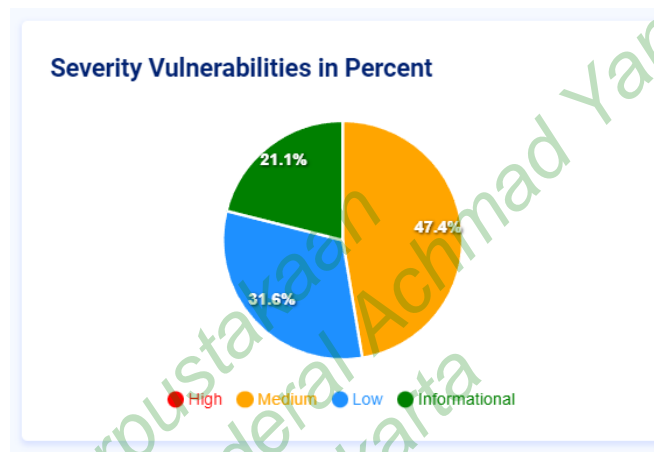


## BAB 4

### HASIL PENELITIAN

#### 4.1 RINGKASAN HASIL PENELITIAN

Hasil dari proses penilaian kerentanan ditemukan beberapa celah kerentanan pada situ web target [pordik.unjaya.ac.id](http://pordik.unjaya.ac.id).



**Gambar 4.1** Tingkat kerentanan dalam presentase

Berdasarkan gambar 4.1 menampilkan tingkat kerentanan dalam bentuk persentase paling banyak pada tingkatan kerentanan *medium* 47,4%, tingkatan kerentanan *low* 31,6%, dan 21,1% hanya sebatas *informational*.

#### 4.2 ASSESSMENT

##### 4.2.1 Information Gathering

*Information Gathering* merupakan tahap awal untuk melakukan penilaian kerentanan dalam sebuah situs web, dalam penelitian ini penulis menggunakan tools situs web *sitereport.netcraft.com*. Berdasarkan hasil *scanning* dengan Netcraft didapatkan hasil pemindaian yang dapat dilihat pada gambar 4.2.

The screenshot displays the Netcraft website scan results for the site `http://pordik.unjaya.ac.id`. The interface is divided into two main sections: **Background** and **Network**.

**Background Information:**

- Site title:** Portal Akademik | Universitas Jenderal Achmad Yani Yogyakarta
- Date first seen:** October 2018
- Site rank:** Not Present; Netcraft Risk Rating: 1/10
- Description:** Not Present; Primary language: Indonesian

**Network Information:**

- Site:** `http://pordik.unjaya.ac.id`
- Domain:** `unjaya.ac.id`
- Netblock Owner:** PT SELARAS CITRA TERABIT
- Nameserver:** `ns1.fastcloud.id`
- Hosting company:** Terabit Network
- Domain registrar:** unknown
- Hosting country:** ID
- Nameserver organisation:** unknown
- IPv4 address:** `103.247.15.33 (VirusTotal #)`
- Organisation:** unknown
- IPv4 autonomous systems:** `AS131706`
- DNS admin:** `ceknjs@qwords.co.id`
- IPv6 address:** Not Present
- Top Level Domain:** Indonesia (.ac.id)
- IPv6 autonomous systems:** Not Present
- DNS Security Extensions:** unknown
- Reverse DNS:** `ip-33-15-247.terabit.net.id`

**IP delegation:**

IPv4 address (103.247.15.33)

IP range	Country	Name	Description
<code>::ffff:0:0:0/96</code>	United States	IANA-IPV4-MAPPED-ADDRESS	Internet Assigned Numbers Authority
<code>1.103.0.0-103.255.255.255</code>	Australia	APNIC-AP	Asia Pacific Network Information Centre

**Gambar 4.2** Pemindaian dengan Netcraft

Hasil pemindaian menggunakan tools netcraft diperoleh informasi mengenai IP dan informasi umum tentang situs web pordik unjaya berhasil diperoleh. Hasil pemindaian yang disajikan dalam bentuk tabel didapatkan beberapa informasi yang dapat dilihat pada tabel 4.1.

