DVWA 2.3 Pen testing findings report

Testing Period: 29.12.2023 – 09.01.2023

Submission Date: 10.01.2023

Performed by: AIS 2023/24 team

A report on the penetration testing findings for Damn Vulnerable Web Application (DVWA) 2.3 typically includes comprehensive details outlining vulnerabilities discovered, their severity levels, and recommendations for mitigation. Here's a structure you might consider:

Sudurjanie

### Title: Penetration Testing Findings Report for DVWA 2.3

1. \*\*Introduction\*\*

- Brief overview of the purpose and scope of the penetration test.

- Explanation of the DVWA 2.3 environment tested.

2. \*\*Methodology\*\*

- Description of the tools, techniques, and approaches used during the penetration testing.

- Details on the testing environment setup.

3. \*\*Executive Summary\*\*

- High-level summary of critical findings and their potential impact on security.

- Overview of the most severe vulnerabilities discovered.

4. \*\*Vulnerability Assessment\*\*

- \*\*Critical Vulnerabilities\*\*

- Description of critical vulnerabilities (e.g., SQL injection, Cross-Site Scripting) found, including their impact and exploitation scenarios.

- Steps to reproduce the vulnerabilities.

- Risk assessment and potential consequences if exploited.

- Recommendations for immediate mitigation.

- \*\*High/Medium/Low Severity Vulnerabilities\*\*

- Categorization of vulnerabilities based on severity.

- Description, impact, and potential risk of each identified vulnerability.

- Recommendations for remediation.

5. \*\*Risk Assessment\*\*

- Overall risk assessment based on the combined impact of discovered vulnerabilities.

- Prioritization of vulnerabilities based on severity and potential impact.

6. \*\*Recommendations\*\*

- Detailed actionable steps to address and mitigate identified vulnerabilities.

- Best practices and security measures to enhance the overall security posture of the DVWA 2.3 environment.

7. \*\*Conclusion\*\*

- Summary of key findings and recommendations.

- Final thoughts and suggestions for ongoing security measures.

8. \*\*Appendix\*\*

- Additional details such as raw scan results, logs, or any supplementary information.

Each vulnerability should be documented with relevant technical details, including affected components, proof of concept (if applicable), and clear steps to reproduce the issue. The report should also emphasize the importance of addressing these vulnerabilities promptly to bolster the security of the DVWA 2.3 environment.

Certainly, here's a sample disclaimer for a penetration testing report:

---

\*\*Disclaimer:\*\*

Absolutely, here's a modified disclaimer tailored to your specifications:

---

\*\*Disclaimer:\*\*

This penetration testing report is exclusively created for the purpose of identifying vulnerabilities within the production environment of Damn Vulnerable Web Application (DVWA) 2.3, owned and operated by Stoyan Kolev Ltd. The findings, assessments, and recommendations presented in this report are based on the observations and tests conducted during the designated testing period and with the provided information. Time period – 23-24. It is essential to note the following:

1. \*\*Scope Limitation:\*\* The penetration test was conducted within the agreed scope and constraints defined by AIS 2023/2024. The findings are confined to the specified scope and may not encompass all potential vulnerabilities within the entire system or network.

2. \*\*Assessment Timing:\*\* The security landscape is subject to continual evolution, and new vulnerabilities may emerge post-assessment. The findings in this report reflect the state of the DVWA 2.3 environment at the time of testing.

3. \*\*No Guarantee of Exhaustive Coverage:\*\* While exhaustive efforts were made to identify vulnerabilities, it is impossible to ensure the discovery of every potential security flaw. There might exist unidentified vulnerabilities that were not within the scope of this assessment.

4. \*\*Authorized Engagement:\*\* The penetration testing was conducted with explicit consent from Stoyan Kolev Ltd, the authorized owner of the DVWA 2.3 production environment. All testing activities were performed within the agreed-upon scope and did not involve any unauthorized or malicious activities.

5. \*\*Limited Liability:\*\* The recommendations provided in this report aim to bolster security measures. However, their implementation does not guarantee absolute protection against all possible threats. Any actions taken based on this report are the sole responsibility of Stoyan Kolev Ltd.

6. \*\*Confidentiality:\*\* This report contains sensitive information regarding vulnerabilities and potential risks within the DVWA 2.3 production environment. It is intended solely for Stoyan Kolev Ltd and should be handled with utmost confidentiality. Any unauthorized access, disclosure, or modification of this report is strictly prohibited.

7. \*\*Verification and Validation:\*\* Prior to implementing any recommendations or remediation steps outlined in this report, it is advised to perform additional verification and validation to ensure compatibility and minimize any unintended consequences.

By accessing this report, Stoyan Kolev Ltd acknowledges and accepts the terms outlined in this disclaimer. Any use or reliance upon the information provided in this report is at their own risk.

Findings

* This is where teeh fun begins