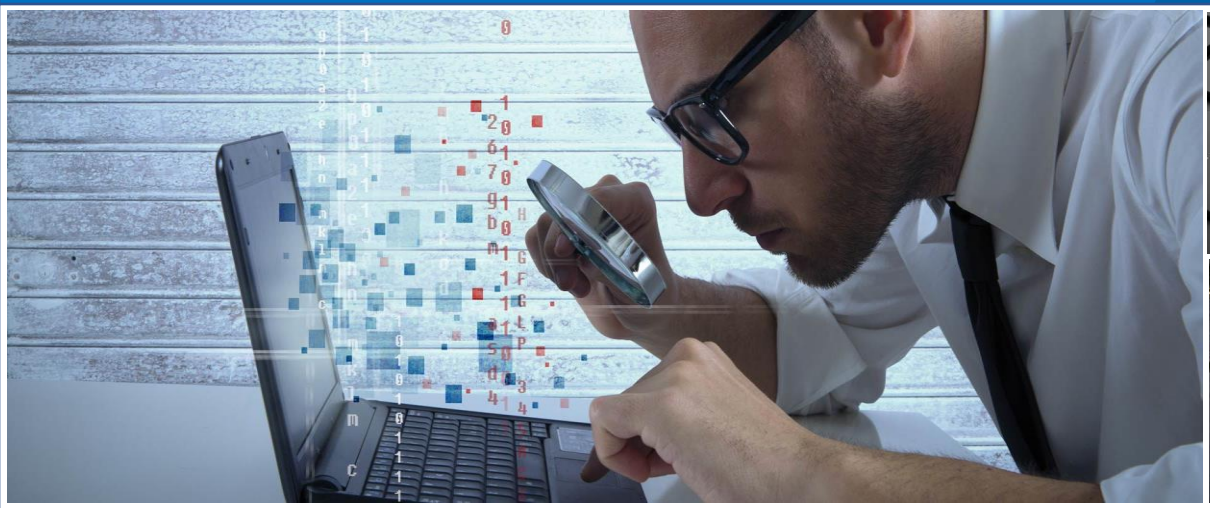
Summary Initial Testing Report

Black-Box Penetration Testing

Mitsubishi Elevator (Thailand) Co., Ltd.



SECURE SERVE Co., Ltd.

MITSUBISHI ELECTRIC
ELEVATORS AND ESCALATORS

Document Properties

Title	Mitsubishi : Black-box Penetration Testing Report : Initial-Testing
Version	1.0
Security Assessor	Ravipas Chareonwari
Prepared by	Ravipas Chareonwari
Reviewed By	Vorawut Sanitnok
Approved By	Vorawut Sanitnok
Classification	**Confidential**

Version Control

Version	Date	Description
0.1	Feb 07, 2024	Initial version
1.0	Feb 08, 2024	Final version

Legal Noticed

Table Contents

1. Executive Summary

The digital security landscape is ever-changing, necessitating continuous vigilance and adaptive measures to safeguard organizational digital assets. Penetration testing and vulnerability assessments are indispensable for identifying weaknesses and enhancing the security resilience of an organization.

Following the initial comprehensive vulnerability assessment and black-box web application penetration testing conducted by Secure Serve Co., Ltd. for Mitsubishi Elevator (Thailand) Co., Ltd. on September 07-08, 2023, a re-testing was carried out on February 04-06, 2024. This subsequent assessment aimed to evaluate the remediation efforts on previously identified issues and to uncover any new vulnerabilities that could compromise the security of https://www.mitsubishielevator.co.th and 119.46.115.163

The re-testing focused on:

- Assessing the effectiveness of the remediations applied to the previously identified low-severity issues.
- Identifying new vulnerabilities that could pose threats to the security posture of Mitsubishi Elevator (Thailand) Co., Ltd.
- Providing insights and recommendations to further enhance the security measures.

The re-testing revealed that Mitsubishi has successfully addressed several of the low-severity issues identified during the initial testing phase. The actions taken demonstrate the company's commitment to maintaining robust security standards and its capability to effectively respond to identified vulnerabilities. However, a few low-severity issues still persist, indicating areas where further improvements are needed.

A significant finding from the re-testing is the discovery of a high-severity vulnerability related to a software flaw in PHP. This vulnerability poses a considerable risk as it could potentially be exploited to compromise the system's integrity and confidentiality of data. It is imperative that Mitsubishi prioritizes the remediation of this issue to prevent possible exploitation.

Mitsubishi continues to demonstrate a strong security posture through its proactive measures and responsiveness to identified vulnerabilities. The successful remediation of several previously identified issues reflects positively on the company's commitment to cybersecurity. However, the discovery of a new high-severity vulnerability underscores the importance of ongoing vigilance and continuous security assessments to adapt to the evolving cybersecurity landscape.

2. Penetration Testing Key Finding Summary

No	Issue	Affected Host	Result	Re-Testing
PT-001	Encryption Vulnerability: Lucky13	https://www.mitsubishielevator.co.th	Low	Low
PT-002	Missing Feature Policy	https://www.mitsubishielevator.co.th	Low	Low
PT-003	X-Content-Type Option missing	https://www.mitsubishielevator.co.th	Low	Low
PT-004	XSS Protection Header not found	https://www.mitsubishielevator.co.th	Low	Fixed
PT-005	Sensitive Cookie in HTTPS Session Without 'Secure' Attribute	https://www.mitsubishielevator.co.th	Low	Low
PT-006	Vulnerable Software detected : PHP 8.2.1 (New)	https://www.mitsubishielevator.co.th		High

3. Penetration Testing and Vulnerability Assessment Methodology

Penetration Testing Objective

The Penetration Testing project will be established for exclusive purposes following:

- To determine security weaknesses of the targeted system
- To minimize downtime by evaluating the vulnerability, flow, and risk that could be clause the organization operation.
- To improve security, consider configuration reviews.
- To Identify and exploit business logic flaw on the mobile application.
- Try to gain access to restricted information.
- To seek for approximate security control for the existing vulnerabilities
- To comply with ISO/IEC 27001:2013 or PCI-DSS for annual security testing or significant change requirements (if any)

Penetration Testing Methodology

The primary objective for IT Infrastructure testing is to identify exploitable vulnerabilities in applications before hackers can discover and exploit them. Penetration Testing will reveal real-world opportunities for hackers to be able to compromise applications in such a way that allows for unauthorized access to sensitive data or event take-over systems for malicious/non-business purposes.

