

**PRAKTIKUM
KEAMANAN INFORMASI 1
PERTEMUAN 12**

Web Dynamic Pentest



Disusun oleh

Nama : Riva Mahyuli

NIM : 21/478709/SV/19365

Kelas : R1AA

**PROGRAM STUDI D-IV
TEKNOLOGI REKAYASA INTERNET
DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA
SEKOLAH VOKASI
UNIVERSITAS GADJAH MADA
2023**

Link: https://github.com/RIVAMAHYULi/LapKI_RivaMahyuli_478709_Pertemuan12.git

A. Landasan Teori

Web Dynamic Pentest (Web Dynamic Penetration Testing) adalah proses pengujian keamanan yang bertujuan untuk mengevaluasi kerentanan dan kelemahan pada aplikasi web yang berbasis dinamis. Metode ini melibatkan simulasi serangan secara aktif terhadap aplikasi web dengan menggunakan teknik dan alat yang relevan untuk mengidentifikasi celah keamanan yang dapat dimanfaatkan oleh penyerang.

Web Dynamic Pentest membantu dalam mengidentifikasi kerentanan dan celah keamanan pada aplikasi web yang berbasis dinamis, sehingga memungkinkan organisasi untuk mengambil langkah-langkah perbaikan yang diperlukan guna meningkatkan keamanan aplikasi tersebut.

Nessus adalah salah satu perangkat lunak (software) yang digunakan untuk melakukan pemindaian keamanan atau sering disebut sebagai vulnerability scanner. Dengan menggunakan Nessus, Anda dapat memeriksa kerentanan (vulnerability) pada sebuah website atau jaringan dengan tujuan untuk mengidentifikasi titik lemah yang dapat dieksploitasi oleh penyerang.

Nessus melakukan pemindaian terhadap sistem target dan menganalisis berbagai komponen, termasuk sistem operasi, aplikasi, layanan jaringan, dan konfigurasi yang mungkin rentan terhadap serangan. Setelah pemindaian selesai, Nessus akan menghasilkan laporan yang mencantumkan kerentanan yang ditemukan, tingkat keparahan, dan saran tindakan untuk memperbaiki kerentanan tersebut.

B. Langkah Kerja

1. Install nessus , sebelum melakukan pemindaian terhadap suatu web kita membutuhkan software bernama Nessus.
2. Buka web browser cari download nessus , pilih download by curl dan copy link-nya.
3. Di terminal kalilinux ketikan seperti gambar dibawah.



```
(root@kali)~[/home/kali]
# curl --request GET \
--url 'https://www.tenable.com/downloads/api/v2/pages/nessus/files/Nessus-10.5.2-ubuntu1404_amd64.deb' \
--output 'Nessus-10.5.2-ubuntu1404_amd64.deb'
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload  Total   Spent    Left   Speed
100 62.2M    0 62.2M    0    0  10.3M      0 --:--:--  0:00:05 --:--:-- 10.5M
```

4. Lihat apakah file sudah ada

```
(root@kali)-[/home/kali]
# ls
ls: cannot access 'thinclient_drives': Permission denied
cnf.v2.tar.gz  Music                                Public                                upd_mutillidae.sh
Desktop       Nessus-10.5.1-debian10_amd64.deb    Templates                            Videos
Documents     Nessus-10.5.2-ubuntu1404_amd64.deb Test                                xfce4.sh
Downloads     Pictures                            thinclient_drives                    xfce4.sh.1
```

5. Lalu ketikkan `sudo apt install -f` untuk menginstall software Nessus

```
(root@kali)-[/home/kali]
# sudo apt install -f ./Nessus-10.5.2-ubuntu1404_amd64.deb
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Note, selecting 'nessus' instead of './Nessus-10.5.2-ubuntu1404_amd64.deb'
The following package was automatically installed and is no longer required:
  php7.4-mysql
Use 'sudo apt autoremove' to remove it.
The following NEW packages will be installed:
  nessus
```

6. Aktifkan dan jalankan Nessus

```
(root@kali)-[/home/kali]
# sudo systemctl enable nessusd
Created symlink /etc/systemd/system/nessusd.service → /lib/systemd/system/nessusd.service.
Created symlink /etc/systemd/system/multi-user.target.wants/nessusd.service → /lib/systemd/system/nessusd.service.

(root@kali)-[/home/kali]
# sudo systemctl start nessusd
```

