



**[slims, pentest.sttbandung]
Security Assessment Findings Report**

Dokumen Rahasia

Table of Contents

Table of Contents

Business Confidential	1
Table of Contents	2
Confidentiality Statement	3
Disclaimer	3
Contact Information	3
Assessment Overview	4
Finding Severity Ratings	5
Lingkup / Scope	6
Ringkasan Waktu Pelaksanaan	6
Lingkup dan Waktu	6
Ringkasan Kerentanan	7
Internal Penetration Test Findings	7
Technical Findings	9
Internal Penetration Test Findings	9

Pernyataan Rahasia

Dokumen ini adalah milik eksklusif PUSDATIN (Pusat Data dan Informasi). Dokumen ini berisi informasi kepemilikan dan rahasia. Duplikasi, redistribusi, atau penggunaan, seluruhnya atau sebagian, dalam bentuk apa pun, memerlukan izin dari PUSDATIN (Pusat Data dan Informasi).

PUSDATIN (Pusat Data dan Informasi) dapat membagikan dokumen ini dengan auditor berdasarkan perjanjian kerahasiaan untuk menunjukkan kepatuhan persyaratan uji penetrasi.

Disclaimer

Dokumen ini adalah untuk membantu organisasi dalam melakukan pengujian dan pemeriksaan keamanan informasi teknis, menganalisis temuan, dan mengembangkan strategi mitigasi. keterlibatan yang terbatas waktu tidak memungkinkan dilakukannya evaluasi penuh terhadap semua kontrol keamanan. Pentester memprioritaskan penilaian ini untuk mengidentifikasi kontrol keamanan terlemah yang dapat dieksploitasi oleh penyerang. Pentester merekomendasikan dilakukannya penilaian serupa setiap tahun oleh pentester internal atau pihak ketiga untuk memastikan keberhasilan pengendalian yang berkelanjutan.

Informasi Kontak

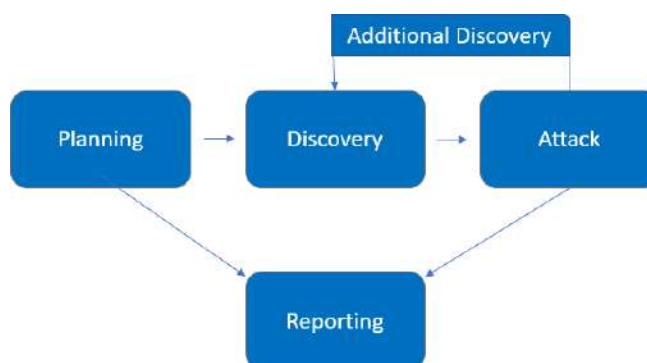
Name	Title	Contact Information
Demo Corp		
John Smith	Global Information Security Manager	Email: jsmith@democorp.com
Pentester		
Shaskia Putri Devi 21552011082	Mahasiswa	Email: shaskiapdv@gmail.com

Assessment Overview

Mulai **12 Juli 2024** hingga **31 Juli 2024**, Pentester mengevaluasi postur keamanan dan menggunakan praktik terbaik industri saat ini yang mencakup uji penetrasi aplikasi web. Semua pengujian yang dilakukan didasarkan pada Panduan Teknis **NIST SP 800-115** untuk Pengujian dan Penilaian Keamanan Informasi, Panduan Pengujian OWASP, dan kerangka pengujian OWASP WEB (Web Security Testing Guide / WSTG v4) yang disesuaikan.

Tahapan kegiatan pengujian penetrasi antara lain sebagai berikut:

- **Planning** – Sasaran pelanggan dikumpulkan dan aturan keterlibatan diperoleh.
- **Discovery** – Lakukan pemindaian dan enumerasi untuk mengidentifikasi potensi kerentanan, area lemah, dan eksploitasi.
- **Attack** – Konfirmasikan potensi kerentanan melalui eksploitasi dan lakukan penemuan tambahan pada akses baru.
- **Reporting** – Dokumentasikan semua kerentanan dan eksploitasi yang ditemukan, upaya yang gagal, serta kekuatan dan kelemahan perusahaan.



Menemukan Peringkat Keparahan/ Finding Severity Ratings

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

Severity	CVSS V3 Score Range	Definition
Critical	9.0-10.0	Eksplorasi bersifat langsung dan biasanya menghasilkan kompromi di tingkat sistem. Disarankan untuk segera membuat rencana tindakan dan melakukan penambalan.
High	7.0-8.9	Eksplorasi lebih sulit namun dapat menyebabkan peningkatan hak istimewa dan berpotensi hilangnya data atau downtime. Disarankan untuk membuat rencana tindakan dan penambalan sesegera mungkin.
Moderate	4.0-6.9	Kerentanan ada tetapi tidak dapat dieksploitasi atau memerlukan langkah tambahan seperti rekayasa sosial. Disarankan untuk membuat rencana tindakan dan perbaikan setelah masalah prioritas tinggi diselesaikan.
Low	0.1-3.9	Kerentanan tidak dapat dieksploitasi namun akan mengurangi permukaan serangan organisasi. Disarankan untuk membuat rencana tindakan dan patch selama masa pemeliharaan berikutnya.
Informational	N/A	Tidak ada kerentanan. Informasi tambahan diberikan mengenai item yang diperhatikan selama pengujian, kontrol yang kuat, dan dokumentasi tambahan.

