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

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

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.

xynexis
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#/

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 It 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 It 2, Jl Imam Bonjol No 61, Jakarta 10310 (access via VPN)

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

severity Assessment Method

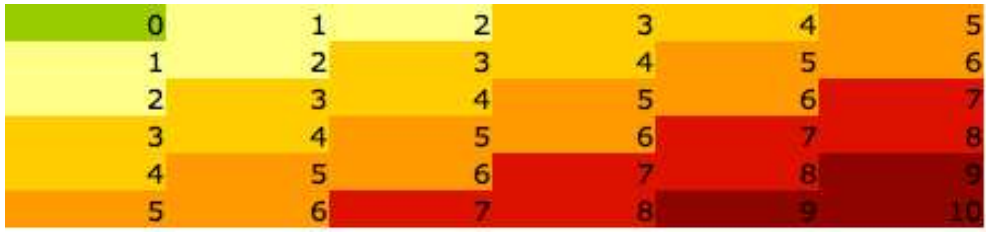
Description

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

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

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

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

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.

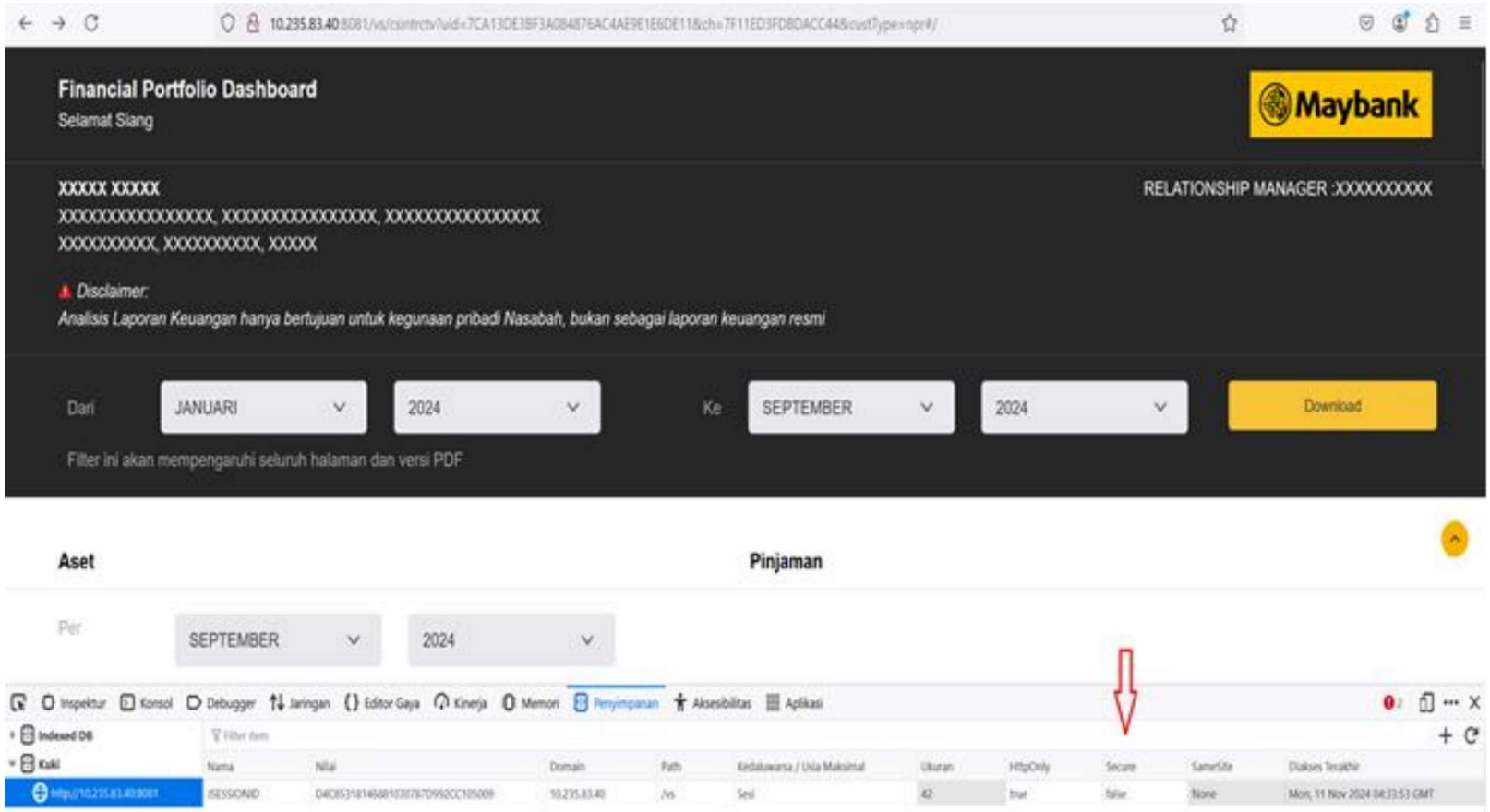
https://owasp.org/www-community/controls/SecureCookieAttribute

Retest Result:

Retest result shows the vulnerability is fixed.

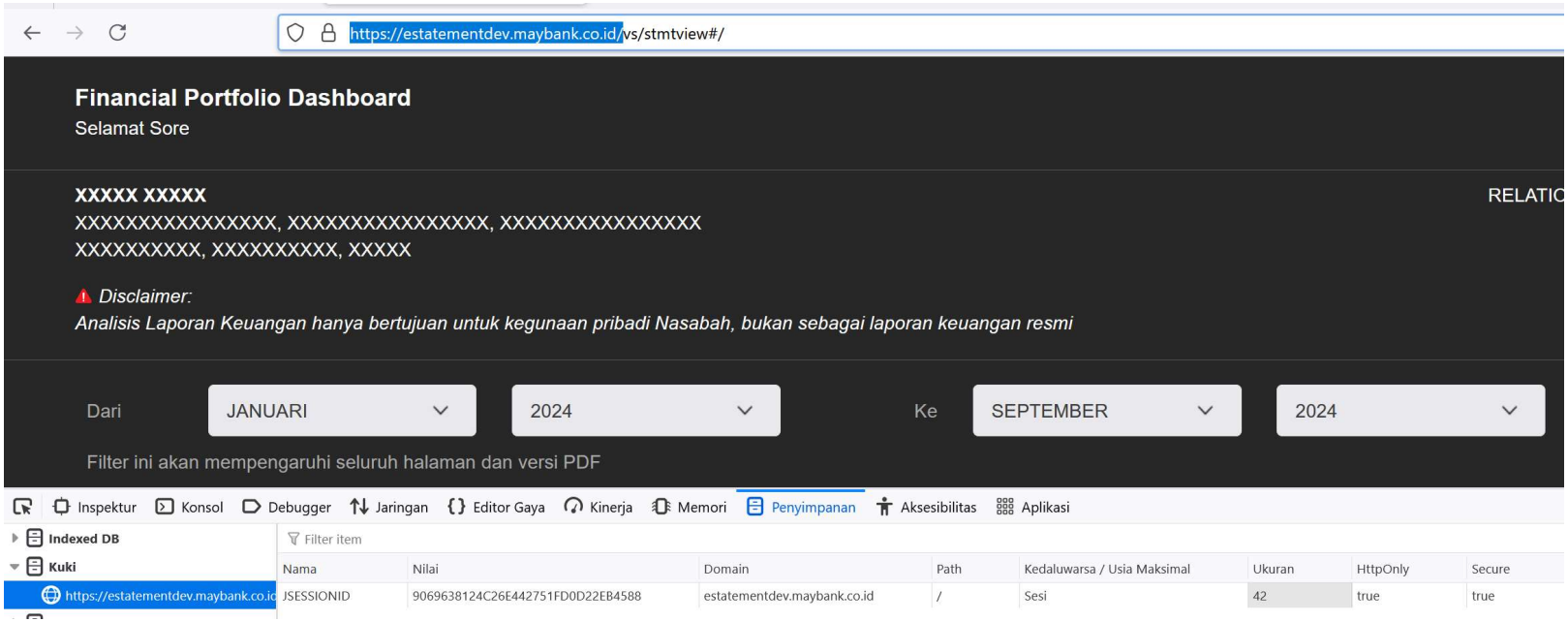
Graha Mandiri 2nd floor, Jalan Imam Bonjol No. 61, Jakarta 10310.
T: +6221-39834116 F: +6221-39834114 E: sales@xynexis.com

Cookie Implementation



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

Cookie Implementation



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

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=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:

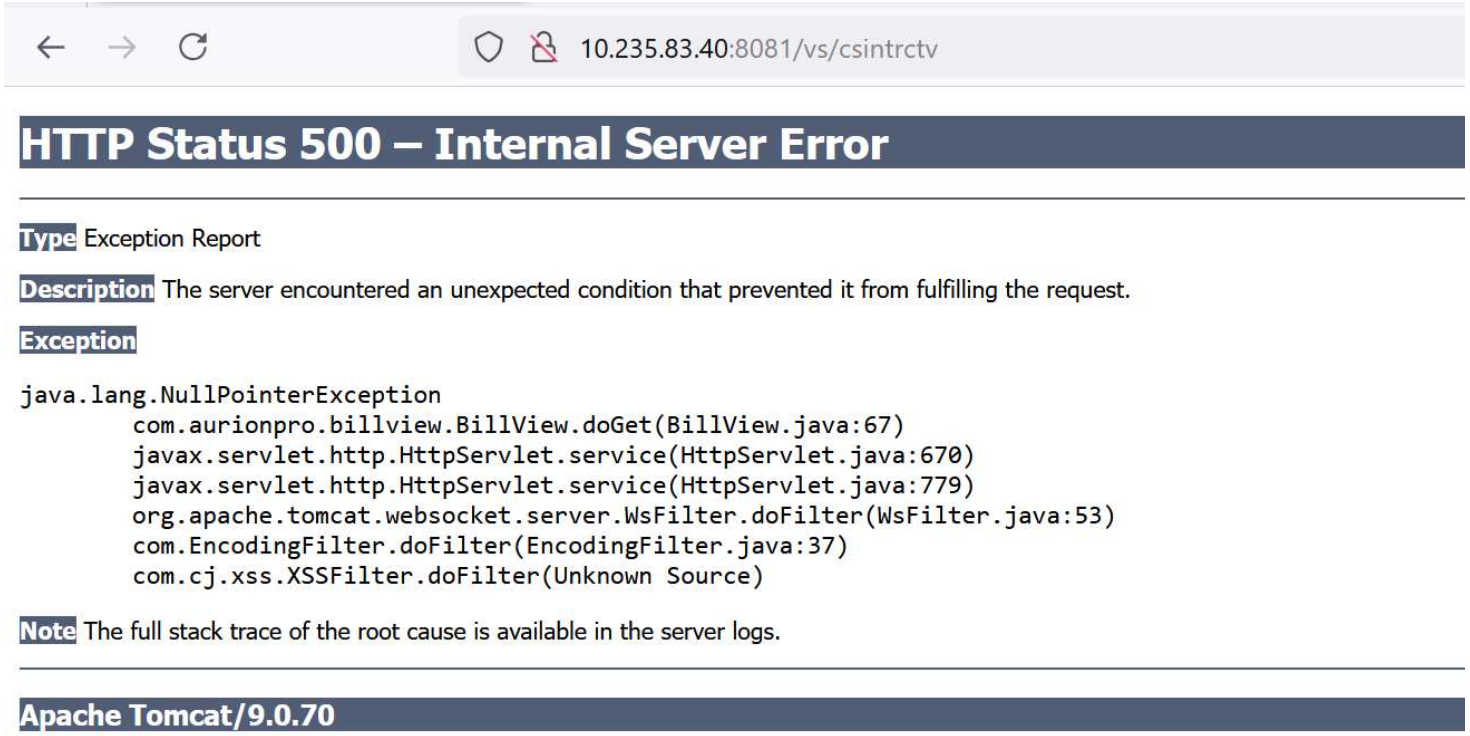
We recommend to implement custom error message to prevent information exposure.

Retest Result:

Retest result shows the vulnerability is fixed.

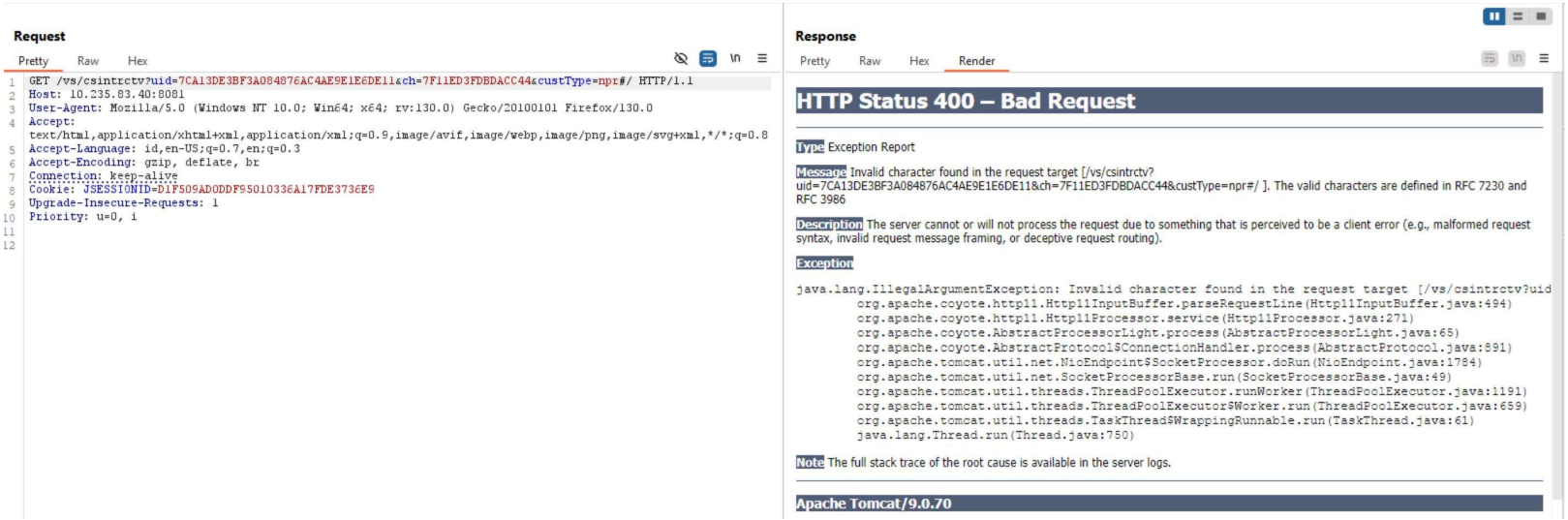
Graha Mandiri 2nd floor, Jalan Imam Bonjol No. 61, Jakarta 10310.
T: +6221-39834116 F: +6221-39834114 E: sales@xynexis.com

Error Message Information Exposure



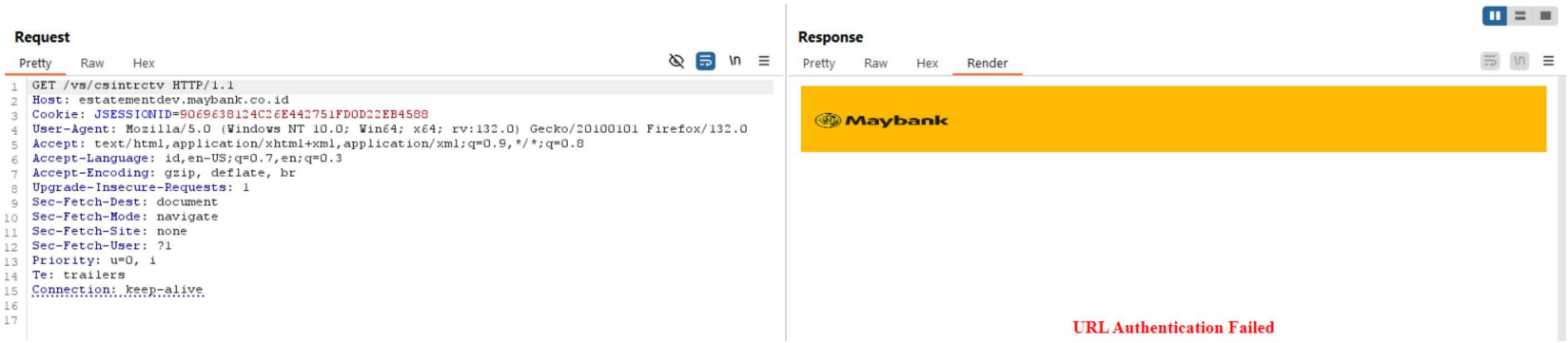
Graha Mandiri 2nd floor, Jalan Imam Bonjol No. 61, Jakarta 10310.
T: +6221-39834116 F: +6221-39834114 E: sales@xynexis.com

Error Message Information Exposure



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

Error Message Information Exposure



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

Error Message Information Exposure

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

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:

