SQL Injection Vulnerability Report

Scan Date: 2025-07-23 13:15:28
Target URL: http://testphp.vulnweb.com/listproducts.php?cat=1
Request Method: GET
Total Payloads Tested: 6

Overview of SQL Injection Techniques and Their Impact

The following SQL injection techniques were detected:
1. Error-based SQL Injection
2. Union-based SQL Injection

Analysis of Real-World SQL Injection CVEs

CVE ID	Title	Description	Impact
CVE-2023-34362	MOVEit Transfer SQL Injection	A UNION-based SQL injection in MOVEit Transfer allowed attackers to enumerate and exfiltrate sensitive data.	Used in a large-scale ransomware attack affecting multiple organizations.

■ Explanation of PoC Methodology and Detection Logic

The SQL Injection PoC tool dynamically detects different types of SQLi vulnerabilities by analyzing the server's response to crafted payloads.

Detected Techniques: Error-based SQL Injection, Union-based SQL Injection

Detection Logic:

Error-based SQL Injection
- Payloads are injected to force SQL errors (e.g., `'`, `"`, or malformed queries). - The tool examines the response for database error messages such as `SQLSTATE`, `You have an error in your SQL syntax`, etc.

Union-based SQL Injection
- The tool attempts to use `UNION SELECT` statements to extract additional data from other tables. - Detection is based on successful merging of query results with the existing page.

■ Recommendations for Preventing SQL Injection

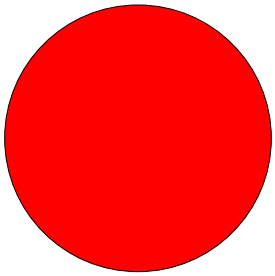
Error-based SQL Injection

• Do not expose detailed SQL error messages to end users.
• Use generic error messages and log internally.

Union-based SQL Injection

• Validate and sanitize user inputs.
• Use least privilege principle for DB user accounts.

Scan Summary Pie Chart



Detailed Payload Scan Results

Parameter	Payload	Status	Note
cat	' OR '1'='1' --	VULNERABLE	SQL error detected: 'you have an error in your sql syntax;'
cat	" OR "1"="1" --	VULNERABLE	SQL error detected: 'you have an error in your sql syntax;'
cat	' UNION SELECT NULL--	VULNERABLE	SQL error detected: 'you have an error in your sql syntax;'
cat	' UNION SELECT 1,2,3 --	VULNERABLE	SQL error detected: 'you have an error in your sql syntax;'
cat	'; WAITFOR DELAY '00:00:05' --	VULNERABLE	SQL error detected: 'you have an error in your sql syntax;'
cat	'; SELECT SLEEP(5) --	VULNERABLE	SQL error detected: 'you have an error in your sql syntax;'