Lingkup / Scope

Assessment	Details
Website	https://slims.devops-learning.my.id/ https://pentest.sttbandung.ac.id

Ringkasan Waktu Pelaksanaan

Pentester mengevaluasi postur keamanan aplikasi web xxxxx melalui pengujian penetrasi dari 12 Juli 2024 hingga 30 Juli 2024. Bagian berikut memberikan ikhtisar tingkat tinggi mengenai kerentanan yang ditemukan, upaya yang berhasil dan tidak berhasil, serta kekuatan dan kelemahan

Lingkup dan Waktu

Lingkup pengujian kali ini hanya terbatas pada aplikasi web.

Batasan waktu diberlakukan untuk pengujian penetrasi aplikasi web diizinkan selama lima (5) hari kerja

Ringkasan Kerentanan

Tabel berikut menggambarkan kerentanan yang ditemukan berdasarkan dampak :

Temuan Uji Penetrasi Internal/Internal Penetration Test Findings

0	4	3	1	2
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
Internal Penetration Test		
Finding IPT-001: Web information scanning	Low	<ol style="list-style-type: none"> 1. Hapus atau sembunyikan meta tag generator dan informasi lain yang tidak perlu dari halaman web. Jika menggunakan WordPress, gunakan plugin seperti "WP Hide & Security Enhancer". 2. Pasang WAF untuk mencegah pemindaian otomatis dan melindungi aplikasi web dari berbagai serangan.
Finding IPT-002: Directory and file search	High	<ol style="list-style-type: none"> 1. Pastikan file dan direktori yang mengandung data sensitif atau konfigurasi dilindungi dengan baik. Gunakan kontrol akses yang tepat seperti otentikasi dan otorisasi untuk melindungi akses ke file-file ini. 2. Pastikan file dan direktori yang mengandung data sensitif atau konfigurasi dilindungi dengan baik. Gunakan kontrol akses yang tepat seperti otentikasi dan otorisasi untuk melindungi

		<p>akses ke file-file ini.</p> <p>3. Terapkan pengaturan keamanan web yang ketat seperti pembatasan akses, firewall aplikasi web, dan pemantauan keamanan untuk mencegah akses tidak sah ke direktori dan file."</p>
Finding IPT-003: HTTPS on link	Informational	<p>Pertahankan implementasi saat ini</p> <ol style="list-style-type: none"> 1. Terus pastikan bahwa semua halaman dan sumber daya di situs web disajikan melalui HTTPS. 2. Secara berkala memperbarui sertifikat SSL/TLS untuk mempertahankan standar enkripsi. 3. Implementasikan HSTS (HTTP Strict Transport Security) untuk memastikan bahwa browser hanya terhubung ke situs menggunakan HTTPS.
Finding IPT-004: HTTP OPTIONS enabled	Informational	<ol style="list-style-type: none"> 1. Nonaktifkan Metode OPTIONS: Konfigurasi server web untuk menonaktifkan metode OPTIONS jika tidak diperlukan. 2. Batasi Metode yang Diizinkan: Pastikan hanya metode HTTP yang diperlukan yang diizinkan, seperti GET dan POST, untuk meminimalkan potensi risiko."
Finding IPT-005: Server software and technology found	Moderate	<ol style="list-style-type: none"> 1. Hapus atau sembunyikan meta tag generator dan informasi lain yang tidak perlu dari halaman web. Jika

		meggunakan WordPress, gunakan plugin seperti "WP Hide & Security Enhancer". 2. Pasang WAF untuk mencegah pemindaian otomatis dan melindungi aplikasi web dari berbagai serangan."
Finding IPT-006: Brute Force	High	<ul style="list-style-type: none"> • Tambahkan CAPTCHA pada halaman login untuk mencegah bot melakukan percobaan login berulang kali. • Batasi jumlah percobaan login yang dapat dilakukan dalam periode waktu tertentu. • Kunci akun pengguna setelah beberapa percobaan login yang gagal. • Pastikan kata sandi disimpan menggunakan algoritma hash yang kuat seperti bcrypt.
Finding IPT-007: Acces JavaScript Files	High	<ul style="list-style-type: none"> • Pastikan file JavaScript tidak mengandung informasi sensitif seperti kunci API, kredensial, atau logika detail yang dapat membantu penyerang. • Minimalkan paparan file internal dan konfigurasi dengan membatasi akses hanya ke sumber daya yang diperlukan. • Obfuscate file JavaScript untuk membuatnya lebih sulit dipahami oleh penyerang.
Finding IPT-008: Testing for Session Fixation	High	<ul style="list-style-type: none"> • Setelah pengguna berhasil login, aplikasi harus mengeluarkan ID sesi baru. • Menggunakan Cookie dengan Atribut HttpOnly dan Secure untuk

		<p>memastikan bahwa ID sesi hanya dapat diakses melalui HTTP dan HTTPS.</p> <ul style="list-style-type: none">• Mengatur timeout untuk sesi sehingga sesi yang tidak aktif akan dihapus secara otomatis.
<p>Finding IPT-009: Slowloris DoS Attack (https://pentest.sttbandung.ac.id/)</p>	Moderate	<ul style="list-style-type: none">• Sesuaikan batas waktu koneksi idle pada server web untuk memutuskan koneksi yang tidak aktif dalam waktu singkat.• Terapkan firewall aplikasi web untuk memantau dan membatasi koneksi yang mencurigakan.• Batasi jumlah koneksi yang dapat dilakukan oleh satu alamat IP.• Gunakan load balancer untuk mendistribusikan lalu lintas dan mencegah satu server dari kelebihan beban.

