10 Injection Vulnerabilities

That Will Haunt You in Your Sleep

There are many different ways to inject harmful code into systems. We have put together a list with 10 particularly dangerous and frequent injection vulnerabilities.

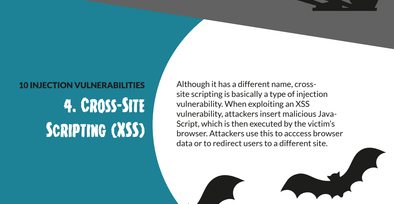
10 INJECTION VULNERABILITIES

1. Code Injection

Code injections are a highly common type of web vulnerabilities, in which the attacker injects code through the text input. This is possible if the application lacks input validation. The consequences of such an attack are often data theft and functionality.

10 INJECTION VULNERABILITIES

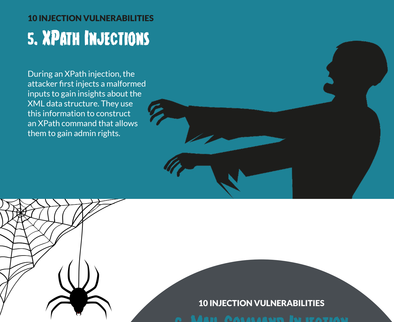
2. SQL Injection



To communicate with databases, most web services use SQL as a data access language. Attackers can exploit this by inserting an SQL query to the database via a text field. This allows attackers to make changes to the database and extract or destroy information.

10 INJECTION VULNERABILITIES

3. Command Injection



During command injections, attackers mimic the command that the web application would normally send to the operating system. Unfixed command injection vulnerabilities can lead to exposure of sensitive information or give attackers control over the entire system.

10 INJECTION VULNERABILITIES

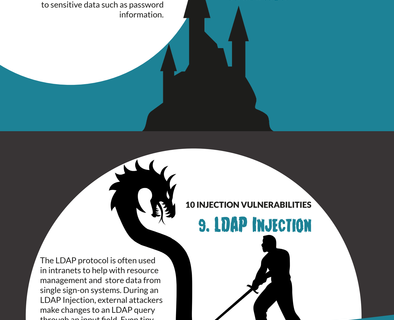
4. Cross-Site Scripting (XSS)

Although it has a different name, cross-site scripting is basically a type of injection vulnerability. When exploiting an XSS vulnerability, attackers insert malicious Java-Script, which is then executed by the victim's browser. Attackers use this to acccess browser data or to redirect users to a different site.

10 INJECTION VULNERABILITIES

5. XPath Injections

During an XPath injection, the attacker first injects a malformed inputs to gain insights about the XML data structure. They use this information to construct an XPath command that allows them to gain admin rights.



10 INJECTION VULNERABILITIES

6. Mail Command Injection

When email servers are not properly secured, they become vulnerable to injection attacks. To exploit email servers and services that build IMAP/SMTP statements, attackers inject malicious code via email messages. This allows them to override server restrictions and send spam messages from the server.

10 INJECTION VULNERABILITIES

7. CRLF Injection

Carriage return and line feed, is an input that represents the end of a line or command in several web protocols (HTTP, MIME, NNTP). When user input is not validated sufficiently, attackers can inject CRLF code snipets which allow them to extract data, modify cookies and conduct further injection attacks.

10 INJECTION VULNERABILITIES

8. Host Header Injection

The main target of a host header injection is actually the virtual host of a web application. To exploit this vulnerability, attackers inject code, through the host header, straight to a virtual host. This attack could grant attackers access to sensitive data such as password information.

10 INJECTION VULNERABILITIES

9. LDAP Injection

The LDAP protocol is often used in intranets to help with resource management and store data from single sign-on systems. During an LDAP injection, external attackers make changes to an LDAP query through an input field. Even tiny changes in the LDAP, can give attackers ungranted access.

10 INJECTION VULNERABILITIES

10. XXE-Injection

During an XXE injection, attackers aim to inject code into legacy functionality in XML parsers. Attackers can then design XML documents to execute various commands, such as f.e. remote code executions. XEE injections are listed number four in the OWASP top ten vulnerability ranking.

CODE INTELLIGENCE
Rheinwerkallee 6
D-53227 Bonn

CONTACT US
+49 228 2869 5830
sales@code-intelligence.com