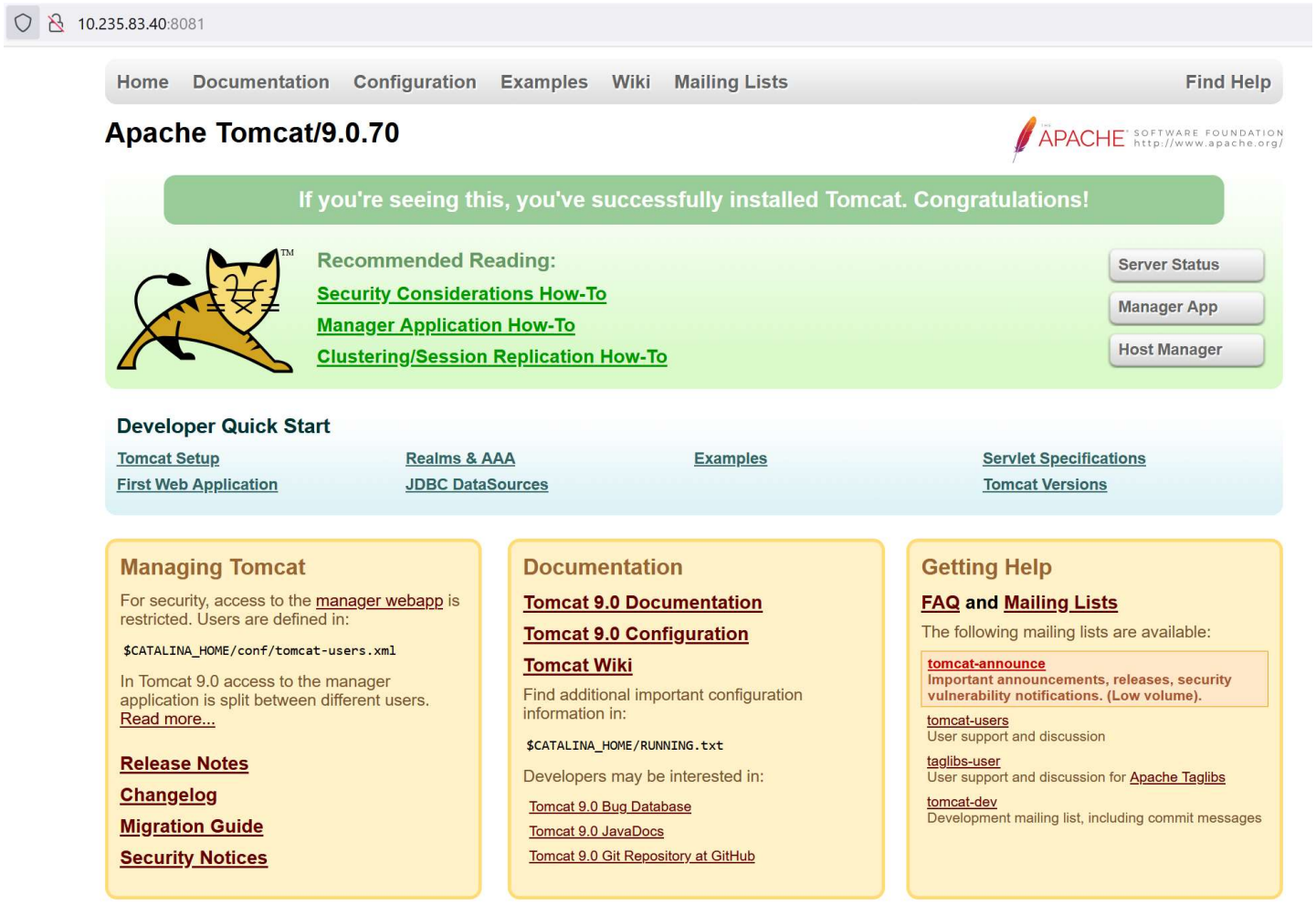
We recommend to implement restriction on access to prevent information exposure.

Retest Result:

Retest result shows the vulnerability is fixed.

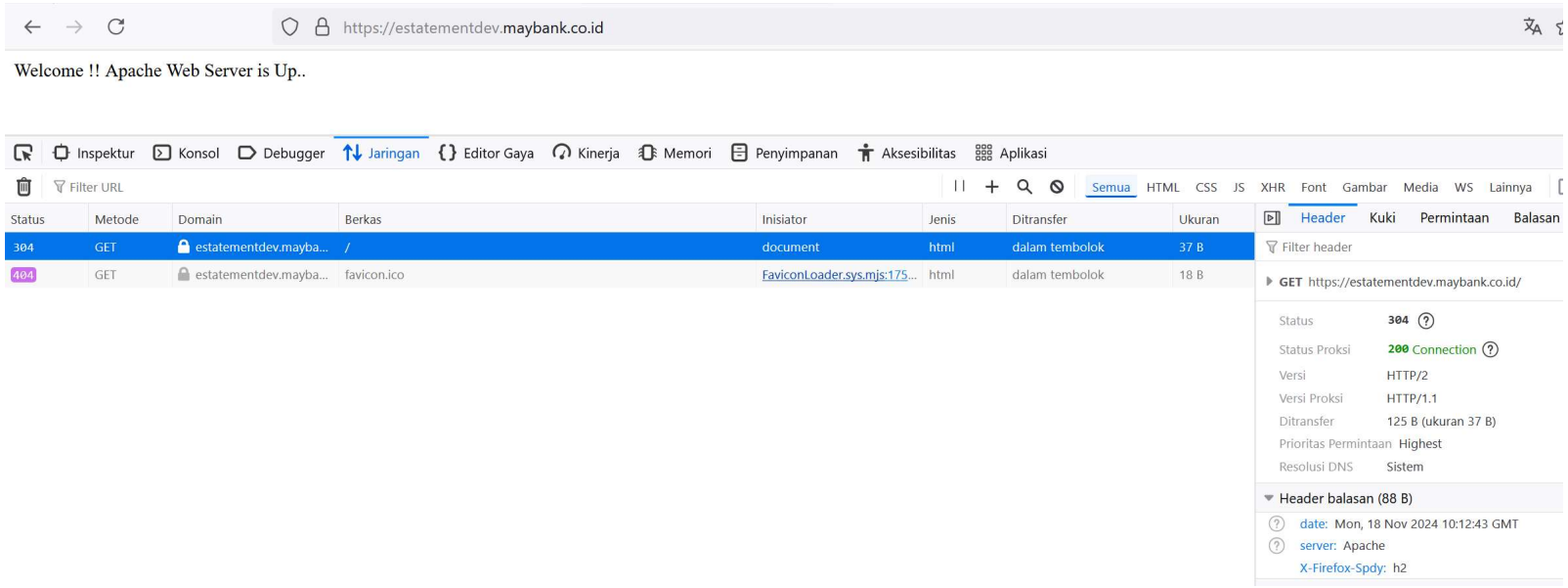
xynexis
Graha Mandiri 2nd floor, Jalan Imam Bonjol No. 61, Jakarta 10310.
T: +6221-39834116 F: +6221-39834114 E: sales@xynexis.com

Default Apache Tomcat Page Information Exposure



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

Default Apache Tomcat Page Information Exposure



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

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.

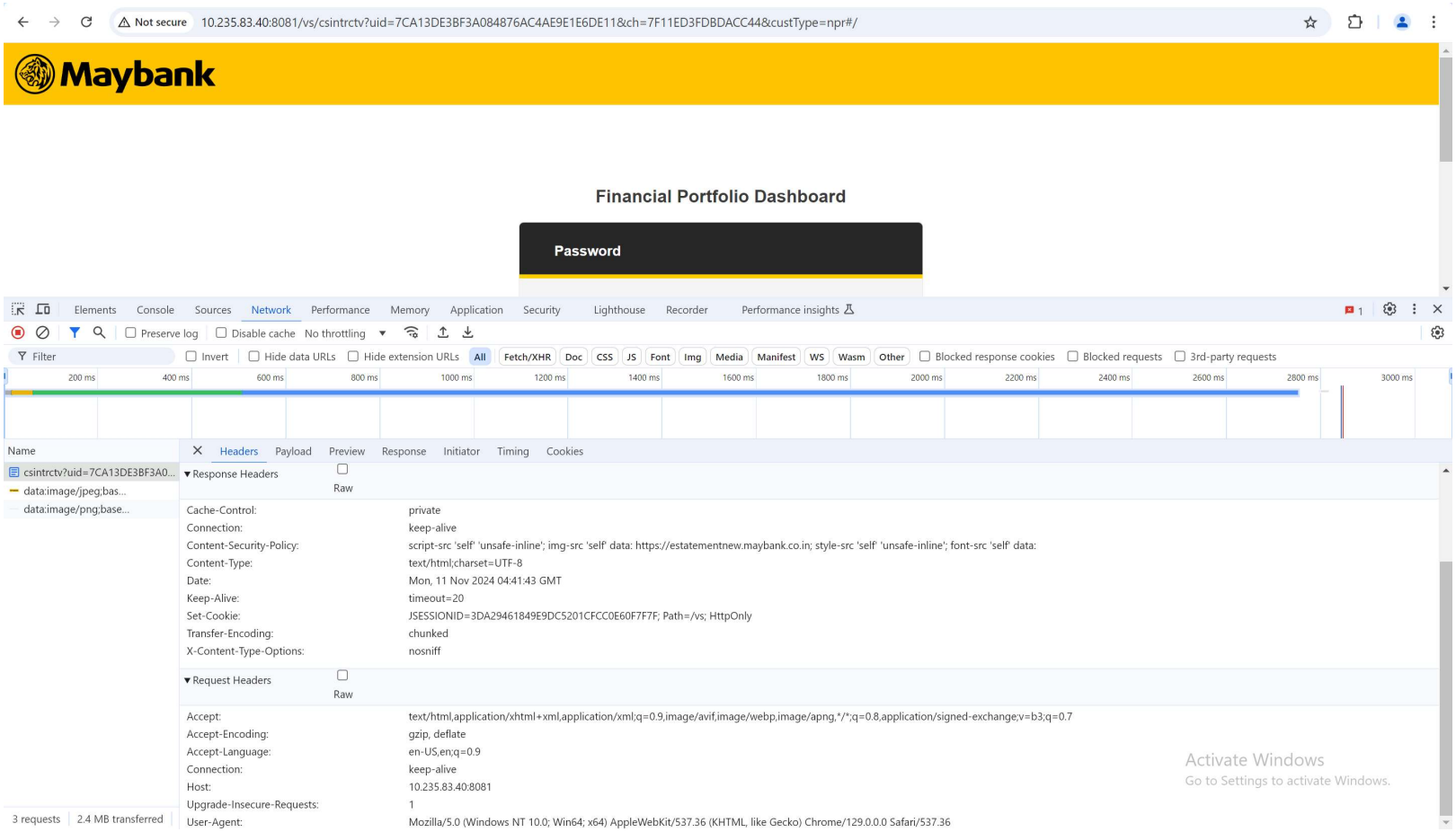
https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Headers_Cheat_Sheet.html