**Tabel 4.1** Hasil dari *Information gathering*

No.	Informasi	Hasil
1.	<i>Site title</i>	Portal Akademik   Universitas Jenderal Achmad Yani Yogyakarta Site rank
2.	<i>Date first seen</i>	Oktober 2018
3.	<i>Site</i>	<code>http://pordik.unjaya.ac.id/</code>
4.	<i>Netblock Owner</i>	PT SELARAS CITRA TERABIT
5.	<i>Hosting company</i>	Terabit Network
6.	<i>Hosting Country</i>	ID
7.	<i>IPv4 address</i>	103.247.15.33
8.	<i>Reverse DNS</i>	<code>ip-33-15-247.terabit.net.id</code>

9.	<i>Main Domain</i>	unjaya.ac.id
10.	<i>Nameserver</i>	ns1.fastcloud.id
11.	<i>OS</i>	Linux
12.	<i>Web Server</i>	Apache/2.4.41 Ubuntu
13.	<i>Last seen</i>	20-Aug-2022
14.	<i>Top Level Domain</i>	Indonesia (.ac.id)
15.	<i>DNS admin</i>	teknis@qwords.co.id

Hasil dari *Information Gathering* mendapatkan beberapa informasi seperti *Date first seen* pada Oktober 2018, *Hosting company* menggunakan Terabit Network, dan *DNS admin* menggunakan teknis@qwords.co.id.

#### 4.2.2 Network Mapping

Tahap *network mapping* dilakukan untuk mengetahui konfigurasi jaringan pada situs web target. Dalam melakukan network mapping peneliti menggunakan tools *zenmap*. Informasi yang telah didapatkan pada tahap sebelumnya diambil untuk mendapatkan topology jaringan pada situs web target.

```

Zenmap
Scan Tools Profile Help
Target: 103.247.15.33
Command: nmap -T4 -A -v 103.247.15.33
Hosts Services Nmap Output Ports/Hosts Topology Host Details Scans
OS * Host
ip-33-15-247.terabit 443/tcp closed nmap
AddressLine OS guesses: Linux 5.0 (95%), Linux 5.0 - 5.4 (95%), Linux 5.4 (94%), HP P2000 G3 NAS device (93%), Linux 4.15 - 5.6 (93%), Linux 5.3 - 5.4 (93%), Linux 2.6.32 (92%), Infomir MAG-250 set-top box (92%), Ubiquiti AirMax NanoStation MAP (Linux 2.6.32) (92%), Linux 3.7 (92%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 9.557 days (since Mon Aug 15 20:53:25 2022)
Network Distance: 11 hops
IP Sequence Prediction: Difficulty=261 (Good luck!)
IP Sequence Generation: All zeros
TRACEROUTE (using port 21/tcp)
HOP RTT ADDRESS
1 1.00 ms 192.168.100.1
2 12.00 ms 149.113.14.1
3 13.00 ms be4-pe03-cg03.fast.net.id (202.73.96.74)
4 13.00 ms be4-cg03-pe03.fast.net.id (202.73.96.73)
5 14.00 ms fm-dyn-110-136-64-217.fast.net.id (118.136.64.217)
6 ...
7 12.00 ms 43.252.146.73
8 22.00 ms 10.20.25.169
9 23.00 ms ip-214-135-101.terabit.net.id (121.101.135.250)
10 23.00 ms ip-214-135-101.terabit.net.id (121.101.135.214)
11 23.00 ms ip-33-15-247.terabit.net.id (103.247.15.33)
NSE: Script Post-scanning.
Initiating NSE at 10:15
Completed NSE at 10:15, 0.00s elapsed
Initiating NSE at 10:15
Completed NSE at 10:15, 0.00s elapsed
Initiating NSE at 10:15
Completed NSE at 10:15, 0.00s elapsed
Raw data files from C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.40 seconds
Raw packets sent: 2065 (92.544KB) | Rcvd: 275 (22.329KB)

```

**Gambar 4.3** Pemindaian dengan Zenmap

Berdasarkan gambar 4.3 hasil pemindaian dengan menggunakan tools *zenmap* ditemukan mengenai informasi konfigurasi jaringan pada situs web produk

unjaya. Hasil pemindaian informasi yang didapatkan dari tahapan *network mapping* dapat dilihat pada tabel 4.2.