Temuan Teknis/Technical Findings

Temuan Uji Penetrasi Internal/Internal Penetration Test Findings

Finding IPT-001: Web information scanning (<https://pentest.sttbandung.ac.id>) (Low)

Description:	WhatWeb berfungsi untuk mengumpulkan informasi terkait teknologi yang digunakan oleh situs web, seperti jenis server, bahasa pemrograman, CMS (Content Management System), framework, library JavaScript, dan banyak lagi.
Risk:	Informasi yang terungkap melalui pemindaian WhatWeb dapat memberikan wawasan kepada penyerang tentang teknologi dan konfigurasi yang digunakan oleh situs tersebut. Dengan mengetahui versi CMS atau library yang digunakan, penyerang dapat mencoba mengeksploitasi kerentanan yang diketahui. Informasi seperti alamat email dapat digunakan untuk serangan phishing atau social engineering.
System:	
Tools Used:	Whatweb
References:	

Evidence

```

$ whatweb https://slims.devops-learning.my.id/
https://slims.devops-learning.my.id/ [200 OK] Bootstrap, Cookies[SenayanMember], Country[EUROPEAN UNION][id], Email[ido.alit@gmail.com], Frame, HTML5, HTTPServer[cloudflare], HttpOnly[SenayanMember], IP[188.114.96.0], JQuery, MetaGenerator[SLIMS 9 (Bulian)], Open-Graph-Protocol[book], Script, Title[whoami | jangan ganti], UncommonHeaders[x-content-type-options,content-security-policy,cf-cache-status,report-to,nel,cf-ray,alt-svc], X-Frame-Options[SAMEORIGIN, SAMEORIGIN, SAMEORIGIN], X-UA-Compatible[IE=edge], X-XSS-Protection[1; mode=block, 1; mode=block, 1; mode=block]
  
```

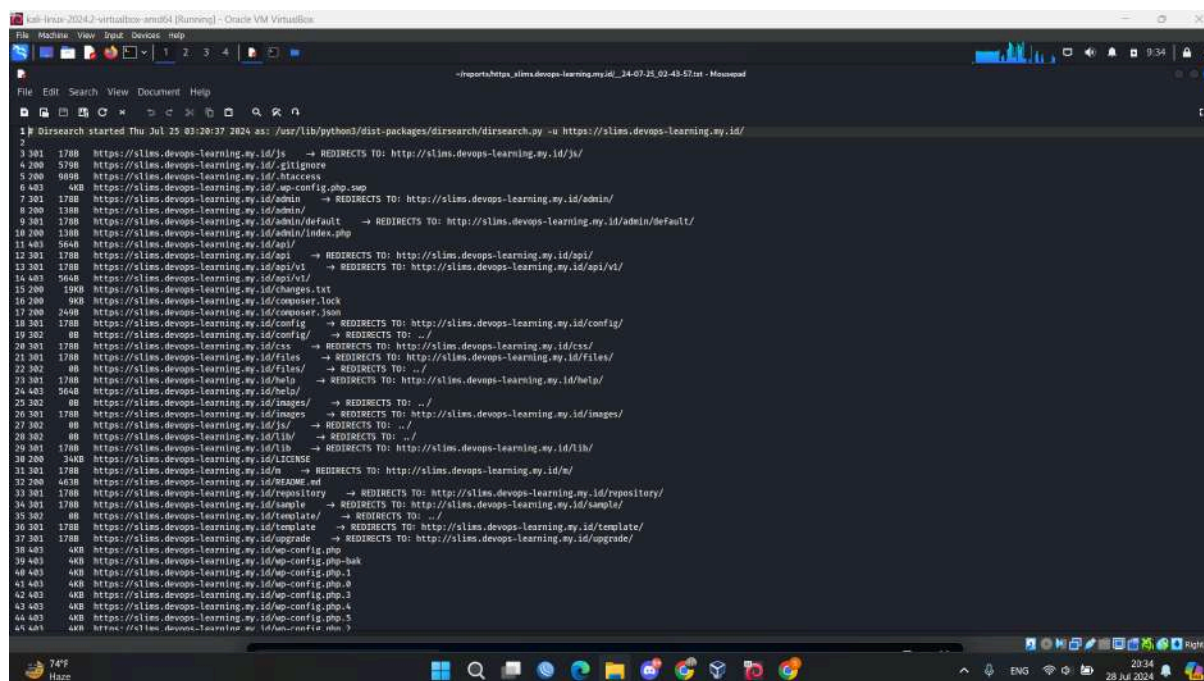
Remediation

1. Hapus atau sembunyikan meta tag generator dan informasi lain yang tidak perlu dari halaman web. Jika menggunakan WordPress, gunakan plugin seperti "WP Hide & Security Enhancer".
2. Pasang WAF untuk mencegah pemindaian otomatis dan melindungi aplikasi web dari berbagai serangan.