The penetration testing methodology is based on the following standard:

- NIST SP800-115: Technical Guide to Information Security Testing and Assessment
- PTEST (Penetration Testing Execution Standard) Technical Guideline
- Certified Ethical Hacker Framework (CEH)
- OWASP Top 10 (Open Web Application Security Project)
- OWASP Web Security Testing Guide (OTG)
- OWASP Application Security Verification Standard (ASVS)

Penetration Testing Tools

We have Open Source Penetration Tools which are almost used by hacker such as

- Nikto, Vega, Tenable Nessus, OWASP ZAP: Web Application Scanners
- Metasploit Framework: Exploitation Tool
- Tenable Nessus, Open Vase: Vulnerability Assessment Tool
- Sploitus, Exploit DB: exploit database
- Burp Suit, OWASP ZAP: Proxy Tools
- Various hacker tools are up to vulnerabilities found

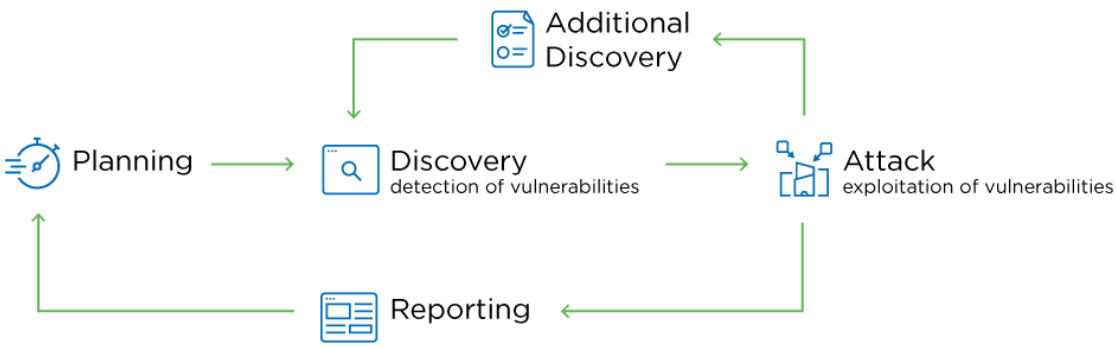
For Penetration Testing Commercial Tool are **Exploit Pack Premium Edition** which is used for exploited the target and developed next exploit code for attacking. For Web

Penetration Testing we used **Burp Suit Professional Edition** as a main tool to finding web application vulnerability.

3Es Penetration Testing Approach

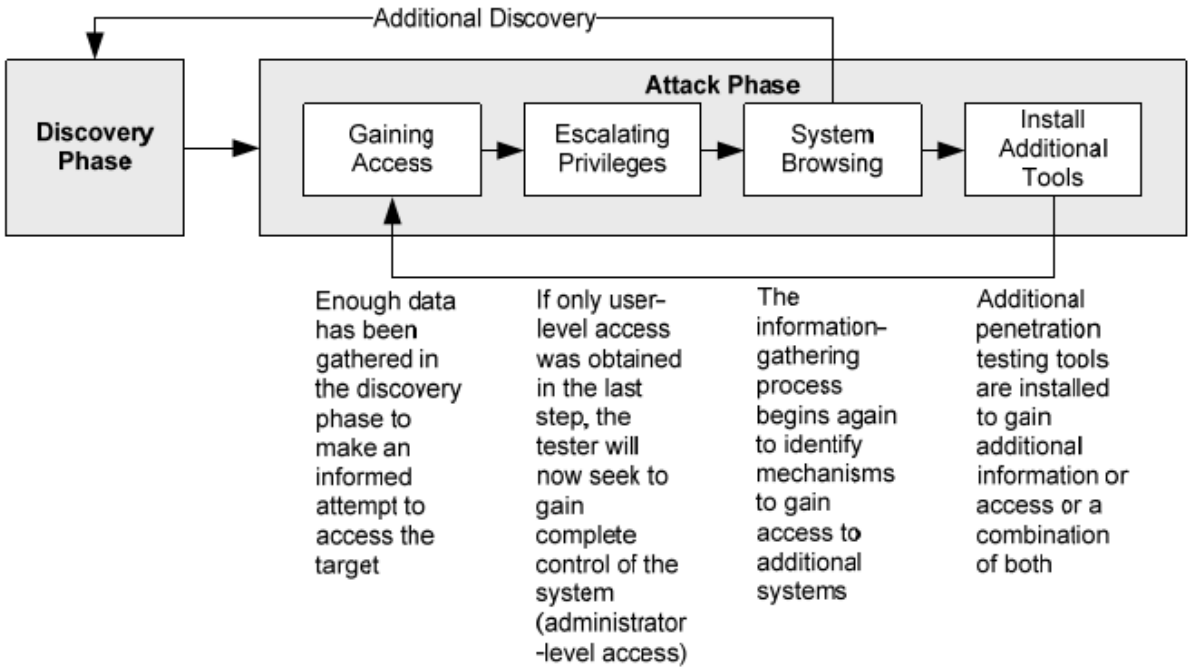
- **Exploit:** We will execute well-known attacks for 3 testing levels are
  - Infrastructure Level: This level we will focus attack on Operating System and Web Server vulnerability by open source hacker tools and commercial penetration testing tool by simulate real-world attacks.
  - Network Communication Level: We will focus attack on weakness communication between endpoint to web application for example Man-In-Middle Attacks, clear text transmission etc.
  - Web Application Level: The testing level leverage the Open Web Application Security Project (OWASP), a comprehensive framework for assessing the security of web-based application.
- **Explore:** Using the treat modeling techniques is DREAD to identify high-risk, risk areas and determine the impact should they be penetrated.
- **Educate:** After testing is complete, we will deliver a final report and presentation

As the figure below represents the four phases of penetration testing according to technical guideline NIST SP800-115



Infrastructure Penetration Testing and **Communication Penetration Testing** focus on Security Devices, Network Devices, Operating System on Opened Services that are used for the both testing (External and Internal Penetration testing). There are including 4 steps testing:

- Discovery phase
- Attack phase
- Post-attack phase
- Analysis and Reporting



Post-Attack Phase

At this stage, we restored the systems exploited back to their original states. This includes activities such as removing uploaded root kits or backdoor programs, removing exploited vulnerabilities, and cleaning up the Registry entries added during the exploitation and installation of programs on the compromised target, as well as removing shares and connections established during the gaining access phase.

Web Application Penetration Testing

Web Application Penetration Testing service utilized a comprehensive, risk-based approach to manually identify critical application-centric vulnerabilities that exist on all in-scope applications

1. Information Gathering
2. Threat Modeling
3. Vulnerability Analysis
4. Exploitation
5. Post-Exploitation
6. Reporting

Using this industry-standard approach, our comprehensive method covers the classes of vulnerabilities in the **Open Web Application Security Project (OWASP) Top 10** are including Injection, Cross-Site Scripting, Cross-Site Request Forgery, Unvalidated Redirects & Forwards, Broken Authentication & Session Management, Security Misconfiguration, Insecure Direct Object Access and more.

What is OWASP?

OWASP stands for "Open Web Application Security Project". These are specific point that vulnerability detection services are used to help pinpoint areas of weakness and stop security issues before they happen. Some of the projects work are a guide to define security requirements to build secure Web Applications and Developing an industry standard testing framework for Web Application Security.