**Tabel 4.2** Hasil dari *Network Mapping*

No.	Informasi	Hasil
1.	<i>Open Port</i>	80/Apache httpd.2.4.4.1 (Ubuntu)
2.	<i>Closed port</i>	20
3.	<i>Closed port</i>	21
4.	<i>Closed Port</i>	443
5.	<i>Scanned Port</i>	1000
6.	<i>Housting Country</i>	ID
7.	<i>IPv4 address</i>	103.247.15.33
8.	<i>Reverse DNS</i>	ip-33-15-247.terabit.net.id

Hasil dari *Network Mapping*, menampilkan ada satu *port* yang berstatus *open* yaitu port 80, dengan protokol TCP (*Transmission Control Protocol*) dan tiga *port* yang berstatus *closed* yaitu 20,21. Dengan adanya *port* yang terbuka, maka *port* tersebut memiliki risiko terjadinya serangan.

#### 4.2.3 *Vulnerability Identification*

Pada tahap awal ini penulis menggunakan beberapa tools untuk mencari informasi detail mengenai situ web target pordik.unjaya.ac.id yang dilakukan menggunakan tools Nikto website scanner dan Helium security.

#### 4.2.4 Nikto Website Scanner

Pemindaian kerentanan yang pertama menggunakan *tools* Nikto untuk mengumpulkan informasi mengenai situs web target pordik unjaya secara lebih lanjut. *Tools* nikto website scanner dijalankan pada sistem operasi linux. Perintah yang dijalankan untuk melakukan pemindaian dengan menuliskan perintah *nikto -h http://pordik.unjaya.ac.id/ -o result.html*, selanjutnya nikto akan melakukan proses scanning yang berlangsung selama 10 menit. Hasil pemindaian dengan menggunakan *tools* nikto website scanner ditampilkan pada gambar 4.4

```

(root@kali)-[~]
└─# nikto -h http://pordik.unjaya.ac.id/ -o result.html
- Nikto v2.1.6

+ Target IP: 103.247.15.33
+ Target Hostname: pordik.unjaya.ac.id
+ Target Port: 80
+ Start Time: 2022-08-18 03:30:05 (GMT-4)
Informasi Situs Web

+ Server: Apache/2.4.41 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the use
  r agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user age
  nt to render the content of the site in a different fashion to the MIME type
Informasi Celah Kerentanan
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Web Server returns a valid response with junk HTTP methods, this may cause
  false positives.
+ /config.php: PHP Config file may contain database IDs and passwords.
+ 7941 requests: 0 error(s) and 5 item(s) reported on remote host
+ End Time: 2022-08-18 03:34:17 (GMT-4) (252 seconds)

```

**Gambar 4.4** Pemindaian dengan Nikto

Berdasarkan gambar 4.4 pemindaian dengan nikto berhasil mendapatkan informasi yang terdapat dalam situs web pordik.unjaya seperti server yang digunakan adalah Apache/2.4.4.1 (Ubuntu) dengan alamat IP 103.247.15.33, dan port yang digunakan adalah port 80. Berdasarkan hasil pemindain dengan nikto website scanner berhasil menemukan kerentanan yang ada pada situs web pordik.unjaya yang dilihat pada tabel 4.3.