Retest Result:

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

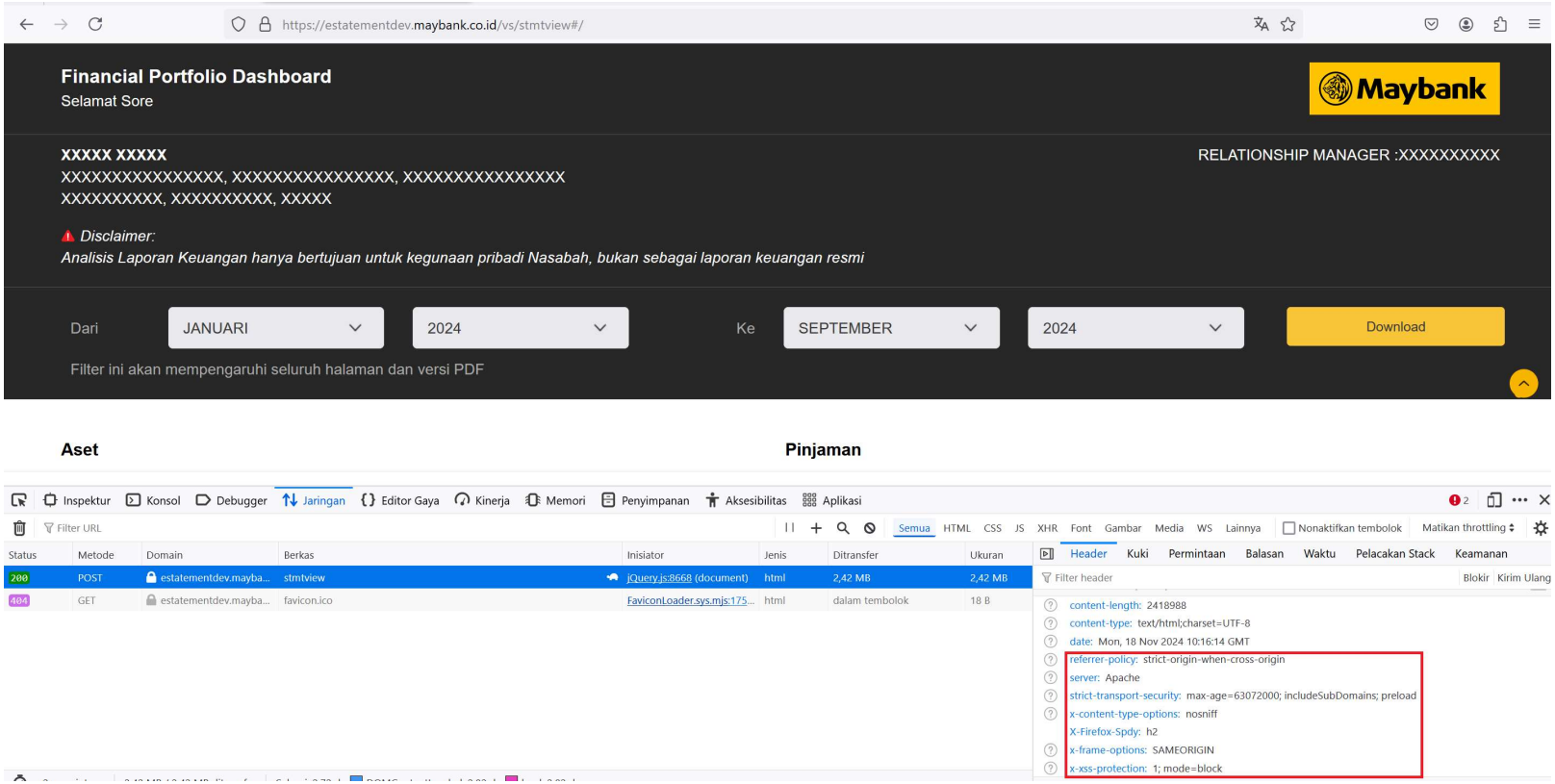
Graha Mandiri 2nd floor, Jalan Imam Bonjol No. 61, Jakarta 10310.
T: +6221-39834116 F: +6221-39834114 E: sales@xynexis.com

Security Header Configuration



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

Security Header Configuration



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

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:

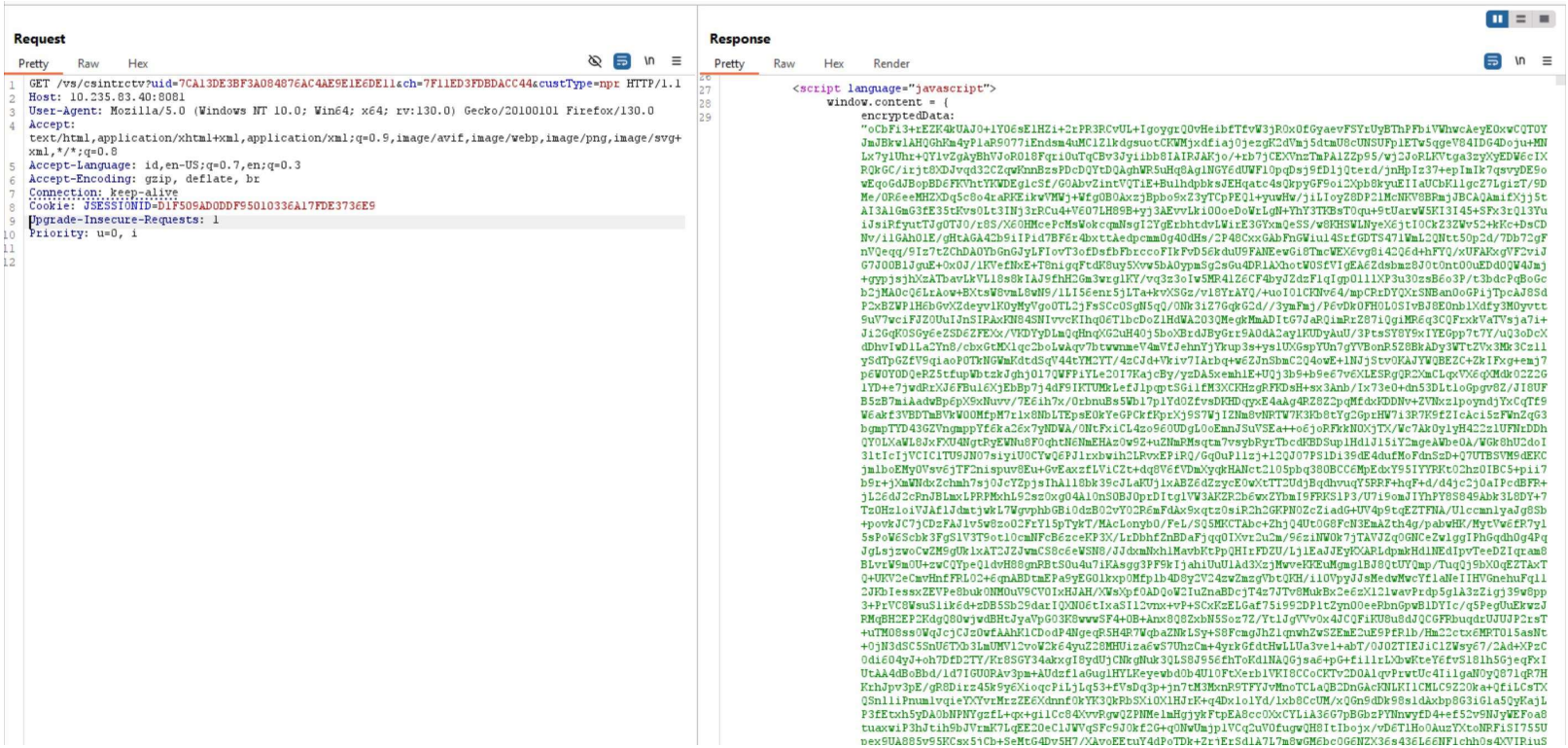
We recommend to implement verification on user authentication before the data is given.

Retest Result:

Retest result shows the vulnerability is fixed.

