**IT Health Check (ITHC)**

**ΩREPORT\_NAMEΩ**

ΩDATEΩ

Version XXX

 Prepared by: **ΩCONSULTANT\_NAMEΩ**

Security Engineer Team (SET)

# Table of Content

Table of Content 2

Document Version Control 3

Document History 3

1 Executive Summary 4

1.1 Overview 4

1.2 Total Issues 4

2 Description/Rationale 4

3 Risk Ratings 5

4 Risk Issues Summary 6

5 Detailed findings 7

5.1 πtitleπ 7

Description 7

Details 7

Recommended Countermeasures 7

# Document Version Control

|  |  |
| --- | --- |
| Data Classification: | OFFICIAL-SENSITIVE |
| Client Name: | ΩSHORT\_COMPANY\_NAMEΩ |
| Document Title: | ΩREPORT\_NAMEΩ |
| Author: | ΩCONSULTANT\_NAMEΩ |

# Document History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Issue Date | Issued By | Description |
|  |  |  |  |
|  |  |  |  |

# 

# Executive Summary

## Overview

Overview

## Total Issues

In total XXX issues were identified during testing:

|  |  |
| --- | --- |
| CVSS Score | Title |
| æreport/findings\_list/findings:::CVSS\_TOTAL>0æ∞cvss\_total∞ | æreport/findings\_list/findings:::CVSS\_TOTAL>0æ∞title∞ |

# Description/Rationale

Testing was carried out by XXX. The testing was conducted from XXX and onsite from MoJ.

Testing was performed against the following servers:

* XXX

The application Security Assessment was performed against the following URL:

* XXX

**Credentials**

Credentials

**Kali Box:**

* XXX (External Interface)
* XXX (Internal Interface)

For the Web application assessment, several accounts with different user’s roles were provided:

* XXX

**Scope**

The scope for this assessment was to XXX

**XXX**

Automated scanning XXX

**Web Application Penetration Testing**

The Scope of the assessment was to carry out a web application penetration against the XXX application covering mainly but not limited OWASP top 10

**Considerations**

The servers that were part of the scope were accessible from the XXX

**Standards Followed**

The following vulnerability categories (aligned with OWASP Top 10 2013) have been used for web application related findings:

A1 - Injection

A2 - Broken Authentication and Session Management

A3 - Cross-Site Scripting (XSS)

A4 - Insecure Direct Object References

A5 - Security Misconfiguration

A6 - Sensitive Data Exposure

A7 - Missing Function Level Access Control

A8 - Cross-Site Request Forgery (CSRF)

A9 - Using Components with Known Vulnerabilities

A10 - Unvalidated Redirects and Forwards

A99 - Other

# Risk Ratings

CVSS is a vendor-independent industry open standard, which provides a universal method for rating IT vulnerabilities. It is designed to convey the severity of vulnerabilities, and to help organizations priorities their responses.

It should be stressed that quantifying the overall business risk posed by any of the issues found in any test is outside our remit. This means that some risks may be reported as high from a technical perspective but may, as a result of other controls unknown to us, be considered acceptable.

Not all vulnerabilities fall within CVSS. Issues that do not fall within the system’s scope are referred to as custom issues and have a risk rating severity of critical, high, medium, low or informational.

|  |  |  |
| --- | --- | --- |
| Rating | CVSSv3 Score | Explanation |
| CRITICAL | 9.0 - 10 | A vulnerability was discovered that has been rated as critical. |
|  |  | This requires resolution as quickly as possible. |
| HIGH | 7.0 - 8.9 | A vulnerability was discovered that has been rated as important. |
|  |  | This requires resolution in the short term |
| MEDIUM | 4.0 - 6.9 | A vulnerability was discovered that has been rated as of medium criticality. |
|  |  | This should be resolved as part of the ongoing security maintenance of the system. |
| LOW | 0.1 - 3.9 | A vulnerability was discovered that has been rated as of low criticality. |
|  |  | This should be addressed as part of routine maintenance tasks |
| NONE | 0 | Good security practices were being followed or an audit item was found to be |
|  |  | present and correct |

# Risk Issues Summary

|  |  |
| --- | --- |
| CVSS Score | Title |
| æreport/findings\_list/findings:::CVSS\_TOTAL>0æ∞cvss\_total∞ | æreport/findings\_list/findings:::CVSS\_TOTAL>0æ∞title∞ |

##### 

# Detailed findings

¬report/findings\_list/findings:::CVSS\_Total>0¬

## πtitleπ

|  |  |
| --- | --- |
| Impact Rating  Medium | πtitleπ |
| Likelihood: | Unlikely |
| CVSSv3 Score: | πCVSS\_totalπ |

### Description

¬overview/paragraph¬ µzzzzµ π.π

ƒparagraphƒ π.π

ƒcodeƒ π.π

ƒitalicsƒ π.π

• ƒbulletƒ π.π

ƒh4ƒ π.π

÷ π.π ≠

### Details

πpoc/paragraphπ

### Recommended Countermeasures

¬remediation/paragraph¬ µzzzzµ π.π

ƒparagraphƒ π.π

ƒcodeƒ π.π

ƒitalicsƒ π.π

• ƒbulletƒ π.π

ƒh4ƒ π.π

÷ π.π ≠

∆