Security audit report of <PRODUCTS>

COMPANY LOGO HERE

Version: 1.0

Document Security: Confidential

***Contact at PENTEST COMPANY:***

NAME [EMAIL@company.com](mailto:EMAIL@company.com) PHONE NUMBER

NAME [EMAIL@company.com](mailto:EMAIL@company.com) PHONE NUMBER

***Contact at COMPANY NAME:***

NAME [EMAIL@company.com](mailto:EMAIL@company.com) PHONE NUMBER

NAME [EMAIL@company.com](mailto:EMAIL@company.com) PHONE NUMBER

***PENTEST COMPANY ADDRESS:***

***COMPANY Address:***

***Document History:***

**Version: Date:** **Status:** **Author:**

1.0 DATE Initial NAME(s)

Table of Contents

1. Summary of Results Pg. #

1-1: Management Overview Pg. #

1-2: Technical Summary Pg. #

1-3: Recommendation Summary Pg. #

1-4: Product(s) Overview and Further Analysis Pg. #

1-5: Risk Matrix Pg. #

1-6: Explanation of Risk Matrix Pg. #

1-7: Proof of Concepts for Vulnerabilities Pg. #

Appendix Pg. #

Tools Pg. #

Methodology Pg. #

Scope Pg. #

ADD MORE PAGE NUMBERS IF NEEDED. EX:

1.

2.

3.

1. Summary of Results

ADD SUMMARY HERE. This should be brief and share little to zero technical details and highlight more business risks, security risks, and product risks.

**SECTION: 1-1. Management Overview**

ADD MANAGEMENT OVERVIEW HERE. Include vulnerabilities found but do not go into detail about them. Little information may be provided but it is better to add more detail in the technical summary. Section 1-1 should be on its own page so it may be given to a CTO, CEO or other executive for a quick run-down to save time and not cause confusion.

**SECTION: 1-2. Technical Summary**

The following deficiencies were identified during the security assessment of the applications:

ADD VULNERABILITIES AND FLAWS FOUND HERE: Go into more detail from section 1-1 and add EVERYTHING that was found during the security audit. Also add references to vulnerabilities found. Ex: RCE found on example.com (1). Each vulnerability is in its own paragraph with proper notation and formatting. ADD NETWORK DIAGRAMS IF NEEDED.

**SECTION: 1-3. Recommendation Summary**

ADD RECOMMENDATIONS AND REMIDIATIONS HERE:

The recommendations for mitigating the key risks are summarized in the following table:

**SECTION: 1-4. Product(s) Overview and Further Analysis**

The goal of this project was to gain an overview of the applications and identify which ones require more detailed testing. Therefore, report does not only list the vulnerabilities discovered during the penetration test but also provides an evaluation of whether an application should undergo further in-depth testing. The following table presents recommendations for further penetration testing.

It is recommended that all findings listed in this report be reevaluated in a follow-up assessment.

**SECTION: 1-5. Risk Matrix**

The following matrix shows the different vulnerabilities identified during the assessment along with their individual probability of occurrence and their possible impact. The classification of the vulnerabilities in this matrix also considers the business impact in addition to the technical impact. ADD REFRENCE NUMBERS IN THE RISK MATRIX

*IMPACT*

*PROBABILITY*

**SECTION: 1-6. Explanation of Risk Matrix**

To determine the risk arising from a successful exploitation of the individual vulnerabilities, two factors were considered: The probability of exploiting the vulnerability and the possible impact caused by an exploitation.

The following table explains the four levels used for evaluating the probability of an exploitation:

The following table explains the four levels used for evaluating the possible impact of an exploitation:

The values of the two obtained ratings (V1 × V2) are then multiplied to determine the respective risk, in the case of the informational column, it is to be disregarded. The urgency to resolve the respective threat or associated vulnerability is determined based on the resulting risk index.

**SECTION: 1-7. Proof of Concepts for Vulnerabilities**

The following images demonstrate commands, source code, packet captures and pentesting tool outputs to aid with the proof of concept for vulnerabilities found during the engagement.

For added privacy and security of the pentester and the web application, certain items may be redacted such as login credentials as well as bearer tokens. ADD EACH VULNERABILITY FOUND WITH IMAGES AND REFRENCES FOR THE IMAGE. Append each SECTION: with a number relating to the vulnerability found from Section: 1-2. EX: SECTION: 1-7-1 RCE on Admin Login Portal.

For convivence add a footnote related to the vulnerability on how to remediate it with a link to the source.

APPENDIX

The appendix will cover the following tools, methodology, and scope used for the security audit.

**TOOLS & APPLICATIONS:**

ADD ALL PENTESTING & SECURITY TOOLS USED IN DROP DOWN FORMAT. EX:

-Nmap

-John

-Hydra

**METHODOLOGY:**

A pentest can vary in terms of how it is deemed successful. Typically, a successful pentest follows the following phases. Proper OPSEC (operational security) procedures and techniques must be implemented throughout the entire security audit.

PHASE I: RECON

Pentester(s) will commence recon and/or enumeration of the target(s) via passive and active OSINT (open-source intelligence) techniques.

PHASE II: EXPLOITATION

Once vulnerabilities have been identified via the recon phase, pentester(s) will attempt to hack the target(s) for finding vulnerabilities and points of exploit and entry.

PHASE III: PRIVELEGE ESCALATION & PERSISTENCY

When pentester(s) successfully exploit the target(s) and a foothold is established, privilege escalation techniques are used to gain access to users and/or accounts with higher privileges such as “root” on Linux / Unix based systems, Administrator or NT AUTHORIRTY on Windows systems. Persistency is also established allowing pentester(s) to have persistent access to compromised system(s) to perform further attacks such as accessing private networks not accessible via the public.

