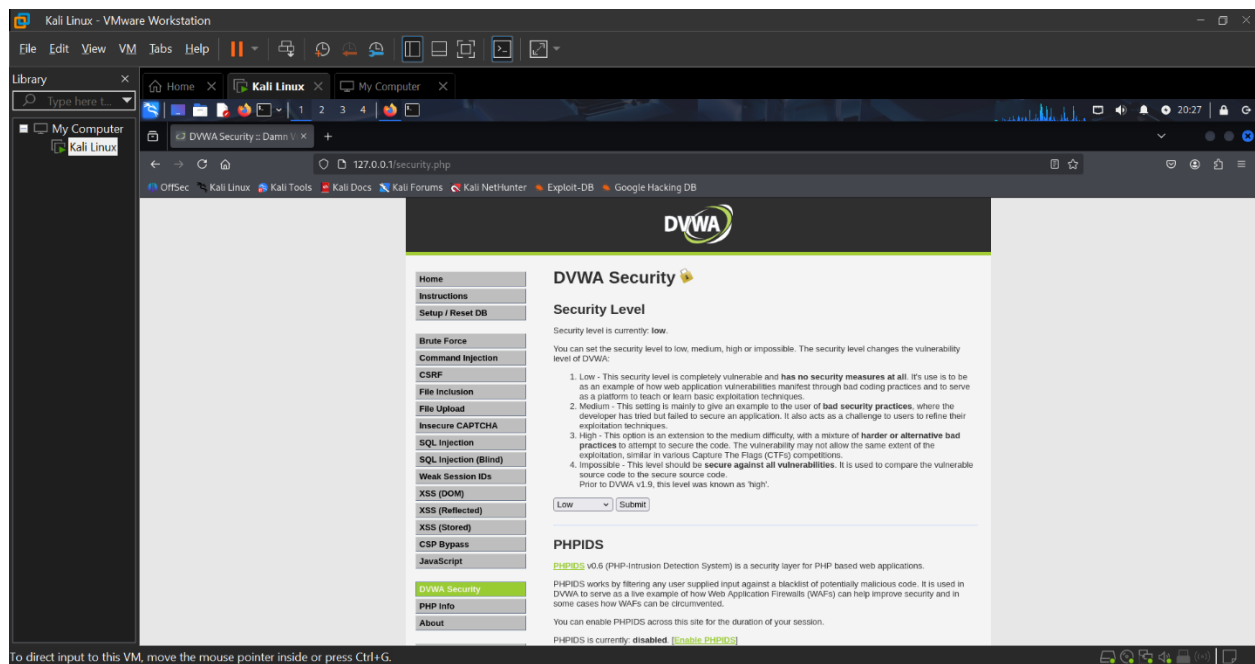
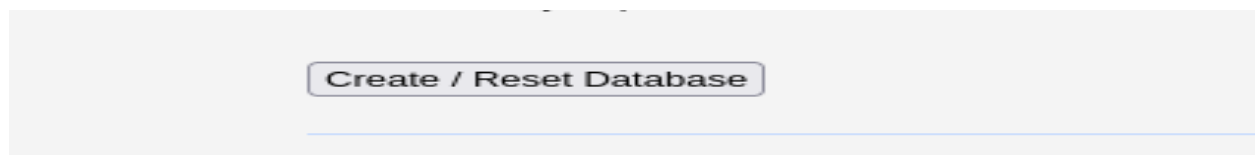
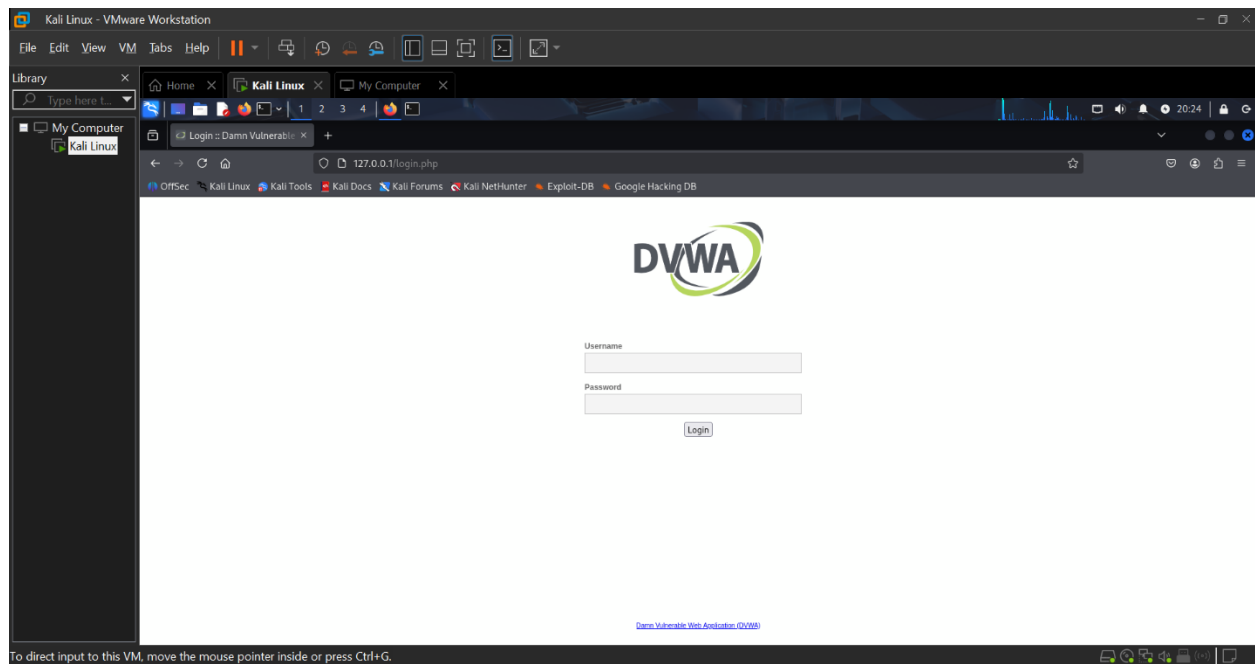
## Kerentanan *Security Misconfiguration* (Potensi):