7. Cek status Nessus

```
(root@kali)-[/home/kali]
# sudo systemctl status nessusd.service
● nessusd.service - The Nessus Vulnerability Scanner
   Loaded: loaded (/lib/systemd/system/nessusd.service; enabled; vendor preset: disabled)
   Active: active (running) since Mon 2023-05-29 20:40:36 CDT; 22s ago
     Main PID: 675980 (nessus-service)
        Tasks: 14 (limit: 4635)
       Memory: 97.4M
          CPU: 22.303s
    CGroup: /system.slice/nessusd.service
            └─675980 /opt/nessus/sbin/nessus-service -q
              └─675982 nessusd -q

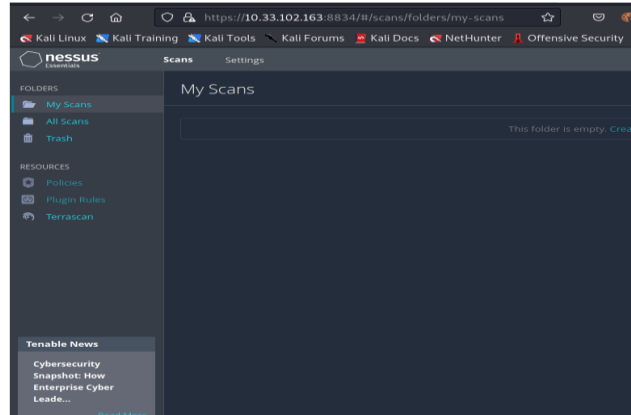
May 29 20:40:36 kali systemd[1]: Started The Nessus Vulnerability Scanner.
May 29 20:40:37 kali nessus-service[675982]: Cached 0 plugin libs in 0msec
May 29 20:40:37 kali nessus-service[675982]: Cached 0 plugin libs in 0msec

(root@kali)-[/home/kali]
# sudo ss -ant | grep 8834
LISTEN 0      1024          0.0.0.0:8834      0.0.0.0:*
LISTEN 0      1024          [::]:8834        [::]:*
```

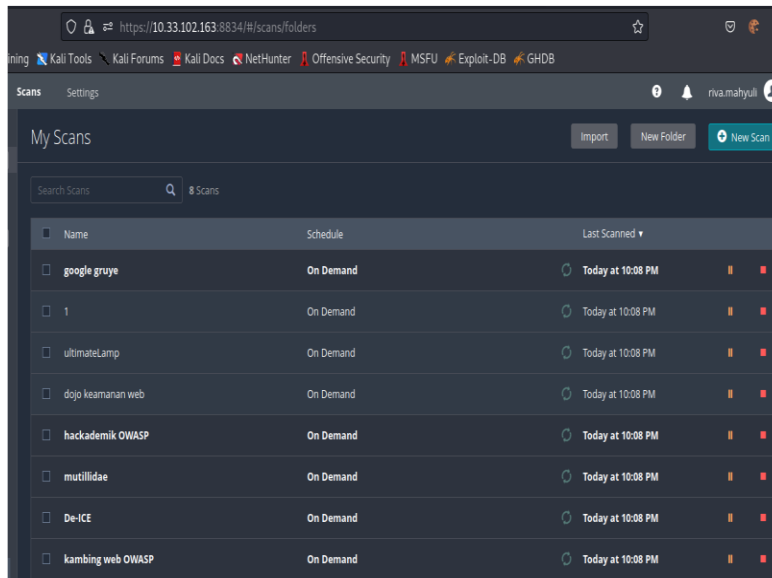
8. Di Web Browser ketikkan [https://IP Address PC\(10.33.102.163\).8834/#/](https://10.33.102.163:8834/#/) untuk membuat akun Nessus