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

Business Logic Flaw Data Breach



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

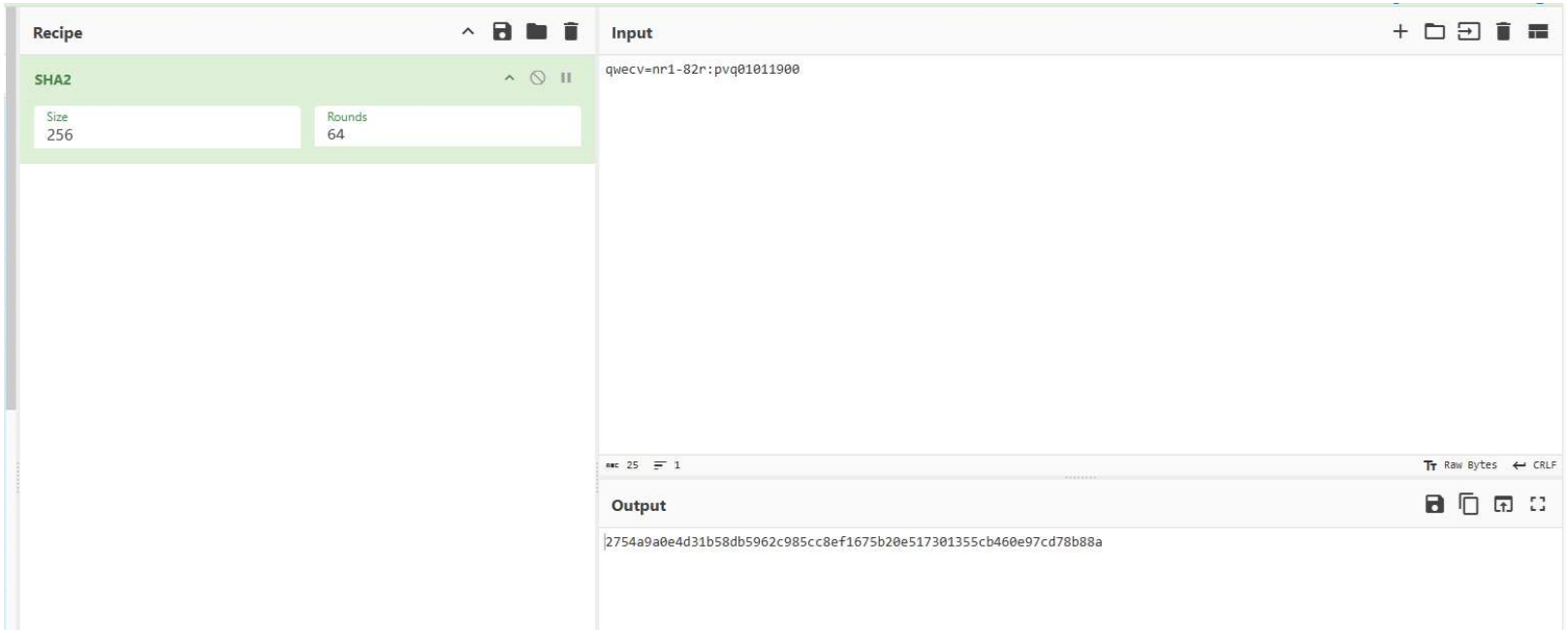
Business Logic Flaw Data Breach

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

Business Logic Flaw Data Breach

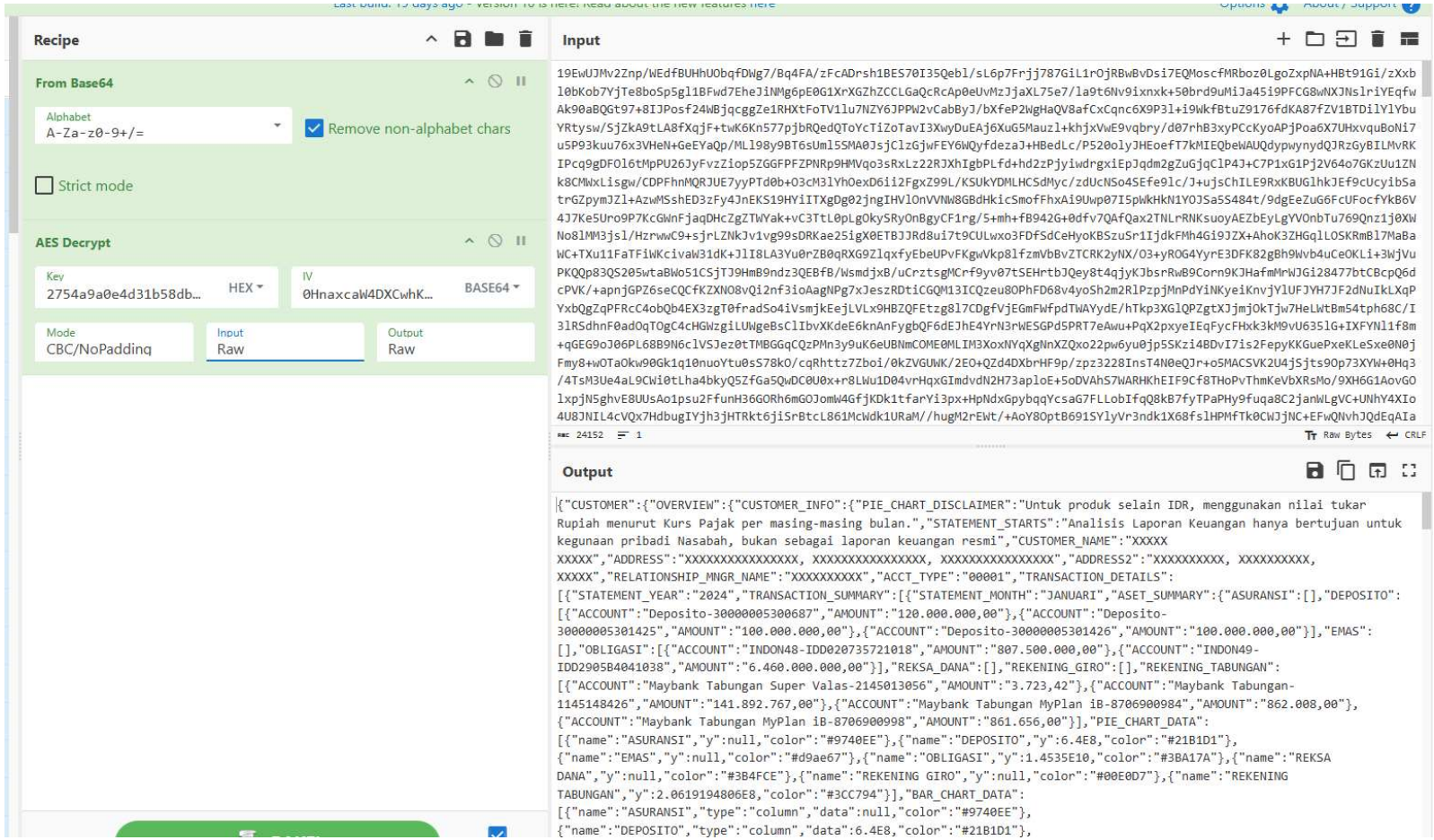
Graha Mandiri 2nd floor, Jalan Imam Bonjol No. 61, Jakarta 10310.
T: +6221-39834116 F: +6221-39834114 E: sales@xynexis.com

Business Logic Flaw Data Breach



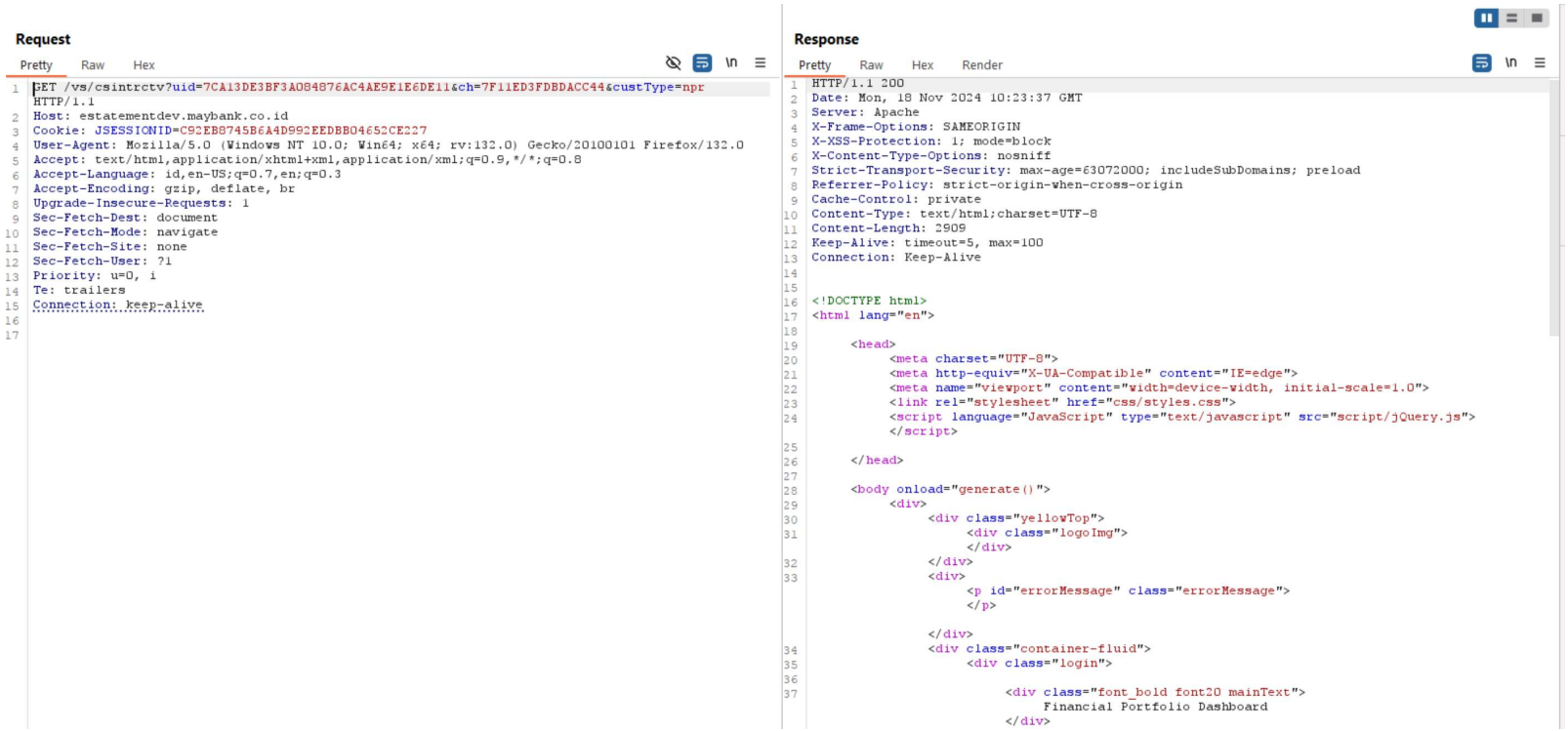
Graha Mandiri 2nd floor, Jalan Imam Bonjol No. 61, Jakarta 10310.
T: +6221-39834116 F: +6221-39834114 E: sales@xynexis.com