- Mengungkapkan versi *software* secara spesifik memudahkan penyerang untuk mencari kerentanan publik (*exploits*) yang sudah diketahui untuk versi Apache 2.4.25. Dalam dunia nyata, *misconfiguration* terjadi jika versi yang digunakan adalah versi lama yang rentan (*Vulnerable and Outdated Components*).
- Solusi: Administrator harus menyembunyikan atau membatasi informasi versi ini (*Banner Hiding*) dan memastikan *software* selalu diperbarui.

## 2. Penggunaan Kredensial Default yang Tidak Aman

Ini adalah kerentanan *Misconfiguration* yang paling dasar dan dapat dikonfirmasi melalui Pemeriksaan Manual di DVWA:

- **Kerentanan:** Penggunaan Kredensial Default dan Mudah Ditebak.
- **Bukti (Manual):** Aplikasi web menggunakan pasangan username dan password baku: admin / password.
- **Dampak:** Penyerang dapat dengan mudah mendapatkan akses penuh ke akun administrator tanpa perlu melakukan serangan brute force atau mengeksploitasi kerentanan lain. Ini adalah kegagalan fatal dalam konfigurasi awal.
- **Rekomendasi Perbaikan:** Wajib mengubah semua kredensial default segera setelah instalasi, dan menerapkan kebijakan password yang kuat.