PHASE IV: DATA EXFILTRATION & ANTI-FORENSICS

If data exfiltration is necessary pentester(s) will steal information found within system(s) to prove that data can be stolen via a potential threat actor. If anti-forensics is applicable pentester(s) will perform anti-forensics to remove their tracks, logs and evidence that can trace back to how, where, and when the security professional gained access to the system(s) and what actions and/or commands were used for previous phases.

PHASE V: EXFILTRATION

Once the pentester(s) deem the security audit to be successful and no further actions are needed, they may perform an exfiltration as the last phase of the audit and report back to contractor(s) with a report based on their findings.

**SCOPE:**

A scope was provided to the pentesters from <PENTEST COMPANY>, that outlined in detail what was allowed to be tested and what was not allowed to be tested.

MENTION ITEMS OUT OF SCOPE HERE:

ADD MORE INFORMATION RELATED TO TARGET AND PRODUCT(S):

FINALIZE REPORT HERE W/ CONCLUSION:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Recommendation (Vulnerability)  ADD VULNERABILITY HERE, and color code the Addressed risk section from left to right. HIGH -> MEDIUM -> LOW -> INFORMATIONAL. Add reference such as V(1), V(2), etc… for each vulnerability. | Addressed Risk   |  |  |  |  | | --- | --- | --- | --- | |  |  |  |  | |
| ADD VULNERABILITY HERE | |  |  |  |  | | --- | --- | --- | --- | |  |  |  |  | |
| ADD VULNERABILITY HERE | |  |  |  |  | | --- | --- | --- | --- | |  |  |  |  | |
| ADD VULNERABILITY HERE | |  |  |  |  | | --- | --- | --- | --- | |  |  |  |  | |
| ADD VULNERABILITY HERE | |  |  |  |  | | --- | --- | --- | --- | |  |  |  |  | |
| ADD VULNERABILITY HERE | |  |  |  |  | | --- | --- | --- | --- | |  |  |  |  | |
| ADD VULNERABILITY HERE | |  |  |  |  | | --- | --- | --- | --- | |  |  |  |  | |
| ADD VULNERABILITY HERE | |  |  |  |  | | --- | --- | --- | --- | |  |  |  |  | |

|  |  |  |
| --- | --- | --- |
| Application | Further Testing Needed | Prioritization |
| ADD APPLICATION HERE | Yes OR No | Low, Medium, High |
| ADD APPLICATION HERE | Yes OR No | Low, Medium, High |
| ADD APPLICATION HERE | Yes OR No | Low, Medium, High |

|  |  |  |  |
| --- | --- | --- | --- |
| CRITICAL |  |  |  |
| HIGH |  |  |  |
| MEDIUM |  |  |  |
| LOW |  |  |  |
| INFORMATIONAL |  |  |  |

|  |  |  |
| --- | --- | --- |
| Probability | Description | Rating V1 |
| Informational | There is no probability for an exploit, but information is discovered aiding an attacker.  Example: Simple port scans of a server or website reveal what it is running and if vulnerabilities exist for services. | 0 |
| Low | The probability of a successful exploitation of the vulnerability can be classified as low.  Example: The exploit must be run with a variety of other exploits and tools. | 1 |
| Medium | The probability of a successful exploitation of the vulnerability can be classified as medium.  Example: The vulnerability requires the user to possess credentials for exploitation. | 2 |
| High | The probability of a successful exploitation of the vulnerability can be classified as high.  Example: The vulnerability can easily be exploited without much knowledge and is simple to use. | 3 |
| Critical | The probability of a successful exploitation of the vulnerability can be classified as critical.  Example: The vulnerability can easily be exploited with zero knowledge and has a high percentage of success. | 4 |

|  |  |  |
| --- | --- | --- |
| Impact | Description | Rating V2 |
| Low | The impact resulting from an exploitation of the vulnerability can be classified as low.  Example: Broadcasting information relating to services and header messages of a host. | 1 |
| Medium | The impact resulting from an exploitation of the vulnerability can be classified as medium.  Example: Manipulating headers can cause malicious files to be uploaded to a website. | 2 |
| High | The impact resulting from an exploitation of the vulnerability can be classified as high.  Example: Credentials can be stolen via XSS or SQLi on a web application. | 3 |
| Critical | The impact resulting from an exploitation of the vulnerability can be classified as critical.  Example: Outside users of a system can execute code remotely and gain access to the system. | 4 |

|  |  |  |
| --- | --- | --- |
| Risk Index (V1 × V2) | Rating | Description of the resulting overall risk |
| 12 | |  |  |  |  | | --- | --- | --- | --- | |  |  |  |  | | **Critical**: Measures to fix the vulnerability or compensating  measures must be taken immediately. |
| 8-9 | |  |  |  |  | | --- | --- | --- | --- | |  |  |  |  | | **High**: Measures must be taken as soon as possible. |
| 4-6 | |  |  |  |  | | --- | --- | --- | --- | |  |  |  |  | | **Medium**: Measures are required. |
| 2-3 | |  |  |  |  | | --- | --- | --- | --- | |  |  |  |  | | **Low**: Measures for remediation are recommended. |
| 1 | |  |  |  |  | | --- | --- | --- | --- | |  |  |  |  | | **Anomaly/Good Practice Violation**: A violation of good practices  has been found. Although the good practice violation does not  pose a direct security risk, it should be fixed as it might make exploiting other vulnerabilities much easier or lead to a  vulnerability in the future. |

|  |  |
| --- | --- |
| ITEM | AGREEMENT |
| ADD ITEM ex: Test Window, IP Range, etc |  |
| ADD ITEM |  |
| ADD ITEM |  |
| ADD ITEM |  |
| ADD ITEM |  |
| ADD ITEM |  |