



Graha Mandiri 2nd floor, Jalan Imam Bonjol No. 61, Jakarta 10310.
T: +6221-39834116 F: +6221-39834114 E: sales@xynexis.com

Project Nemean

Retest Report - M2U Web Interactive Statement

Date : 18 November 2024

Ver: 00

PROPRIETARY & CONFIDENTIAL

Information contained in this document is proprietary and highly confidential to [Maybank Indonesia](#). No part of this document shall be duplicated, used, copied, reproduced, distributed or disclosed to third party in whole or in part, in any form and by any means, outside of [Maybank Indonesia](#), without the express written authorisation from [Maybank Indonesia](#). Do not remove from [Maybank Indonesia](#) premises.

Confidentiality Statement

Information contained in this document is proprietary and highly confidential to Maybank Indonesia. No part of this document shall be duplicated, used, copied, reproduced, distributed or disclosed to third party in whole or in part, in any form and by any means, outside of Maybank Indonesia, without the express written authorisation from Maybank Indonesia. Do not remove from Maybank Indonesia premises.

Certain parts of this report is proprietary to PT Xynexis International.

List of Revision:

- 18 November 2024 — First release.

Note

As part of our internal security policy, we allocate a code name for each and every client, to ensure that their identity can be better protected during public discussion of project activities. To this effect, we have allocated the code **Nemean** to refer to Maybank Indonesia. In all our discussions below, we use this code in describing the company.



Graha Mandiri 2nd floor, Jalan Imam Bonjol No. 61, Jakarta 10310.
T: +6221-39834116 F: +6221-39834114 E: sales@xynexis.com

Executive Summary

Xynexis perform IT security assessment on Nemean System and application. The assessment was conducted in a form of blackbox and greybox penetration testing from external network against Nemean System and application.

The assessment revealed 3 type of MEDIUM severity vulnerabilities, and 4 type of LOW severity vulnerabilities. The test result demonstrated how remote exploitation of these vulnerabilities can be used successfully by attacker to compromise the confidentiality, integrity, and availability of information contained within the Nemean application.

Considering the strategic value of Nemean application, and the potential threat of the discovered vulnerabilities, Nemean is therefore advised to expedite the implementation of each recommended technical solution outlined in this report.



Graha Mandiri 2nd floor, Jalan Imam Bonjol No. 61, Jakarta 10310.
T: +6221-39834116 F: +6221-39834114 E: sales@xynexis.com

Assessment Scope

The scope of work for this project is limited to the following:

M2U Web Interactive Statement

[http://10.235.83.40:8081/vs/csintrctv?
uid=7CA13DE3BF3A084876AC4AE9E1E6DE11&ch=7F11ED3FDBDACC44&custType=npr#/](http://10.235.83.40:8081/vs/csintrctv?uid=7CA13DE3BF3A084876AC4AE9E1E6DE11&ch=7F11ED3FDBDACC44&custType=npr#/)



Graha Mandiri 2nd floor, Jalan Imam Bonjol No. 61, Jakarta 10310.
T: +6221-39834116 F: +6221-39834114 E: sales@xynexis.com

Date & Location

The pentest was conducted on November 11th 2024. Most, if not all, project activities were conducted at:

- **External Penetration Test:** PT Xynexis International, Graha Mandiri Lt 2, Jl Imam Bonjol No 61, Jakarta 10310 (access via VPN)

The retest was conducted on November 18th 2024. Most, if not all, project activities were conducted at:

- **External Penetration Test:** PT Xynexis International, Graha Mandiri Lt 2, Jl Imam Bonjol No 61, Jakarta 10310 (access via VPN)

severity Assessment Method

Description

The assessment method used to calculate the severity of all vulnerabilities in this report is CVSS (Common Vulnerability Scoring System). CVSS is a vulnerability scoring system designed to provide an open and standardized method for rating IT vulnerabilities. CVSS helps organizations prioritize and coordinate a joint response to security vulnerabilities by communicating the base, temporal and environmental properties of a vulnerability.

CVSS Score | severity

CVSS Score	severity
0 - 2,0	Very Low
2,1 - 4,0	Low
4,1 - 6,0	Medium
6,1 - 8,0	High
8,1 - 10	Very High

Color Code



References

CVSS Calculator <http://nvd.nist.gov/cvss.cfm?calculator&adv&version=2>

Finding Summary

No	Vulnerabilities	CVSS Base Score	CVSS Temporal Score	CVSS Score	Severity	Status
1	Cookie Implementation	5	3.7	3.7	Low	Closed
2	Error Message Information Exposure	5	3.7	3.7	Low	Closed
3	Default Apache Tomcat Page Information Exposure	5	3.7	3.7	Low	Closed
4	Security Header Configuration	5	3.7	3.7	Low	Partial
5	Business Logic Flaw Data Breach	5.5	4.3	4.3	Medium	Closed
6	UID & CH Enumeration Vulnerability	5.5	4.3	4.3	Medium	Open
7	Improper Captcha Validation Password Enumeration	5.5	4.3	4.3	Medium	New

Note :

* **CVSS Base Score** : represents the intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environments

** **CVSS Temporal Score** : represents the characteristics of a vulnerability that change over time but not among user environments

Cookie Implementation

Description:

Our assessment on the target shows the application current application cookie implementation is missing SECURE flag.

Exploitation Effort:

Low – Attacker can check for known vulnerability

Affected target:

<http://10.235.83.40:8081/vs/csintrctv?uid=7CA13DE3BF3A084876AC4AE9E1E6DE11&ch=7F11ED3FDBDACC44&custType=npr#/>

Severity:

Low – Attacker can use the information for future attack

CVSS Score:

CVSS Base Score: 5. CVSS Temporal Score: 3.7. CVSS Exploitability Score: 10. CVSS Impact Score: 2.9.

Recommendation:

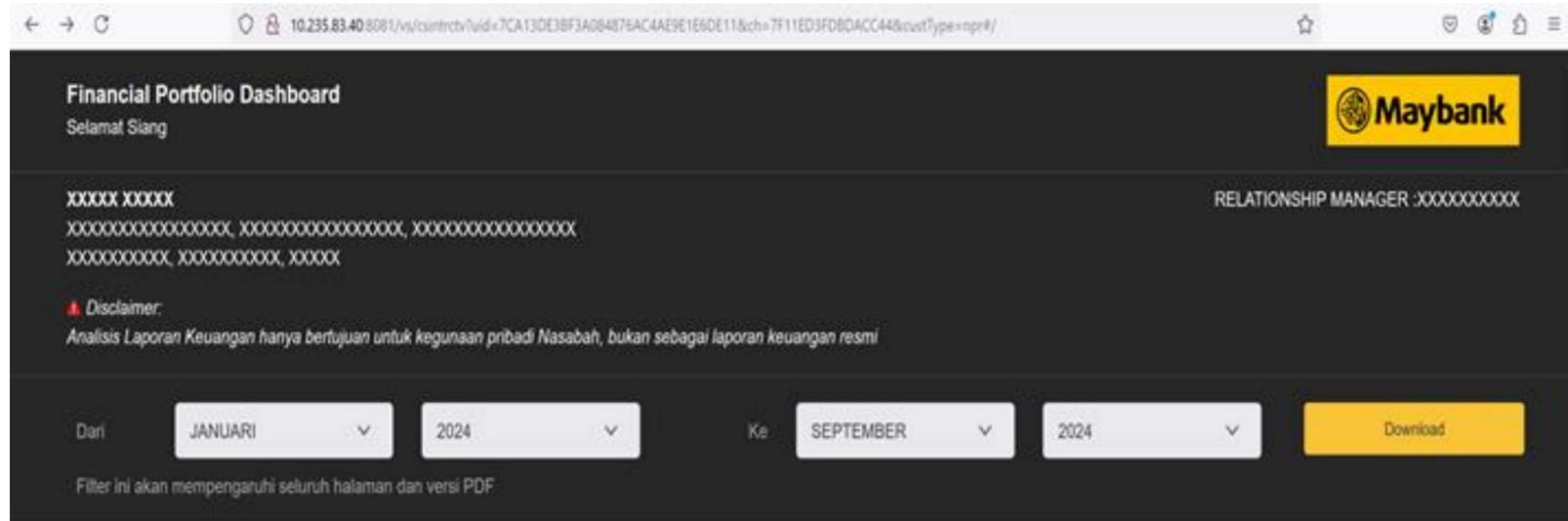
We recommend to implement SECURE flag on cookie.

<https://owasp.org/www-community/controls/SecureCookieAttribute>

Retest Result:

Retest result shows the vulnerability is fixed.

