OWASP Top 10 Application Security Audit

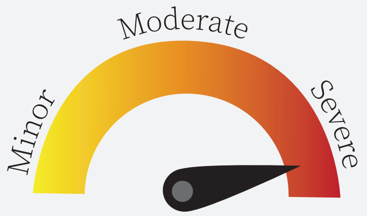
The Open Web Application Security Project is a 501(c)3 worldwide organization focused on improving the security of software. OWASP maintains a Top 10 List that outlines the most critical web application security flaws. The list follows, along with commentary from Imaginary Landscape.

A1 Security Risk Description: Injection

Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

OWASP Injection Risk Ratings

Exploitability of Attack Vectors	Prevalence of Security Weakness	Detectability of Security Weakness
EASY	COMMON	AVERAGE



Identified Open Security Risk Vulnerabilities

There are instances where the ORM has been circumvented with direct SQL queries via ©psycopg2 execute statements. Some of these raw queries are not properly passing query parameters, which could expose the query to SQL injection attack. See Appendix A for a complete listing.

Technical and Business Impact

The injection vector identified poses significant risk as it is using an INSERT argument. As constructed, the raw SQL statements can be co-opted by an attack to manipulate the database in unintended ways such as the ability to create accounts, drop full tables and retrieve lists of sensitive data.

Recommended Risk Remediation

1. Identify each instance of injection vulnerability (see appendix A)
2. Review the underlying task for each instance
3. Transfer the task into the ORM
4. Test to ensure expected results

A3 Security Risk: Cross-Site Scripting (XSS)

Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.