Business Logic Flaw Data Breach



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

Business Logic Flaw Data Breach



Request

Pretty Raw Hex

```
GET /vs/csintrctv?uid=7CA13DE3BF3A084876AC4AE9E1E6DE11&ch=7F11ED3FDBDACC44&custType=npr
HTTP/1.1
Host: estatementdev.maybank.co.id
Cookie: JSESSIONID=C92EB8745B6A4D992EEDBB04652CE227
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:132.0) Gecko/20100101 Firefox/132.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: id,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
Connection: keep-alive
```

Response

Pretty Raw Hex Render

```
HTTP/1.1 200
Date: Mon, 18 Nov 2024 10:23:37 GMT
Server: Apache
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
Referrer-Policy: strict-origin-when-cross-origin
Cache-Control: private
Content-Type: text/html;charset=UTF-8
Content-Length: 2909
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive


<!DOCTYPE html>
<html lang="en">

    <head>
        <meta charset="UTF-8">
        <meta http-equiv="X-UA-Compatible" content="IE=edge">
        <meta name="viewport" content="width=device-width, initial-scale=1.0">
        <link rel="stylesheet" href="css/styles.css">
        <script language="JavaScript" type="text/javascript" src="script/jQuery.js">
        </script>

    </head>

    <body onload="generate()">
        <div>
            <div class="yellowTop">
                <div class="logoImg">
                </div>
            </div>
            <div>
                <p id="errorMessage" class="errorMessage">
                </p>

            </div>
            <div class="container-fluid">
                <div class="login">

                    <div class="font_bold font20 mainText">
                        Financial Portfolio Dashboard
                    </div>
```

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

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:

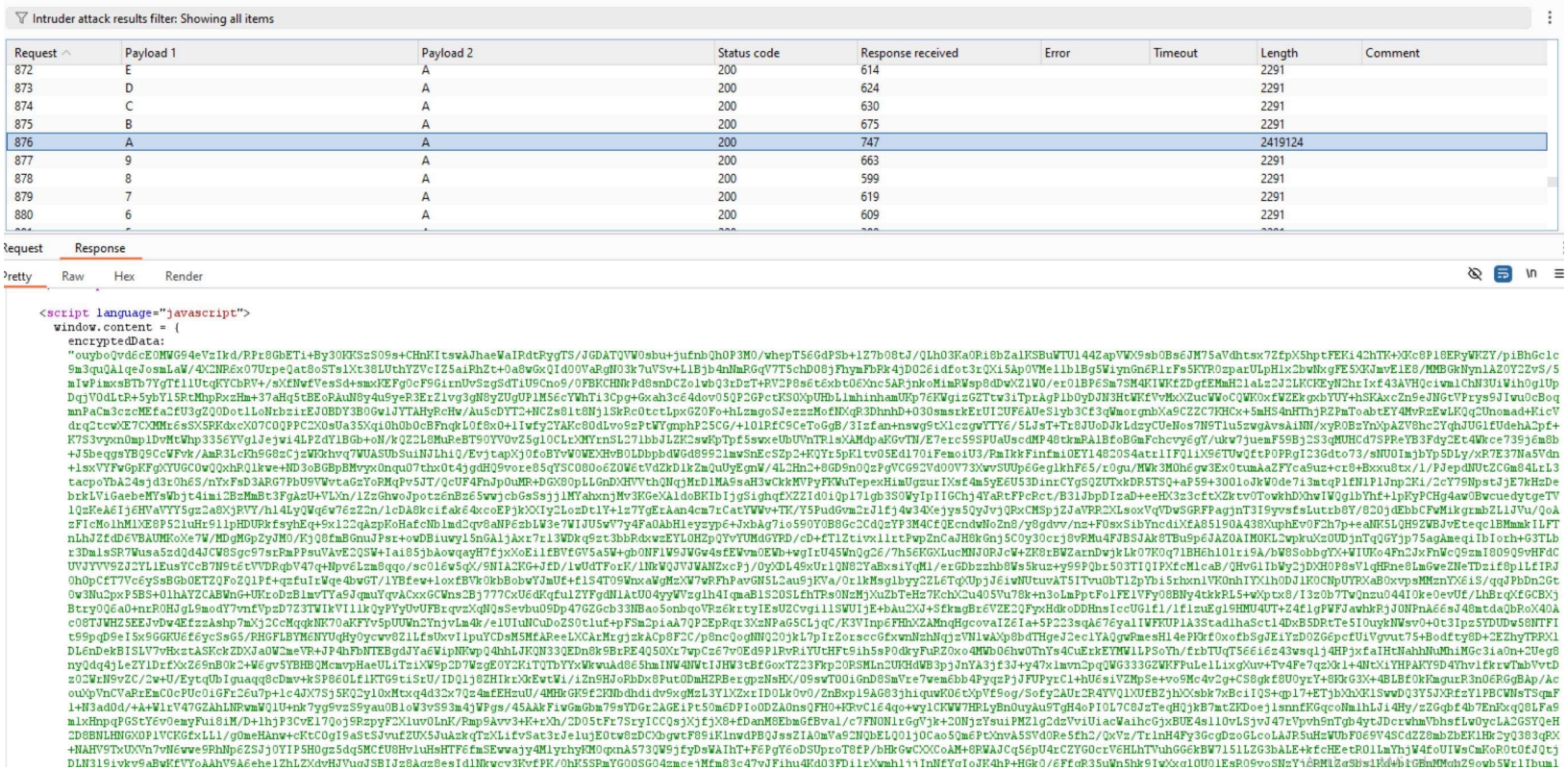
We recommend to implement limitation on request, for example using token and captcha, to prevent enumeration attack.

Retest Result:

Retest result shows the vulnerability still exist.

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

UID & CH Enumeration Vulnerability



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

UID & CH Enumeration Vulnerability

Request	Payload 1	Payload 2	Status code	Response received	Error	Timeout	Length	Comment
0			200	551			2419124	
746	4	E	200	366			2419124	
879	7	A	200	354			2419124	
1049	7	5	200	356			2419124	
1	Z	Z	200	175			2259	
2	Y	Z	200	174			2259	
3	X	Z	200	67			2259	
4	W	Z	200	66			2259	
5	V	Z	200	76			2259	