An Introduction to the OWASP Top 10

OWASP is always changing and evolving to help web security professional protect and fortify websites and network against possible attacks. OWASP has becomes a considerable knowledgebase that experts can draw upon to them foresee and meet security challenges and vulneraries head-on.

To help simplify and proactively defense against these threats, OWASP data is divided into 10 unique categories, with each one dedicated to a specific type of security hole or issue. The OWASP Top 10 refers to the top 10 attacks that experts deal with and prevent.

Web Application Testing: These include some of the following activities:

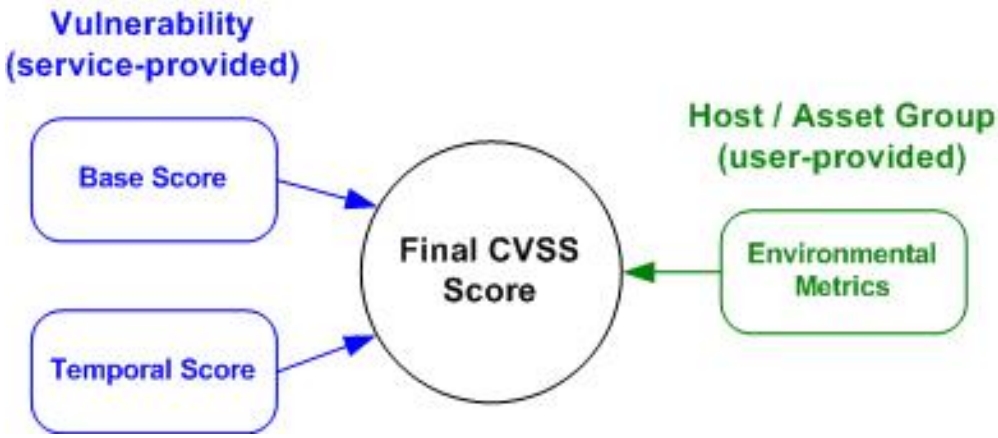
- Injection (SQL injection)
- Broken Authentication & Session Management
- XSS (Cross Site scripting)

Insecure Direct Object Reference

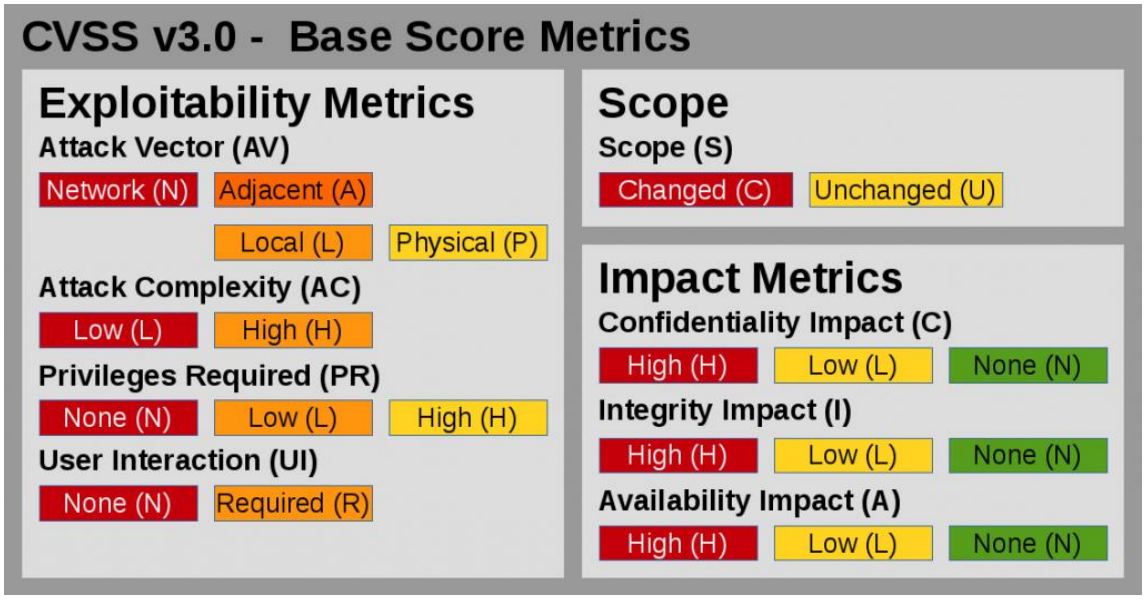
- Security Misconfiguration
- Sensitive Data Exposure
- Missing Function Level Access Control
- Cross Site Request Forgery (CSRF or XSRF)
- Using Components with knows vulnerabilities.
- Unvalidated Redirect and Forwards

Common Vulnerability Scoring System (CVSS)

The Common Vulnerability Scoring System (CVSS) is a framework for rating the severity of security vulnerabilities in software. Operated by the Forum of Incident Response and Security Teams (FIRST), the CVSS uses an algorithm to determine three severity rating scores: Base, Temporal and Environmental. The scores are numeric; they range from 0.0 through 10.0 with 10.0 being the most severe.



The Base score is the metric most relied upon by enterprises and deals with the inherent qualities of a vulnerability. The Temporal scores represent the qualities of the vulnerability that change over time, and the Environmental score represents the qualities of the vulnerability that are specific to the affected user's environment. According to the most recent version of the CVSS, v3.0 are



The CVSS allows organizations to prioritize which vulnerabilities to fix first and gauge the impact of the vulnerabilities on their systems. Many organizations use the CVSS, and the National Vulnerability Database provides scores for most known vulnerabilities.

According to the NVD, a CVSS base score of 0.0-3.9 is considered "Low" severity; a base CVSS score of 4.0-6.9 is "Medium" severity; and base score of 7.0-10.0 is "High" severity.

Categories of CVSS v2.0

Categories of CVSS v3.0

4. Penetration Testing Check List

OWASP Checklist

Information Gathering	Test Name	Status
OTG-INFO-001	Conduct Search Engine Discovery and Reconnaissance for Information Leakage	Tested
OTG-INFO-002	Fingerprint Web Server	Tested
OTG-INFO-003	Review Webserver Metafiles for Information Leakage	Tested
OTG-INFO-004	Enumerate Applications on Webserver	Tested
OTG-INFO-005	Review Webpage Comments and Metadata for Information Leakage	Tested
OTG-INFO-006	Identify application entry points	Tested
OTG-INFO-007	Map execution paths through application	Tested
OTG-INFO-008	Fingerprint Web Application Framework	Tested
OTG-INFO-009	Fingerprint Web Application	Tested
OTG-INFO-010	Map Application Architecture	Tested
Configuration and Deploy Management Testing	**Test Name**	**Status**
OTG-CONFIG-001	Test Network/Infrastructure Configuration	Tested
OTG-CONFIG-002	Test Application Platform Configuration	Tested
OTG-CONFIG-003	Test File Extensions Handling for Sensitive Information	Tested
OTG-CONFIG-004	Backup and Unreferenced Files for Sensitive Information	Tested
OTG-CONFIG-005	Enumerate Infrastructure and Application Admin Interfaces	Tested
OTG-CONFIG-006	Test HTTP Methods	Tested
OTG-CONFIG-007	Test HTTP Strict Transport Security	Tested
OTG-CONFIG-008	Test RIA cross domain policy	Tested
Identity Management Testing	**Test Name**	**Status**
OTG-IDENT-001	Test Role Definitions	Test
OTG-IDENT-002	Test User Registration Process	N/A
OTG-IDENT-003	Test Account Provisioning Process	N/A
OTG-IDENT-004	Testing for Account Enumeration and Guessable User Account	Tested
OTG-IDENT-005	Testing for Weak or unenforced username policy	N/A
OTG-IDENT-006	Test Permissions of Guest/Training Accounts	Tested