Cookie Implementation

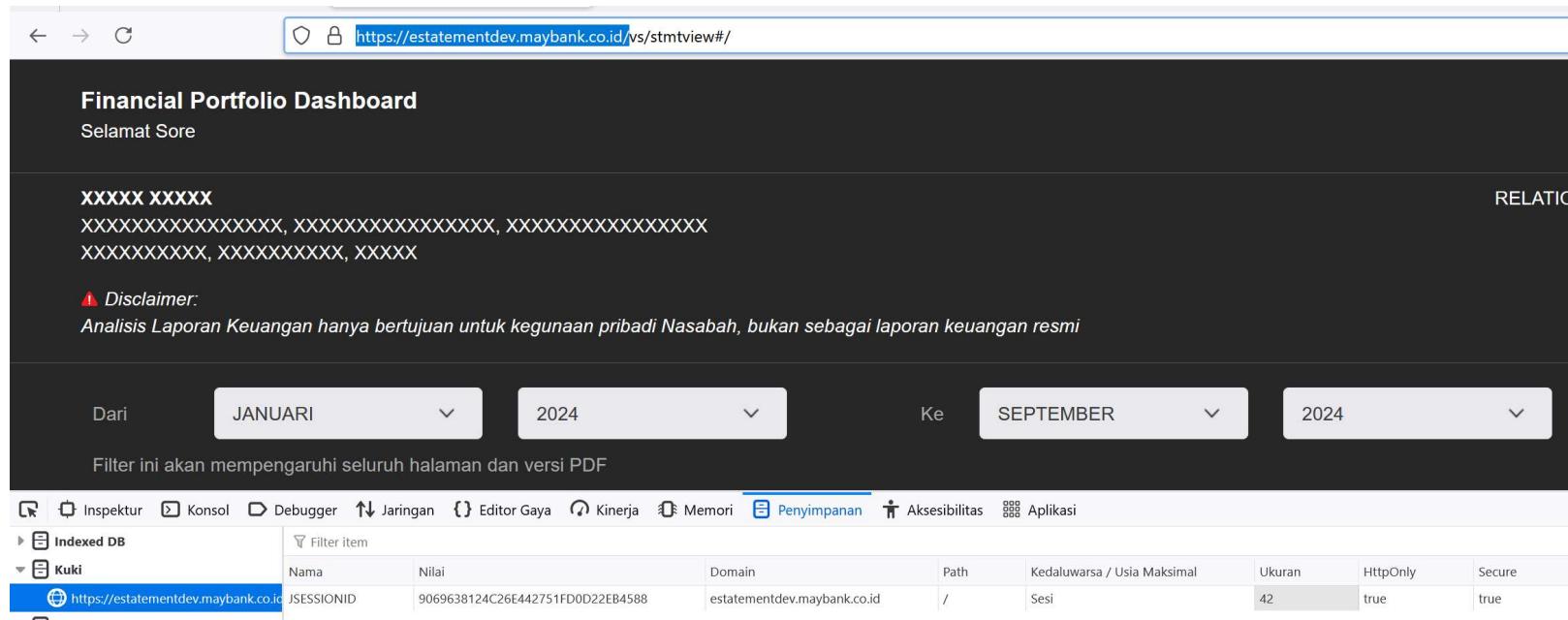


The screenshot shows a financial portfolio dashboard for Maybank. At the top, it displays a message: "Selamat Siang" and "xxxxx XXXXX". Below this, there is a disclaimer: "Analisis Laporan Keuangan hanya bertujuan untuk kegunaan pribadi Nasabah, bukan sebagai laporan keuangan resmi". The dashboard includes date filters for "Dari JANUARI 2024" and "Ke SEPTEMBER 2024", and a "Download" button. A note below the filters states: "Filter ini akan mempengaruhi seluruh halaman dan versi PDF".



The screenshot shows the Network tab of a browser developer tools window. It lists two cookies: "IndexedDB" and "Kuki". The "Kuki" cookie is selected, showing its details: Name: SESSIONID, Value: 04C05318146881538787D992CC105009, Domain: 10.235.83.40, Path: /vs, and Sesi. An arrow points to the "SESSIONID" value in the "Value" column.

Cookie Implementation



The screenshot shows a browser window displaying a "Financial Portfolio Dashboard". The dashboard has a dark theme with white text. It includes a greeting "Selamat Sore", some placeholder text "XXXXX XXXXX" followed by several "XXXXXX" strings, and a disclaimer in Indonesian. Below the dashboard, there are date selection dropdowns for "Dari" (From) and "Ke" (To), both set to "JANUARI 2024" and "SEPTEMBER 2024" respectively. At the bottom, there's a note about filtering affecting the entire page and PDF versions.

Below the browser window, the browser's developer tools Network tab is visible. It shows a table of cookies. One cookie is highlighted in blue: "https://estatementdev.maybank.co.id JSESSIONID". The table columns are: Nama (Name), Nilai (Value), Domain (Domain), Path (Path), Kedaluwarsa / Usia Maksimal (Expiration/Max Age), Ukuran (Size), HttpOnly (HttpOnly), and Secure (Secure).

Nama	Nilai	Domain	Path	Kedaluwarsa / Usia Maksimal	Ukuran	HttpOnly	Secure
https://estatementdev.maybank.co.id JSESSIONID	9069638124C26E442751FD0D22EB4588	estatementdev.maybank.co.id	/	Sesi	42	true	true

Error Message Information Exposure

Description:

Our assessment on the target shows the application current error message shows database information of the application.

Exploitation Effort:

Low – Attacker can check for known vulnerability

Affected target:

<http://10.235.83.40:8081/vs/csintrctv>

<http://10.235.83.40:8081/vs/csintrctv?uid=7CA13DE3BF3A084876AC4AE9E1E6DE11&ch=7F11ED3FDDBDACC44&custType=npr#/>

Severity:

Low – Attacker can use information for future attack

CVSS Score:

CVSS Base Score: 5. CVSS Temporal Score: 3.7. CVSS Exploitability Score: 10. CVSS Impact Score: 2.9.

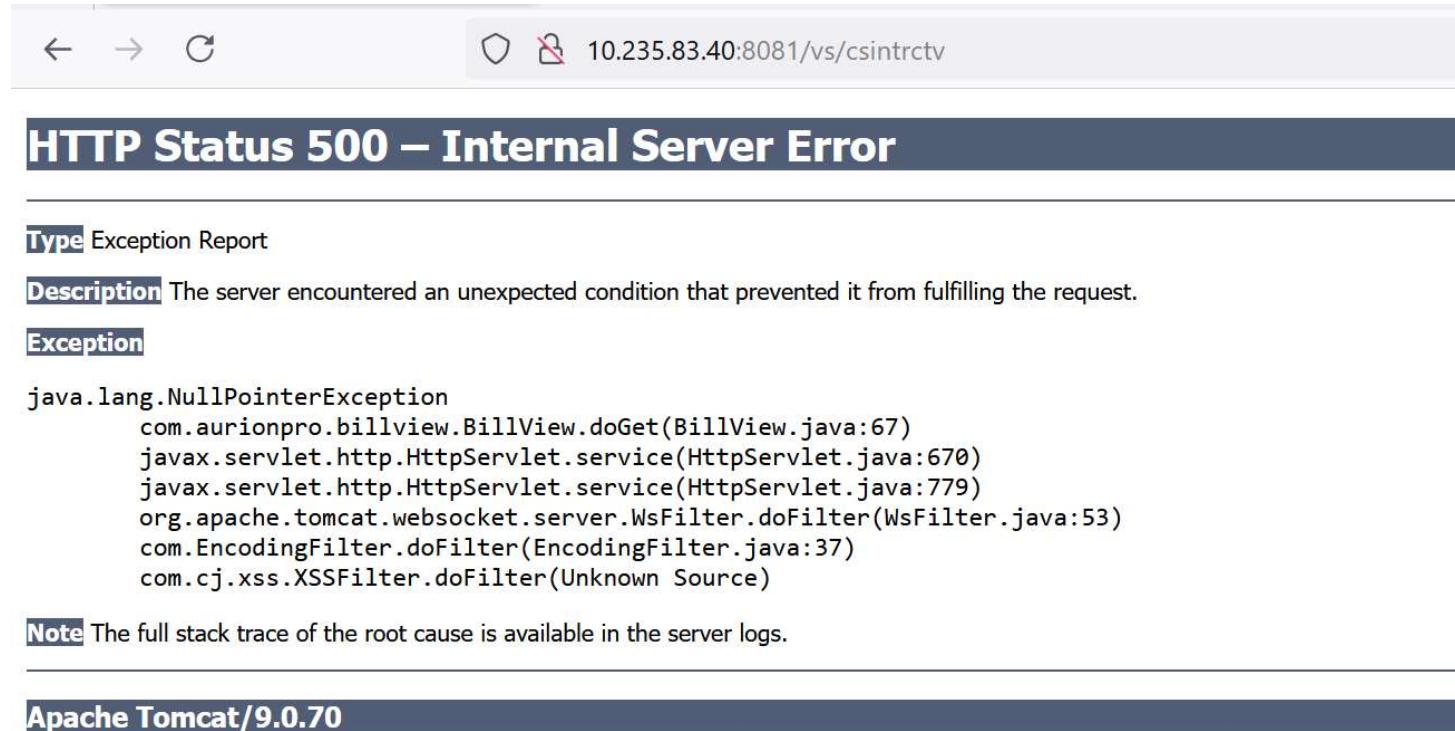
Recommendation:

We recommend to implement custom error message to prevent information exposure .

Retest Result:

Retest result shows the vulnerability is fixed.

Error Message Information Exposure



The screenshot shows a browser window with the following details:

- Address Bar:** 10.235.83.40:8081/vs/csintrctv
- Title Bar:** HTTP Status 500 – Internal Server Error
- Type:** Exception Report
- Description:** The server encountered an unexpected condition that prevented it from fulfilling the request.
- Exception:**

```
java.lang.NullPointerException
    com.aurionpro.billview.BillView doGet(BillView.java:67)
    javax.servlet.http.HttpServlet.service(HttpServlet.java:670)
    javax.servlet.http.HttpServlet.service(HttpServlet.java:779)
    org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:53)
    com.EncodingFilter.doFilter(EncodingFilter.java:37)
    com.cj.xss.XSSFilter.doFilter(Unknown Source)
```
- Note:** The full stack trace of the root cause is available in the server logs.
- Apache Tomcat/9.0.70**

Error Message Information Exposure

Request

Pretty Raw Hex

```

1 GET /vs/csintrctv?uid=7CA13DE3BF3A084876AC4AE9E1E6DE11&ch=7F11ED3FDBDACC44&custType=npr#/ HTTP/1.1
2 Host: 10.235.83.40:8081
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:130.0) Gecko/20100101 Firefox/130.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
5 Accept-Language: id,en-US;q=0.7,en;q=0.3
6 Accept-Encoding: gzip, deflate, br
7 Connection: keep-alive
8 Cookie: JSESSIONID=B1F5050AD0DDF9501033EA17FDE3736ES
9 Upgrade-Insecure-Requests: 1
10 Priority: u=0, i
11
12

```

Response

Pretty Raw Hex Render

HTTP Status 400 – Bad Request

Type Exception Report

Message Invalid character found in the request target [/vs/csintrctv?uid=7CA13DE3BF3A084876AC4AE9E1E6DE11&ch=7F11ED3FDBDACC44&custType=npr#/]. The valid characters are defined in RFC 7230 and RFC 3986

Description The server cannot or will not process the request due to something that is perceived to be a client error (e.g., malformed request syntax, invalid request message framing, or deceptive request routing).

