|  |  |  |
| --- | --- | --- |
|  |  | Penetration testing report  Version 1.0  By EGCI477-Pentest Services, Inc. |

August 10, 2024

# for Faculty of Engineering, Mahidol university, Thailand [3]



**Engagement Details [1]**

Contractor Company: Pentest Services, Inc.

Client Company: Faculty of Engineering, Mahidol University, Thailand

Contract Number: PSI20240801/001

Contract Date: Nov 15, 2023

Start Date: Dec 1, 2023

End Date: Dec 31, 2023

**Document Details [1]**

Document Title: Penetration Testing Report

Date: Jan 8, 2024  
Ref No.: PSI20240801/001

Classification: {Public, **Internal**, Confidential, Highly Confidential}

Document Type: Report

**Document History [1]**

Date: Jan 8, 2024

Version: 1.0

Authors: Mr. Pentester

Comments: {**Initial Draft**, Review and Formatting, Final}

**Table of Contents [5]**

1. **Executive Summary ……………………………………………………………...………………………………… x**
   1. Background

**………………………………………….………………………………..………….…… x**

* 1. Objectives

**………………………………………….………………………………..………….…… x**

* 1. Scope

**………………………………………….………………………………..………….…… x**

* 1. Methodology

**………………………………………….………………………………..………….…… x**

* 1. Key Findings

**………………………………………….………………………………..………….…… x**

* 1. Recommendations

**………………………………………….………………………………..………….…… x**

* 1. Tabular Summary

**………………………………………….………………………………..………….…… x**

* 1. Graphical Summary

**………………………………………….………………………………..………….…… x**

* 1. Disclaimer

**………………………………………….………………………………..………….…… x**

1. **List of tests performed ……………………………………………………………...………………………………… x**
2. **Technical Findings ……………………………………………………………...………………………………… x**
   1. Server software and technology found **………………………………………….………………………………..………….…… x**
   2. Vulnerabilities found **………………………………………….………………………………..………….…… x**
   3. Details of each vulnerability **………………………………………….………………………………..………….…… x**
3. **Conclusion ……………………………………………………………...………………………………… x**
4. **Appendices**

**……………………………………………………………...………………………………… x**

5.1. Appendix A – Finding Risk Level

**………………………………………….………………………………..………….…… x**

1. **Executive Summary [29]**

* **Background** [1]

{{CONTRACTOR\_COMPANY}} was contracted by {{CLIENT\_COMPANY}} to perform a penetration testing on its Internet facing systems in order to determine the effectiveness of the implemented security measures.

The test was agreed in the Contract No. {{CONTRACT\_NUMBER}} of {{CONTRACT\_DATE}} between {{CLIENT\_COMPANY}} and {{CONTRACTOR\_COMPANY}}.

The fieldwork was completed between {{START\_DATE}} and {{END\_DATE}}.

* **Objectives** [What] [1]

The objective of the penetration testing was to evaluate the current state of the websites in scope from a security perspective and determine the risk of a successful attack by a hacker or malicious user from the Internet.

* **Scope** [Where/When][1]

The following systems belonging to {{CLIENT\_COMPANY}} were in scope:

|  |  |
| --- | --- |
| {Host/Network Address/**URL**}: | The main website for Faculty of Engineering, Mahidol University, Thailand <https://www.eg.mahidol.ac.th> |
| Start date/time: | Dec 30, 2023 / 04:29:56 |
| Finish date/time: | Dec 30, 2023 / 04:30:54 |
| Tests performed: | 12/12 |
| Status: | Finished |

* **Methodology** [How] [3]

The penetration testing was performed in a "black box" manner, meaning that we did not have any prior information about the target systems. Our tests simulated an external threat (hacker, malicious user) located somewhere on the Internet who tried to find vulnerabilities in the target systems and exploit them in order to gain unauthorized access to sensitive information or affect the correct functionality of the systems.

All of our tests were performed by combining our professional experience with well-known methodologies such as OWASP Top 10 and NIST 800-115.

The followings are the tools used in the penetration testing:

* The NMAP Version 7.95.
* **Key Findings** [Results][6]
* A buffer overflow can occur that allows attackers to execute arbitrary code or eliminate expected cryptographic properties due to the Keccak XKCP SHA-3 reference implementation flaw.
* {SQL Injection, Cross-Site Scripting (XSS), File Inclusion, OS Command Injection,

Session fixation, Open redirect, Detailed error messages, Session does not expire,

Internal IP disclosure, Default credentials in use, Debug functionality present, XML External Entity vulnerability}

* **Recommendations** [Results][6]

This penetration testing revealed several high risk vulnerabilities together with multiple medium and low risk issues. We recommend implementing the measures suggested for each finding in order to improve the security posture of the affected systems.