OTG-IDENT-007	Test Account Suspension/Resumption Process	N/A
Authentication Testing	**Test Name**	**Status**
OTG-AUTHN-001	Testing for Credentials Transported over an Encrypted Channel	Tested
OTG-AUTHN-002	Testing for default credentials	Tested
OTG-AUTHN-003	Testing for Weak lock out mechanism	Tested
OTG-AUTHN-004	Testing for bypassing authentication schema	Tested
OTG-AUTHN-005	Test remember password functionality	Tested
OTG-AUTHN-006	Testing for Browser cache weakness	Tested
OTG-AUTHN-007	Testing for Weak password policy	Tested
OTG-AUTHN-008	Testing for Weak security question/answer	N/A
OTG-AUTHN-009	Testing for weak password change or reset functionalities	N/A
OTG-AUTHN-010	Testing for Weaker authentication in alternative channel	N/A
Authorization Testing	**Test Name**	**Status**
OTG-AUTHZ-001	Testing Directory traversal/file include	Tested
OTG-AUTHZ-002	Testing for bypassing authorization schema	Tested
OTG-AUTHZ-003	Testing for Privilege Escalation	Tested
OTG-AUTHZ-004	Testing for Insecure Direct Object References	N/A
Session Management Testing	**Test Name**	**Status**
OTG-SESS-001	Testing for Bypassing Session Management Schema	Tested
OTG-SESS-002	Testing for Cookies attributes	Issue
OTG-SESS-003	Testing for Session Fixation	Tested
OTG-SESS-004	Testing for Exposed Session Variables	Tested
OTG-SESS-005	Testing for Cross Site Request Forgery	Tested
OTG-SESS-006	Testing for logout functionality	Tested
OTG-SESS-007	Test Session Timeout	Tested
OTG-SESS-008	Testing for Session puzzling	Tested
Data Validation Testing	**Test Name**	**Status**
OTG-INPVAL-001	Testing for Reflected Cross Site Scripting	Tested
OTG-INPVAL-002	Testing for Stored Cross Site Scripting	Tested
OTG-INPVAL-003	Testing for HTTP Verb Tampering	Tested
OTG-INPVAL-004	Testing for HTTP Parameter pollution	Tested
OTG-INPVAL-005	Testing for SQL Injection	Tested
	Oracle Testing	N/A
	MySQL Testing	N/A
	SQL Server Testing	N/A

	Testing PostgreSQL	N/A
	MS Access Testing	N/A
	Testing for NoSQL injection	N/A
OTG-INPVAL-006	Testing for LDAP Injection	N/A
OTG-INPVAL-007	Testing for ORM Injection	N/A
OTG-INPVAL-008	Testing for XML Injection	N/A
OTG-INPVAL-009	Testing for SSI Injection	Tested
OTG-INPVAL-010	Testing for XPath Injection	Tested
OTG-INPVAL-011	IMAP/SMTP Injection	Tested
OTG-INPVAL-012	Testing for Code Injection	Tested
	Testing for Local File Inclusion	Tested
	Testing for Remote File Inclusion	Tested
OTG-INPVAL-013	Testing for Command Injection	Tested
OTG-INPVAL-014	Testing for Buffer overflow	Tested
	Testing for Heap overflow	N/A
	Testing for Stack overflow	N/A
	Testing for Format string	Tested
OTG-INPVAL-015	Testing for incubated vulnerabilities	Tested
OTG-INPVAL-016	Testing for HTTP Splitting/Smuggling	Tested
Error Handling	**Test Name**	**Status**
OTG-ERR-001	Analysis of Error Codes	Tested
OTG-ERR-002	Analysis of Stack Traces	Tested
Cryptography	**Test Name**	**Status**
OTG-CRYPST-001	Testing for Weak SSL/TSL Ciphers, Insufficient Transport Layer Protection	Issue
OTG-CRYPST-002	Testing for Padding Oracle	Tested
OTG-CRYPST-003	Testing for Sensitive information sent via unencrypted channels	Tested
Business logic Testing	**Test Name**	**Status**
OTG-BUSLOGIC-001	Test Business Logic Data Validation	Tested
OTG-BUSLOGIC-002	Test Ability to Forge Requests	Tested
OTG-BUSLOGIC-003	Test Integrity Checks	Tested
OTG-BUSLOGIC-004	Test for Process Timing	Tested
OTG-BUSLOGIC-005	Test Number of Times a Function Can be Used Limits	Tested
OTG-BUSLOGIC-006	Testing for the Circumvention of Work Flows	N/A
OTG-BUSLOGIC-007	Test Defenses Against Application Mis-use	N/A
OTG-BUSLOGIC-008	Test Upload of Unexpected File Types	N/A
OTG-BUSLOGIC-009	Test Upload of Malicious Files	N/A
Client Side Testing	**Test Name**	**Status**
OTG-CLIENT-001	Testing for DOM based Cross Site Scripting	Tested

OTG-CLIENT-002	Testing for JavaScript Execution	Tested
OTG-CLIENT-003	Testing for HTML Injection	Tested
OTG-CLIENT-004	Testing for Client Side URL Redirect	Tested
OTG-CLIENT-005	Testing for CSS Injection	Tested
OTG-CLIENT-006	Testing for Client Side Resource Manipulation	Tested
OTG-CLIENT-007	Test Cross Origin Resource Sharing	Tested
OTG-CLIENT-008	Testing for Cross Site Flashing	Tested
OTG-CLIENT-009	Testing for Clickjacking	Tested
OTG-CLIENT-010	Testing WebSockets	Tested
OTG-CLIENT-011	Test Web Messaging	Tested
OTG-CLIENT-012	Test Local Storage	Tested

5. Penetration Testing Detail

PT-001: Encryption Vulnerability: Lucky13

PT-001: Encryption Vulnerability: Lucky13					
Risk Level	Low				
CVSS Score	2.6 (AV:N/AC:H/Au:N/C:P/I:N/A:N)				
Re-Testing	Low				
Base Score	Exploitability Metrics				
	Attack Vector	Network	Adjacent Network	Local	Physical
	Attack Complexity	Low	High		
	Privileges Required	None	Low	High	
	User Interface	None	Required		
	Scopes	Unchanged	Changed		
	Impact Metrics				
	Confidentiality	None	Low	High	
	Integrity	None	Low	High	
	Availability	None	Low	High	