Request Response

Pretty Raw Hex Render

encryptedData:
"tUqVWh9/15CEmP7Fh/7xC9I6i4ésI53+Vf8E9j0rB831ZclFFk/ApTyjwE6ba6rLrF518K66o5Y0N7sBW5ZEKIUZy+VSfcN0S3XitcHpqi36IFSMRrCTXdcPA2PLdRXVRqYE6ZyJzX8qA0oh1/f9RJYLoVN0WMGy3779uJt9Yn+SR+XCn8Cj Dn5LP1CX4qIYEeHf5xI3RRim+P2KwhS
HZLu5gLtChRzjiLEBrPSQFuiS+IdDWnT/uCLcThKjHHPEbXJ+gjYHlejdESKhhGVVBIOrEKLtlo16JZt1SUABRWX/sl3FxgRM8WzWalcEHDXmN3ZW4lXoydHaZcK2r7IoTZNuYKAPntfsRe+TRyxPV5BAeio8ev9rpSV2o8ecSXufxiJ2rdtQ3rTZyLTdG50w38I8z0nDsTJ4p0yymaR
nnmAW+ukDLNWYU5/mTlYAyRdsRj8abDBbYOorTQZ+45rEXMkAamfXXpPbAIFXbSQpywLJEiGx3Ujs9UByAYAO6nXeacyC8A9tPvIWAYYrNDNWb3c4cDY52NxJs5hOHQxmlFbzzlefctS5bJlob/I9ANE0Tho0EN2ZGf15BEjjyQpdCSgFMyATHzQt/lwtIzqgtVq22VP3RXp7Z8MdmSg
qGeRBjgVmdXzXRjJmJjiwOgrb4mTDMPwcEu+rb4gwWeba+BYKk+hlXJteFqAFg/lAoXSjlDVCBvdMP/Lmpz1P3AJZP5Z505dRZklg6Ig9wm62c6yTYVRSE3OG8TJ7DkUlKV8/0f8YBM5m7GaAul/wdqQVwAK5NhvesRwiCL4fwLzo5ni3ABmSpkpdbkh8pGSGGbKSHAcgNXlUW4e5uXm
njJ6jriCwizNrAWCt6qSWJtVX0TMqQukJ53vEw4qplYZM+fAXuaEkjarH2Y4sQd+YAZm4hpxL7Upt75ePéSZ8hcyW0bF305k0dlAgv2RJH37iKzoz74Z5Yb1G5sXEnB5JuZXEGA27qHnlV1qZULu2JR/MGeR0RZZ/b+OoaMh9Hj1EH02hUuADTpYUvk3XmtcH7MqHlRyBes5GRJrWro/
DaAciDyrJJOX7FtdCH56WNPnFmQErsHhha+L7ij/wXBnjUCRLFIHncZtYODfvjhMBsPEHdr8SP8NSRW0nBhSo/fEEYvtY2j2M23jsRYblmZFéGm0xU6qpAnqJfLNZzmX5ob30pV9AKz//p6M0I+la+r7T3BoW234Qcg8a643BZMc6DG4HYwllQdzdxArRg+lQRcXzjgj0NnIpT7KoMGT
xYDxa0aJX/DEffMmp7FjcWQ13XVYIaKQoxYQHZ30Biz4h3mv/gJQYZHcz50YfWSKI/6M+9tLZHtmXOQMhaP7qJ4F6B0BpKNL0Fw0Dkkk9G+8jSXWhZccm/p7ZA+Zk83reMJ66EXb9uTcGBUXn9KW7tYWmjl57Ak QlkES7Pvaib43lj/tzuw6lTnfYxcdDK7GDlYChCqFJFdZRFiqDiX9
BtuV86SRC53jMg5BkNvlLGsn3orjPgVs74/+vX5Pr5iWc8Hm+2Fr/TSntY2R/LliUl7bEfikAKrc4vN+PRFPkqWeDcFOXJCzllUpUsbKtKL+CwbPSC5YGBA2vVR8+BqkaQ06lKlbPDiz9LGQoMjP0SGegq+DXMEHPD8TcFKHiWiyX++rC5olatxdHYYDVmU2SG55VEgWugGRs3kusekS
4q8i5MSqhlg54/SPvjWZh5BK00RzQmog7CvWrfBdjAQukTMCnQPTtp/eg2Y/07SpUqT5rvScSlehjkV4HQyzgqRrSzHkaQrVrsav39s7FupX4FaBQ/GGNMQwT77UCXvjJYuO8gAb9E+BZfy2zc5Er4FBUZMm/GZ8zZLYWfU9yMfJNm3Yg2X4H5afTuOG/oSEUnyJq8qtX3RVnL60JNK/
w6Nb0dBe7mzZFyBHfIRlWMvvJbz3KNa2SigZfYuuffjCIKbjpqPKLW4hlPrKtwlhpgxRxzw01084f/8Pj5n9lj4zGY/8wqjtUr+3J7l+5xBZT3s80V5n4kl+lhjPVxOq6jS2uuMvlD8CCrkFQOmoHR0wQu7G4OFb48ULkC1M/BMpesSWJuwwTTJ3YuMzqzOPbTHePuL9rIo0nopMEL4o
ZX0kaL5DZvoSoCBkw47ztsiAIOMt+qqjEQXIbF2Ga4ve18g+cbjOJ4V1XlW97N3Q/42cPyrSJPkjx9gaC2lY14BL0TddKqBhQxFg8DNypg3n8malKKKtNGbwUUJ1Snvn4KVqDvccvgwqT+WTDzoPY/xA/iEmGx59oNvsgzZOOO+YGCbUbuKucZ2T+Qe+td6dU5Xxr/nDqYEo6+BGkmQ
iNWRaVaxir6AZ3KxUxmZUchEKg7AUb9cZc8CUjKUqxe///E9kwJ67JTEGjwQqzHJhDUaltt93NOh0Qd6lPOnqTVGHbWg9+tSJ5LmKiM/ih+ILwVLXT+gaJookY8hHfVWEMnYMsEBHhGocaLPbNT+f+OYYtfNASKi29+UzkEZufp4lciobIoQAfg5ZoGGh04PqukLJZybQz6i2OIwexh
/H4XzUoxefB27e9WQE2LAc3uFWmUOy0V/lNAuMbfO9KcHWSA8Fw0DNwJmJwqETzUpLiQr/8oLDcWljilg7TFfHPWO73H0RkQNjgA43N0tlTHhsGlbHsW+ZWmVmXnxe6tLpWqOokYraXyCIRfBa7/nWGAX85AaDbKUF0L376uQkQAXGunR9/TJmkS/x3Ek2g6XIagmlLAcfQrrxXzoEdH
8e9X+7aQ4xFJQdX/TpYaynZMNConuIWP///d0ggaMDSUgCh8WBSETgE9kPL26xe5G/dbZW+N427uLK2BkbPfPHn68IofqqOaEEq3YLwG+QLV5WYjR+20P5DwxeQRcxD5RZlpbDthgrwEBw/Fjokqcy4uCWPHIa6tJ1r4MbRzkrfF0axUmVQtVlZDgGDUi700vTm54rhlbUn2Su4JjYi
wGXPslfTkhYOMyerR0mmFmpXRrGgl+hNR0SePwyVSLP02qgxMRGYYAG9JQElxnA7FmatovyuOiffEfoP4vtZ2vrMKEyYlzi22IePvowRi2kzwZ2FOCG8zaqX9y+9V6ylxfPIPwIVFjvNr2ukn0SRZYS0a7/049+sKB/AoD/XSG3UoKxKTgHzNAGV+NQA5ZiLH+oE
sPh4SSykV2jarEExMCe2qih9IMDWpdfVo4vXKYjd93PnQ4XfKhpUp4kZzUVRzGJQgZomtEVmtg07d5iGrkfjP4w3ZMYcwIwdo4dKyg7ix9iKUibH8YFRydRuUlk/S2nKoDayOufl7r74gDpsP4Oal3uC4MaAEJnBqL9sScdagpQH3oOKDmYo7OLjjixFlLG56?sp58/llfFD/ZmIeHLO
MIiTAGH5aeTR4/BMtbRVdBzHIdyZhYqwbQI2cceHt4fpR5AiRJdTlQbuNlie1vKjgC6Gbg72Wor9+AQ+W3+SDpcuYKeUUn07DXLunFewPlZB9Q/FWHTOpmkmo3JoOkAH7SuGY703GnFsVC27GHlle3PyFtMTP3902mpAckUBitRkNKnh//GbzGuWVHimkvI/ipNxIO/FPjxiKd+Ypn
DnMPRpvIw+9AxifvR2jYZBhohESb2j/Tha5OEHk+UWLSEtvnu2+5w2xCx/Nt6DscqiEUXgQsajhEwqDP08x2qEpxhN8rAwsIuLDfvDiycAGy53IolDOcomEN5wLZkklYef/+iGYqSU0iCWmms+eHS9Vzz/sjoPFK2/m00DTGbhN7xPMgynbcBFUU5Rbe+X9SiUSkiUwDpt533xZAND
twRcxwkhSRfBZ+bxrS2iPallM33VJQ4CZKSx0jXFzZh+z+9nzNWUgZW+dDMfdDyXuL2DGpcqHqalt4csmzJhA07NsHYTkpqORSRAiRRrXFNBlP4dkvBbP4D+UHJLf4I/YGEtras4ejBbO7TKoDNqiZVHxkBO4D+TJwiNnjo6Guk6ZVPcYvWWED0ctDA
XHTgQZ7S3t+4dws8l9i84450etqoa2nGJHOA2toy/JqBhk1lWBdlR45AVi6N2FTY0jgGAzdb7Qppj3AAydjr1d5a2d3S52knKlHZO4hi65e3ejYPHetW/WpsXFx4FH+fblz/Zyhk6oF1C6SsXfY6SuzSEUgEsqehFWBhqXCTrJutmj4E7usL0l+rHPRzy345Zueyxi4BJWVljpICTge
gdRJ5I/jQd06hXOd8VaDF0uB48tbhz5ZJhzkZ5E2SqFm+NJPFlZfYR/T7CL30YXFzvjobgjIRDuIFTu68r5HSvslélSdq+8+pslcMB+nLdFVqfF5eQe7SyctHlWmVyyAO08kIéa7Fi0DfqVO7ms15TujNUcWaOErtZjlCEh3mdan8AqjBloGp/WPuYvlTjSYPJ10Dhi6HGo4IaTHwv0j
dcmVlAqPU7w8VVxS+Lx8kPkn+cn3C06nA+PaCt/gopENhu2TqR3DAYNwoD18GWyBjsK6kLalAJmqD0h+HbgmiGSsKDzHkEe35iP4rJIzévI+dBPQP6UUXbqc5us8GWsbsaQQVfi7ZwtDcwxPok15oFhQJ6swA7nlkFFrPpHKgDisbRNClkXV1GSE487ySV5vXpltQJ4ZK3DXNfNlEVS
wZOcZtJSwv8CyHInPqhNDJHgSyv/loI4//SDZMUb3ixqmknfrAWZz0fW49cz9pmWupAi0sxhuLc2de7TuldskFxlpmFML5CdgcWJuLBCRNZ3YYoKZ/uaMlcX53QxTSTGysge5n5zJhbIqO/PSR2XKoGJ+STS2ulWbf67M4njZDéGlkéGAM8BfzVvggi9UnU3pSoQJuPLOoxXqzaRiEru
lmDiFaTxVvpN5K89QlNpLXak6CISty3Kr6RT8CNUJMlqwBV8Ml4e0/NqkohDWwHC4UmM6SnbEqFmel+7wxe9tEggPqauGKlMrzW/N9Tzfs5jg03R7fETRR6AtWlkg/v9lDE8DIcmN7Cz2EdJQqpLtj/SbU+lG3hwyDTK2gkatO50AaOfcl7jBOKTZoxylGB229lysXVaqNZ+uw/QmOhx
Ry5Rr5gcSxWYdLNDNPiaPgQXyLShuok0AH5TTyEXZYFXUvgcRHCCE/PNLKfu7+g5w0V1eG4DL17tfzQyk07J0ML04VqFHgl2W6xp6EpkyhAUnU8OZmw8dKDtN6bVc8Q+seZ3l5eyCArKvedZ1USPRwPeGxmze0+Xi5p/zZM422SUdZHnj8ZpTeYykhLzWWlEys/j9a4M1OhX0ij0R4+
r+gdb8gNzUPgieiE14VL9sHSkLJw7xmSrLqJYtVQMdGzM4V83USBYIoUwZKR6+0ZJ1lSzyP0ttFD/ZoxWv2fSWfC7PH6btgTLX8DLFATHlc2phlo+KL/M7UiDXeiU5qNaIJVyQtODqoArvNPBo4ePlCUwGGYN/3umdseemwqxoKztXEJg2nTt9vUAFW9L3lgiu5Lagjo3igtrWgSHtdr
qZDeaq8vCo+U+z3rnMp6F9WCtv+A2lK9EgmDpHVrHlas8TqVlXHpgq3VUPQQwOJRe5bCa4X8tDp0AiZu+q3VSaNn706pPwtMcU+THVL+aWQg0lNGnJcMugmrrzjJPCRixValRF+5G/fDdXlJslb+4de9c055uPFbE6iTb4wGYRUBllyBb4sE0GIBSHUoJ70pSlGiZFCaSYRhFDas+Pdd
7UtxgQSBq2aLgxeHxLKyDkNBohALU+hWcyMclpvuMbTdLlKFm9Pd2PnL94gk03NMZrRSPRXPqFY7KAqn72IxuTBUWjUXL//mYoP4/HwcObQ2XQi7Sh4d9oOhHZJSpbmgbl9IGE8at96jwojy2CGHl2+NJhqnoJTaFhhP8Dfv8N8LxBHCT4BAEuuZmXQUJ94+x901QSfGv9S9VzTQSAzW
2zXLH5RHylm8Yv6IB/vmiWGjFflv4P3dZyTFXKTwIBGkt/sPfqHjM+ATEEaQIYn+gFf3Wq4SGaVj2xHohOFyfixApratFdpZAi0q+ekciyancQx6HXr5DwN+A4iTLRho3IJ817z4B44KkbSAcOKpg6H32FrpDVYt2e2XUikcwMfVyVLGWU3+m83qUZnAmjupJrFXDD88jN0iZJ+DqVdl
MDOzN2bSkko7kMi5gC6GnLKYi/V6CC0VI4oAC2I4f/gaQs4e4MH2vgcFtF8CRBSbd9hXVKtAz/M0ulc4jfwGUkEBOepWse0svcMqKoks7K5lZp0onab1ZNWF6h5yUGQmETuhuE4B3rlMQ8RjJ87emvJavQUuvKcSrdYqfxQ9DkJ8yRHjpK+4JN7M3sjHL9Wg0lK6d23GuXOyxpWDyPpz
DS7mwQrxIts7vwwAgq43fbeVXtqKg/BBhTytSzkslwSwIXbmMchG5f70kq2NBgYEXrQf2cJivSWg3qEVp45sYjWNXUaGi17DxzGgvJ+lvA7EUashWk6vlv25JBbMP8iDoQFThKlz+CzDnEDwURCoqOGzyvLvgDGoBxgAV9sihM27E/PZchw8rLNDGK5A5l2qImn5SqffdEc2IzkZTku5
tN913mFjlnLpvLT6t2bUpbH+Iyi6ONJmMz+lnLVelwvAji6eASnC0SLS7Yne9dVlA7m2w9fd+rKsrnneKHI/+UIM9u8W5Pusbqp5o90lEdafNXxCYixuPhxKxTzsc5hEX3MpXK/gAv6XhlG7P0ogkt6E43ic+TfqA/oVguqvv+DQW+QAWoAr0efvlxYyNhGDJFJPh03S9o/BRMzbeWLi
08+sUazvyEcOEDhmBnSnFFVamlv4VKUGa9344Lo7/QJvKnitLYKMXIh0HIv9wcW4gxQmHtyXWZsBJao8TTkxcXSSR9ah4svWKzfsPQOPC7o5joL6TuW8gZ58O/fHmTB3EWPD0BKfjktpGkaV3LAvu/2evFiilpawjCPVaMdiwzwqllQiQEdHPuGPCPwOAiSHZZyNM/zmcrFZFjnbsKp+

