

Vulnerability Assessment Report

*For bWAPP Web Application*By [Abdulazeez Uthman]

Executive Summary

This Vulnerability Assessment Report, prepared as part of an internship challenge with **Digitanotion Limited**, provides a detailed analysis of the security weaknesses identified in the **bWAPP (Buggy Web Application)** environment. The assessment was conducted to simulate real-world scenarios, focusing on identifying, scoring, and recommending fixes for vulnerabilities in the application.

The assessment uncovered several vulnerabilities across various categories, including input validation, authentication, and misconfigurations. Each vulnerability was evaluated using the **Common Vulnerability Scoring System (CVSS)** to determine its severity and prioritize remediation efforts effectively.

Key findings include:

* **High-Risk Issues**: Critical vulnerabilities that could lead to data breaches, unauthorized access, or complete system compromise.
* **Medium-Risk Issues**: Weaknesses that could facilitate attacks when combined with other vulnerabilities.
* **Low-Risk Issues**: Minor security concerns that, while not immediately critical, could be exploited over time.

To address these vulnerabilities, specific remediation steps are recommended, including improving input validation, enforcing stronger authentication mechanisms, and following best practices in application security.

This report demonstrates the practical application of vulnerability assessment techniques, emphasizing the importance of identifying and mitigating security flaws to build secure web applications. The insights and experience gained through this exercise contribute to the development of future-ready cybersecurity talent.

**Table of Contents**

[1. Scan Request Information](#_gjdgxs) 4

[2. Scope of the Vulnerability Assessment or Review](#_3dy6vkm) 5

[3. Summary of Recommendations](#_1t3h5sf) 6

[4. Detailed Observations](#_4d34og8) 7

[Appendix A: Definitions of Likelihood and Consequence Matrix](#_17dp8vu) 9

[Appendix B – Supplemental Scan and Review Details](#_3rdcrjn) 10

# **Scan Request Information**

| **Request Ticket** | RT09219 |
| --- | --- |
| **Request and Report Date** | 08/05/2025 |
| Product or Service Under Review | [{Identify service, URL, hostname, application involved in this security review or scan request, E.g, vulnerable IPs, Web Servers, URLs}] **To be completed by intern**. |
| Organization | **Digitanotion Limited** |
| Administrative Authority | Divine Ezelibe is the **Chief Information Security Officer** for this project |
| Support Contacts | In the event of unexpected outages or challenge, etc. to the services while reviewing or scanning, you can request for help properly in the “Stream” session of Google classroom. |
| Information Security Analyst | [[Kindly Attach your details below]]  Name: Abdulazeez Uthman  Title: Vulnerability Assessment Report  Supervisor:  Department: VAPT  Phone number: 09032649916  Email: abdulazeezuthman662@gmail.com |

# **Scope of the Vulnerability Assessment or Review**

This “white box” vulnerability assessment focuses on evaluating the security of the **bWAPP (Buggy Web Application)** hosted in a home lab using Docker. The goal is to identify, analyze, and report vulnerabilities to simulate real-world cybersecurity tasks.

**Key activities include:**

* Identifying vulnerabilities using manual and automated methods.
* Prioritizing risks using CVSS scoring.
* Recommending actionable remediation steps.

The scope covers application functionality, common web vulnerabilities (e.g., SQL Injection, XSS), and misconfigurations, with testing limited to the controlled bWAPP environment.

# **Summary of Recommendations**

[[Provide a brief bullet point list of the recommendations identified in assessment]]

• Add Anti-CSRF Tokens to forms to protect against Cross-Site Request Forgery (CSRF) attacks.

• Disable Directory Browsing to prevent attackers from viewing the website’s file structure.

• Set a Content Security Policy (CSP) Header to reduce the risk of Cross-Site Scripting (XSS) attacks.

• Hide or secure hidden files that are not meant to be publicly accessible.

• Fix error messages that expose technical details about the application or server.

• Add missing security headers, such as X-Content-Type-Options, to prevent MIME type sniffing.

• Update or remove vulnerable JavaScript libraries found in the application.

• Remove server version information from HTTP response headers to reduce exposure to targeted attacks.