**Tabel 4.3** Hasil Pemindaian dengan Nikto Website Scanner

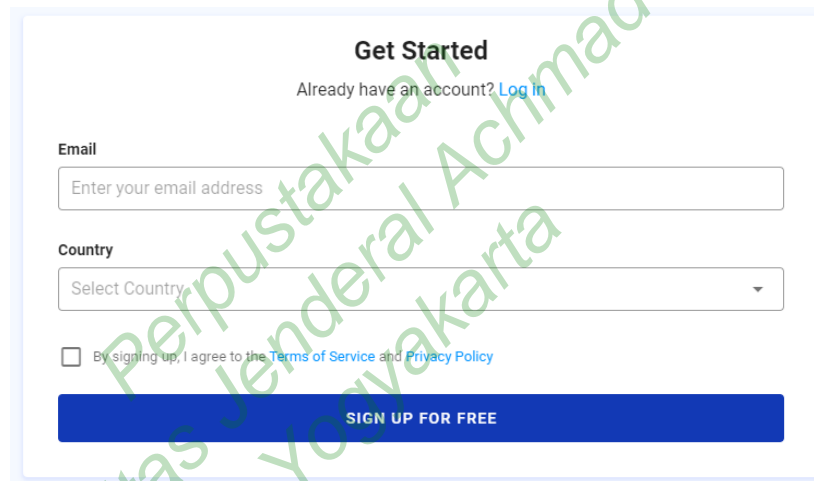
No.	Kerentanan
1.	<i>The anti-clickjacking X-Frame-Options header is not present.</i>
2.	<i>The X-XSS-Protection header is not defined.</i>
3.	<i>The X-Content-Type-Options header is not set.</i>
4.	<i>Web Server returns a valid response with junk HTTP methods, this may cause false positives.</i>
5.	<i>/config.php: PHP Config file may contain database IDs and passwords.</i>
6.	<i>The site uses SSL and the Strict-Transport-Security HTTP header is not defined.</i>

Berdasarkan hasil pemindaian dengan menggunakan nikto, ditemukan juga kerentanan seperti *X-XSS-Protection header is not defined*, *X-Content-Type-Options header is not set*, *anti-clickjacking X-Frame-Options header is not present*,

maka situs web pordik terindikasi terdapat celah kerentanan *Cross Slide Scripting* (XSS), yang memungkinkan terjadinya serangan pada situs web pordik unjaya.

#### 4.2.5 Helium Security

Helium security merupakan sebuah tools yang digunakan untuk melakukan penilaian kerentanan berbasis cloud yang kuat untuk mengetahui sebuah kerentanan security headers, SSL/TLS Scanner, dan berbagai kerentanan lainnya.



**Get Started**  
Already have an account? [Log in](#)

**Email**  
Enter your email address

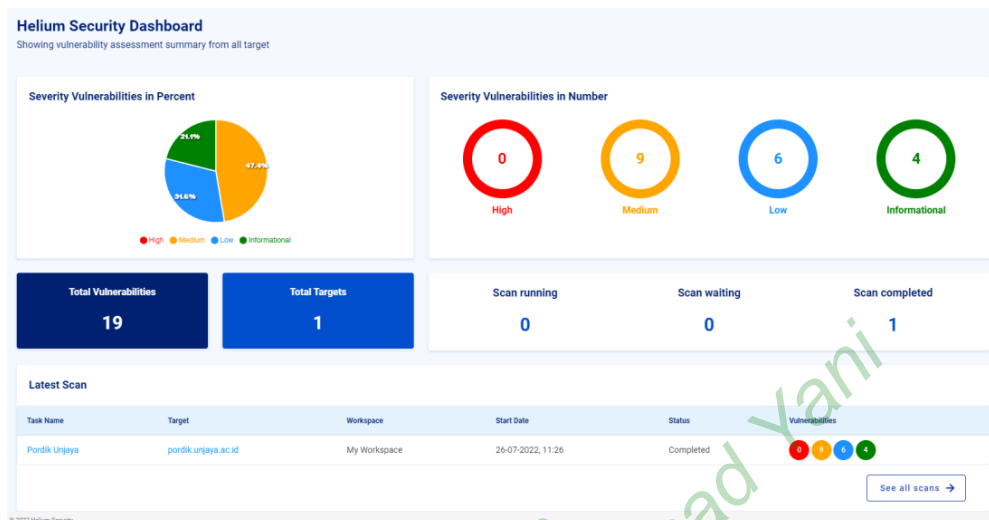
**Country**  
Select Country

By signing up, I agree to the [Terms of Service](#) and [Privacy Policy](#)