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

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

```
<form action="stmtview" id="login-form" method="POST" autocomplete="off">
  <div class="password">
    <div>
      <label htmlFor="password" class="loginfont-color whiteClr font18" >
        Password <br/>
      </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="refreshBtn" id="refreshBtn" >
        <i class="fas fa-sync">
        </i>
         Refresh Captcha
```

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

UID & CH Enumeration Vulnerability

Request	Payload 1	Payload 2	Status code	Response received	Error	Timeout	Length	Comment
961	Y	1	200	51			2537	
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

```
<form action="stmtview" id="login-form" method="POST" autocomplete="off">
  <div class="password">
    <div>
      <label htmlFor="password" class="loginfont-color whiteClr font18" >
        Password <br/>
      </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="refreshBtn" id="refreshBtn" >
        <i class="fas fa-sync">
        </i>
         Refresh Captcha
      </div>
```

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:

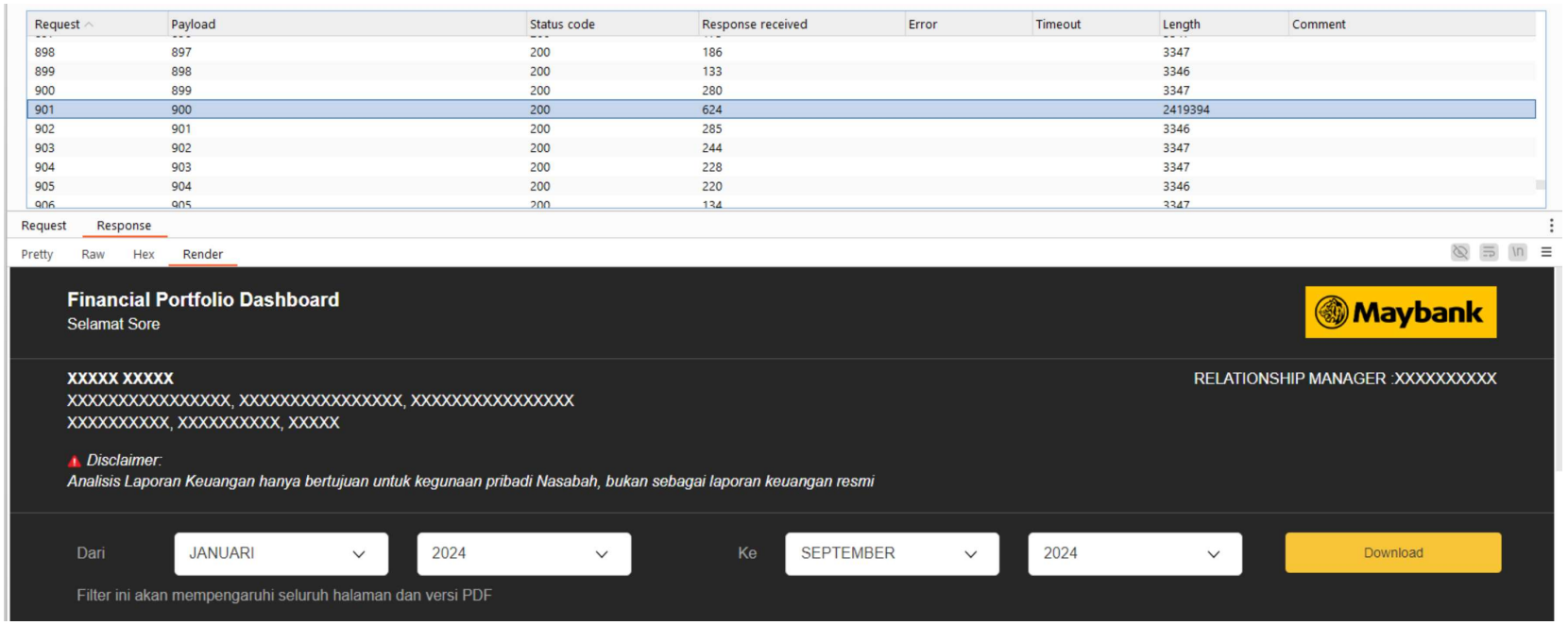
CVSS Base Score: 5 CVSS Temporal Score: 4.3. CVSS Exploitability Score: 10. CVSS Impact Score: 2.9.

Recommendation:

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

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

Improper Captcha Validation Password Enumeration



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	