Description

- Testing for Weak SSL TLS Ciphers Insufficient Transport Layer Protection

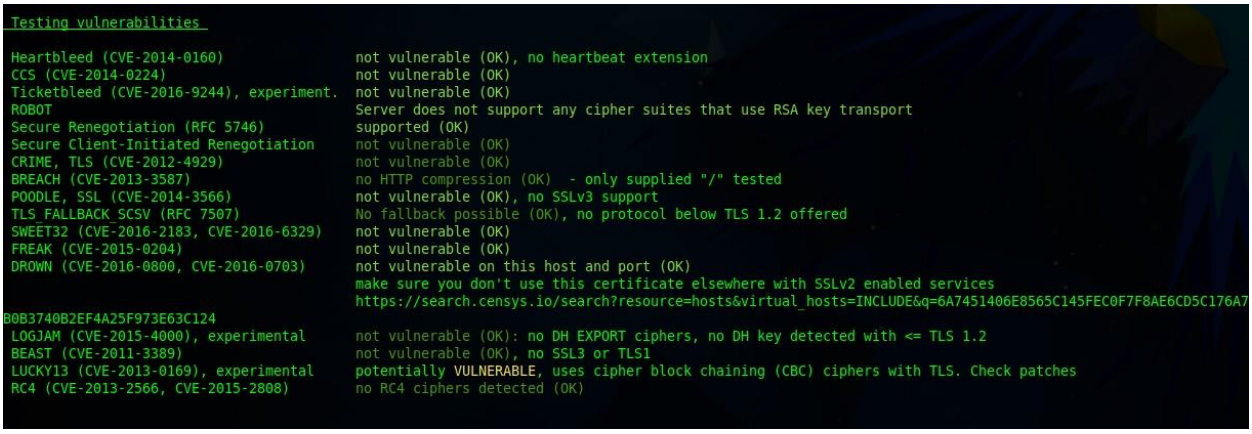
Tools

- Tessl.sh

Affected Hosts

- https://www.mitsubishielevator.co.th

How to



```
 Testing vulnerabilities

 Heartbleed (CVE-2014-0160)                not vulnerable (OK), no heartbeat extension
 CCS (CVE-2014-0224)                       not vulnerable (OK)
 Ticketbleed (CVE-2016-9244), experiment.  not vulnerable (OK)
 ROBOT                                     Server does not support any cipher suites that use RSA key transport
 Secure Renegotiation (RFC 5746)           supported (OK)
 Secure Client-Initiated Renegotiation     not vulnerable (OK)
 CRIME, TLS (CVE-2012-4929)                not vulnerable (OK)
 BREACH (CVE-2013-3587)                    no HTTP compression (OK)  - only supplied "/" tested
 POODLE, SSL (CVE-2014-3566)               not vulnerable (OK), no SSLv3 support
 TLS FALLBACK SCSV (RFC 7507)              No fallback possible (OK), no protocol below TLS 1.2 offered
 SWEET32 (CVE-2016-2183, CVE-2016-6329)    not vulnerable (OK)
 FREAK (CVE-2015-0204)                     not vulnerable (OK)
 DROWN (CVE-2016-0800, CVE-2016-0703)      not vulnerable on this host and port (OK)
                                           make sure you don't use this certificate elsewhere with SSLv2 enabled services
                                           https://search.censys.io/search?resource=hosts&virtual_hosts=INCLUDE&q=6A7451406E8565C145FEC0F7F8AE6CD5C176A7
B0B3740B2EF4A25F973E63C124
 LOGJAM (CVE-2015-4000), experimental      not vulnerable (OK): no DH EXPORT ciphers, no DH key detected with <= TLS 1.2
 BEAST (CVE-2011-3389)                     not vulnerable (OK), no SSL3 or TLS1
 LUCKY13 (CVE-2013-0169), experimental     potentially VULNERABLE, uses cipher block chaining (CBC) ciphers with TLS. Check patches
 RC4 (CVE-2013-2566, CVE-2015-2808)        no RC4 ciphers detected (OK)
```

Recommendation

- Disable TLS 1.0 and TLS 1.1
- For Apache server : https://httpd.apache.org/docs/trunk/ssl/ssl_howto.html
- For Apache Tompcat : https://www.owasporg/index.php/Talk:Securing_tomcat#Disabling_weak_ciphers_in_Tomcat
- For nginx : https://libre-software.net/tls-nginx/
- More detail at https://crashtest-security.com/prevent-ssl-lucky13/

Re-Testing Result

```
 Testing vulnerabilities

 Heartbleed (CVE-2014-0160)                not vulnerable (OK), no heartbeat extension
 CCS (CVE-2014-0224)                       not vulnerable (OK)
 Ticketbleed (CVE-2016-9244), experiment.  not vulnerable (OK)
 ROBOT                                     Server does not support any cipher suites that use RSA key transport
 Secure Renegotiation (RFC 5746)           supported (OK)
 Secure Client-Initiated Renegotiation     not vulnerable (OK)
 CRIME, TLS (CVE-2012-4929)                not vulnerable (OK)
 BREACH (CVE-2013-3587)                    potentially NOT ok, "gzip" HTTP compression detected. - only supplied "/" test
ed
                                           Can be ignored for static pages or if no secrets in the page
 POODLE, SSL (CVE-2014-3566)               not vulnerable (OK), no SSLv3 support
 TLS_FALLBACK_SCSV (RFC 7507)              No fallback possible (OK), no protocol below TLS 1.2 offered
 SWEET32 (CVE-2016-2183, CVE-2016-6329)    not vulnerable (OK)
 FREAK (CVE-2015-0204)                     not vulnerable (OK)
 DROWN (CVE-2016-0800, CVE-2016-0703)      not vulnerable on this host and port (OK)
                                           make sure you don't use this certificate elsewhere with SSLv2 enabled services
                                           https://search.censys.io/search?resource=hosts&virtual_hosts=INCLUDE&q=6A74514
06E8565C145FEC0F7F8AE6CD5C176A7B0B3740B2EF4A25F973E63C124
 LOGJAM (CVE-2015-4000), experimental      not vulnerable (OK): no DH EXPORT ciphers, no DH key detected with <= TLS 1.2
 BEAST (CVE-2011-3389)                     not vulnerable (OK), no SSL3 or TLS1
 LUCKY13 (CVE-2013-0169), experimental     potentially VULNERABLE, uses cipher block chaining (CBC) ciphers with TLS. Che
ck patches
 RC4 (CVE-2013-2566, CVE-2015-2808)        no RC4 ciphers detected (OK)
```

PT-002: Missing Feature Policy

PT-002: Missing Feature Policy					
Risk Level	Low				
CVSS Score	3.1				
Re-Testing	Low				
Base Score	Exploitability Metrics				
	Attack Vector	Network	Adjacent Network	Local	Physical
	Attack Complexity	Low	High		
	Privileges Required	None	Low	High	
	User Interface	None	Required		
	Scopes	Unchanged	Changed		
	Impact Metrics				
	Confidentiality	None	Low	High	
	Integrity	None	Low	High	
	Availability	None	Low	High	

Description

- Feature Policy Header is an added layer of security that helps to restrict from unauthorized access or usage of browser/client features by web resources. This policy ensures the user privacy by limiting or specifying the features of the browsers can be used by the web resources. Feature Policy provides a set of standard HTTP headers that allow website owners to limit which features of browsers can be used by the page such as camera, microphone, location, full screen etc.

