Vulnerability Assessment Report

For bWAPP Web Application

By [OKEKE NKASIOBI IRENE]

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

Request Ticket	RT09219

Request and Report Date	To be completed by 9th December. [[9th April, 2025]]
Product or Service Under Review	Bwapp, http://localhost/bWAPP/
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	Name: OKEKE NKASIOBI IRENE Title: Miss Supervisor: Department: VAPT Phone number: 09064932389 Email: okekenkasy@gmail.com

2. 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.

3. Summary of Recommendations

- **SQL injection:** vulnerability found in the login form. Implement proper input sanitization and use parameterized queries.
- **Cross-site scripting XSS:** escape user inputs to prevent malicious javascript execution.
- **Outdated transfer protocol:** updating the http server to https for secure encryption.

4. Detailed Observations

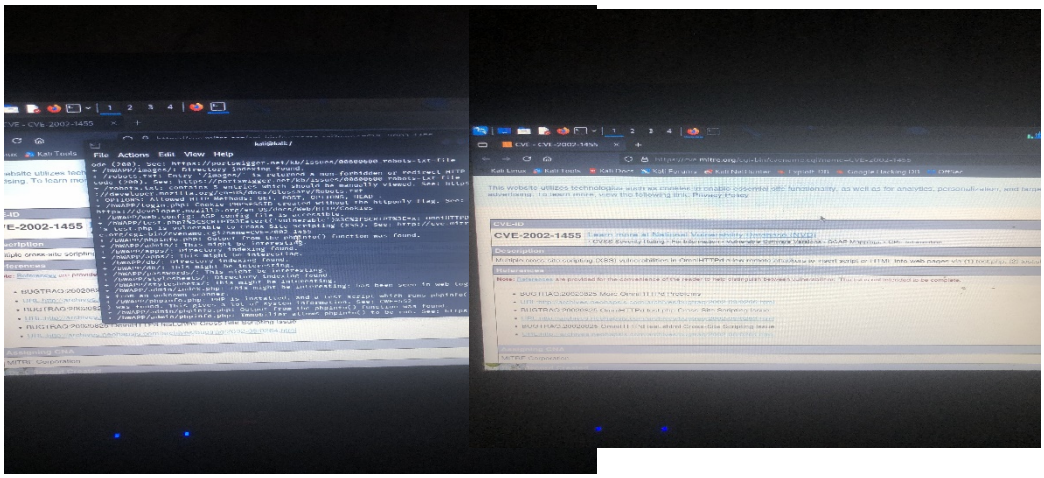
Proof of Concept

1. Service Vulnerability 1 (XSS)

Reference	Impact Rating
WEB_VUL_01	**Medium**
CVE ID (if applicable)	**CVSS Score**
[e.g., CVE-2002-1455	6.5 (medium)
Tools Used	
Nikto	
Vulnerability Description	
Nikto detected an XSS vulnerability in /test.php where user input is not properly sanitized allowing attackers to inject malicious javascript.	
How It Was Discovered	
Manual Analysis/ Auto analysis: nikto injected an xss payload (<script>alert("vulnerable')</script>).	
Vulnerable Services/URLs	
/test.php	
Consequences of not Fixing the Issue	
This vulnerability could allow attackers to steal session cookies, redirect users to malicious websites or perform actions on behalf of the user.	
Suggested Countermeasures	
Sanitize all user inputs, use proper output encoding (HTML escaping) and implement content security policy CSP headers to mitigate xss attacks.	
References	
• BUGTRAQ:20020825 More OmniHTTPd problems • URL:archives.neophasis.com/archives/bugtraq/2002-08/0266.html •	

Figure 1: Evidence of Vulnerability Assessment

[Placeholder for Screenshots/Logs]



1. Identified Vulnerability: XSS
2. Affected Component: /test.php
3. Scanner/Tool Results:
   +/bwapp/test.php?%3cscript%3Ealert(‘vulnerable’)3c%2FSCRIPT%3E=x
   OmniHTTPD’s test.php is vunerable to xss.

(Make sure to redact any sensitive information before adding the screenshot

2. Service Vulnerability 2 (directory listing)

Reference	**Impact Rating**
WEB_VUL_02	
CVE ID (if applicable)	**CVSS Score**
Tools Used	
Nikto	
Vulnerability Description	
Nikto found that directory listing is enabled on several directories such as /images/, /admin, /passwords, /db.	
How It Was Discovered	
Nikto discovered that the sever was not configured to prevent directory listing	
Vulnerable Services/URLs	
/images/, /admin, /passwords, /db.	

Consequences of not Fixing the Issue
Attackers could access files that might contain sensitive information such as config files, logs or backup files.
Suggested Countermeasures
References
Disable directory listing.

3. Service Vulnerability 2 (http cookies lack httponly flag)

Reference	Impact Rating
WEB_VUL_03	**high**
CVE ID (if applicable)	**CVSS Score**
Tools Used	
Nikto	
Vulnerability Description	
The application does not set the httponly flag on cookies.	
How It Was Discovered	
Nikto discovered that the sever was not configured to prevent directory listing	
Vulnerable Services/URLs	
Affects all pages setting cookies.	
Consequences of not Fixing the Issue	
If an Attacker could successfully exploits an xss vulnerability, they can steal session cookies and hijack user sessions	
Suggested Countermeasures	
Ensure that cookies are set with httponly flag to prevent acces via javascript. Also set the secure flag for cookies when using https.	
References	
Disable directory listing.	

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]				
		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] 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.

1	Low	Low	Low	Low	Medium

Appendix B – Supplemental Scan and Review Details