Finding IPT-002: Directory and file search (High)

Description:	Dirsearch adalah alat untuk mencari direktori dan file dalam sebuah website menggunakan daftar kata kunci yang telah ada.
Risk:	<ol style="list-style-type: none"> 1. Jika Dirsearch menemukan direktori atau file yang mengandung informasi sensitif seperti file konfigurasi, kredensial, atau data pribadi, hal ini dapat mengakibatkan kebocoran data yang serius. Seperti file config.php yang berisi kredensial database. 2. Mengetahui lokasi direktori atau file tertentu dapat memberikan informasi kepada penyerang tentang struktur aplikasi, yang dapat digunakan untuk merencanakan serangan lebih lanjut. 3. Data pribadi yang tidak dilindungi dengan baik dapat diakses oleh pihak yang tidak berwenang, mengakibatkan pelanggaran privasi. Contoh: File yang berisi data pengguna atau catatan transaksi.
System:	Directory
Tools Used:	Dirsearch
References:	

Evidence



```

1 Dirsearch started Thu Jul 25 03:20:37 2024 as: /usr/lib/python2/dist-packages/dirsearch/dirsearch.py -u https://slims.devops-learning.my.id/
2
3 301 1700 https://slims.devops-learning.my.id/js → REDIRECTS TO: http://slims.devops-learning.my.id/js/
4 200 5200 https://slims.devops-learning.my.id/gilignore
5 200 9000 https://slims.devops-learning.my.id/.htaccess
6 403 400 https://slims.devops-learning.my.id/wp-config.php.swp
7 301 1700 https://slims.devops-learning.my.id/admin → REDIRECTS TO: http://slims.devops-learning.my.id/admin/
8 200 1300 https://slims.devops-learning.my.id/admin/
9 301 1700 https://slims.devops-learning.my.id/admin/default → REDIRECTS TO: http://slims.devops-learning.my.id/admin/default/
10 200 1300 https://slims.devops-learning.my.id/admin/index.php
11 403 5600 https://slims.devops-learning.my.id/api/
12 301 1700 https://slims.devops-learning.my.id/api → REDIRECTS TO: http://slims.devops-learning.my.id/api/
13 301 1700 https://slims.devops-learning.my.id/api/v1 → REDIRECTS TO: http://slims.devops-learning.my.id/api/v1/
14 403 5600 https://slims.devops-learning.my.id/api/v1/
15 200 1900 https://slims.devops-learning.my.id/changelog.txt
16 200 900 https://slims.devops-learning.my.id/composer.lock
17 200 2400 https://slims.devops-learning.my.id/composer.json
18 301 1700 https://slims.devops-learning.my.id/config → REDIRECTS TO: http://slims.devops-learning.my.id/config/
19 302 00 https://slims.devops-learning.my.id/config/ → REDIRECTS TO: ../
20 301 1700 https://slims.devops-learning.my.id/css → REDIRECTS TO: http://slims.devops-learning.my.id/css/
21 301 1700 https://slims.devops-learning.my.id/files → REDIRECTS TO: http://slims.devops-learning.my.id/files/
22 302 00 https://slims.devops-learning.my.id/files/ → REDIRECTS TO: ../
23 301 1700 https://slims.devops-learning.my.id/help → REDIRECTS TO: http://slims.devops-learning.my.id/help/
24 403 5600 https://slims.devops-learning.my.id/help/
25 302 00 https://slims.devops-learning.my.id/images/ → REDIRECTS TO: ../
26 301 1700 https://slims.devops-learning.my.id/images → REDIRECTS TO: http://slims.devops-learning.my.id/images/
27 302 00 https://slims.devops-learning.my.id/js/ → REDIRECTS TO: ../
28 302 00 https://slims.devops-learning.my.id/lib → REDIRECTS TO: ../
29 301 1700 https://slims.devops-learning.my.id/lib → REDIRECTS TO: http://slims.devops-learning.my.id/lib/
30 200 3400 https://slims.devops-learning.my.id/LICENSE
31 301 1700 https://slims.devops-learning.my.id/n → REDIRECTS TO: http://slims.devops-learning.my.id/n/
32 200 4630 https://slims.devops-learning.my.id/README.md
33 301 1700 https://slims.devops-learning.my.id/repository → REDIRECTS TO: http://slims.devops-learning.my.id/repository/
34 301 1700 https://slims.devops-learning.my.id/sample → REDIRECTS TO: http://slims.devops-learning.my.id/sample/
35 302 00 https://slims.devops-learning.my.id/template/ → REDIRECTS TO: ../
36 301 1700 https://slims.devops-learning.my.id/template → REDIRECTS TO: http://slims.devops-learning.my.id/template/
37 301 1700 https://slims.devops-learning.my.id/upgrade → REDIRECTS TO: http://slims.devops-learning.my.id/upgrade/
38 403 400 https://slims.devops-learning.my.id/wp-config.php
39 403 400 https://slims.devops-learning.my.id/wp-config.php-bak
40 403 400 https://slims.devops-learning.my.id/wp-config.php.1
41 403 400 https://slims.devops-learning.my.id/wp-config.php.2
42 403 400 https://slims.devops-learning.my.id/wp-config.php.3
43 403 400 https://slims.devops-learning.my.id/wp-config.php.4
44 403 400 https://slims.devops-learning.my.id/wp-config.php.5
45 403 400 https://slims.devops-learning.my.id/wp-config.php.6
  
