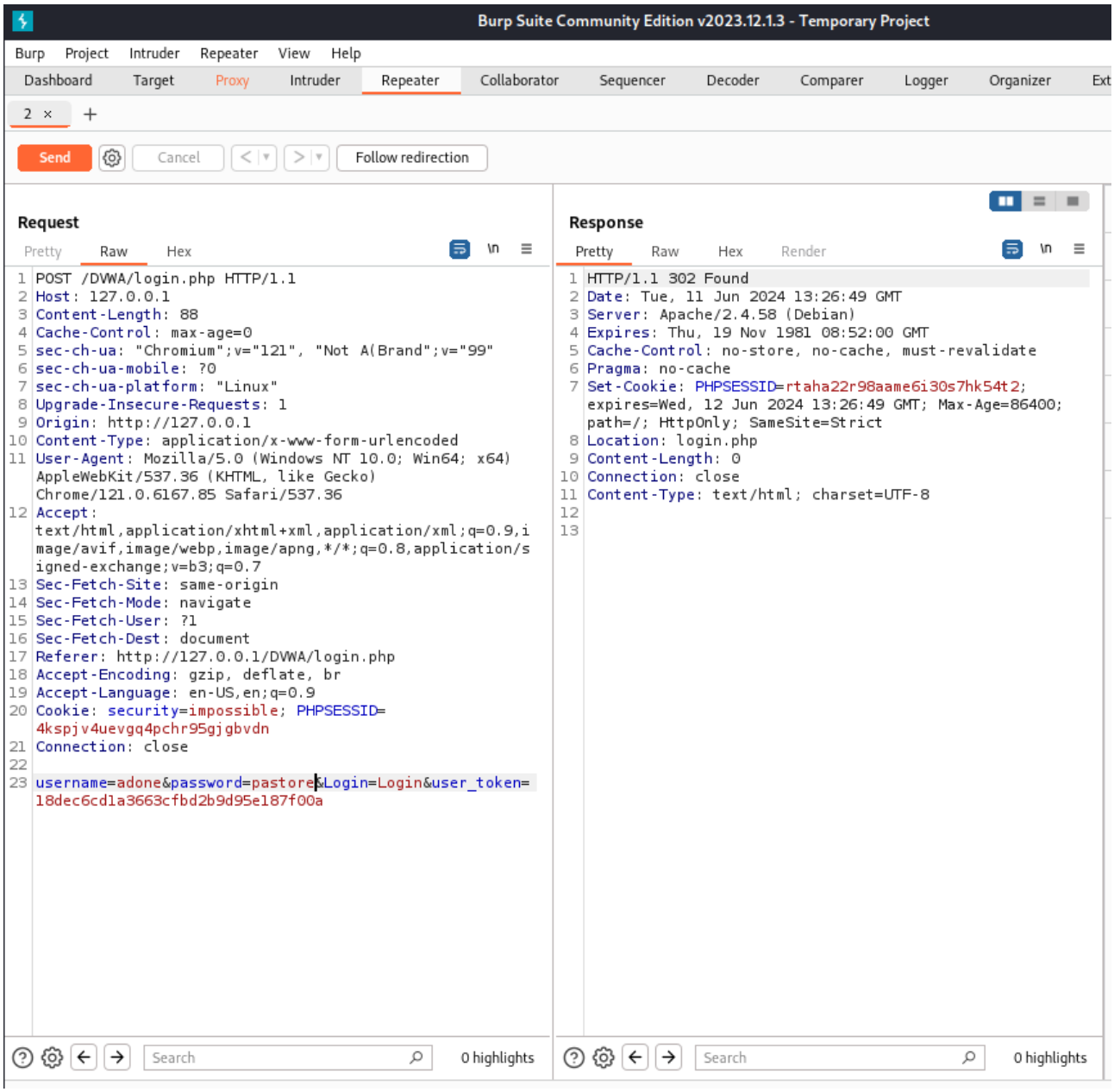