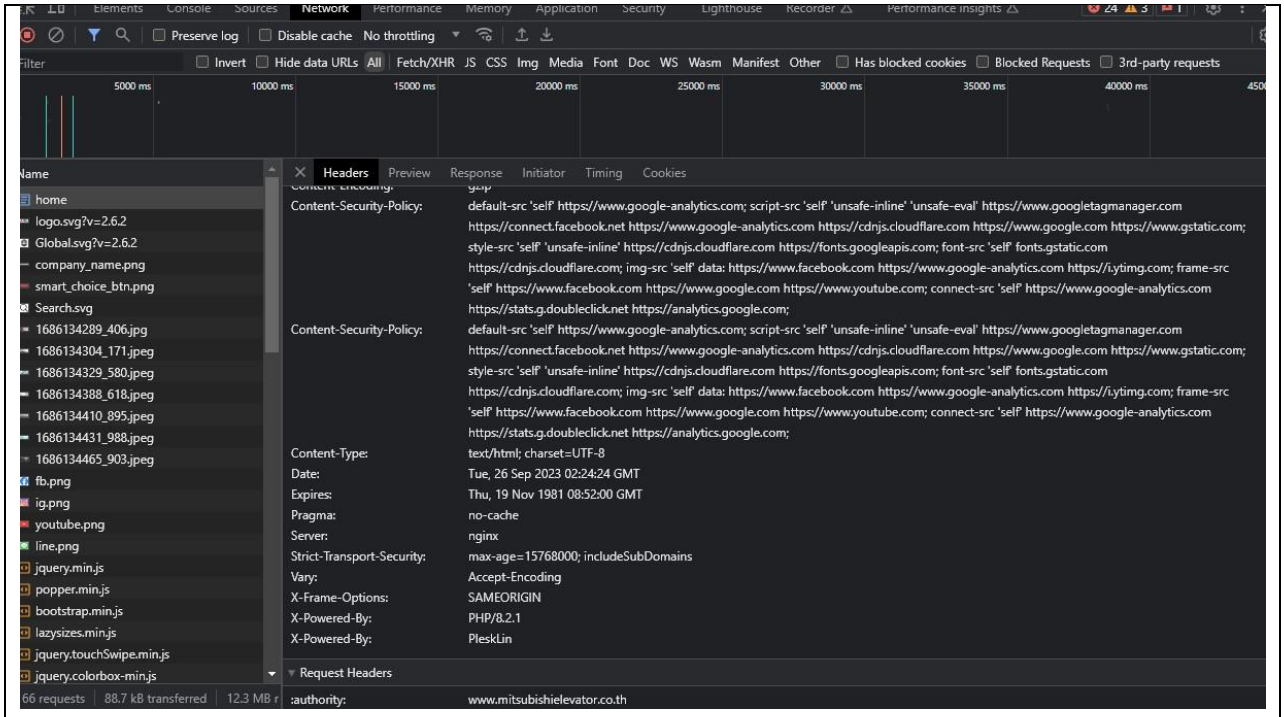
Tools

- OWASP ZAP
- Burp Suite

Affected Hosts

- https://www.mitsubishielevator.co.th

How to



Recommendation

- Enable your web server, application server is configured to set the Feature-Policy header

Re-Testing Result

```
Content-Type: text/html; charset=UTF-8
Content-Length: 0
X-Powered-By: PHP/8.2.1
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Set-Cookie: PHPSESSID=ma5lu9s2nkc26ghabil2md17f8; path=/; secure
X-Xss-Protection: 1; mode=block
Location: http://www.mitsubishielevator.co.th/2018/en/home
Content-Security-Policy: default-src 'self' https://www.google-analytics.com; script-src 'self' 'unsafe-inline' 'u
https://www.google-analytics.com https://i.ytimg.com; frame-src 'self' https://www.facebook.com https://www.google
Strict-Transport-Security: max-age=15768000; includeSubDomains
X-Powered-By: PleskLin
Content-Security-Policy: default-src 'self' https://www.google-analytics.com; script-src 'self' 'unsafe-inline' 'u
https://www.google-analytics.com https://i.ytimg.com; frame-src 'self' https://www.facebook.com https://www.google
X-Xss-Protection: 1; mode=block
```

PT-003: X-Content-Type Option missing

PT-003: X-Content-Type Option missing					
Risk Level	Low				
CVSS Score	3.1 CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N				
Re-Testing	Low				
Base Score	Exploitability Metrics				
	Attack Vector	Network	Adjacent Network	Local	Physical
	Attack Complexity	Low	High		
	Privileges Required	None	Low	High	
	User Interface	None	Required		
	Scopes	Unchanged	Changed		
	Impact Metrics				
	Confidentiality	None	Low	High	
	Integrity	None	Low	High	
	Availability	None	Low	High	

Description

- The only defined value, “nosniff”, prevents Internet explorer and Google Chrome from MIME-sniffing a response away from the declared content-type. This also applies to Google Chrome, when downloading extensions. This reduces exposure to drive-by download attacks and sites serving user uploaded content that by clever naming could be treated by MSIE as executable or dynamic HTML file