**SIGN UP FOR FREE**

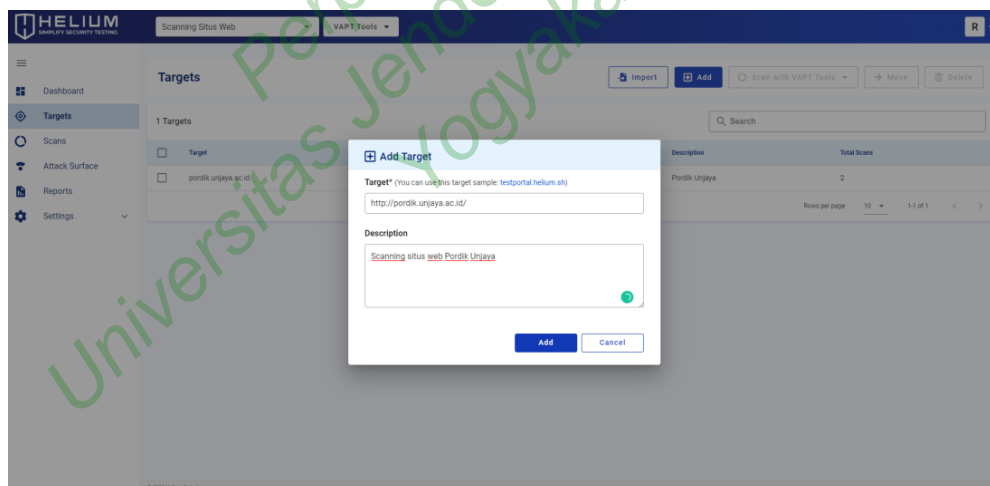
**Gambar 4.5** Tampilan Sign UP Helium

Gambar 4.5 merupakan tampilan sign up dari helium security, sebelum melakukan proses scanning harus melakukan pendaftaran terlebih dahulu. Dalam penelitian ini menggunakan helium free plan.



**Gambar 4.6** Dashboard Helium Security

Gambar 4.6 menunjukkan dashboard *helium security* yang menampilkan hasil presentasi *scanning* pada domain *prodik.unjaya.ac.id*. Helium security mengklasifikasikan tingkatan kerentanan tersebut yaitu High, Medium, Low.



**Gambar 4.7** Tampilan Add Target

Gambar 4.7 merupakan tampilan add target pada *helium security* yang berfungsi untuk menambahkan *scanning* pada situs web. Dalam penelitian ini objek

penelitian adalah situs web pordik.unjaya.ac.id, maka target yang ditambahkan adalah pordik.unjaya.ac.id.



**Gambar 4.8** Hasil pemindaian Helium

Gambar 4.8 merupakan hasil dari pengujian *vulnerability identification* menggunakan tools helium security terhadap beberapa kerentanan pada situs web pordik.unjaya.ac.id terdapat 19 jenis kerentanan, dimana terdapat 9 tingkatan kerentanan *medium*, 6 tingkatan kerentanan *low*, dan 4 *informational*. Hasil ringkasan *risk level vulnerability* dapat dilihat pada tabel 4.4.

**Tabel 4.4** Risk level Vulnerability

<i>Risk Level</i>	<i>Number of Alerts</i>
<i>High</i>	0
<i>Medium</i>	9
<i>Low</i>	6
<i>Informational</i>	4

Berdasarkan Tabel 4.4 yang digambarkan dalam bentuk persentase yaitu risk level kerentanan pada tabel high mendapatkan nilai 0% atau tidak ada kerentanan, selanjutnya pada level medium mendapatkan nilai kerentanan 47,4%, kerentanan yaitu: *Absence of Anti-CSRF Tokens, Anti-CSRF Tokens Check, Backup File Disclosure, Content Security Policy (CSP) Header Not Set, Directory Browsing, HTTP Only Site, Missing Anti-clickjacking Header, Relative Path Confusion, Vulnerable JS Library*, dan pada tingkat kerentanan low mendapatkan



nilai 31,6% kerentanan yaitu: *Cookie No HttpOnly Flag*, *Cookie without SameSite Attribute*, *Cookie without SameSite Attribute*, *Cross-Domain JavaScript Source File Inclusion*, *Server Leaks Version Information via "Server" HTTP Response Header Field*, *Timestamp Disclosure - Unix*, *X-Content-Type-Options Header Missing*, dan pada level informational mendapatkan nilai 21,1% kerentanan yaitu: *Cookie Slack Detector*, *Information Disclosure - Suspicious Comments*, *Modern Web Application*, *User Agent Fuzzer*. Dari kerentanan yang didapatkan tersebut, situs web pordik unjaya masih dikategorikan aman dengan tingkat kerentanan tertinggi pada *level medium*.