Exception

```

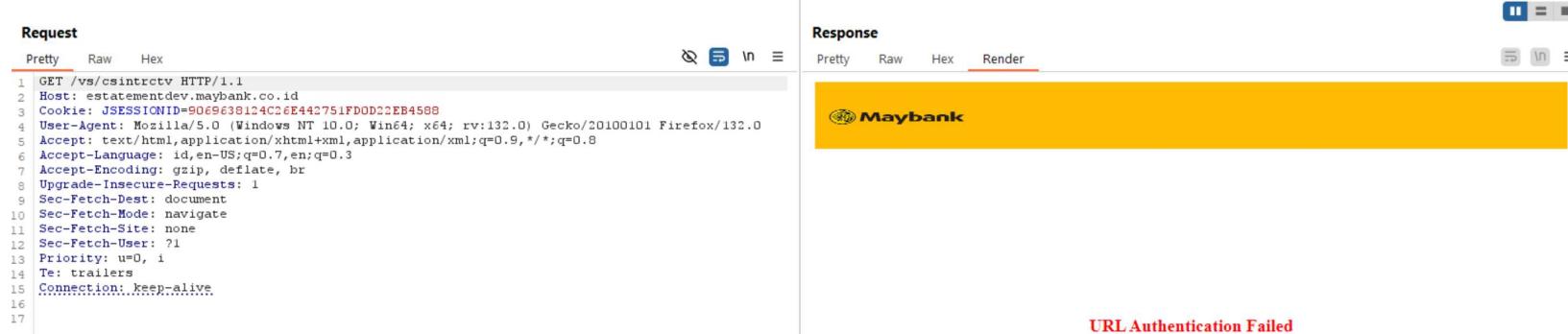
java.lang.IllegalArgumentException: Invalid character found in the request target [/vs/csintrctv?uid
org.apache.coyote.http1.Http1InputBuffer.parseRequestLine(Http1InputBuffer.java:494)
org.apache.coyote.http1.Http1Processor.service(Http1Processor.java:271)
org.apache.coyote.AbstractProcessorLight.process(AbstractProcessorLight.java:65)
org.apache.coyote.AbstractProtocol$ConnectionHandler.process(AbstractProtocol.java:891)
org.apache.tomcat.util.net.NioEndpoint$SocketProcessor.doRun(NioEndpoint.java:1784)
org.apache.tomcat.util.net.SocketProcessorBase.run(SocketProcessorBase.java:49)
org.apache.tomcat.util.threads.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1191)
org.apache.tomcat.util.threads.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:659)
org.apache.tomcat.util.threads.TaskThread$WrappingRunnable.run(TaskThread.java:61)
java.lang.Thread.run(Thread.java:750)

```

Note The full stack trace of the root cause is available in the server logs.

Apache Tomcat/9.0.70

Error Message Information Exposure



Request

Pretty Raw Hex

```
1 GET /vs/csintrctrlv HTTP/1.1
2 Host: estatementdev.maybank.co.id
3 Cookie: JSESSIONID=9069638104C26E442751FDOD22EB4588
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:132.0) Gecko/20100101 Firefox/132.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
6 Accept-Language: id,en-US;q=0.7,en;q=0.3
7 Accept-Encoding: gzip, deflate, br
8 Upgrade-Insecure-Requests: 1
9 Sec-Fetch-Dest: document
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-Site: none
12 Sec-Fetch-User: ?1
13 Priority: u=0, i
14 Te: trailers
15 Connection: keep-alive
16
17
```

Response

Pretty Raw Hex Render

 Maybank

URL Authentication Failed

Error Message Information Exposure

Request

Pretty Raw Hex

```
1 GET /vs/csintrctv?uid=7CA13DE3BF3A084876AC4AE9E1E6DE11&ch=7F11ED3FDBDACC44&custType=npr#/HTTP/1.1
2 Host: estatementdev.maybank.co.id
3 Cookie: JSESSIONID=9069638124C26E442751FD0D22EB4588
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:132.0) Gecko/20100101 Firefox/132.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
6 Accept-Language: id,en-US;q=0.7,en;q=0.3
7 Accept-Encoding: gzip, deflate, br
8 Upgrade-Insecure-Requests: 1
9 Sec-Fetch-Dest: document
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-Site: none
12 Sec-Fetch-User: ?1
13 Priority: u=0, i
14 Te: trailers
15 Connection: keep-alive
```

Response

Pretty Raw Hex Render

Bad Request

Default Apache Tomcat Page Information Exposure

Description:

Our assessment on the target shows the application Apache Tomcat page is accessible to the network.

Exploitation Effort:

Low – Attacker can check for known vulnerability

Affected target:

<http://10.235.83.40:8081/>

Severity:

Low – Attacker can use information for future attack

CVSS Score:

CVSS Base Score: 5. CVSS Temporal Score: 3.7. CVSS Exploitability Score: 10. CVSS Impact Score: 2.9.

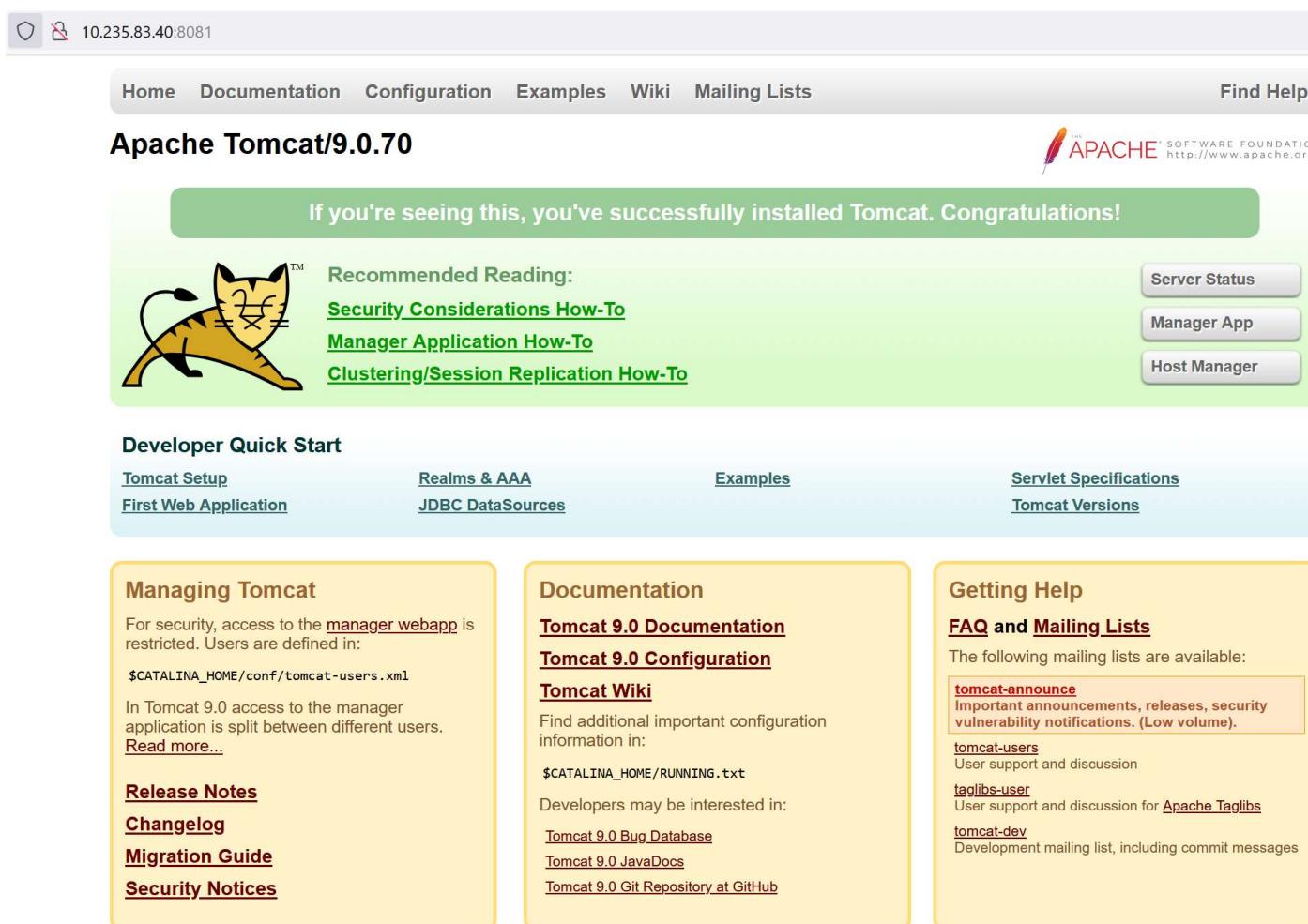
Recommendation:

We recommend to implement restriction on access to prevent information exposure.

Retest Result:

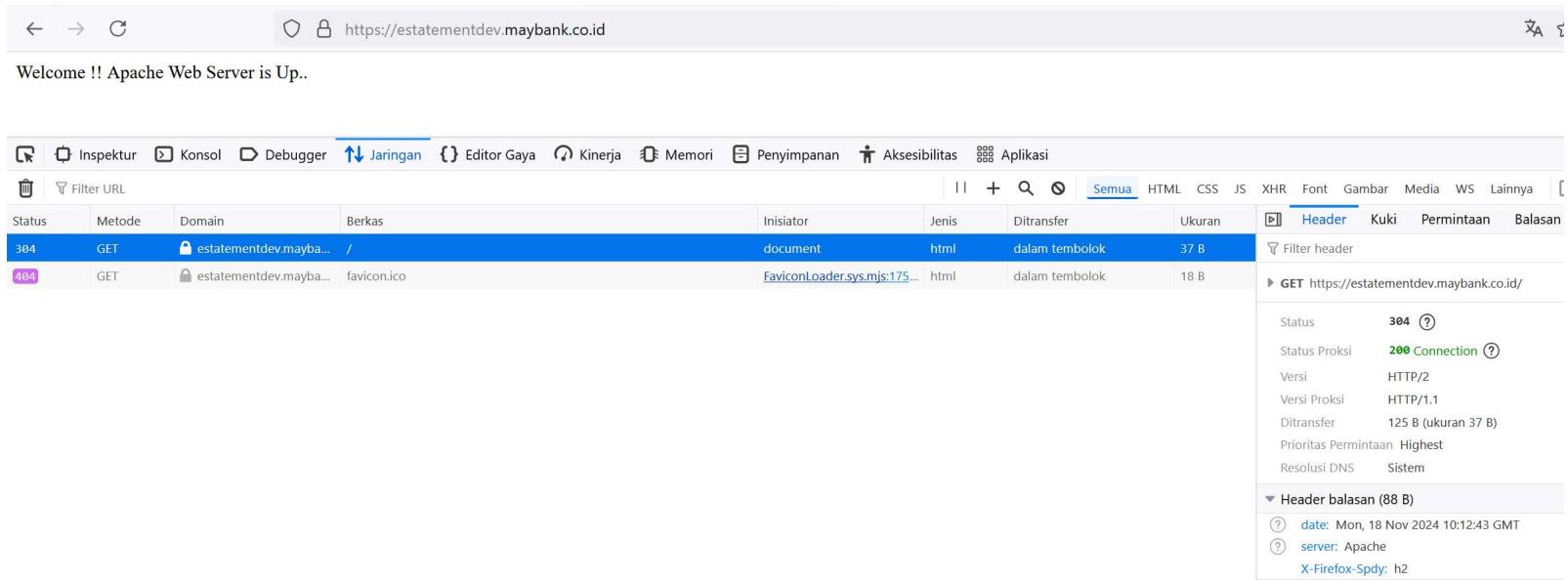
Retest result shows the vulnerability is fixed.