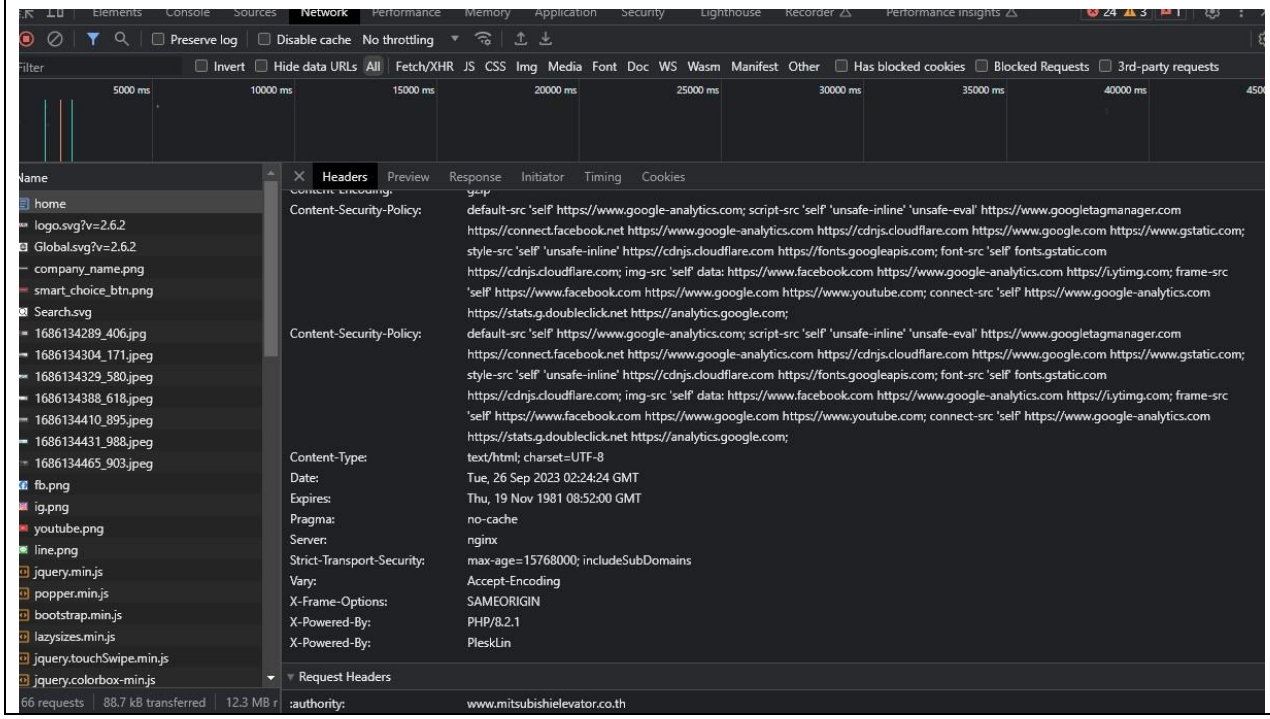
Tools

- Burp suite

Affected Hosts

- https://www.mitsubishielevator.co.th

How to



Recommendation

- The X-Content-Type-Options HTTP response header can be used to indicate whether or not a browser should be allowed to sniff a response away from the declared content-type. Sites can used this to avoid MIME-sniffing a response away from the declared content-type.

Re-Testing Result

```
Content-Type: text/html; charset=UTF-8
Content-Length: 0
X-Powered-By: PHP/8.2.1
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Set-Cookie: PHPSESSID=ma5lu9s2nkc26ghabil2md17f8; path=/; secure
X-Xss-Protection: 1; mode=block
Location: http://www.mitsubishielevator.co.th/2018/en/home
Content-Security-Policy: default-src 'self' https://www.google-analytics.com; script-src 'self' 'unsafe-inline' 'u
nttps://www.google-analytics.com https://i.ytimg.com; frame-src 'self' https://www.facebook.com https://www.google
Strict-Transport-Security: max-age=15768000; includeSubDomains
X-Powered-By: PleskLin
Content-Security-Policy: default-src 'self' https://www.google-analytics.com; script-src 'self' 'unsafe-inline' 'u
nttps://www.google-analytics.com https://i.ytimg.com; frame-src 'self' https://www.facebook.com https://www.google
X-Xss-Protection: 1; mode=block
```

PT-004: XSS Protection Header not found

PT-004: XSS Protection Header not found					
Risk Level	Low				
CVSS Score	3.1				
Re-Testing	Fixed				
Base Score	Exploitability Metrics				
	Attack Vector	Network	Adjacent Network	Local	Physical
	Attack Complexity	Low	High		
	Privileges Required	None	Low	High	
	User Interface	None	Required		
	Scopes	Unchanged	Changed		
	Impact Metrics				
	Confidentiality	None	Low	High	
	Integrity	None	Low	High	
	Availability	None	Low	High	

Description

- Cross-Site Scripting (XSS) attacks occur when: Data enters a Web application through an untrusted source, most frequently a web request. The data is included in dynamic content that is sent to a web user without being validated for malicious code. The malicious content sent to the web browser often takes the form of a segment of JavaScript, but may also include HTML, Flash or any other type of code that the browser may execute. The variety of attacks based on XSS is almost limitless, but they commonly include transmitting private data like cookies or other session information to the attacker, redirecting the victim to web content controlled by the attacker, or performing other malicious operations on the user's machine under the guise of the vulnerable site.

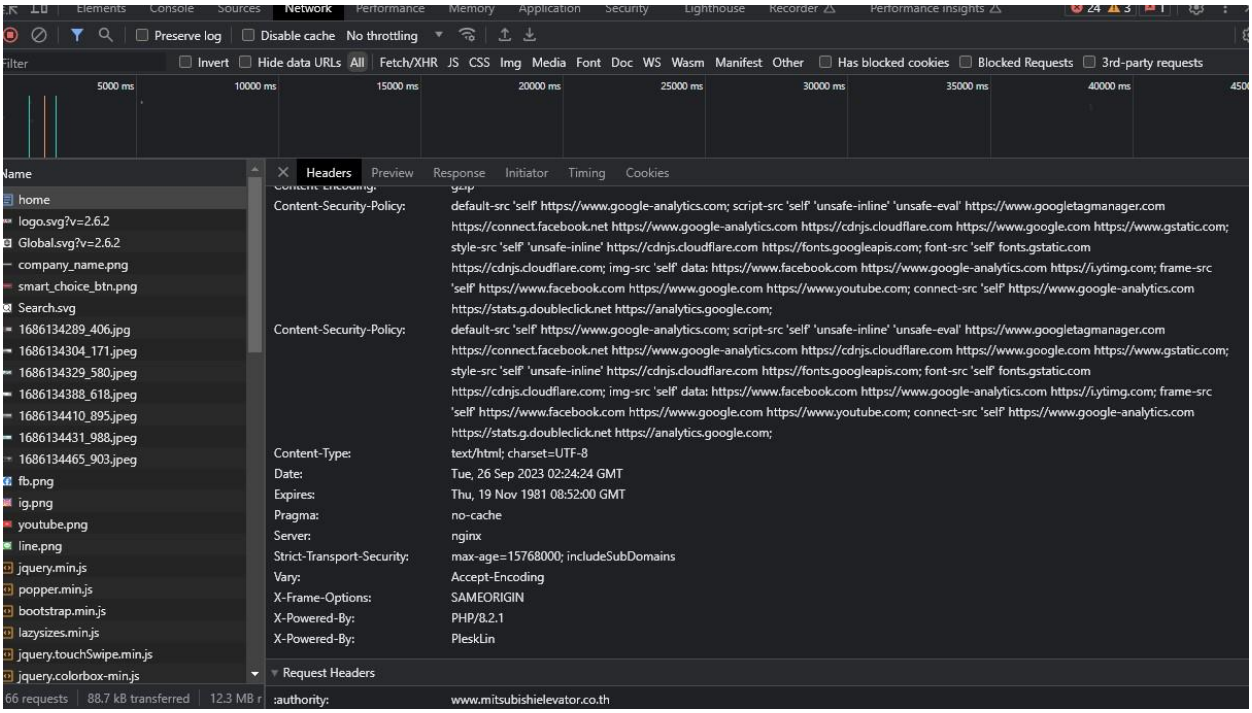
Tools

- Burp suite

Affected Hosts

- https://www.mitsubishielevator.co.th
-

How to



Recommendation

- Add the X-XSS-Protection header with a value of "1; mode= block".