# **Detailed Observations**

# **Proof of Concept**

This section contains the proof of the above vulnerabilities as the screenshot of the vulnerability of the lab

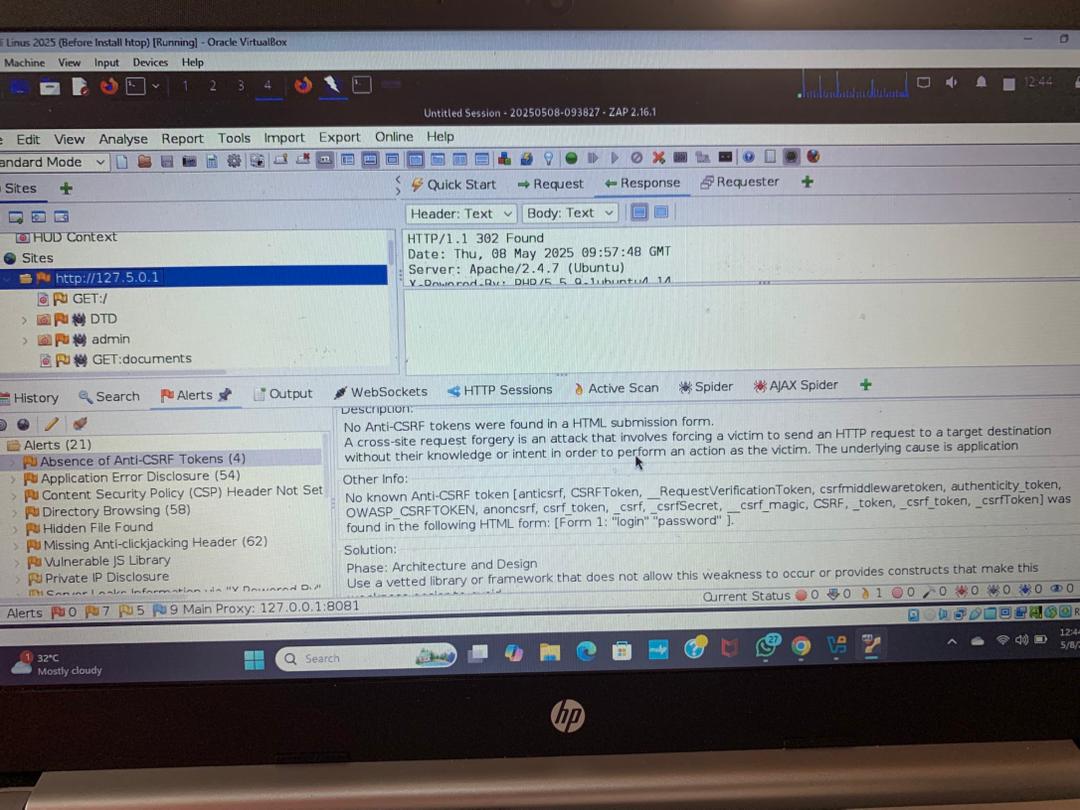
# **1. Service Vulnerability 1 (Absence of Anti-CSRF Tokens)**

| **Reference: Ref\_02** | **Impact Rating** |
| --- | --- |
| WEB\_VUL\_01: http://127.0.0.1:8081/login.php | **Medium** |
| **CVE ID (if applicable): N/A** | **CVSS Score** |
| [e.g., CVE-2023-XXXXX] | [Approx. 6.1)] |
| **Tools Used** | |
| [ OWASP ZAP, Openvas] | |
| **Vulnerability Description** | |
| [No Anti-CSRF tokens were found in HTML submission forms. This makes the application susceptible to Cross-Site Request Forgery (CSRF) attacks, where a malicious site can trick a user into performing actions on a target site without their consent. | |
| **How It Was Discovered** | |
| Auto (OWASP ZAP Active Scan) | |
| **Vulnerable Services/URLs** | |
| /login.php | |
| **Consequences of not Fixing the Issue** | |
| Attackers may forge requests on behalf of authenticated users, potentially altering data, changing passwords, or initiating financial transactions. | |
| **Suggested Countermeasures** | |
| Implement anti-CSRF tokens for state-changing operations.  Use frameworks or libraries that support CSRF protection by default.  Validate tokens server-side for each sensitive action. | |
| **References** | |
| https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site\_Request\_Forgery\_Prevention\_Cheat\_Sheet.html | |

**Figure 1: Evidence of Vulnerability Assessment**

***[Placeholder for Screenshots/Logs]***

Insert screenshot(s) output here, demonstrating the results of the vulnerability scan or manual assessment. Use annotations to highlight the key findings, such as:

1. Identified Vulnerability: Mark the specific vulnerability found (Anti-CSRF).
2. Affected Component: Highlight the area or component where the vulnerability exists (e.g., URL endpoint, input field).
3. Scanner/Tool Results: Point out relevant parts of the scan output, such as severity levels or detailed findings.
4. 