The high risk vulnerabilities need to be managed immediately.

* Upgrade the PHP to version 7.4.33 or 8.0.25 or 8.1.12

The medium risk vulnerabilities need to be managed in a short period of time (1 month).

The low risk vulnerabilities need to be managed in a short period of time (3 months).

* **Tabular Summary** [Results][5]

The table below summarizes the findings identified in this penetration testing:

{{FINDINGS\_SUMMARY\_TABLE}}

* **Graphical Summary** [Results][5]

This is a visual representation of overall risk level:

Overall risk level: ()

|  |  |  |
| --- | --- | --- |
| High | **Medium** | Low |

Risk ratings: (Risk = CVSS)

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| High: | 1 |  |  |  |  |  |  |  |  |
| Medium: | 3 |  |  |  |  |  |  |  |  |
| Low: | 6 |  |  |  |  |  |  |  |  |

* **Disclaimer** [1]

Please note that it is impossible to test networks, information systems and people for every potential security vulnerability. This report does not form a guarantee that your assets are secure from all threats. The tests performed and their results are only from the point of view of {{CONTRACTOR\_COMPANY}}. {{CONTRACTOR\_COMPANY}} is unable to ensure or guarantee that your assets are completely safe from any form of attack, including those that are not known at the time of the penetration test.

Furthermore, any changes to the tested systems may have an impact on their security level either in a negative or positive way.Our tests were performed in a time limited approach and our service was best-effort.

1. **List of tests performed [3]**
   1. Website accessibility...
   2. Website technologies...
   3. HttpOnly flag of cookie...
   4. Secure flag of cookie...
   5. Vulnerabilities of server-side software...
   6. Client access policies...
   7. Absence of the security.txt file...
   8. Use of untrusted certificates...
   9. Enabled HTTP debug methods...
   10. Directory listing...
   11. Domain too loose set for cookies...
   12. Unsafe HTTP header Content Security Policy...
2. **Technical Findings [42]**
   1. **Server software and technology found [2]**

Software/Version | Category

Windows Server | Operating systems

IIS 10.0 | Web servers

PHP 7.3.1 | Programming languages

Open Graph | Miscellaneous

Facebook Login | Authentication

Bootstrap 3.3.7 | UI frameworks

Facebook Chat Plugin | Live chat

jQuery 1.12.4 | JavaScript libraries

Google Analytics GA4 | Analytics

Google Font API | Font scripts

* 1. **Vulnerabilities found [20]**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Risk Level | CVSS | CVE/CWE | Summary | [Exploit](https://www.exploit-db.com/) | Affected Software |
|  | *9.8* | *CVE-2022-37454* | *The Keccak XKCP SHA-3 reference implementation before fdc6fef has an*  *integer overflow and resultant buffer overflow that allows attackers to*  *execute arbitrary code or eliminate expected cryptographic properties.*  *This occurs in the sponge function interface.* | *N/A* | *php 7.3.1* |
|  | *7.5* | *CVE-2019-11043* | *In PHP versions 7.1.x below 7.1.33, 7.2.x below 7.2.24 and 7.3.x below*  *7.3.11 in certain configurations of FPM setup it is possible to cause FPM*  *module to write past allocated buffers into the space reserved for FCGI*  *protocol data, thus opening the possibility of remote code execution.* | [*https://www.exploit-db.com/exploits/48182*](https://www.exploit-db.com/exploits/48182) | *php 7.3.1* |
|  | *4.3* | *CVE-2015-9251* | *jQuery before 3.0.0 is vulnerable to Cross-site Scripting (XSS) attacks*  *when a cross-domain Ajax request is performed without the dataType*  *option, causing text/javascript responses to be executed.* | *N/A* | *Jquery 1.12.4* |
|  | *N/A* | *CWE-693* | *The Content-Security-Policy (CSP) header activates a protection mechanism implemented in web browsers which prevents*  *exploitation of Cross-Site Scripting vulnerabilities (XSS). If the target application is vulnerable to XSS, lack of this header makes it*  *easily exploitable by attackers.* | *N/A* | *HTTP Header* |

* 1. **Details of each vulnerability [20]**

3.3.1 CVE-2022-37454

Risk description:

The Keccak XKCP SHA-3 reference implementation before fdc6fef has an integer overflow and resultant buffer overflow that allows attackers to execute arbitrary code or eliminate expected cryptographic properties. This occurs in the sponge function interface

Recommendation:

Upgrade the PHP to version 7.4.33 or 8.0.25 or 8.1.12

References:

<https://nvd.nist.gov/vuln/detail/CVE-2022-37454>

<https://www.rapid7.com/db/vulnerabilities/php-cve-2022-37454/>

<https://www.cvedetails.com/cve/CVE-2022-37454/>

Classification:

CWE: [*CWE-190*](https://cwe.mitre.org/data/definitions/190.html)

CVE:[*CVE-2022-37454*](https://nvd.nist.gov/vuln/detail/CVE-2022-37454)

OWASP Top 10 - 2017 : [A9 - Using Components with Known Vulnerabilities](https://owasp.org/www-project-top-ten/2017/A9_2017-Using_Components_with_Known_Vulnerabilities.html)

1. **Conclusion [10]**

Due  to  the  impact  to  the  overall  organization  as  uncovered  by  this  penetration  test,  appropriate  resources should be allocated to ensure that remediation efforts are accomplished in a timely manner. While  a  comprehensive  list  of  items  that  should  be  implemented  is  beyond  the  scope  of  this  engagement, some high level items are important to mention.

* 1. **Implement and enforce implementation of change control across all systems:**

Misconfiguration and insecure deployment issues were discovered across the various systems. The vulnerabilities that arose can be mitigated through the use of change control processes on all server systems.

* 1. **Implement regular firewall rule set reviews:**

Review the firewall rule set on a regular basis to ensure that all systems open to internal traffic continue to have a business reason to exist. We recommend that NIST SP 800-­‐417 be consulted for guidelines on firewall configuration and testing.

* 1. **Implement a patch management program:**

Operating a consistent patch management program per the guidelines outlined in NIST SP 800-­‐408 is an important component in maintaining good security posture. This will help to limit the attack surface that results from running unpatched internal services.

* 1. **Conduct  regular  vulnerability  assessments:**

As  part  of  an  effective  organizational  risk management strategy, vulnerability assessments should be conducted on a regular basis. Doing so will allow the organization to determine if the installed security controls are installed properly, operating as intended, and producing the desired outcome. Consult NIST SP 800-­‐309 for guidelines on operating an effective risk management program.

* 1. **Restrict  network  access  to  server  management  interfaces:**

Proper  network  segmentation  will reduce exposure to internal attacks against the server environment. Operating a well-­‐designed DMZ will allow Archmake to conduct its e-­‐commerce business in a manner that does not expose internal systems to attack. Consult FIPS 19110 for guidelines on securing local area networks.

* 1. **Restrict access to critical systems:**

It is recommended that the database server be isolated from other systems. If possible, a whitelist of database commands should be implemented specifying the minimum number of commands required to support business operations. This is inline with the system design concept of least privilege, and will limit the amount of damage an attacker can inflict on corporate resources. Consult NIST SP 800-­‐27 RevA11 for guidelines on achieving a security baseline for IT systems.

* 1. **Apply  industry  methodologies  for  secure  software  design:**

The  use  of  hard  coded  credentials within custom applications is highly discouraged. Users should have a need to know, and be required  to  provide,  credentials  before  accessing  confidential  and  proprietary  data.  This provides better security, and an audit trail that allows the business to tie actions to specific user accounts.

1. **Appendices [5]**
   1. **Appendix A – Finding Risk Level**

Each finding has been assigned a risk level of high, medium, and low. The level is based on an assessment of the priority with which each finding should be viewed and the potential impact each has on the confidentiality, integrity, and availability of client’s data (Impact).

|  |  |
| --- | --- |
| Risk Level | Definition |
| High | Exploitation of the technical or procedural vulnerability will cause substantial harm. Significant political, financial, and/or legal damage is likely to result. The threat exposure is high, thereby increasing the likelihood of occurrence. Security controls are not effectively implemented to reduce the severity of impact if the vulnerability were exploited. |
| Medium | Exploitation of the technical or procedural vulnerability will significantly impact the confidentiality, integrity, and/or availability of the system, application, or data. Exploitation of the vulnerability may cause moderate financial loss or public embarrassment. The threat exposure is moderate-to-high, thereby increasing the likelihood of occurrence. Security controls are in place to contain the severity of impact if the vulnerability were exploited, such that further political, financial, or legal damage will not occur. The vulnerability is such that it would otherwise be considered High Risk, but the threat exposure is so limited that the likelihood of occurrence is minimal. |
| Low | Exploitation of the technical or procedural vulnerability will cause minimal impact to operations. The Confidentiality, Integrity and Availability (CIA) of sensitive information are not at risk of compromise. Exploitation of the vulnerability may cause slight financial loss or public embarrassment. The threat exposure is moderate-to-low. Security controls are in place to contain the severity of impact if the vulnerability were exploited, such that further political, financial, or legal damage will not occur. The vulnerability is such that it would otherwise be considered Medium Risk, but the threat exposure is so limited that the likelihood of occurrence is minimal. |