Lab 2: OWASP Top 10 Web Application Testing for GRC Professionals

REG NO:2025/GRC/11032

To: CISO & Application Development Management

From: GRC Audit Team

Date: 21-09-2025

Executive Summary

An assessment of the OWASP BWA server multiple high-risk vulnerabilities that align with the OWASP Top 10. These issues indicate gaps in application security and pose a risk to both customer and company data.

Key Findings:

- Broken Access Control (A01:2021): By changing the typeid parameter from 6—2 in BodgeIt's product .jsp, allowed access to product categories without proper authorization. This confirms that unauthorized users could view or manipulate data they shouldn't have access to.

- SQL Injection (A03:2021): The search field is vulnerable and could allow attackers to retrieve or modify the database.

- Cryptographic Failures (A02:2021): Credentials are transmitted in cleartext, which could be intercepted.

- Other WordPress Scan Findings: Automated scanning of the WordPress site revealed SSL Injection, HTTP Request Smuggling, and LDAP Injection vulnerabilities. These were not manually exploited, but highlight additional potential risks.

Recommended Actions:

1. **Immediate Mitigation**: Restrict access to affected systems until proper access controls are implemented.

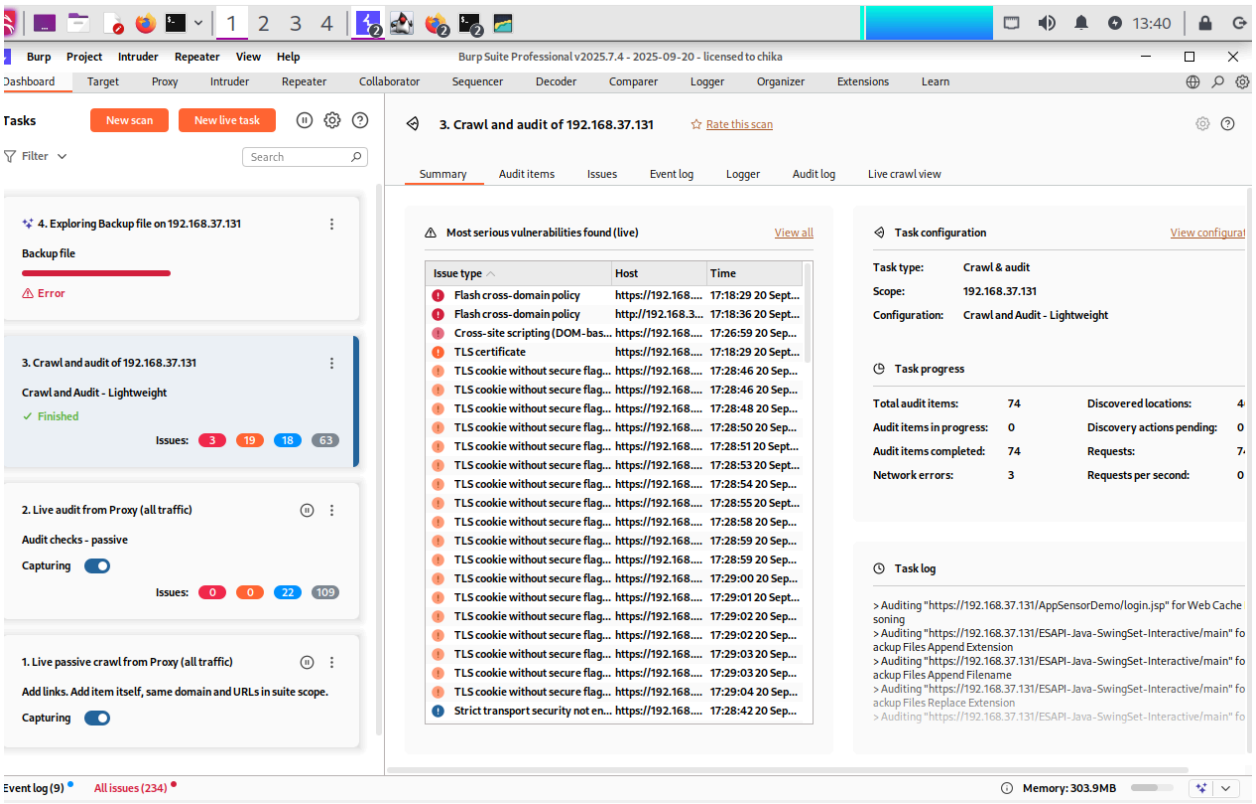
2. **Remediation:** Apply server-side authorization checks, enforce ACLs, and use indirect object references to prevent unauthorized data access.