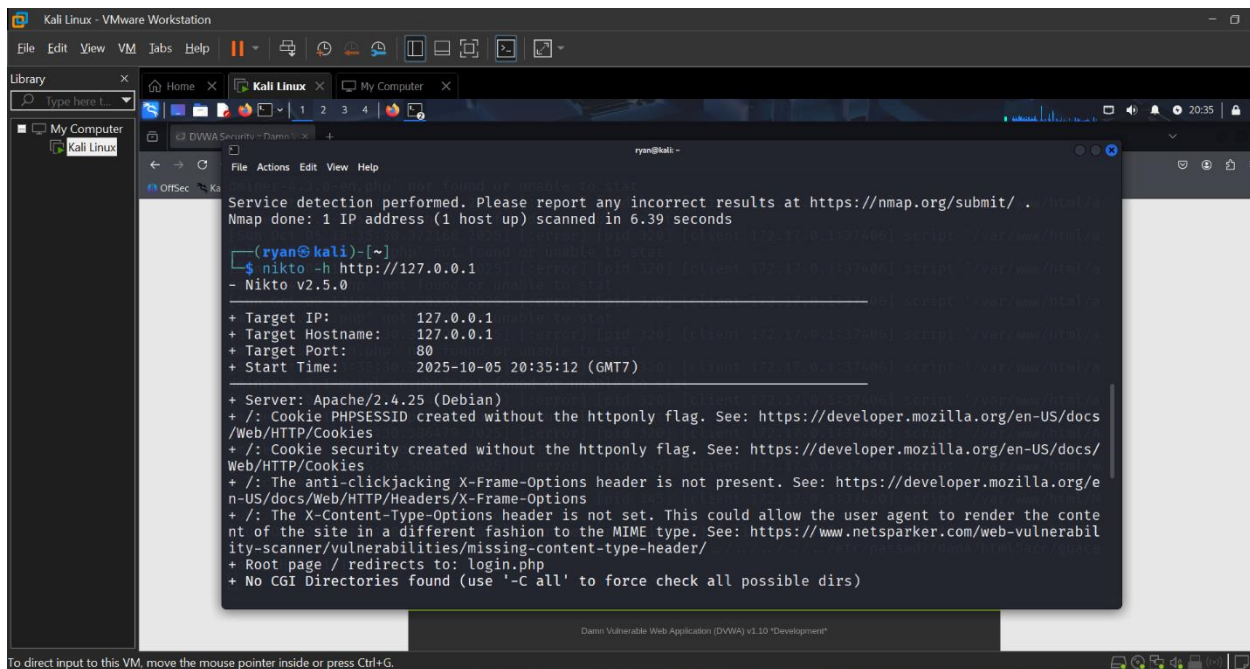




### 3. Ketidakmampuan Security Header (Rentan Clickjacking)

Ini adalah temuan yang pasti akan dilaporkan oleh Nikto dan merupakan contoh misconfiguration server web yang umum:

- **Kerentanan:** Missing Security Headers (Tidak adanya Header Keamanan HTTP), khususnya X-Frame-Options.
- **Bukti (Nikto Diharapkan):** Laporan Nikto akan menunjukkan bahwa header X-Frame-Options tidak ada atau diatur secara tidak benar pada respons HTTP server.
- **Dampak:** Tanpa header ini, halaman DVWA rentan terhadap serangan Clickjacking, di mana halaman login dapat disematkan (embed) di dalam iframe di situs berbahaya lain untuk menipu pengguna agar mengklik tautan atau memasukkan kredensial tanpa sadar.
- **Rekomendasi Perbaikan:** Konfigurasi server Apache untuk mengirim header X-Frame-Options: SAMEORIGIN atau DENY pada setiap respons HTTP.



```
Kali Linux - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Kali Linux
i2 DVWA Security - Darn...
ryan@kali: ~
$ nikto -h http://127.0.0.1
- Nikto v2.5.0

+ Target IP: 127.0.0.1
+ Target Hostname: 127.0.0.1
+ Target Port: 80
+ Start Time: 2025-10-05 20:35:12 (GMT7)

+ Server: Apache/2.4.25 (Debian)
+ /: Cookie PHPSESSID created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie security created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Root page / redirects to: login.php
+ No CGI Directories found (use '-C all' to force check all possible dirs)

Damn Vulnerable Web Application (DVWA) v1.10 "Development"
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```

Kali Linux - VMware Workstation

File Edit View VM Tabs Help

Library

My Computer

Kali Linux

DVWA Security - Damn Vulnerable Web Application

```
ryan@kali:~$ -iconsreadme/
+ /login.php: Admin login page/section found.
+ /.gitignore: .gitignore file found. It is possible to grasp the directory structure.
+ /wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wordpress/wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wordpress/wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wordpress/wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /assets/mobirise/css/meta.php?filesrc=: A PHP backdoor file manager was found.
+ /login.cgi?cli=aa%20aa%27cat%20/etc/hosts: Some D-link router remote command execution.
+ /shell?cat+/etc/hosts: A backdoor was identified.
+ 8074 requests: 0 error(s) and 21 item(s) reported on remote host
+ End Time: 2025-10-05 20:35:30 (GMT7) (18 seconds)

+ 1 host(s) tested

(ryan@kali)-[~]
$
```

Damn Vulnerable Web Application (DVWA) v1.10 "Development"

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.