```

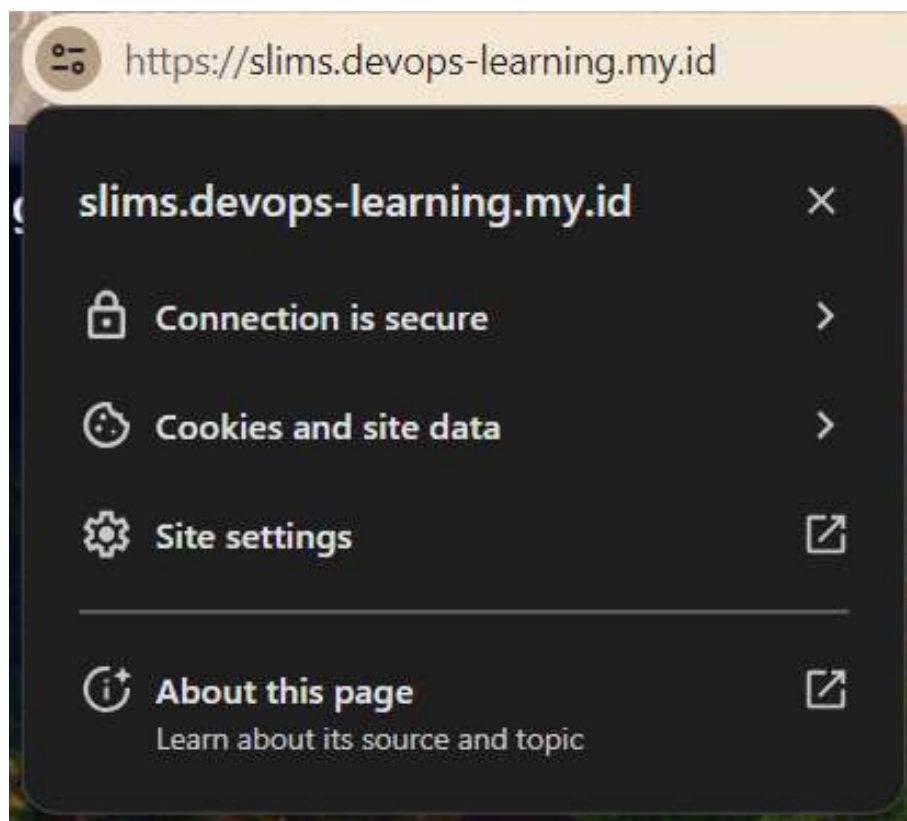
Remediation

- Pastikan file dan direktori yang mengandung data sensitif atau konfigurasi dilindungi dengan baik. Gunakan kontrol akses yang tepat seperti otentikasi dan otorisasi untuk melindungi akses ke file-file ini.
- Pastikan file dan direktori yang mengandung data sensitif atau konfigurasi dilindungi dengan baik. Gunakan kontrol akses yang tepat seperti otentikasi dan otorisasi untuk melindungi akses ke file-file ini.
- Terapkan pengaturan keamanan web yang ketat seperti pembatasan akses, firewall aplikasi web, dan pemantauan keamanan untuk mencegah akses tidak sah ke direktori dan file.

Finding IPT-003: HTTPS on link (informational)

Description:	Situs web aman dengan menggunakan HTTPS, yang memastikan komunikasi antara browser pengguna dan server terenkripsi dan aman. Ini membantu melindungi data sensitif, seperti kredensial login dan informasi pribadi, dari penyadapan oleh pihak yang tidak berwenang.
Risk:	<p>Dampak Potensial: Positif</p> <ol style="list-style-type: none">1. Integritas Data: HTTPS memastikan bahwa data yang dikirim antara klien dan server tidak dirusak selama transmisi.2. Privasi: Komunikasi terenkripsi mencegah pihak ketiga untuk melihat isi data yang dipertukarkan.3. Kepercayaan: Browser menunjukkan ikon gembok untuk situs HTTPS, menunjukkan kepada pengguna bahwa situs tersebut aman, yang dapat meningkatkan kepercayaan dan keyakinan pengguna.
System:	Link
Tools Used:	
References:	

Evidence



Remediation

Pertahankan implementasi saat ini

- Terus pastikan bahwa semua halaman dan sumber daya di situs web disajikan melalui HTTPS.
- Secara berkala memperbarui sertifikat SSL/TLS untuk mempertahankan standar enkripsi.
- Implementasikan HSTS (HTTP Strict Transport Security) untuk memastikan bahwa browser hanya terhubung ke situs menggunakan HTTPS.

Finding IPT-004: HTTP OPTIONS enabled (Informational)

Description:	Melakukan permintaan HTTP OPTIONS. Server merespons dengan kode status 200 dan header Allow: GET, HEAD.
Risk:	<ol style="list-style-type: none"> 1. Pengungkapan Informasi: Metode OPTIONS dapat mengungkapkan informasi tentang metode HTTP yang tersedia di server target. Ini dapat memberi petunjuk kepada penyerang tentang metode yang dapat digunakan untuk mengakses atau mengeksploitasi server. 2. Risiko Keamanan: Jika metode debug HTTP diungkapkan, hal ini dapat menyebabkan informasi sensitif seperti informasi autentikasi atau kunci rahasia menjadi terekspos.
System:	HTTP OPTIONS
Tools Used:	nmap
References:	