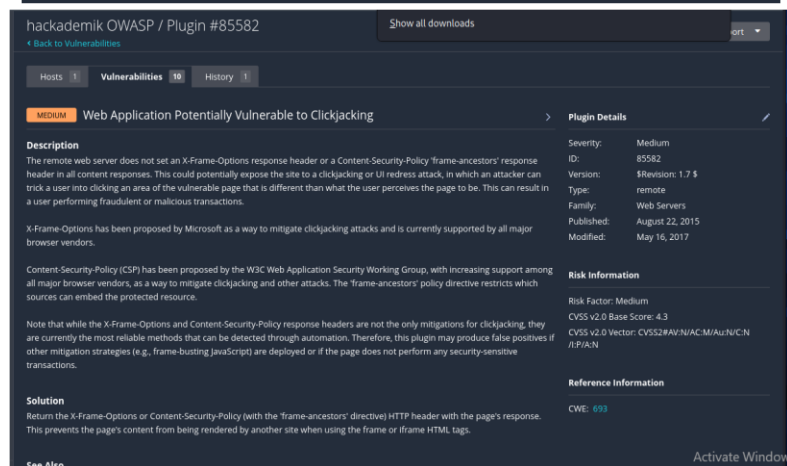
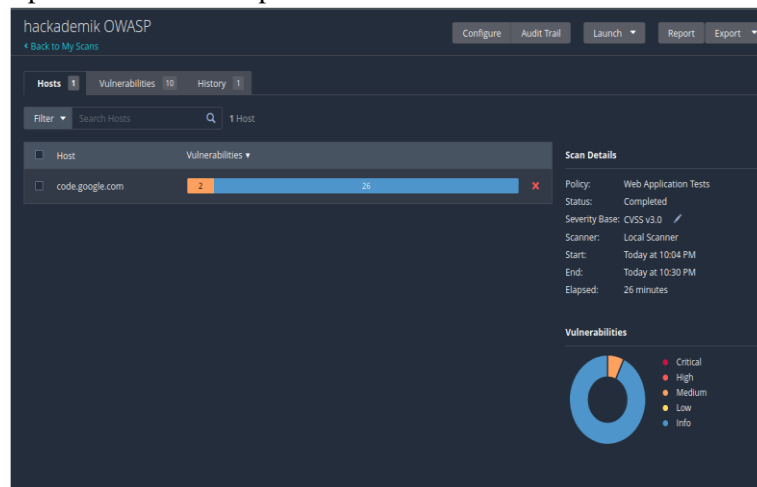
9. Setelah selesai membuat akun maka tampilan web akan seperti ini



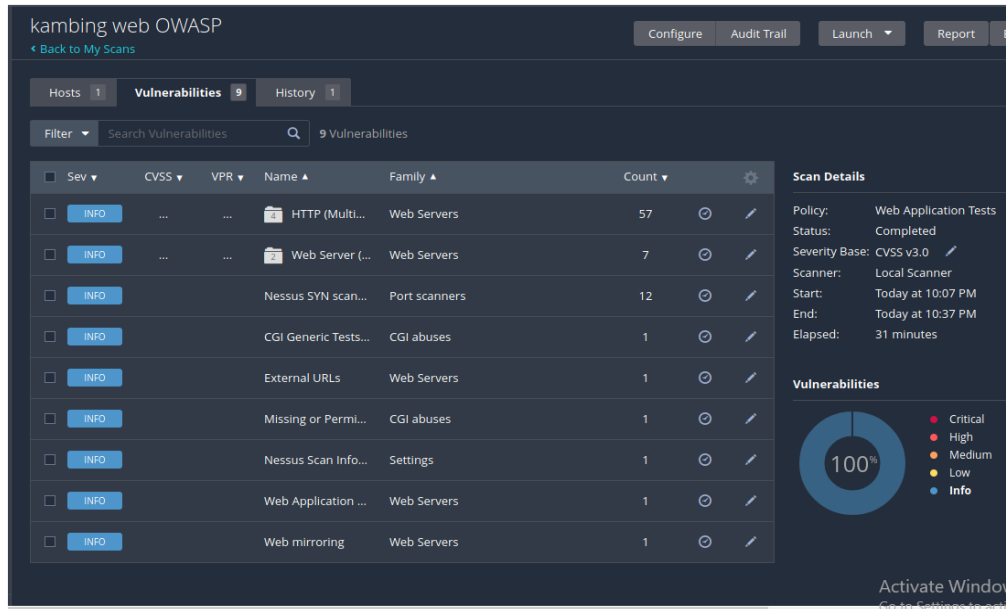
10. Setelah selesai kita akan melakukan pengujian Vulnerability dengan Nessus
11. Klik new scan dan pada bagian deskripsi kita akan memasukan link dari web yang ingin kita pindai.