### 4.3 PEMBAHASAN

Pada pembahasan, berisi saran yang direkomendasi oleh tools Helium Security. Dari beberapa temuan kerentanan yang ada penulis memberikan rekomendasi solusi dari masing-masing kerentanan yang ditemukan.

#### 4.3.1 Penanggulangan *Absence of Anti-CSRF Tokens*

1. Nilai token tidak boleh diprediksi, misalnya dapat dihasilkan dengan generator acak yang dapat dipercaya dan dikonfigurasi dengan benar.
2. Token kedaluwarsa setelah beberapa saat, sehingga tidak dapat digunakan kembali.
3. Jangan menggunakan stempel waktu lokal sebagai token tanpa enkripsi sisi server.
4. Jangan mengirim token anti CSRF dalam permintaan HTTP GET, sehingga tidak bocor di URL atau header permintaan.

#### 4.3.2 Penanggulangan *Anti-CSRF Tokens Check*

1. Nilai token tidak boleh diprediksi, misalnya dapat dihasilkan dengan generator acak yang dapat dipercaya dan dikonfigurasi dengan benar.
2. Token kedaluwarsa setelah beberapa saat, sehingga tidak dapat digunakan kembali.
3. Jangan menggunakan stempel waktu lokal sebagai token tanpa enkripsi sisi server.

4. Jangan mengirim token anti CSRF dalam permintaan HTTP GET, sehingga tidak bocor di URL atau header permintaan.

#### 4.3.3 Penanggulangan *Backup File Disclosure*

1. Jangan pernah menyimpan file cadangan di server, karena file bisa mencakup data sensitif seperti file kata sandi atau kode sumber aplikasi.
2. Menerapkan otorisasi kontrol akses yang sesuai untuk setiap akses ke semua URL, skrip, atau file yang dibatasi. Pertimbangkan untuk menggunakan kerangka kerja berbasis MVC seperti Struts

#### 4.3.4 Penanggulangan *Content Security Policy (CSP) Header Not Set*

1. Dengan mengaktifkan fitur CSP dalam CPanel untuk mencegah serangan XSS pada sebuah situs web.
2. Dengan mengonfigurasi server web Anda untuk mengembalikan Content-Security-Policy HTTP Header dan memberinya nilai untuk mengontrol sumber daya apa yang boleh dimuat oleh browser untuk halaman Anda.

Script:

```
Content-Security-Policy: <policy-directive>; <policy-directive>
```

#### 4.3.5 Penanggulangan *Directory Browsing*

1. Membuat *index.html* kosong dan letakkan di setiap direktori. Dengan ini dapat mencegah daftar direktori dan menampilkan halaman kosong di browser web.
2. Menonaktifkan daftar direktori untuk seluruh aplikasi webserver.
3. Dengan menonaktifkan daftar direktori dengan mengatur direktif Opsi di file *httpd.conf* Apache dengan menambahkan baris berikut:

```
<Directory/pordik.unjaya.ac.id/directory>Options -Indexes</Directory>
```

#### 4.3.6 Penanggulangan *HTTP Only Site*

1. Melakukan konfigurasi pada situs web pordik unjaya menggunakan protokol SSL (https), dengan mengaktifkan sertifikat SSL pada sistem cpanel.
2. Langkah-langkah install SSL di CPanel:

- a. Login ke cPanel.
- b. Masuk ke menu 'SSL/TLS' pada cPanel.
- c. Masuk ke 'Install and Manage SSL for your site (HTTPS)' klik 'Manage SSL sites.' di dalam menu 'SSL/TLS'.
- d. Lalu silahkan paste isi certificate SSL Anda pada kolom "Upload a New Certificate".
- e. Langkah terakhir adalah klik tombol 'Install Certificate'.