Evidence

```

(kali@kali)-[~]
└─$ nmap --script http-methods --script-args http-method.test-all ='/104.21.15.169' 104.21.15.169
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-28 09:51 EDT
Unable to split netmask from target expression: "=/104.21.15.169"
Nmap scan report for 104.21.15.169
Host is up (0.031s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
| http-methods:
|_ Supported Methods: HEAD POST
443/tcp   open  https
| http-methods:
|_ Supported Methods: GET POST OPTIONS
8080/tcp  open  http-proxy
8443/tcp  open  https-alt
| http-methods:
|_ Supported Methods: GET HEAD OPTIONS
Nmap done: 1 IP address (1 host up) scanned in 24.91 seconds
  
```

Remediation

- Nonaktifkan Metode OPTIONS: Konfigurasi server web untuk menonaktifkan metode OPTIONS jika tidak diperlukan.
- Batasi Metode yang Diizinkan: Pastikan hanya metode HTTP yang diperlukan yang diizinkan, seperti GET dan POST, untuk meminimalkan potensi risiko.

Finding IPT-005: Server software and technology found (slims.devops-learning.my.id)
(Medium)

Description:	Perangkat lunak dan teknologi server ditemukan
Risk:	Penyerang dapat menggunakan informasi ini untuk melakukan serangan spesifik terhadap jenis dan versi perangkat lunak yang teridentifikasi.
System:	All
Tools Used:	Whatweb
References:	

Evidence

SOFTWARE / VERSION	CATEGORY
Google Maps	Maps
Cloudflare	CDN
Bootstrap 4.2.1	UI frameworks
toastr 2.1.4	JavaScript frameworks
HTTP/3	Miscellaneous
jQuery 3.2.1	JavaScript libraries
Open Graph	Miscellaneous
Popper	Miscellaneous
Vue.js 2.6.11	JavaScript frameworks

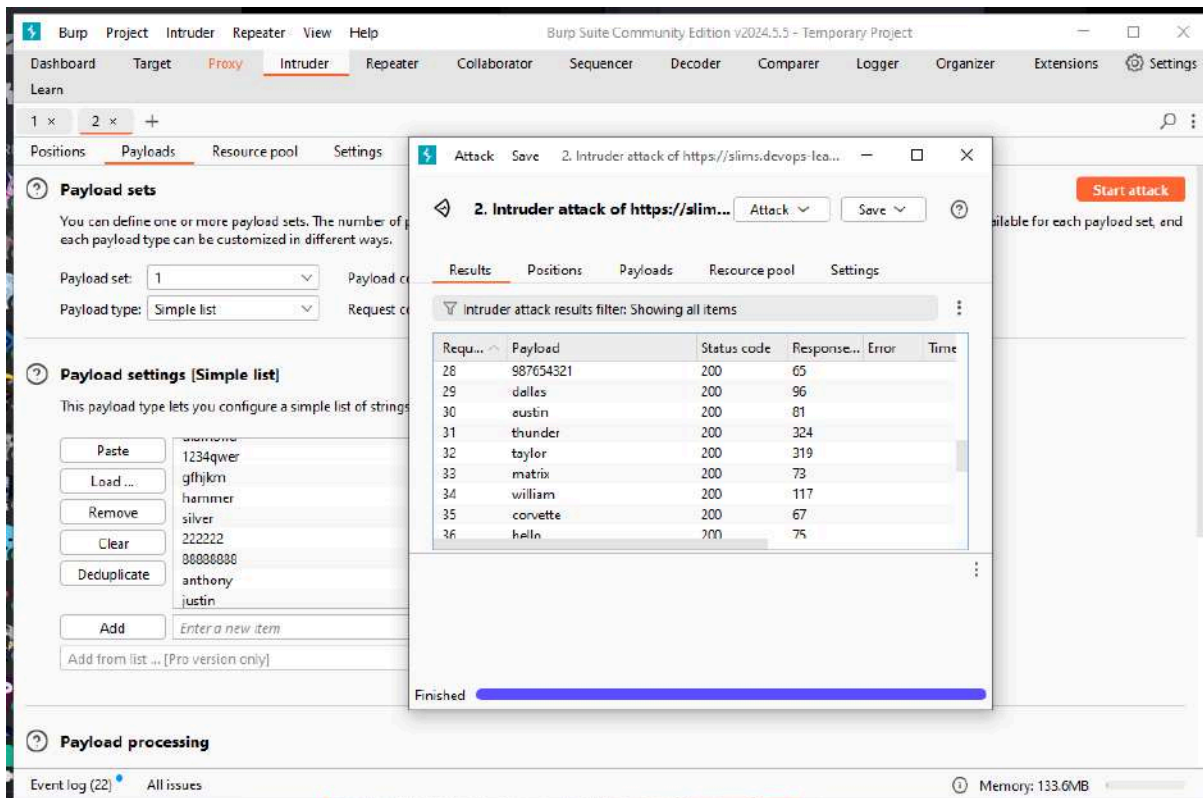
Remediation

1. Hapus atau sembunyikan meta tag generator dan informasi lain yang tidak perlu dari halaman web. Jika menggunakan WordPress, gunakan plugin seperti "WP Hide & Security Enhancer"
2. Pasang WAF untuk mencegah pemindaian otomatis dan melindungi aplikasi web dari berbagai serangan.