Default Apache Tomcat Page Information Exposure



The screenshot shows the Apache Tomcat 9.0.70 default page. At the top, there's a navigation bar with links to Home, Documentation, Configuration, Examples, Wiki, and Mailing Lists, along with a Find Help button. Below the navigation is the Apache logo. A green banner at the top of the main content area says "If you're seeing this, you've successfully installed Tomcat. Congratulations!" In the center, there's a cartoon cat icon and a "Recommended Reading" section with links to Security Considerations How-To, Manager Application How-To, and Clustering/Session Replication How-To. To the right, there are three buttons: Server Status, Manager App, and Host Manager. The main content area is divided into several sections: Developer Quick Start (with links to Tomcat Setup, First Web Application, Realms & AAA, JDBC DataSources, Examples, and Servlet Specifications), Managing Tomcat (with links to Release Notes, Changelog, Migration Guide, Security Notices, and documentation for Tomcat 9.0 Documentation, Configuration, and Wiki), Documentation (with links to RUNNING.txt, Bug Database, JavaDocs, and Git Repository), and Getting Help (with links to mailing lists like tomcat-announce, tomcat-users, taglibs-user, and tomcat-dev). The footer contains copyright information and a page number.

Default Apache Tomcat Page Information Exposure



The screenshot shows a NetworkMiner tool interface capturing traffic for the URL <https://estatementdev.maybank.co.id>. The tool displays two captured requests:

Status	Metode	Domain	Berkas	Inisiator	Jenis	Ditransfer	Ukuran
304	GET	estatementdev.mayba...	/	document	html	dalam tembolok	37 B
404	GET	estatementdev.mayba...	favicon.ico	FaviconLoader.sys.mjs:175...	html	dalam tembolok	18 B

The right pane shows the detailed response for the first request (Status 304). It includes the following details:

- Status: 304 (Connection)
- Status Proksi: 200 Connection
- Versi: HTTP/2
- Versi Proksi: HTTP/1.1
- Ditransfer: 125 B (ukuran 37 B)
- Prioritas Permintaan: Highest
- Resolusi DNS: Sistem

Under the "Header balasan" section, the following headers are listed:

- Date: Mon, 18 Nov 2024 10:12:43 GMT
- Server: Apache
- X-Firefox-Spdy: h2

Security Header Configuration

Description:

Our assessment on the target shows the application current security header is not implemented.

Exploitation Effort:

Low – Attacker can check for known vulnerability

Affected target:

<http://10.235.83.40:8081/vs/csintrctv?uid=7CA13DE3BF3A084876AC4AE9E1E6DE11&ch=7F11ED3FDBDACC44&custType=npr#/>

Severity:

Low – Attacker can use information for future attack

CVSS Score:

CVSS Base Score: 5. CVSS Temporal Score: 3.7. CVSS Exploitability Score: 10. CVSS Impact Score: 2.9.

Recommendation:

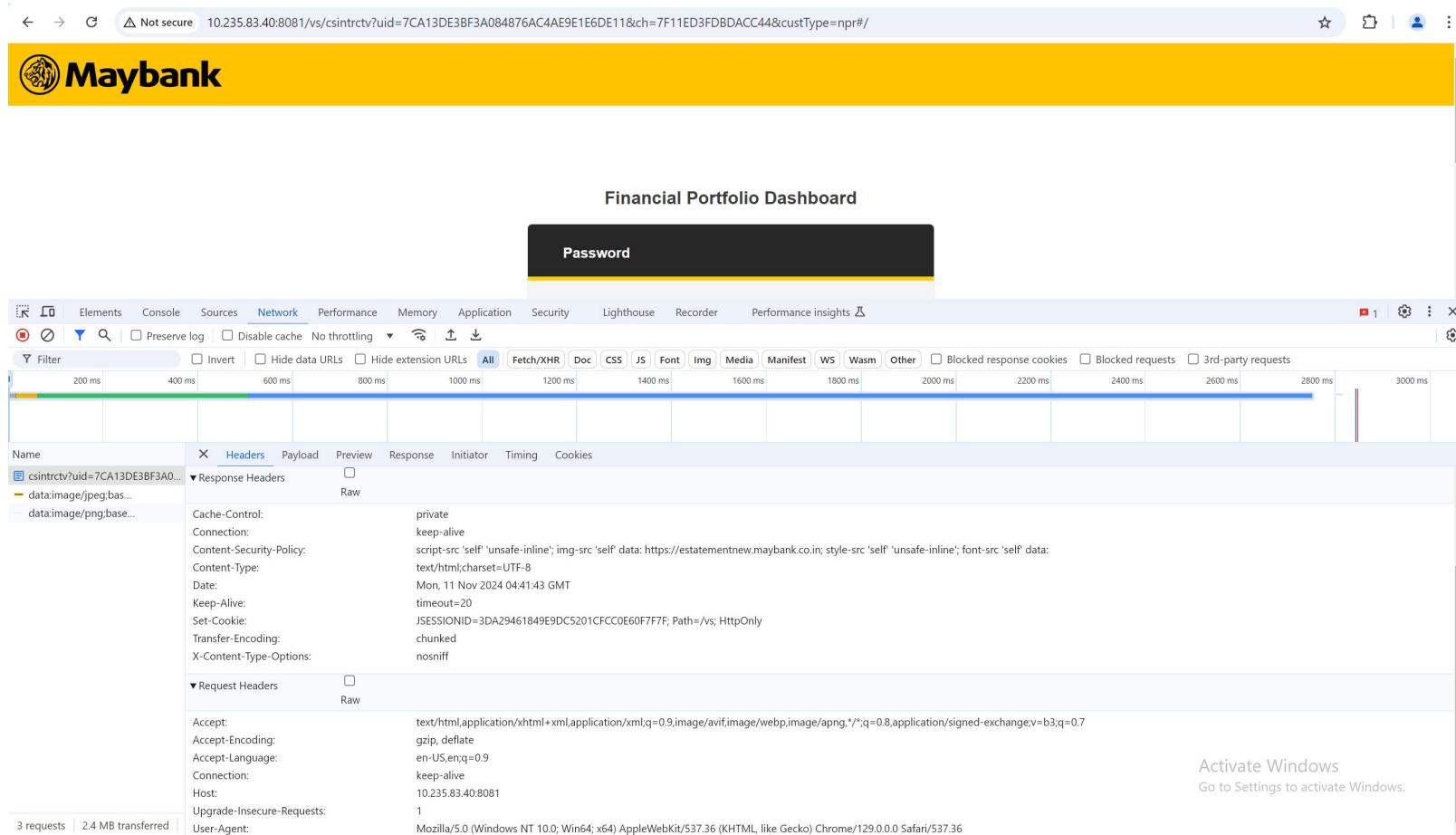
We recommend to implement security header on production version.

https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Headers_Cheat_Sheet.html

Retest Result:

Retest result shows the vulnerability is partially fixed. CSP header still missing.

Security Header Configuration



The screenshot shows a browser developer tools Network tab with the following details:

Network Tab Headers:

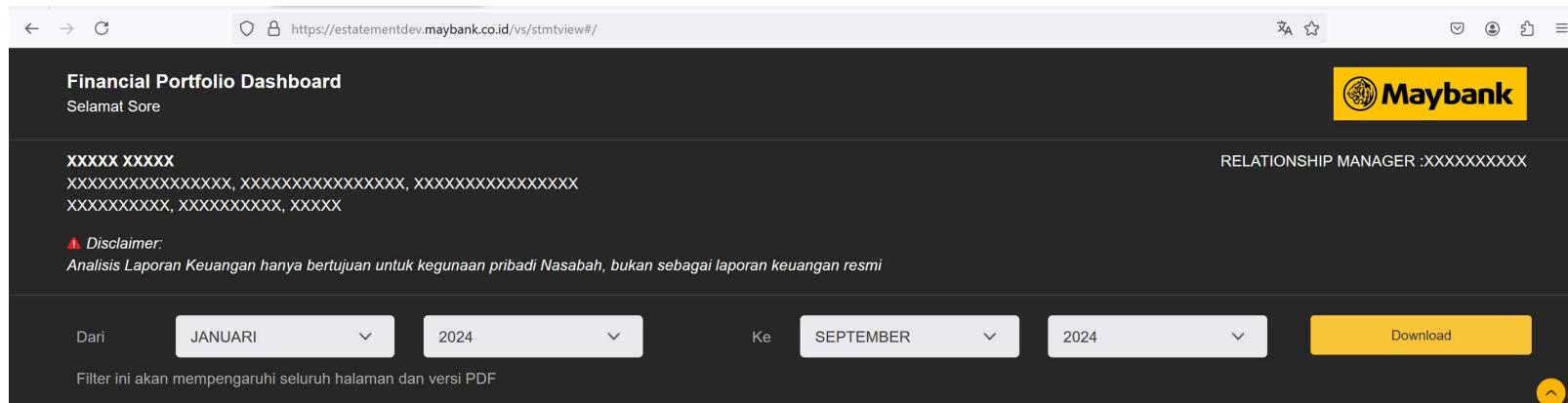
Name	Value
Content-Security-Policy	script-src 'self' 'unsafe-inline'; img-src 'self' data: https://estatementnew.maybank.co.in; style-src 'self' 'unsafe-inline'; font-src 'self' data:
Content-Type	text/html; charset=UTF-8
Date	Mon, 11 Nov 2024 04:41:43 GMT
Keep-Alive	timeout=20
Set-Cookie	JSESSIONID=3DA29461849E9DC5201CFCC0E60F7F7F; Path=/vs; HttpOnly
Transfer-Encoding	chunked
X-Content-Type-Options	nosniff

Request Headers:

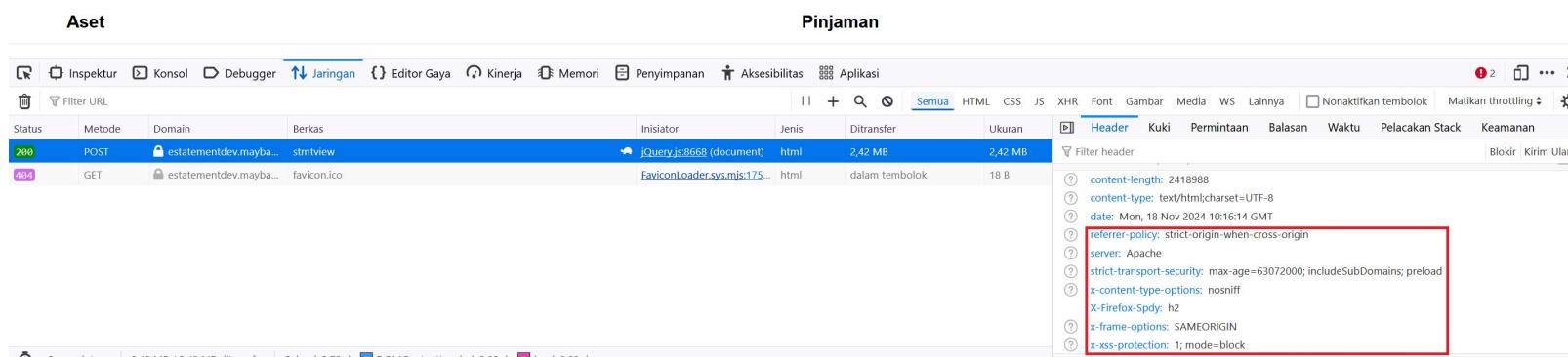
Name	Value
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding	gzip, deflate
Accept-Language	en-US,en;q=0.9
Connection	keep-alive
Host	10.235.83.40:8081
Upgrade-Insecure-Requests	1
User-Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.0.0 Safari/537.36

Activate Windows
Go to Settings to activate Windows.