  X-XSS-Protection: 1; mode=block

Re-Testing Result

```
Content-Type: text/html; charset=UTF-8
Content-Length: 0
X-Powered-By: PHP/8.2.1
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Set-Cookie: PHPSESSID=ma5lu9s2nkc26ghabil2md17f8; path=/; secure
X-Xss-Protection: 1; mode=block
Location: http://www.mitsubishielevator.co.th/2018/en/home
Content-Security-Policy: default-src 'self' https://www.google-analytics.com; script-src 'self' 'unsafe-inline' 'u
https://www.google-analytics.com https://i.ytimg.com; frame-src 'self' https://www.facebook.com https://www.google
Strict-Transport-Security: max-age=15768000; includeSubDomains
X-Powered-By: PleskLin
Content-Security-Policy: default-src 'self' https://www.google-analytics.com; script-src 'self' 'unsafe-inline' 'u
https://www.google-analytics.com https://i.ytimg.com; frame-src 'self' https://www.facebook.com https://www.google
X-Xss-Protection: 1; mode=block
```

PT-005: Sensitive Cookie in HTTPS Session Without 'Secure' Attribute

PT-005: Sensitive Cookie in HTTPS Session Without 'Secure' Attribute					
Risk Level	Low				
CVSS Score	3.1				
Re-Testing	Low				
Base Score	Exploitability Metrics				
	Attack Vector	Network	Adjacent Network	Local	Physical
	Attack Complexity	Low	High		
	Privileges Required	None	Low	High	
	User Interface	None	Required		
	Scopes	Unchanged	Changed		
	Impact Metrics				
	Confidentiality	None	Low	High	
	Integrity	None	Low	High	
	Availability	None	Low	High	

Description

- If the httpOnly attribute is set on a cookie, then the cookie's value cannot be read or set by client-side JavaScript. This measure makes certain client-side attacks, such as cross-site scripting, slightly harder to exploit by preventing them from trivially capturing the cookie's value via an injected script.

Tools

- Burp suite

Affected Hosts

- https://www.mitsubishielevator.co.th

How to

```
▼ Request Headers
:authority:          www.mitsubishielevator.co.th
:method:             GET
:path:               /2018/en/home
:scheme:             https
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, br
Accept-Language:     th,en-US;q=0.9,en;q=0.8
Cache-Control:       max-age=0
Cookie:              PHPSESSID=a7b4no1c9gte9gg7a7aghg79k4; _ga=GA1.1.1954152613.1695695039; _fbp=fb.2.1695695039655.1109230169;
                     _ga_B0Z7NXL9XC=GS1.1.1695712850.2.0.1695712850.60.0.0
Sec-Ch-Ua:           "Chromium";v="116", "Not)A;Brand";v="24", "Google Chrome";v="116"
Sec-Ch-Ua-Mobile:    ?0
Sec-Ch-Ua-Platform:  "Windows"
Sec-Fetch-Dest:      document
Sec-Fetch-Mode:      navigate
Sec-Fetch-Site:      none
```

Recommendation

- If the cookie contains sensitive information, then the server should ensure that the cookie has
  - Secure Attribute
  - HttpOnly Attribute
  - Domain Attribute

- Path Attribute
- Expires Attribute
- SameSite Attribute

-

Re-Testing Result

- "Secure Attribute" flag is set but "**HttpOnly**" Attribute flag should be set also

-

```
Content-Length: 0
X-Powered-By: PHP/8.2.1
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Set-Cookie: PHPSESSID=ma5lu9s2nkc26ghabil2md17f8; path=/; secure
X-Xss-Protection: 1; mode=block
Location: http://www.mitsubishielevator.co.th/2018/en/home
Content-Security-Policy: default-src 'self' https://www.google-analytics.com; script-src 's
https://www.google-analytics.com https://i.ytimg.com; frame-src 'self' https://www.facebook
Strict-Transport-Security: max-age=15768000; includeSubDomains
X-Powered-By: PleskLin
Content-Security-Policy: default-src 'self' https://www.google-analytics.com; script-src 's
https://www.google-analytics.com https://i.ytimg.com; frame-src 'self' https://www.facebook
X-Xss-Protection: 1; mode=block
```

PT-006: Vulnerable Software detected : PHP 8.2.1 (New)

PT-006: Vulnerable Software detected : PHP 8.2.1 (New)					
Risk Level	High				
CVSS Score	7.5				
Re-Testing					
Base Score	Exploitability Metrics				
	Attack Vector	Network	Adjacent Network	Local	Physical
	Attack Complexity	Low	High		
	Privileges Required	None	Low	High	
	User Interface	None	Required		
	Scopes	Unchanged	Changed		
	Impact Metrics				
	Confidentiality	None	Low	High	
	Integrity	None	Low	High	
	Availability	None	Low	High	

Description

- An outdated software program is one that is no longer supported by the vendor. This means that any new-found bugs in the program are not addressed. Plus, out-of-date software becomes less and less likely to work on new hardware and remain compatible with operating systems.

Tools

- Burp suite

Affected Hosts

- https://www.mitsubishielevator.co.th

How to

```
Content-Length: 0
X-Powered-By: PHP/8.2.1
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Set-Cookie: PHPSESSID=ma5lu9s2nkc26ghabil2md17f8; path=/; secure
X-Xss-Protection: 1; mode=block
Location: http://www.mitsubishielevator.co.th/2018/en/home
Content-Security-Policy: default-src 'self' https://www.google-analytics.com; script-src 'se
https://www.google-analytics.com https://i.ytimg.com; frame-src 'self' https://www.facebook.
Strict-Transport-Security: max-age=15768000; includeSubDomains
X-Powered-By: PleskLin
Content-Security-Policy: default-src 'self' https://www.google-analytics.com; script-src 'se
https://www.google-analytics.com https://i.ytimg.com; frame-src 'self' https://www.facebook.
X-Xss-Protection: 1; mode=block
```

Vulnerability List

- CVE-2023-0567 : Risk Score : 2.1 – Default credentials
- CVE-2023-0568 : Risk Score : 5.1
- CVE-2023-3823 : Risk Score : 5.0 – Xxe
- CVE-2023-3247 : Risk Score : 4.0 – Authentication flaw
- CVE-2023-0662 : Risk Score : Design/Log Flaw
- CVE-2023-3824 : Risk Score 7.5

Recommendation

- Update the latest version.

Re-Testing Result