Finding IPT-006: Brute Force (High)

Description:	Brute force attack adalah metode di mana penyerang mencoba berbagai kombinasi nama pengguna dan kata sandi untuk mendapatkan akses tidak sah ke suatu sistem. Dalam kasus ini, alat Burp Suite telah digunakan untuk melakukan serangan brute force terhadap situs web https://slims.devops-learning.my.id
Risk:	Jika berhasil, penyerang dapat memperoleh akses tidak sah ke akun pengguna, termasuk data pribadi dan sensitif. Selain itu, penyerang dapat melakukan perubahan tidak sah pada sistem dan data.
System:	All
Tools Used:	Burp Suite
References:	

Evidence



The screenshot shows the Burp Suite Intruder tool interface. The 'Attack' window is open, displaying the results of an intruder attack on the target URL <https://slims.devops-learning.my.id>. The 'Results' tab is selected, showing a table of attack results. The table has columns for Request number, Payload, Status code, Response time, Error, and Time. The attack is marked as 'Finished' with a blue progress bar.

Requ...	Payload	Status code	Response...	Error	Time
28	987654321	200	65		
29	dalles	200	96		
30	eustin	200	81		
31	thunder	200	324		
32	taylor	200	319		
33	matrix	200	73		
34	william	200	117		
35	corvette	200	67		
36	heln	200	75		

Remediation

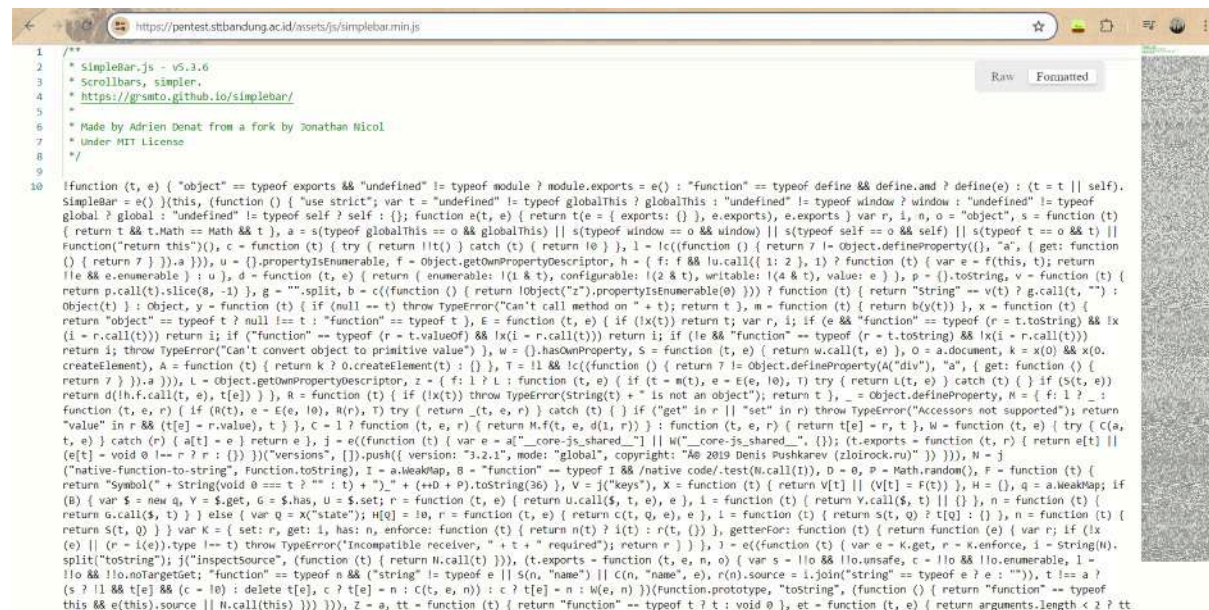
- Tambahkan CAPTCHA pada halaman login untuk mencegah bot melakukan percobaan login berulang kali.
- Batasi jumlah percobaan login yang dapat dilakukan dalam periode waktu tertentu.



- Kunci akun pengguna setelah beberapa percobaan login yang gagal.
- Pastikan kata sandi disimpan menggunakan algoritma hash yang kuat seperti bcrypt

Description:	File JavaScript (simplebar.min.js) yang dapat diakses publik ditemukan di server web. File ini mengandung kode JavaScript yang telah dimodifikasi yang mencakup konfigurasi dan potensi informasi sensitif. Paparan file seperti ini secara publik dapat memberikan wawasan kepada penyerang tentang struktur dan logika aplikasi web, yang mungkin dimanfaatkan dalam serangan.
Risk:	Penyerang dapat mengidentifikasi potensi kerentanan dalam kode JavaScript dan menggunakan informasi ini untuk menyusun serangan yang lebih tertarget.
System:	All
Tools Used:	DirBuster
References:	