Security Header Configuration



The screenshot shows a financial dashboard for Maybank. At the top, it displays a placeholder for a relationship manager's name. Below this, there is a disclaimer stating that the analysis is for personal use only and not a formal financial report. The interface includes dropdown menus for selecting dates from January 2024 to September 2024, and a 'Download' button. A message at the bottom indicates that filters will affect the entire page and PDF version.



The screenshot shows the Network tab of a browser developer tools window. It lists two requests: a POST request for 'stmtview' and a GET request for 'favicon.ico'. The details pane on the right shows the response headers for the POST request, which include several security-related headers highlighted with a red box:

- content-length: 2418988
- content-type: text/html; charset=UTF-8
- date: Mon, 18 Nov 2024 10:16:14 GMT
- referrer-policy: strict-origin-when-cross-origin
- server: Apache
- strict-transport-security: max-age=63072000; includeSubDomains; preload
- x-content-type-options: nosniff
- X-Firefox-Spdy: h2
- x-frame-options: SAMEORIGIN
- x-xss-protection: 1; mode=block

Business Logic Flaw Data Breach

Description:

Our assessment on the target shows the attacker able to perform data breach on application logic due to data being given to user before login although the data given is encrypted.

Exploitation Effort:

Low – Attacker can check for known vulnerability

Affected target:

10.235.83.40:8081/vs/csintrctv?uid=7CA13DE3BF3A084876AC4AE9E1E6DE11&ch=7F11ED3FDBDACC44&custType=npr

Severity:

Medium – Attacker can perform sensitive information exposure

CVSS Score:

CVSS Base Score: 5 CVSS Temporal Score: 4.3. CVSS Exploitability Score: 10. CVSS Impact Score: 2.9.

Recommendation:

We recommend to implement verification on user authentication before the data is given.

Retest Result:

Retest result shows the vulnerability is fixed.

Business Logic Flaw Data Breach

Request	Response
<pre>Pretty Raw Hex 1 GET /vs/csinterrtv?uid=7CA13DE3BF3A084876AC4AE9E1E6DE1&ch=7F1IED3FDBEDACC4&custType=npr HTTP/1.1 2 Host: 10.235.83.40:8081 3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:130.0) Gecko/20100101 Firefox/130.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8 5 Accept-Language: id,en-US;q=0.7,en;q=0.3 6 Accept-Encoding: gzip, deflate, br 7 Connection: keep-alive 8 Cookie: SESSIONID=DI505ADODDF95010336A17FDE3736E9 9 Upgrade-Insecure-Requests: 1 10 Priority: u=0, i 11 12</pre>	<pre>Pretty Raw Hex Render 1 <script language="javascript"> 2 window.content = { 3 encryptedData: 4 ">CfB13+rEZK4rUAJ0+1Y06sE1H2z+1+2rPR3RCvU+l+gooyr40vHeibfTfvW3jP0x0fGyaevFSYrUyBThPfbiWhvcAeyE0xwCOT0Y 5 JmBkxwlAH0Ghbh4yPlaR90771Endsa4uMcL21kdgsuotCKWmjxdfliaj0jezgkCdVm5dmU8cUNSpf1ETw5gev84D4d0cju+Mn 6 Lx7ylUhr+0T1vZgAyBhVvq018Tq10nTq9Bv3zylib81AIrJkf0/+h+7jCEXVnctbPaLZzg5/v5j3oRLN/tga3zyo/EDW6cIX 7 P0k/GC/r1x7DxDjvq132CzqefmBzsPDc0T7d0AfhpWP5uHg8a1gNY6dNUFl0+j9sfldj10terd/jnfplz37+eplmIk7jspryDE8o 8 wEjoqd1BopDfEfVtKwDdeg1csf/GoAbz2inTVEtTLE-Bu1hdpbksJEHqatc4s0kpygF5o1Czbph3kyu81El1aUCHkl1gc27Lqiz/T/6D 9 M/Of6ee+NHZDQx8co4+APFElkwVMj/Fwg0B0xzBpb9s23yTCPEQ1+wffw/jiLltoyZBDP11McNeV8BpajBCAJdAnExJ5t 10 A13AL6mG3fx35tVs0l3t3n1j3rCu4+Ve07LHS8Bv4y3A8vLyk100+DoW1LghYTh3Tf3sToque+stUtarWS5K13145+Fx3x013Yu 11 iJS1fpyntTqj0T0/r8S/XeOHMc/PcNwokcqmgls2YgErbbtdrLW1E3Gym0+SS/wgFHSMNjWx6ej10Ck23ZV52+Kc+8sCD 12 HrV1lAh0lIE/HtAGA42h9IPf1d7BFE4xrttakdpcmcn040d04/2f48CxxGAjFnwGnul45rfGDTs471MwLc0Nt50p2d/7Db72qf 13 nvZeqg/91z7tChDAD07hOnJyLjF1r73ofDfbhccF1kPfD5kdu0F0AewGf8TnHWEvg8142c064hFTQz0fJFAFsqfF2rJ 14 G73J00B1Jgnq+0x0qJ/1Pv+f1fRE+7BnigfTdR3uySxv5bA0ypuSg2s6aDPLA1hboW05CV1Vf0eA2dbmz5j0/0mt00uEd404W48mj 15 +gpp/sjhbzCaThavLkVL18s8k1Aj9hIwvglRY/vng3z3o1wvMR4L1Z6CF4byl2dFlqjqp0111X3j30zxBc0f3/c3bdcbf086c 16 h21MA0c06Lz1Aoy+8xtsW5mLsWv19/1115eenn5j1LTa+kvXSzg/v187YAYQ/+uo101C9Mv4/4/mPcrDY2XeSNBw0oGfajTpcaJ85d 17 P2xB2Wf1H6bGw/Zdxyv10MyVgo0TLL2f1FsSCo5gNSg5/0Nk31Z7G6gC/d/3yqFu/Pcv0KF0HLO5tV8BjE0nbLXbfy3M0yvtt 18 Su97wclFz20Uhu1In51RAkF484N1vvcKlhq0EtlBcDz2LhdWA203MgkMmAd1tG7J4eQ1mPxZ87l1qg1M86/3cQFrkdxVaTvja71+ 19 J12gkR0S0yge2ZD62FExx//VTDYyDmLqHngC6uH0j5b0/Br4jByGr1a0d4a2eyJUUDyAuU/3PtssTY96x/VtEgpp7c7V/u30d6x 20 D1Wv1lL2a7Yn8/checkboxtM1LqC2bLwv/2tbtwnmeV4mVfjeuNtYkrup3+s+ys1u0gVbOn5Z8BkAdy3WTzVx3Hc3z11 21 ys0TpGzfV9qia0oP0tGwMv1atdsq/44t7pC7b74c2zJd+9v1+9tArb+4ZtZhsb0vZ0v0KAjW0EZC2zH1fpx+em7 22 p6w0T0D0+P2z3tfu0Wb2tzJgh10170WP1YLE2017KajcBy/yzDA5xemh1+E+U)j38+9+b5e+7w/7c/LESPrQfCwxc1pVz6/q0fM002Z2G 23 1YD++7w/PvXuXj6PvL11eBp17d4f9fIHTUMbLle1b53DlptG1L1M3XCfHg/fPd4SHt+s3Anb/[1x73+0+d653DlLtoGpwyB2/J18UF 24 B5zB7m1AadBpEp6Dxx0hSwv/12hbmSw5b17p1Yd02fvtzDfHbqyx44akqg4PZ82cpMfd4DDN+7Wbck1poyndtYsCqTf9 25 We4k13VBD7mB0W0Mm971x8NblT2p9E0Y+GpCfW73D3b8tYgCp/HW1/37WfFz12Ac15cFnzG23 26 hbgp/TD43G2VNmappYt6k2z67NDAw/7k12Nm9v0ENtDg0L0EanJvNvSEa+o+ej0PfK4N0X)T/WcA7b0y1y42z:z1uNFNddh 27 QYOLxwLsNxJF04J0t9yVhnaF0ghnGmHaZo92+2tNmPsgtq/7svFyTbDc03BdsupLh1d1J51YageAbw+0A/Wg8B1Ud2oI 28 s1t1c1eV1C10tUSJN07s1y1UO4tP1L1z1CtLpRvE1P1Q/Gq0tE44ufrfFdnsd+o770TB5V9s4ERK 29 jmlboEmyVswvejF2m1spuv8Ei+9gEawv1C2t+dg3v6fVdavcycgHanc1tL05pb+808CCeMp2dYs91Y7Wfrc2h01Bc5+u17 30 b9r+1XwVhd2chm7s1j0j2p1jha1l10b39+7J7KUfj140t72Df1Qd/Bqdhvug/YSFF+hgF+u/(4)cj2o1PfDpBf+F 31 j1Z6eJ2c5knlBlaxPfPMh0l52sz0o4410n50B1D1tg1W3A9PfSL1P3/171s0a117bPT85849Abk3L8y7 32 Tz0Hs1o1+7Vaf1j2wkl17p7gpph0B1j0dzb02vY02PcfaPd4tC9PfN02z1laG+UV4p+gjtZTfNA/1lccnnlyajygb5b 33 +poV955cfh3FgjvSV3t1C8e+7K3X/LdDhB2nDaF1Qfpp1H1fPzDfZU/1jEaJJEY9CAFldqpuHd1nEld1pVt+eD21qram8 34 Blv1W9m0U+wCYp11dvh80gPnBt50u471PAgg3PF91J1ah1Uu1Ad3X2jMve4T7Eduuqg1Bj0j0tUYmp/Tuqj9b9x0qgZETxAT 35 +0tKwCeCavInfrFL02+gauBdtmPfa5p1kxp0Mfp1b4DBy3V+2wZmagfBqJGH/1L0tPpJyUsMedwVw-Yf1aL1IHvNe6hfq11 36 2JQb1essxZEVPe0huw0N0m0wVSvC01RjUJAH/Xwsyf0A0D0W2lu2BDjC74+77WbUuBx2e+o2L1lwavPridp51A1z21y139w8pp 37 +3r+VcWmUs1lk1+d2B5b29dax1Qm06tIxAs1L2mvm+v7+P4Scd+eL1Gaf75i1992D1l2m0n0e+PbnGpWb1DfYc/s5PejuEWxJ 38 FMgBHCEPfKd9g80wyvBHTjyaPnG038wvSF4+OB+An8028dnNs0c72/7c1ljJgVv0x4jCQFlR0u6d0jQGCFPhuugdUJUUPcrsT 39 +uNM08s/wqJc+jCj20wefAh1kCdo+dMge+pSHAF7Wpb2ANL5y+80Fcm9jL21gpmnZwZ2EaCue9PfR1bHmCc+txeMPT015asNt 40 +01N3dsCSmUetD3lmaJmV1zvWk4eaynZ22BMUiliza8w70hzCm+4yRfGdfHwL1Lu3Av1+ab7/1J0ZTTE1J1c1L2Wsy7/Caa4+Xpc 41 ddi604yJ+oh7fd2T7V/kr85GY34akxg1BydUjCnphu3QL8SJ56fhtoKd1NaQjGsa+G+fill1rL0wv+teYfctS181h56jeqxF1 42 UtAA4d0Bh0/l1d71G0U0Rav3pm+1Jdclfa1Gu9HHLFk+eyd0b410fPxe1b1K18CoCfTyvDD0Al(pPwruU-411+galMy0871qr7H 43 KrhJpv3xE/R8d1rz45K9yELogPf11s3+EV3p3-jn7tM3M0nR97FVJyMn1TCLaQjGmGx9JUL1KMLC9Z20k+r+0f1CsTX 44 QSnll1Pnum1vg1eY7vMrzZEExdmnf0kYK3jkBsx10x1HJR+k4Qbx1o1Yd/1x8C0UM/xQGn9dE98s1dakbp8G3161a50yKaJL 45 F3Fetxh5yD0ahNPNTygf1l+gx+q11C84vvRgwQZPNM1mHgjykFp1EA8cc00xCTYL1a36G7PGBgPfTHnvfyD4+ef52vNjyWEf08 46 tuaww1P3hJtih9bJyrmK7LgEE20eC1JWq5Gf930kF24+q0N0UmjP1VcGcu0fuwqJH01t1b0jx/vb6t1HoAuzTXtoNPF1s1755U 47 nex9UA85v595KCsx5iCh+SeMtG4d0v5H7/Xa0EEtuy4DpTbD+2r1ErSd14L7m8wGMb0c06HNZ36s436L66HF1chh0s4vPiRu</pre>

