

**Penetration Tester Professional Report**

Prepared by : Asma

Report for : XXXXX

27 / 1 / 2021

**Table of Contents**

Table of Contents

[Executive Summary 3](#_Toc61948493)

XX………………………………………………………………………………………………………………………………………………………….………..3

XX…………………………………………………………………………………………………………………………………………………………………..3

XX…………………………………………………………………………………………………………………………………………………………………..3

Vulnerability report……………………………………………………………………………………………………………………………………….3

xxx ……………………………………………………………………………………………………………………………………………………………….

xxx ……………………………………………………………………………………………………………………………..………………………………..

xxx ………………………………………………………………………………………………………………………………………………………………..

xxx ………………………………………………………………………………………………………………………………………………………….…….

xxx ……………………………………………………………………………………………………………………………………………………………….

xxxx …………………………………………………………………………………………………………………….……………………………………….

Reference ……………………………………………………………………………………………………………………………………………….

**1 . Executive Summary**

**1. 1 Introductions :**   
[AAAAA] conducted a comprehensive security assessment of [BBBBBB] in order to determine existing vulnerabilities and establish the current level of security risk associated with the environment and the technologies in use.

The assessment provides insight into the resilience of the application to withstand attacks from unauthorized users and the potential for valid users to abuse their privileges and access.

This current report details the scope of testing conducted and all significant findings along with detailed remedial advice.

The summary below provides non-technical audience with a summary of the key findings and section two of this report relates the key findings and contains technical details of each vulnerability that was discovered during the assessment along with tailored best practices to fix.

**1.2 Assessment Summary**

Based on the security assessment for ###### the current status of the identified vulnerabilities set the risk at a CRITICAL level, which if not addressed in time these vulnerabilities could be a trigger for a cybersecurity breach. These vulnerabilities can be easily fixed by following the best practices and recommendation given throughout the report.

The graphs below represent a summary of the total number of vulnerabilities found up until issuing this current report:

**1.3 Strategic Recommendations**

We recommend addressing the CRITICAL and HIGH vulnerabilities before go-live.

**1. 4 Scop**

The Scope of the Penetration test was limited to the following target:

* Web Server: x.x.x.x
* Domain: XXXX
* Subdomain : XXXX

1. **5 Risk Ratings**

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

| Severity | CVSS V3 Score Range | Definition |
| --- | --- | --- |
| Critical | 9.0-10.0 | Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately. |
| High | 7.0-8.9 | Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible. |
| Moderate | 4.0-6.9 | Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved. |
| Low | 0.1-3.9 | Vulnerabilities are non-exploitable but would reduce an organization’s attack surface. It is advised to form a plan of action and patch during the next maintenance window. |
| Note | N/A | No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation. |

**5. 6 Findings Overview**

All the issues identified during the assessment are listed below with a brief description and risk rating for each issue. The risk ratings used in this report are defined in Risk Ratings Section

|  |  |  |
| --- | --- | --- |
|  | Description | Impact Rating |
| 1 | e.g : xss | **Critical** |
| 2 | e.g .: sql | **Critical** |
| 3 |  | **Critical** |
| 4 |  | **Critical** |
| 5 |  | **Critical** |
| 6 |  | **Critical** |
| 7 |  | High |
| 8 |  | High |
| 9 |  | High |
| 10 |  | Medium |
| 11 |  | Medium |
| 12 |  | Medium |
| 13 |  | Low |
| 14 |  | Low |

**1. 7 Vulnerabilities by type**

1. **Vulnerability report**

**.2 . 1 Summery of System information**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Host** | **Open Ports** | **Services** | **Obtained Access** | **Vulnerabilities Exploited** |
|  |  |  |  |  |
|  |  |
|  |  |  |  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |  |  |  |
|  |  |
|  |  |
|  |  |  |  |  |
|  |  |
|  |  |
|  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**2. 2 Detailed Findings:**

**192.168.1.1**

|  |  |
| --- | --- |
| **1.1** | |
| **Cross-Site Scripting (XSS)** | |
| **Brief description** |  |
| **Impact (CVSSv2) - Business impact factored in** |  |
| **References to classifications** |  |
| **Vulnerability ID** |  |
| **System** |  |
| **Affected targets** | |
| **Website pages** | XXXXXXX/ |
| **Risk** | . |
| **Remediation** |  |

**Exploitation proof of concept**

|  |  |
| --- | --- |
| 1.2 | |
| XXXXXXX | |
| **Brief description** |  |
| **Impact (CVSSv2) - Business impact factored in** |  |
| **References to classifications** |  |
| **Vulnerability ID** |  |
| **Affected targets** | |
| **Website pages** |  |
| **Risk** |  |
| **Remediation** |  |
| **Exploitation proof of concept** | |
| XXXXXXXXXXXXXXXXXXXX ( screenshots for exploit ) XXXXXXXXXXXXXXXx | |

|  |  |
| --- | --- |
| 1.3 | |
| XXXXX | |
| **Brief description** |  |
| **Impact (CVSSv2) - Business impact factored in** |  |
| **References to classifications** |  |
| **Vulnerability ID** |  |
| **Affected targets** | |
| **System** |  |
| **Risk** |  |
| **Remediation** |  |
| **Exploitation proof of concept** | |
|  | |

**192.168.1.2**

|  |  |
| --- | --- |
| 2.1 | |
| XXXXXXXX | |
| **Brief description** |  |
| **Impact (CVSSv2) - Business impact factored in** |  |
| **References to classifications** |  |
| **Vulnerability ID** |  |
| **Affected targets** | |
| **System** |  |
| **Risk** |  |
| **Remediation** |  |
| **Exploitation proof of concept** | |
|  | |

**192.168.1.3**

|  |  |
| --- | --- |
| 3.1 | |
|  | |
| **Brief description** |  |
| **Impact (CVSSv2) - Business impact factored in** |  |
| **References to classifications** |  |
| **Vulnerability ID** |  |
| **Affected targets** | |
| **System** |  |
| **Risk** |  |
| **Remediation** |  |
| **Exploitation proof of concept** | |
|  | |

|  |  |
| --- | --- |
| 3.2 | |
|  | |
| **Brief description** |  |
| **Impact (CVSSv2) - Business impact factored in** |  |
| **References to classifications** |  |
| **Vulnerability ID** |  |
| **Affected targets** | |
| **System** |  |
| **Risk** |  |
| **Remediation** |  |
| **Exploitation proof of concept** | |
|  | |

**192.168.1.4**

|  |  |
| --- | --- |
| 4.1 | |
|  | |
| **Brief description** |  |
| **Impact (CVSSv2) - Business impact factored in** |  |
| **References to classifications** |  |
| **Vulnerability ID** |  |
| **Affected targets** | |
| **System** |  |
| **Risk** |  |
| **Remediation** |  |
| **Exploitation proof of concept** | |
|  | |

|  |  |
| --- | --- |
| 4.2 | |
|  | |
| **Brief description** |  |
| **Impact (CVSSv2) - Business impact factored in** |  |
| **References to classifications** |  |
| **Vulnerability ID** |  |
| **Affected targets** | |
| **System** |  |
| **Risk** |  |
| **Remediation** |  |
| **Exploitation proof of concept** | |
|  | |

**Reference:**

* AAAAAAAAA
* AAAAAAAAA
* AAAAAAAAA
* AAAAAAAAA
* AAAAAAAAA