#### 4.3.7 Penanggulangan *Missing Anti-clickjacking Header*

1. Dengan mengaktifkan *header X-Frame-Options* pada konfigurasi web server.
2. Langkah untuk mengaktifkan *X-Frame-Options* pada web server.
  - a. Mengaktifkan di Ngix dengan menambahkan *script*:

```
add_header x-frame-options "SSMEORIGIN" always;
```

- b. Mengaktifkan di Apache dengan menambahkan *script*:

```
header always set x-frame-options "Sameorigin"
```

#### 4.3.8 Penanggulangan *Relative Path Confusion*

1. Mengkonfigurasi web server dengan tidak memberikan respons terhadap URL yang ambigu sehingga jalur relatif URL dapat disalahartikan oleh komponen sisi user atau web server.
2. Dengan menggunakan "*X-Frame-Options*" dalam respons HTTP untuk menonaktifkan "*Quirks Mode*" di browser yang menggunakan serangan pembungkahan.
3. Dengan menggunakan '*X-Content-Type-Options: nosniff*' dalam respons HTTP untuk mencegah '*sniffing*' jenis kontennya oleh browser.

#### 4.3.9 Penanggulangan *Vulnerable JS Library*

1. Sebagai bagian dari manajemen patch, terapkan manajemen versi untuk library *JavaScript*.
2. Dengan menghapus pustaka yang tidak lagi digunakan untuk mengurangi risiko serangan pada web server.

3. Melakukan pemeriksaan *patch* secara berkala, dan meelakukan update ke versi *JavaScript* terbaru.

#### 4.3.10 Penanggulangan *Cookie without HttpOnly Flag Set*

1. Dengan melakukan konfigurasi *HttpOnly* pada *cookie*. Dengan ini bisa mengurangi sebagian besar serangan XSS yang mencoba mengambil cookie dan kemungkinan membocorkan informasi sensitif atau memungkinkan penyerang untuk menyamar sebagai pengguna.
2. Menonaktifkan HTTP TRACE yang dikombinasikan dengan XSS dapat membaca cookie otentikasi, bahkan jika flag *HttpOnly* digunakan.
3. Menyetel *HttpOnly* pada server Apache

Menambahkan script pada *httpd.conf* dan melakukan restart pada server.

```
set_cookie_flag HttpOnly secure;
```

#### 4.3.11 Penanggulangan *Cookie without SameSite Attribute*

Membuat file *undertow-handlers.conf* dan menambahkan script pada aplikasi web.

```
Path(/webapp)->samesite-cookie(mode=None, enable client-checker=false)
```

#### 4.3.12 Penanggulangan *Cross-Domain JavaScript Source File Inclusion*

1. Memastikan *file* sumber *JavaScript* hanya dari sumber terpercaya.
2. Selalu host semua file aplikasi di web server atau layanan pihak ketiga yang terpercaya.
3. Mengaktifkan modul *mod\_headers* dengan *a2enmod header*.
  - a. Mulai ulang apache dengan *systemctl restart apache2*.
  - b. Buka file *httpd.conf* dalam web server apache
  - c. Tambahkan header script

```
set X-Content-Type-Options "nosniff"
```

- d. Mulai ulang apache dengan *systemctl restart apache2*.

#### 4.3.13 Penanggulangan *Server Leaks Version Information*

1. Dengan melakukan konfigurasi pada web server dan perangkat lunak transport HTTP lainnya seperti server proxy dan penyeimbang beban untuk menghapus bidang Server dari header respons HTTP atau menggantinya dengan nilai umum.
2. Melakukan konfigurasi pada server Apache yang di simpan pada folder `web_server/conf file httpd.conf`

```
ServerTokens Prod
ServerSignature Off
```

3. *Restat* web sever apache.