Evidence

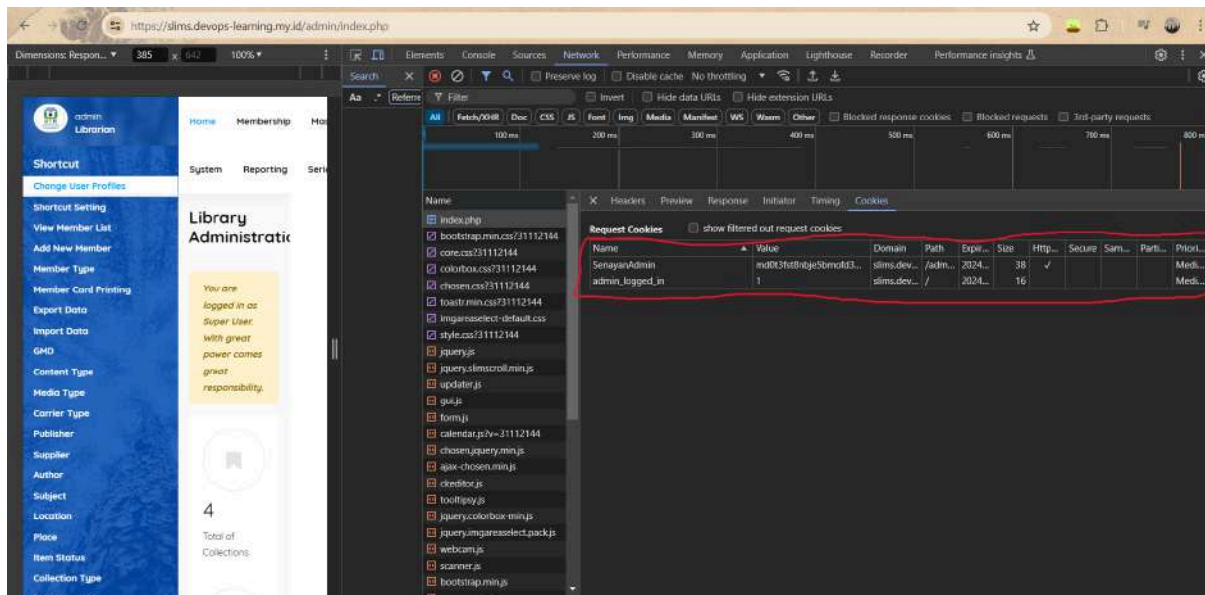


Remediation

- Pastikan file JavaScript tidak mengandung informasi sensitif seperti kunci API, kredensial, atau logika detail yang dapat membantu penyerang.
- Minimalkan paparan file internal dan konfigurasi dengan membatasi akses hanya ke sumber daya yang diperlukan.
- Obfuscate file JavaScript untuk membuatnya lebih sulit dipahami oleh penyerang.

Description:	Session Fixation adalah kerentanan di mana penyerang dapat menentukan atau mengatur ID sesi pengguna yang sah sebelum pengguna tersebut melakukan login ke dalam aplikasi. Dengan demikian, penyerang dapat mencuri sesi yang sah dari pengguna dan mendapatkan akses tanpa harus melakukan otentikasi.
Risk:	Jika serangan berhasil, penyerang dapat mengambil alih sesi pengguna yang sah, mengakses data sensitif dan informasi pribadi dan melakukan tindakan sebagai pengguna yang sah, seperti mengubah data atau melakukan transaksi yang tidak sah.
System:	All
Tools Used:	
References:	

Evidence



Remediation

- Setelah pengguna berhasil login, aplikasi harus mengeluarkan ID sesi baru.
- Menggunakan Cookie dengan Atribut HttpOnly dan Secure untuk memastikan bahwa ID sesi hanya dapat diakses melalui HTTP dan HTTPS.
- Mengatur timeout untuk sesi sehingga sesi yang tidak aktif akan dihapus secara otomatis.

Finding IPT-009: Scanning Vulnerability: Slowloris DoS Attack (Medium)

Description:	Slowloris adalah serangan Denial of Service (DoS) yang mencoba menjaga banyak koneksi ke server web target tetap terbuka dan menahan mereka selama mungkin. Ini dicapai dengan membuka koneksi ke server target dan mengirimkan permintaan parsial. Dengan cara ini, Slowloris membuat server target sibuk, menghabiskan sumber daya server dan menyebabkan Denial of Service.
Risk:	Jika berhasil, serangan Slowloris dapat membuat server web target tidak dapat diakses oleh pengguna yang sah. Ini dapat menyebabkan gangguan besar pada layanan dan kerugian finansial bagi organisasi yang bergantung pada server web tersebut.
System:	All
Tools Used:	
References:	

Evidence

```

(kali@kali)~$ nmap -script vuln 104.21.15.169
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-29 03:01 EDT
Nmap scan report for 104.21.15.169
Host is up (0.039s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
443/tcp   open  https
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|   State: LIKELY VULNERABLE
|   IDS: CVE:CVE-2007-6750
|   Slowloris tries to keep many connections to the target web server open and hold
|   them open as long as possible. It accomplishes this by opening connections to
|   the target web server and sending a partial request. By doing so, it starves
|   the http server's resources causing Denial Of Service.
|
|   Disclosure date: 2009-09-17
|   References:
|     http://ha.ckers.org/slowloris/
|     https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
8080/tcp  open  http-proxy
8443/tcp  open  https-alt
Nmap done: 1 IP address (1 host up) scanned in 562.25 seconds
  
```

Remediation

- Sesuaikan batas waktu koneksi idle pada server web untuk memutuskan koneksi

yang tidak aktif dalam waktu singkat.

- Terapkan firewall aplikasi web untuk memantau dan membatasi koneksi yang mencurigakan.
- Batasi jumlah koneksi yang dapat dilakukan oleh satu alamat IP.
- Gunakan load balancer untuk mendistribusikan lalu lintas dan mencegah satu server dari kelebihan beban.



Last Page