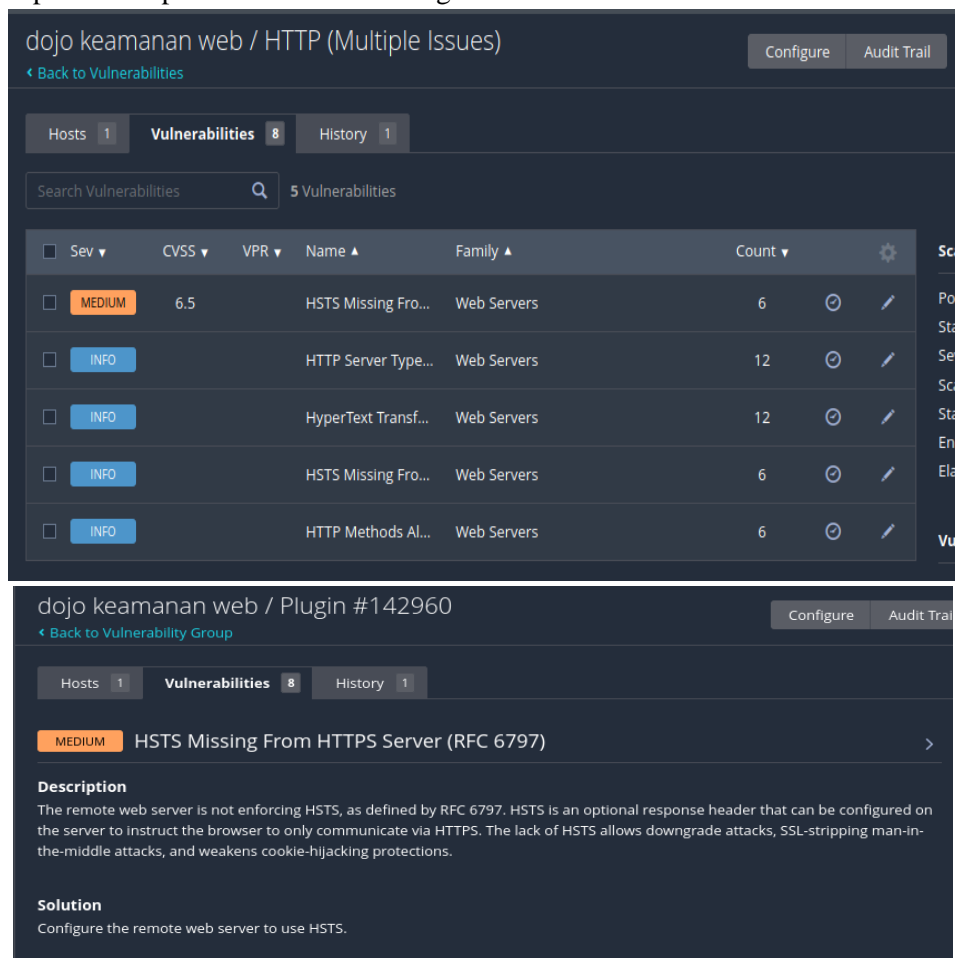
12. Tampilan hasil pemindaian di web pertama



13. Tampilan hasil pemindaian di web kedua



14. Tampilan hasil pemindaian di web ketiga



15. Tampilan hasil pemindaian di web keempat

ultimateLamp [Configure](#) [Audit Trail](#)

[Back to My Scans](#)

Hosts 1 **Vulnerabilities 24** History 1

Filter Search Vulnerabilities 24 Vulnerabilities

<input type="checkbox"/>	Sev	CVSS	VPR	Name	Family	Count		
<input type="checkbox"/>	HIGH	7.5 *		CGI Generic ...	CGI abuses	2		
<input type="checkbox"/>	HIGH	7.5 *		CGI Generic ...	CGI abuses	2		
<input type="checkbox"/>	HIGH	7.5 *		CGI Generic ...	CGI abuses	2		
<input type="checkbox"/>	HIGH	7.5 *		CGI Generic ...	CGI abuses	2		
<input type="checkbox"/>	MEDIUM	6.1	5.7	jQuery 1.2 < ...	CGI abuses : XSS	2		
<input type="checkbox"/>	MEDIUM	5.3		CGI Generic ...	CGI abuses	2		
<input type="checkbox"/>	MEDIUM	5.3		Browsable W...	CGI abuses	1		
<input type="checkbox"/>	MEDIUM	5.0 *	4.2	FlatNuke Ind...	CGI abuses	2		
<input type="checkbox"/>	MEDIUM	5.0 *		Backup Files ...	CGI abuses	2		
<input type="checkbox"/>	MEDIUM	5.0 *		Web Applicat...	CGI abuses	2		
<input type="checkbox"/>	MEDIUM	4.3 *		Web Applicat...	Web Servers	2		
<input type="checkbox"/>	MIXED	HTTP (...)	Web Servers	38		

Scan D
Policy:
Status:
Severit
Scanne
Start:
End:
Elapse

Vulner

16. Tampilan hasil pemindaian di web kelima

De-ICE / HTTP (Multiple Issues) [Configure](#) [Audit Trail](#)