#### 4.3.14 Penanggulangan *X-Content-Type-Options Header Missing*

Melakukan konfigurasi pada server dengan menambahkan script pada header.

```
X-Content-Type-Options=nosniff
```

#### 4.4 REPORTING

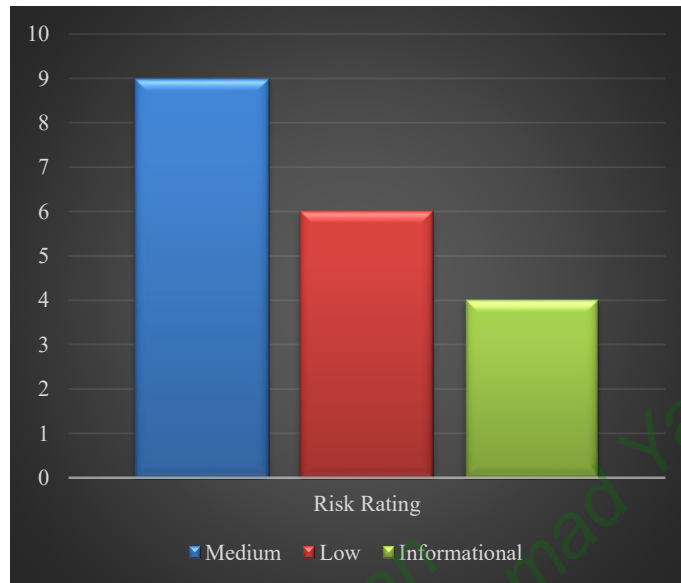
Dari hasil *vulnerability identification* yang telah dilakukan pada proses sebelumnya ditemukan beberapa celah kerentanan yang ada pada situs web prodik unjaya. Penulis mengklasifikasikan tingkat urgensi dari masing-masing kerentanan pada tabel 4.5.

**Tabel 4.5** *Reporting* Hasil Penilaian Kerentanan

No.	Jenis Serangan	Tingkat Risiko	Tingkat Urgensi
1.	<i>Absence of Anti-CSRF Tokens</i>	<i>Medium</i>	Segera
2.	<i>Anti-CSRF Tokens Check</i>	<i>Medium</i>	Segera
3.	<i>Backup File Disclosure</i>	<i>Medium</i>	Segera
4.	<i>Content Security Policy (CSP) Header Not Set</i>	<i>Medium</i>	Segera

5.	<i>Directory Browsing</i>	<i>Medium</i>	Segera
6.	<i>HTTP Only Site</i>	<i>Medium</i>	Segera
7.	<i>Missing Anti-clickjacking Header</i>	<i>Medium</i>	Segera
8.	<i>Relative Path Confusion</i>	<i>Medium</i>	Segera
9.	<i>Vulnerable JS Library</i>	<i>Medium</i>	Segera
10.	<i>Cookie No HttpOnly Flag</i>	<i>Low</i>	Bisa Direncanakan
11.	<i>Cookie without SameSite Attribute</i>	<i>Low</i>	Bisa Direncanakan
12.	<i>Cross-Domain JavaScript Source File Inclusion</i>	<i>Low</i>	Bisa Direncanakan
13.	<i>Server Leaks Version Information via "Server" HTTP Response Header Field</i>	<i>Low</i>	Bisa Direncanakan
14.	<i>X-Content-Type-Options Header Missing</i>	<i>Low</i>	Bisa Direncanakan

Berdasarkan hasil *vulnerability identification* menggunakan *helium security* menunjukkan level risiko dalam bentuk grafik. Hasil perbandingan nilai kerentanan dengan tingkat urgensi ditambihkan dalam diagram 4.1.



**Diagram 4.1** Perbandingan Nilai Kerentanan

Berdasarkan diagram 4.1, perbandingan nilai kerentanan paling banyak pada level *medium* sebanyak 9 kerentanan, nilai kerentanan pada level *low* sebanyak 6 kerentanan, dan nilai *informational* sebanyak 4 kerentanan. Dari masing-masing nilai kerentanan diklasifikasikan tingkat tingkat urgensi pada level *medium* harus Segera dilakukan pembenahan, tingkat urgensi pada level *low* masih bisa Direncanakan.