Business Logic Flaw Data Breach

```
</noscript>
<script language="javascript">
    window.content = {
        encryptedData: "19EWUJHv2Znp/wEdfBUHhUObqfDng7/Bq4FA/zFcADrsh18ES70I35QebI/sL6p7Frjj787giLr0jRBw8vOs17EQWoscfMRboz0LgoZxpNA+H8t91Gj/zXxb10bKob7YjTe8boSp5gl1BFwd7EheJINNg6pE0G1XrXGZhZCCLGaQcRcAp0eUvHzJjaXL75e7/la9t6Nv9ixnxk+50brd9uMjJa45i9PFCG8wIXJNs
        dataLength: "18111",
        signature: "mR1kEnJMtya3zYs3mbp/cD9ahH+VKbb0jf7akhyowuw=",
        pepper: "cv=n1-82:r:pvc",
        iv: "0InaxcaW4DXCwHKDAjPozw=="
    };
</script>
<div id="app"></div>
<script type="text/javascript">
```

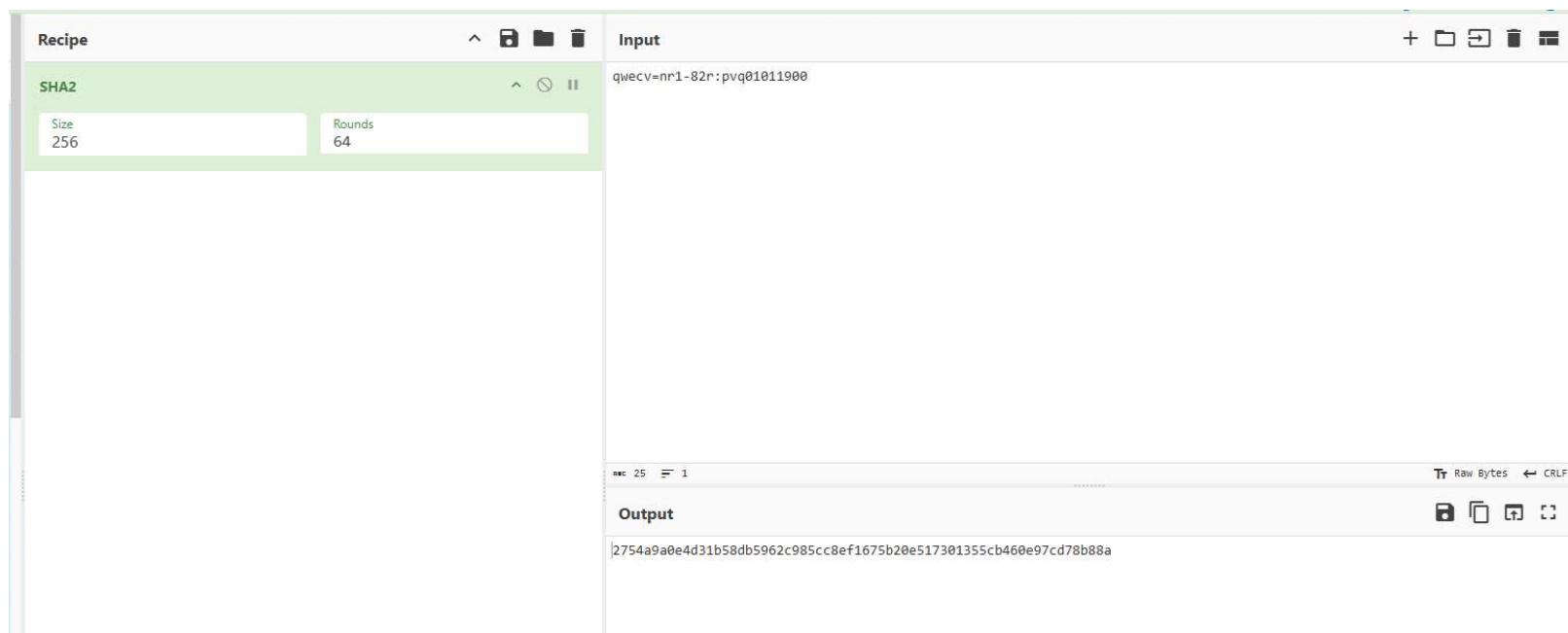
Business Logic Flaw Data Breach



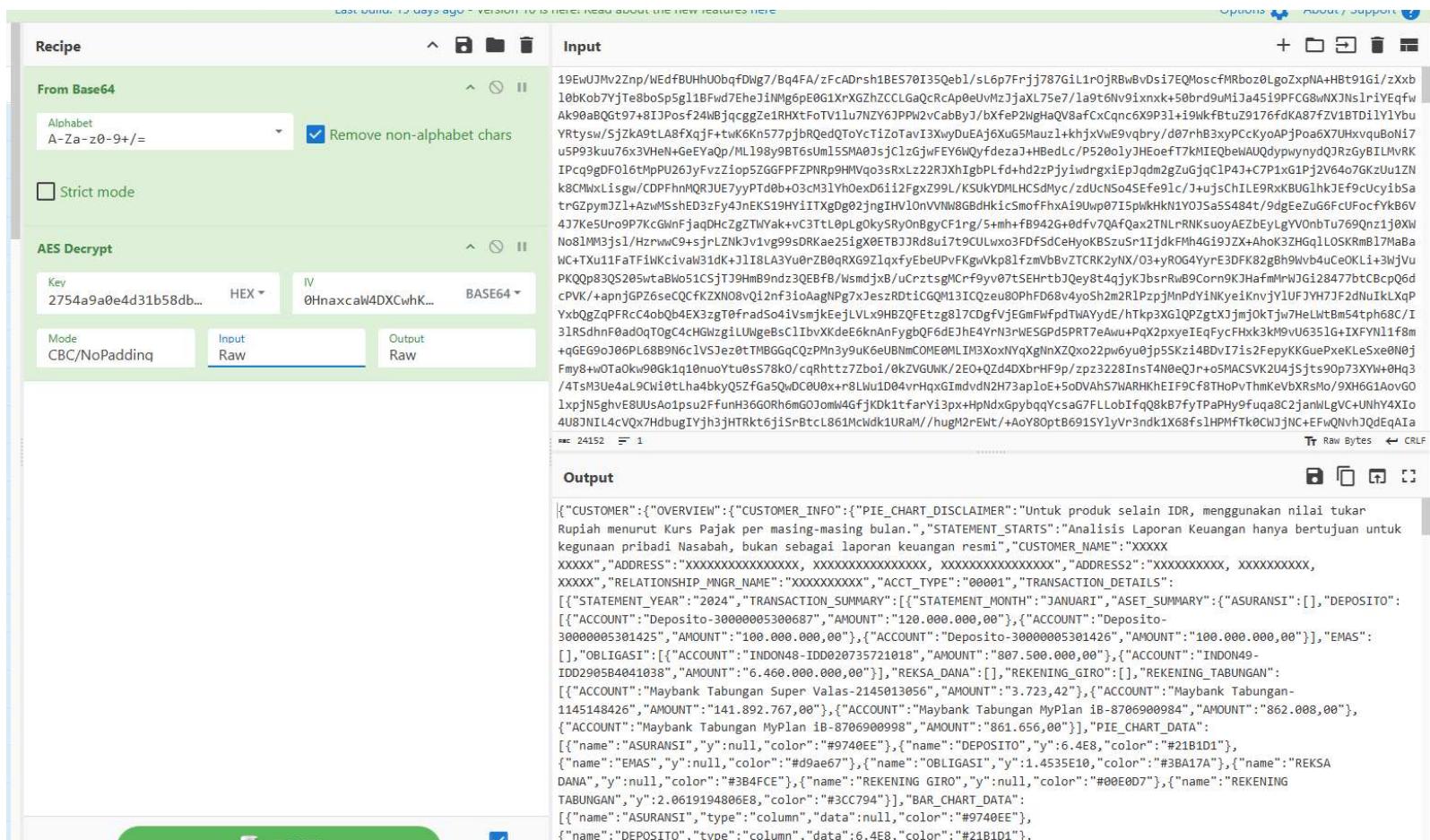
The screenshot shows a debugger interface with the following details:

- Code View:** The code is being executed at line 77. The highlighted line contains the assignment `a.update(e + r + n);`. The variable `e` is highlighted in yellow.
- Watch:** Shows the variable `r = t.pepper` with a value of `50277`.
- Breakpoints:** There are no breakpoints set.
- Scope:** Shows the current scope variables: `this: undefined`, `a: {$super: {}, cfg: {}, _data: r.init, _nDataBytes: 25, init: f, ...}`, `c: {$super: {}, cfg: {}, _xformMode: 2, _key: r.init, init: f, ...}`, `d: undefined`, `e: "que"`, `f: undefined`, `h: undefined`, `i: "0hexaca4DXCwHKD&Jpozw=="`, `m: undefined`, `n: "01011900"`, `o: {$super: {}, words: Array(4), sigBytes: 16, init: f}`, `p: "cvenr1-82r:pvq"`.
- Local:** Shows the local variables: `this: undefined`, `a: {$super: {}, cfg: {}, _data: r.init, _nDataBytes: 25, init: f, ...}`, `c: {$super: {}, cfg: {}, _xformMode: 2, _key: r.init, init: f, ...}`, `d: undefined`, `e: "que"`, `f: undefined`, `h: undefined`, `i: "0hexaca4DXCwHKD&Jpozw=="`, `m: undefined`, `n: "01011900"`, `o: {$super: {}, words: Array(4), sigBytes: 16, init: f}`, `p: "cvenr1-82r:pvq"`.

Business Logic Flaw Data Breach



Business Logic Flaw Data Breach



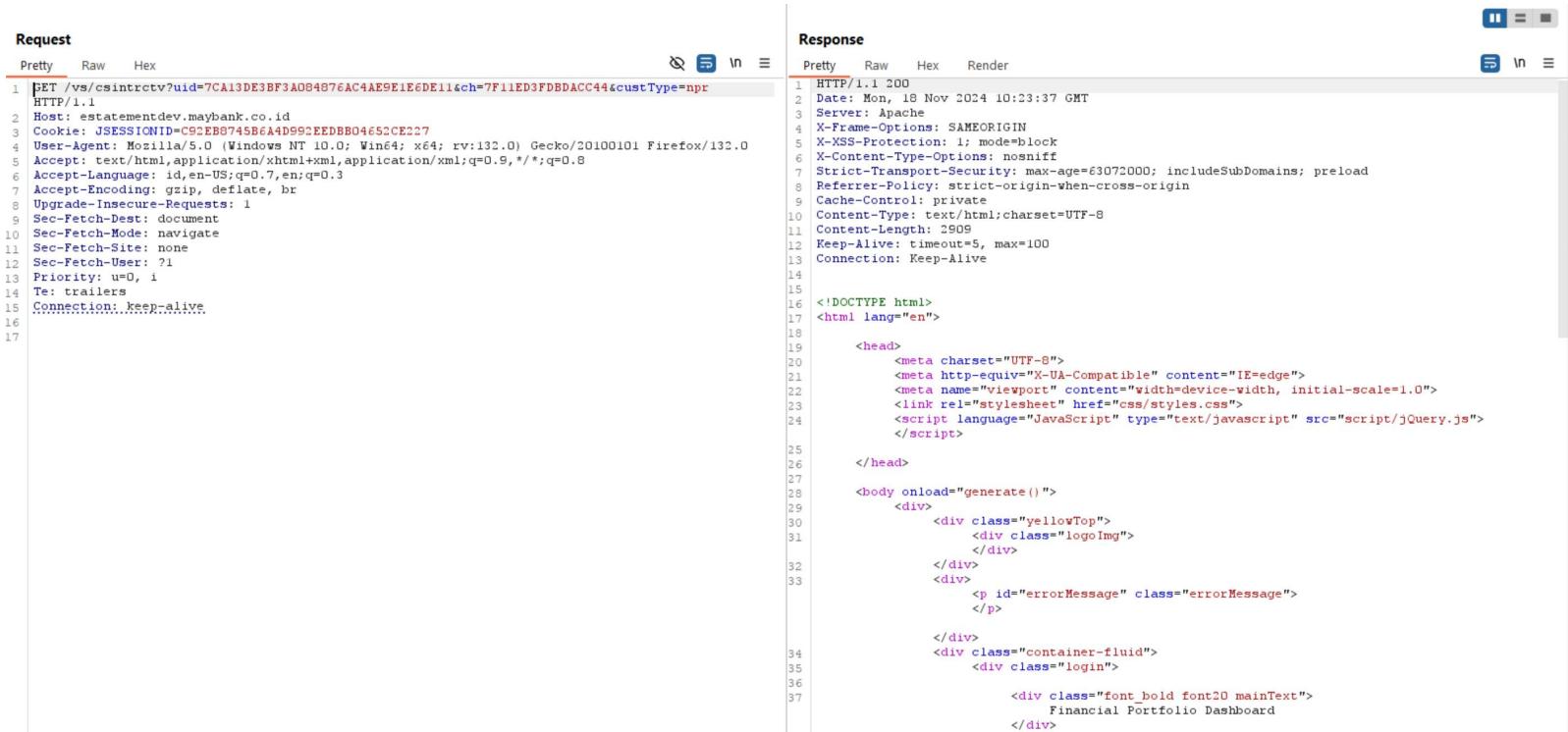
The screenshot shows a web-based application interface for decoding and viewing sensitive data. The main area displays a large amount of Base64-encoded data, which has been decrypted using AES. The decrypted data is presented in a JSON object:

```

{
    "CUSTOMER": {
        "OVERVIEW": {
            "CUSTOMER_INFO": {
                "PIE_CHART_DISCLAIMER": "Untuk produk selain IDR, menggunakan nilai tukar Rupiah menurut Kurs Pajak per masing-masing bulan.",
                "STATEMENT_STARTS": "Analisis Laporan Keuangan hanya bertujuan untuk kegunaan pribadi Nasabah, bukan sebagai laporan keuangan resmi",
                "CUSTOMER_NAME": "XXXXX XXXXX",
                "ADDRESS": "XXXXXXXXXXXXXX, XXXXXXXXXXXXXXX, XXXXXXXXXXXXXXX, ADDRESS2": "XXXXXX, XXXXXXXX, XXXXXX",
                "RELATIONSHIP_MNGR_NAME": "XXXXXX", "ACCT_TYPE": "00001", "TRANSACTION_DETAILS": [
                    {"STATEMENT_YEAR": "2024", "STATEMENT_SUMMARY": [
                        {"STATEMENT_MONTH": "JANUARI", "ASET_SUMMARY": {"ASURANSI": [], "DEPOSITO": [
                            {"ACCOUNT": "Deposito-30000005300687", "AMOUNT": "120.000.000,00"}, {"ACCOUNT": "Deposito-30000005301425", "AMOUNT": "100.000.000,00"}, {"ACCOUNT": "Deposito-30000005301426", "AMOUNT": "100.000.000,00"}], "EMAS": [], "OBIGASI": [{"ACCOUNT": "INDON48-ID020735721818", "AMOUNT": "807.500.000,00"}, {"ACCOUNT": "INDON49-IDD2905B4041038", "AMOUNT": "6.460.000.000,00"}], "REKSA_DANA": [], "REKENING_GIRO": [], "REKENING_TABUNGAN": [{"ACCOUNT": "Maybank Tabungan Super Valas-2145013056", "AMOUNT": "3.723,42"}, {"ACCOUNT": "Maybank Tabungan-1145148426", "AMOUNT": "141.892.767,00"}, {"ACCOUNT": "Maybank Tabungan MyPlan ib-8706900984", "AMOUNT": "862.008,00"}], "ACCOUNT": "Maybank Tabungan MyPlan ib-8706900998", "AMOUNT": "861.656,00}], "PIE_CHART_DATA": [{"name": "ASURANSI", "y": null, "color": "#9740EE"}, {"name": "DEPOSITO", "y": 6.4E8, "color": "#21B1D1"}, {"name": "EMAS", "y": null, "color": "#d9ae67"}, {"name": "OBIGASI", "y": 1.4535E10, "color": "#3BA17A"}, {"name": "REKSA DANA", "y": null, "color": "#384FCE"}, {"name": "REKENING GIRO", "y": null, "color": "#00E0D7"}, {"name": "REKENING TABUNGAN", "y": 2.0619194806E8, "color": "#3CC794"}], "BAR_CHART_DATA": [{"name": "ASURANSI", "type": "column", "data": null, "color": "#9740EE"}, {"name": "DEPOSITO", "type": "column", "data": 6.4E8, "color": "#21B1D1"}]}]
    }
}

```

Business Logic Flaw Data Breach



Request

```

1 GET /vs/csintrctv?uid=7CA13DE3BF3A0B4876AC4AE9E1E6DE11&ch=7F11ED3FDBDACC44&custType=npr
HTTP/1.1
2 Host: estatementdev.maybank.co.id
3 Cookie: JSESSIONID=C92EB8745B6A4D992EEDBB04652CE227
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:132.0) Gecko/20100101 Firefox/132.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
6 Accept-Language: id,en-US;q=0.7,en;q=0.3
7 Accept-Encoding: gzip, deflate, br
8 Upgrade-Insecure-Requests: 1
9 Sec-Fetch-Dest: document
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-Site: none
12 Sec-Fetch-User: ?1
13 Priority: u=0, i
14 Te: trailers
15 Connection: keep-alive
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37

```

Response

```

1 HTTP/1.1 200
2 Date: Mon, 18 Nov 2024 10:23:37 GMT
3 Server: Apache
4 X-Frame-Options: SAMEORIGIN
5 X-XSS-Protection: 1; mode=block
6 X-Content-Type-Options: nosniff
7 Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
8 Referrer-Policy: strict-origin-when-cross-origin
9 Cache-Control: private
10 Content-Type: text/html; charset=UTF-8
11 Content-Length: 2909
12 Keep-Alive: timeout=5, max=100
13 Connection: Keep-Alive
14
15
16 <!DOCTYPE html>
17 <html lang="en">
18
19     <head>
20         <meta charset="UTF-8">
21         <meta http-equiv="X-UA-Compatible" content="IE=edge">
22         <meta name="viewport" content="width=device-width, initial-scale=1.0">
23         <link rel="stylesheet" href="css/styles.css">
24         <script language="JavaScript" type="text/javascript" src="script/jQuery.js">
25     </head>
26
27     <body onload="generate()">
28         <div>
29             <div class="yellowTop">
30                 <div class="logoImg">
31
32             </div>
33             <div>
34                 <p id="errorMessage" class="errorMessage">
35                     </p>
36
37             </div>
38             <div class="container-fluid">
39                 <div class="login">
40                     <div class="font_bold font20 mainText">
41                         Financial Portfolio Dashboard
42                     </div>
43
44             </div>
45         </div>
46     </body>
47 
```

UID & CH Enumeration Vulnerability

Description:

Our assessment on the target shows the attacker able to perform enumeration on UID & CH.