3. **Process Improvement**: Provide security training to developers focused on the OWASP Top 10. Integrate SAST/DAST tools like Burp Suite into CI/CD pipelines.

4. **Penetration Testing**: Conduct a full third-party pentest before deploying similar applications in production.

OWASP Top 10 category	Vulnerability Example	Affected Application	Inherent Risk {L/M/H}	Compliance violation	Business impact
Ao1: Broken Access Control	Unprotected Admin Page	Bodgelt store	H	PCI DSS 7.2.1	Unauthorized access, privilege escalation
A02: Cryptography failures	Cleartext password transmission	WebGoat	H	PCI DSS 4.1	Credential theft, account takeover
AO3: injection	SQL injection in search	Bodgelt store	H	PCI DSS 6.5.1	Full database compromise data loss
A07: Identification Failures	Weak Password Policy	BodgeIt Store	H	NIST CSF PR.AC-	Unauthorized access, initial breach vector

Figure 1: Burp Suite scan results for the WordPress instance showing identified vulnerabilities including SQL Injection, Cross Site Scripting, and Broken Access Controls.



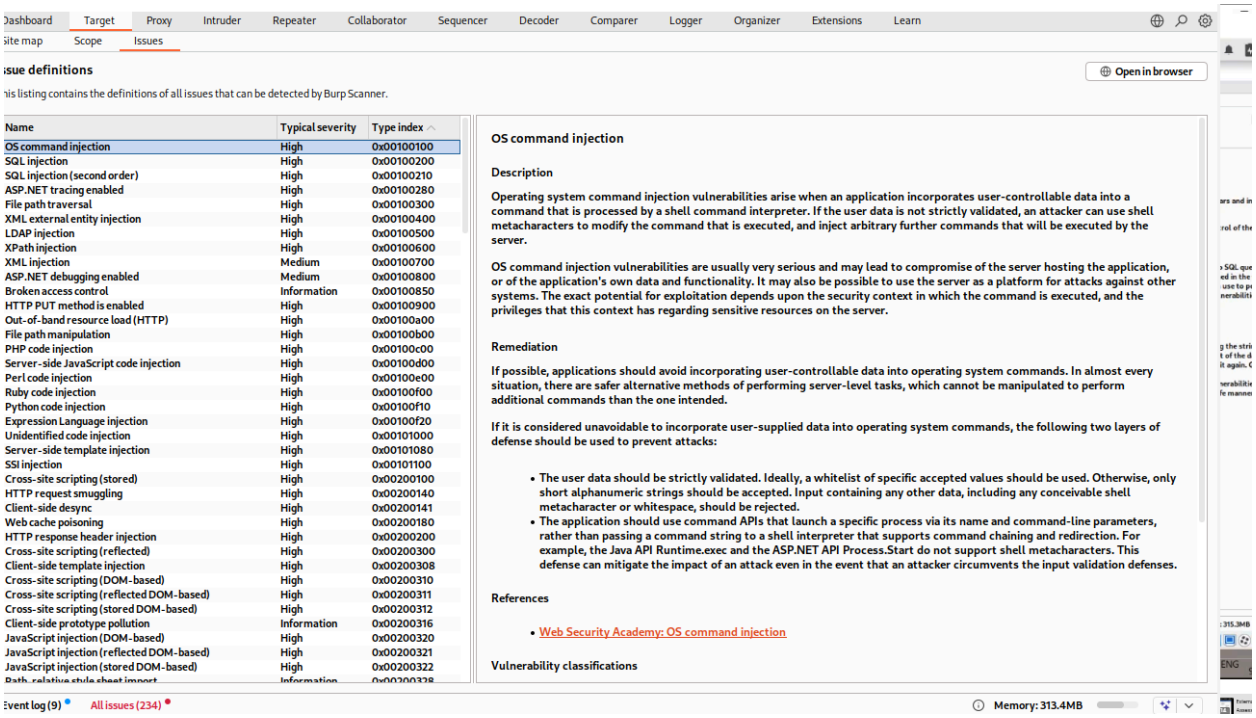
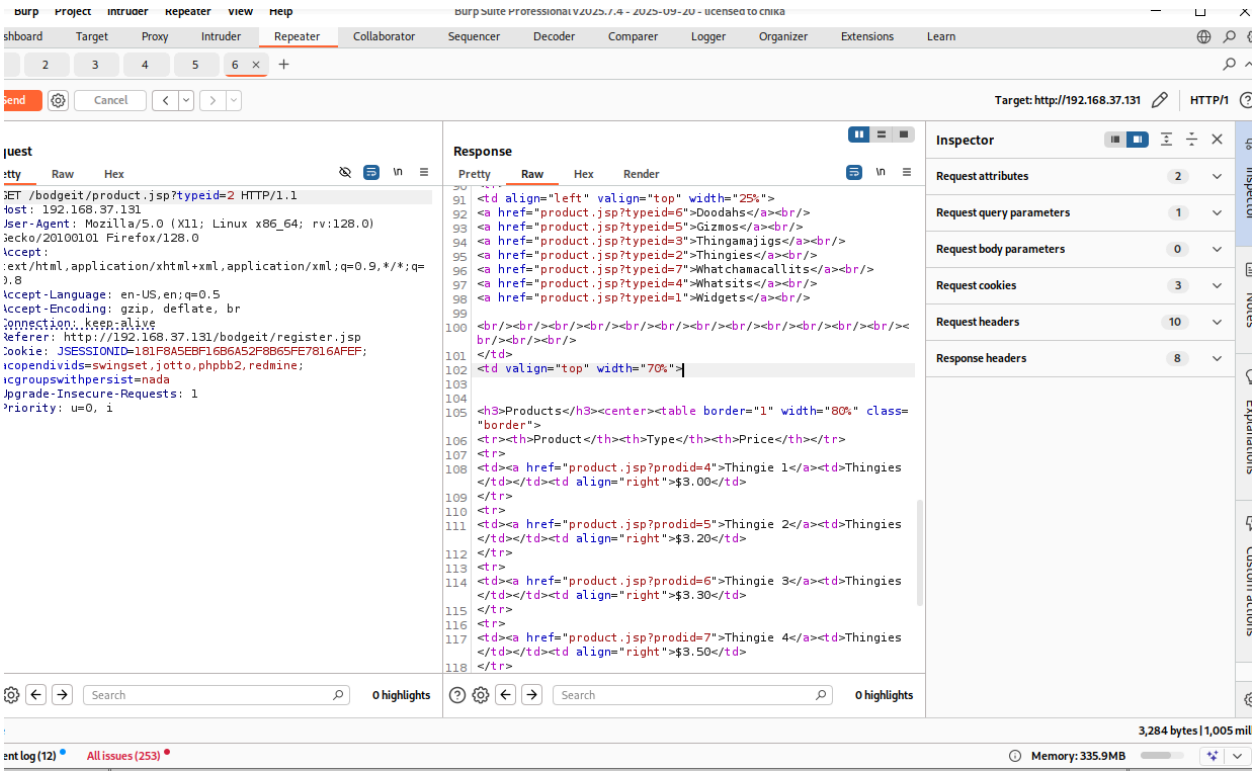


Figure 2: Successful Broken Access Control test using Burp Repeater. Changing the typeid parameter allowed access to restricted product information.



Conclusion:

This assessment demonstrates that even intentionally vulnerable or training applications can present high risk vulnerabilities. For GRC purposes, understanding the QWASP Top 10 is essential for validating security controls, assessing risk, and improving development practice.