Laud Mills

Analysis of SQL Injection and Cross-Site Scripting attacks

1. Name the most effective technique that is used to identify SQL injection vulnerability.

The choice of effectiveness of techniques to identify SQL injection vulnerability mostly depends on the need and the specific scenario being dealt with. There are however many tools such as SQLmap, OWASPZap Burp Suit that can effectively identify SQL injection vulnerabilities.

1. List a few payloads (5 at least) related to SQL injection vulnerability.

They are:

Time-based Blind SQL injection: ' OR IF(1=1, SLEEP(5), 0) –

String-based SQL injection: ' AND 'a' = 'a –

Boolean-based Blind SQL injection: ' AND 1=1 –

Basic Union-based SQL injection: ' UNION SELECT NULL, username, password FROM users –

Error-base SQL injection: ' OR 1=CONVERT(int, (SELECT @@version)) --

1. Can an automated scanner be sufficient to discover SQL Injection?

No. Automated scanning is effective and fast; however, it is prone to problems such as false negatives and positive which might have dire impact on business critical systems. It is therefore very commendable to use manual scanning to complement automated scans.

1. Are stored procedures for authentication sufficient to prevent from SQL injection attack? If “Yes” then justify your answer, if “No” then what else is required to make it robust?

The answer is No. This is because though it is a good practice, it is prone to security failure due to syntax errors, lack of input validation which can have serious consequences. When used with other factors such as Web Application firewalls, the principle of lease privilege, secured password storage etc this could provide a better authentication posture.

1. If a SQL injection vulnerability is available in the application, what exploitation attackers are able to do? List any four.

Data exfiltration, authentication bypass, server compromise and data manipulation.

1. List four methods to prevent the web application from SQL Injection.

Use input validation and sanitization, stored procedures, parameterized queries and least privilege principle

1. Name the three types of XSS (Cross Site Scripting)? And describe the functionality of each.

They are: Stored, Reflected and Document Object Model-based Cross Site Scripting.

The Stored XSS functions as users visit affected pages because the scripts are stored on the server.

The Reflected XSS normally forms part of the form input or URL and it is executed when the user clicks on the URL.

THE DOM XSS functions when the weaknesses in the client side code is exploited by the injection of malicious script.

1. List out key HTML entities used in XSS.

< → &lt;

> → &gt;

& → &amp;

" → &quot;

' → &apos;

1. List three tools and describe the functionality (one-line short answer) that are helpful in identifying XSS vulnerabilities?

Burp Suite: A web vulnerability scanner that intercepts and analyzes HTTP/S traffic to identify potential XSS and other security flaws.

OWASP ZAP : An open-source security scanner that automatically detects XSS vulnerabilities by scanning web applications for common attack vectors.

XSSer: It is an automated penetration testing tool designed to detect and exploit XSS vulnerabilities in web applications.