# Appendix A: Definitions of Likelihood and Consequence Matrix

| Likelihood Rating | | |
| --- | --- | --- |
| Level | **Descriptor** | **Description** |
| 5 | Expected | The risk is expected to occur one or more times in the next four (4) years |
| 4 | Probable | The risk is likely to occur at least once in the next four (4) years |
| 3 | Possible | It is possible that the risk could occur in the next four (4) years |
| 2 | Unlikely | The risk is unlikely to occur in the next four (4) years |
| 1 | Rare | There is a very remote chance the risk will occur – no notice of the risk manifesting itself elsewhere in the industry |

| Consequence Matrix | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| Level | **Descriptor** | **Impact On[[1]](#footnote-0)** | | | | |
| **People (Staff)** | **Stakeholders** | **Mandate / Objectives** | **Financials** | **Reputation** |
| 5 | Catastrophic | Extreme impact on people resulting in a significant loss of personnel. Major business units will be adversely impacted. | Very significant loss to stakeholders, and will severely impact the long term relationship. | Risk will render UVic unable to achieve its overall objectives or mandate. | Critical (>$10M) net asset or revenue loss or >40% impact on business unit budget (revenue or expense). | Critical loss of trust/credibility. Significant media attention. UVic will be subject to inordinate increase in oversight. |
| 4 | Major | Major impact on people and will result in the loss of personnel. Could cause long term dissatisfaction amongst existing staff. | Somewhat significant loss to stakeholders, and could have a long term impact on relationship. | Significant impact on UVic’s and/or business unit’s ability to achieve its objectives. | Significant (>$2.5M) net asset or revenue loss or >30% impact on business unit budget (revenue or expense). | Significant loss of trust/credibility. Guaranteed to generate media attention and increased scrutiny. |
| 3 | Moderate | Moderate impact on people. Morale will be impacted. Loss of key personnel not expected. | Moderate impact on stakeholders, but without any significant long term consequences. | Moderately impacts UVic’s and/or business unit’s ability to achieve its objectives. | Significant (>$1M) net asset or revenue loss or >15% impact on business unit budget (revenue or expense). | Potential for lost trust/credibility. May generate some media attention and result in increased scrutiny. |
| 2 | Minor | Minor impact. Morale could be affected for a short period of time. | Negligible short-term impact on some stakeholders. | Minor impact on the business unit’s ability to achieve its objectives. | Minor negative financial impact for the business unit. | Could have minor impact on business unit credibility. No increase in scrutiny is expected. No media attention. |
| 1 | Insignificant | Little or no impact on people and likely very little awareness of the event. | No impact on stakeholders. | Little or no impact on the business unit’s ability to achieve its objectives. | Impact is within normal operating budget margin fluctuations. | No impact on reputation. |

Likelihood of Potential Harms and Consequence Grid

| Likelihood | Consequence | | | | |
| --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 |
| 5 | Medium | High | High | Extreme | Extreme |
| 4 | Low | Medium | High | High | Extreme |
| 3 | Low | Medium | Medium | High | High |
| 2 | Low | Low | Medium | Medium | High |
| 1 | Low | Low | Low | Low | Medium |

# Appendix B – Supplemental Scan and Review Details

[[Add to individual appendices any relevant diagrams, lists, logs, etc, as deemed relevant and necessary.]]

1. The consequences of a successful cyber-attack is most likely to be felt in impact to reputation (information breach), mandate/objectives (Denial of Service), and stakeholders (information breach). Impact on staff and financials is likely to be moderate or less and most likely attributed to costs and morale from having to respond to an information breach or an attack that causes widespread data integrity disruption. [↑](#footnote-ref-0)