Exploitation Effort:

Low – Attacker can check for known vulnerability

Affected target:

10.235.83.40:8081/vs/csintrctv?uid=7CA13DE3BF3A084876AC4AE9E1E6DE11&
ch=7F11ED3FDBDACC44&custType=npr

Severity:

Medium – Attacker can perform enumeration

CVSS Score:

CVSS Base Score: 5 CVSS Temporal Score: 4.3. CVSS Exploitability Score: 10. CVSS Impact Score: 2.9.

Recommendation:

We recommend to implement limitation on request, for example using token and captcha, to prevent enumeration attack.

Retest Result:

Retest result shows the vulnerability still exist.

UID & CH Enumeration Vulnerability

Request ^	Payload 1	Payload 2	Status code	Response received	Error	Timeout	Length	Comment
1217	3	8	200	47			2537	
1218	4	8	200	51			2537	
1219	5	8	200	46			2537	
1220	6	8	200	49			2537	
1221	7	8	200	49			2537	
1222	8	8	200	46			2537	
1223	9	8	200	46			2537	
1224	0	8	200	46			2537	
1225	A	9	200	44			3420	

Request Response

Pretty Raw Hex Render

```
9  <form action="stmtview" id="login-form" method="POST" autocomplete="off">
0   <div class="password">
1     <div>
2       <label htmlFor="password" class="loginfont-color whiteCir font18" >
3         Password <br/>
4       </label>
5     </div>
6   <div class="login1">
7     <div class="font12 bgGray">
8       Masukkan tanggal lahir Anda dengan format DDMMMYYYY
9     </div>
0   <div>
1     <input type="password" class="form-control submitStyle" name="password" id="password" ref="password" placeholder="Masukkan password di sini" autocomplete="off"/>
2   </div>
3   <div class="captcha-container">
4     <!-- Captcha Image Area -->
5     <div id="image" class="inline">
6       </div>
7
8     <!-- Input Field for Captcha -->
9     <div id="user-input" class="inline">
0       <input type="text" id="captchatxt" placeholder="Enter captcha" autocomplete="off">
1     </div>
2
3     <!-- Refresh Captcha Button -->
4     <div class="refreshBtn" id="refreshBtn" >
5       <i class="fas fa-sync">
6       </i>
7       Refresh Captcha
8
9
0
1
```

UID & CH Enumeration Vulnerability

Request ↗	Payload 1	Payload 2	Status code	Response received	Error	Timeout	Length	Comment
961	Y	I	200	51		2536		
962	Z	1	200	61		2536		
963	1	1	200	71		2536		
964	2	1	200	71		2536		
965	3	1	200	55		2536		
966	4	1	200	58		2536		
967	5	1	200	58		2536		
968	6	1	200	73		3419		
969	7	1	200	52		2536		
...	-	-	---	---		---	---	
Request	Response							
Pretty	Raw	Hex	Render					
<pre> <form action="stmtview" id="login-form" method="POST" autocomplete="off"> <div class="password"> <div> <label htmlFor="password" class="loginfont-color whiteClr font18" > Password
 </label> </div> </div> <div class="login1"> <div class="font12 bgGray"> Masukkan tanggal lahir Anda dengan format DDMMYYYY </div> <div> <input type="password" class="form-control submitStyle" name="password" id="password" ref="password" placeholder="Masukkan password di sini" autocomplete="off"/> </div> <div class="captcha-container"> <!-- Captcha Image Area --> <div id="image" class="inline"> </div> <!-- Input Field for Captcha --> <div id="user-input" class="inline"> <input type="text" id="captchatxt" placeholder="Enter captcha" autocomplete="off"/> </div> <!-- Refresh Captcha Button --> <div class="refreshBn" id="refreshBtn" > <i class="fas fa-sync"> </i> Refresh Captcha </div> </div> </pre>								
								Activate Windows

Improper Captcha Validation Password Enumeration

Description:

Our assessment on the target shows the attacker able to perform password enumeration due to improper captcha validation. Captcha only validated in front end and attacker can bypass directly to backend to perform enumeration.

Exploitation Effort:

Low – Attacker can check for known vulnerability

Affected target:

<https://estatementdev.maybank.co.id/>

Severity:

Medium – Attacker can perform enumeration

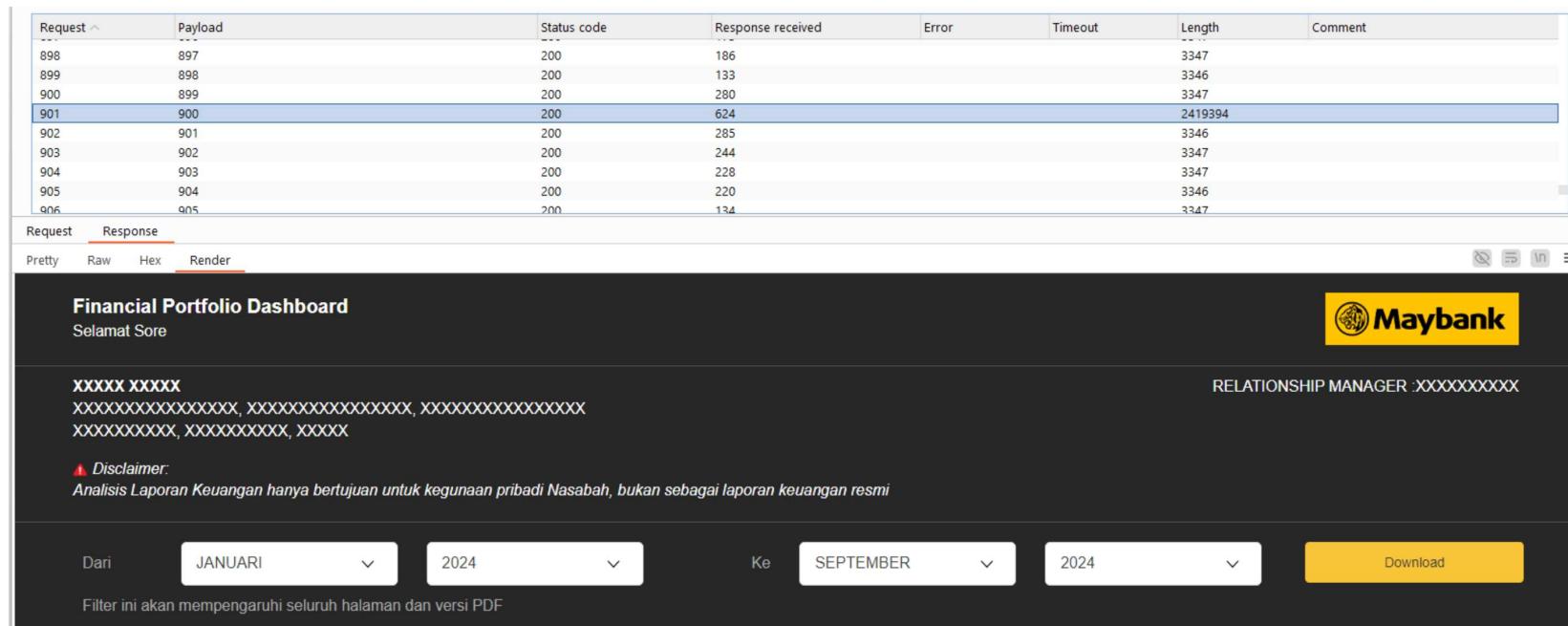
CVSS Score:

CVSS Base Score: 5 CVSS Temporal Score: 4.3. CVSS Exploitability Score: 10. CVSS Impact Score: 2.9.

Recommendation:

We recommend to implement validation of captcha on backend to prevent enumeration attack.

Improper Captcha Validation Password Enumeration



The screenshot shows a browser developer tools interface with the Network tab selected. It displays a list of requests and their corresponding responses. One specific response is highlighted, showing a captured screenshot of a 'Financial Portfolio Dashboard' page from Maybank. The dashboard includes a greeting 'Selamat Sore', a placeholder for a relationship manager name 'RELATIONSHIP MANAGER :XXXXXXXXXX', and a disclaimer stating that the analysis is for personal use only. The captured response also shows date range filters for 'Dari JANUARI 2024' and 'Ke SEPTEMBER 2024'.

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
898	897	200	186			3347	
899	898	200	133			3346	
900	899	200	280			3347	
901	900	200	624			2419394	
902	901	200	285			3346	
903	902	200	244			3347	
904	903	200	228			3347	
905	904	200	220			3346	
906	905	200	134			3347	

Request Response

Pretty Raw Hex Render

Financial Portfolio Dashboard

Selamat Sore

Maybank

XXXXX XXXXX
XXXXXXXXXXXXXX, XXXXXXXXXXXXXXXX, XXXXXXXXXXXXXXXX
XXXXXXXXXX, XXXXXXXXXX, XXXXX

RELATIONSHIP MANAGER :XXXXXXXXXX

⚠ Disclaimer:
Analisis Laporan Keuangan hanya bertujuan untuk kegunaan pribadi Nasabah, bukan sebagai laporan keuangan resmi

Dari JANUARI 2024 Ke SEPTEMBER 2024 Download

Filter ini akan mempengaruhi seluruh halaman dan versi PDF