[Back to Vulnerabilities](#)

Hosts 1 **Vulnerabilities 11** History 1

Search Vulnerabilities 6 Vulnerabilities

<input type="checkbox"/>	Sev	CVSS	VPR	Name	Family	Count		
<input type="checkbox"/>	MEDIUM	6.5		HSTS Missin...	Web Servers	1		
<input type="checkbox"/>	INFO			HyperText Tr...	Web Servers	6		
<input type="checkbox"/>	INFO			HTTP Metho...	Web Servers	2		
<input type="checkbox"/>	INFO			HTTP Server ...	Web Servers	2		
<input type="checkbox"/>	INFO			HyperText Tr...	Web Servers	2		
<input type="checkbox"/>	INFO			HSTS Missin...	Web Servers	1		

Scan D
Policy:
Status:
Severit
Scanne
Start:
End:
Elapse

Vulner

De-ICE / Plugin #142960 [Configure](#) [Audit Trail](#)

[Back to Vulnerability Group](#)

Hosts 1 **Vulnerabilities 11** History 1

MEDIUM HSTS Missing From HTTPS Server (RFC 6797) >

Description

The remote web server is not enforcing HSTS, as defined by RFC 6797. HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

Solution

Configure the remote web server to use HSTS.

17. Tampilan hasil pemindaian di web keenam

mutillidae

Configure Audit Trail Launch

Hosts 1 Vulnerabilities 15 History 1


Filter Search Vulnerabilities 15 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count		
MEDIUM	5.0 *	5.8	Apple Mac O...	Web Servers	2		
MEDIUM	4.3 *		Web Applicat...	Web Servers	2		
MIXED	HTTP (...)	Web Servers	8		
MIXED	Web Se...	Web Servers	6		
INFO	HTTP (...)	CGI abuses	7		
INFO			Nessus SYN ...	Port scanners	6		
INFO			Apache HTT...	Web Servers	2		
INFO			CGI Generic ...	CGI abuses	2		
INFO			External URLs	Web Servers	2		
INFO			Protected W...	Web Servers	2		
INFO			Web Applicat...	Web Servers	2		
INFO			Web Applicat...	Web Servers	2		

Scan Details

Policy:
Status:
Severity Base:
Scanner:
Start:
End:
Elapsed:

Vulnerability



18. Tampilan hasil pemindaian di web ketujuh

1

Configure Audit Trail Launch

Hosts 1 Vulnerabilities 7 History 1


Filter Search Vulnerabilities 7 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count		
MIXED	HTTP (...)	Web Servers	14		
INFO	Web Se...	Web Servers	5		
INFO	HTTP (...)	CGI abuses	3		
INFO			Nessus SYN ...	Port scanners	12		
INFO			External URLs	Web Servers	1		
INFO			Nessus Scan ...	Settings	1		
INFO			Web Applicat...	Web Servers	1		

Scan Details

Policy:
Status:
Severity Base:
Scanner:
Start:
End:
Elapsed:

Vulnerability



19. Tampilan hasil pemindaian di web kedepan

google gruye

Configure

Audit Trail

Launch

Back to My Scans

Hosts1

Vulnerabilities16

History2

Filter

Search Vulnerabilities

16 Vulnerabilities

<input type="checkbox"/>	Sev	CVSS	VPR	Name	Family	Count		
<input type="checkbox"/>	MEDIUM	4.3 *		CGI Generic ...	CGI abuses : XSS	2		
<input type="checkbox"/>	MEDIUM	4.3 *		CGI Generic ...	CGI abuses : XSS	2		
<input type="checkbox"/>	MEDIUM	4.3 *		Web Applicat...	Web Servers	2		
<input type="checkbox"/>	MIXED	Web Se...	Web Servers	7		
<input type="checkbox"/>	INFO	HTTP (...)	Web Servers	7		
<input type="checkbox"/>	INFO	HTTP (...)	CGI abuses	5		
<input type="checkbox"/>	INFO			CGI Generic I...	CGI abuses	2		
<input type="checkbox"/>	INFO			CGI Generic ...	CGI abuses	2		
<input type="checkbox"/>	INFO			External URLs	Web Servers	2		
<input type="checkbox"/>	INFO			Nessus SYN ...	Port scanners	2		

Scan Details

Policy:

Status:

Severity Base:

Scanner:

Start:

End:

Elapsed:

Vulnerabilit