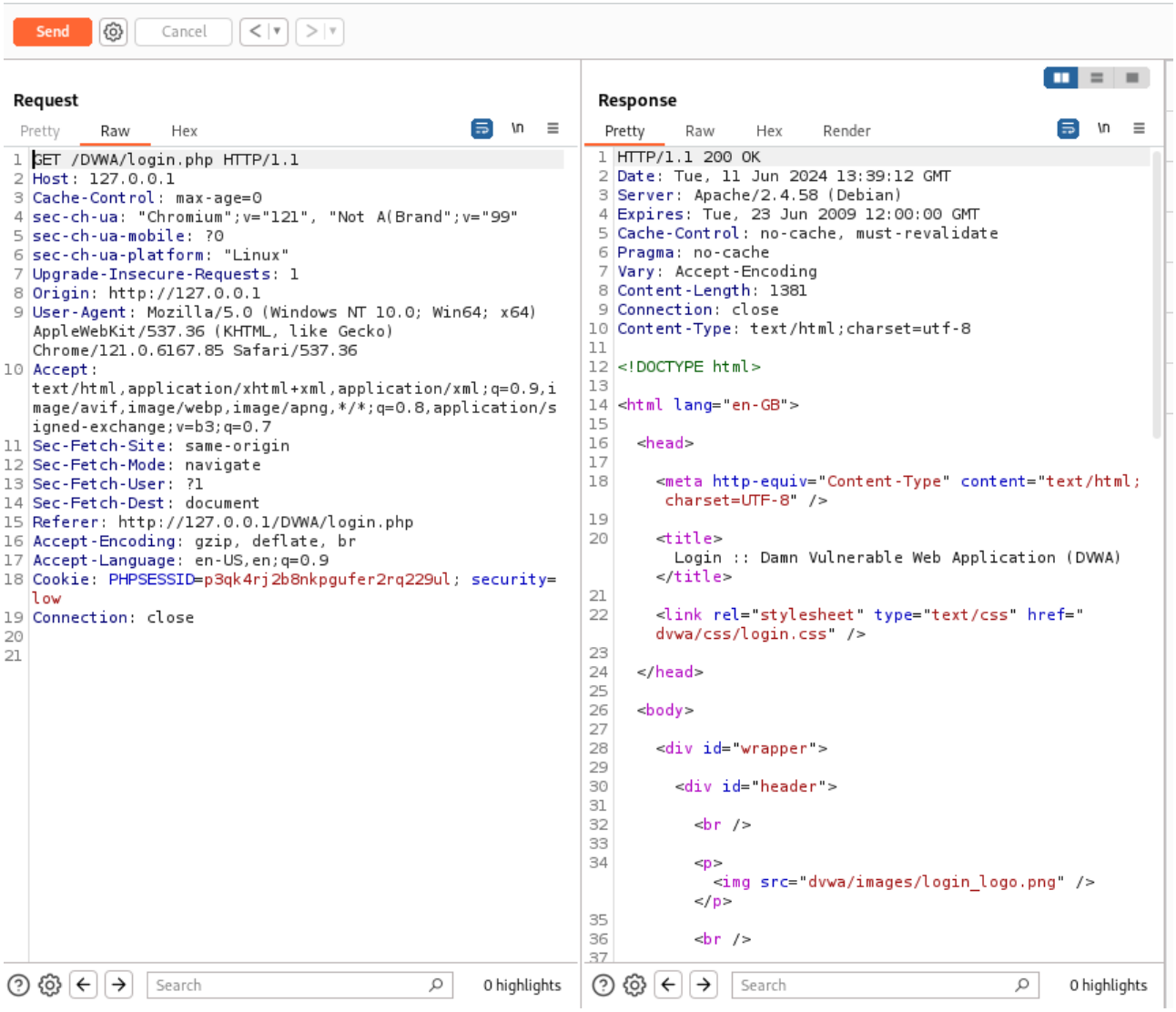
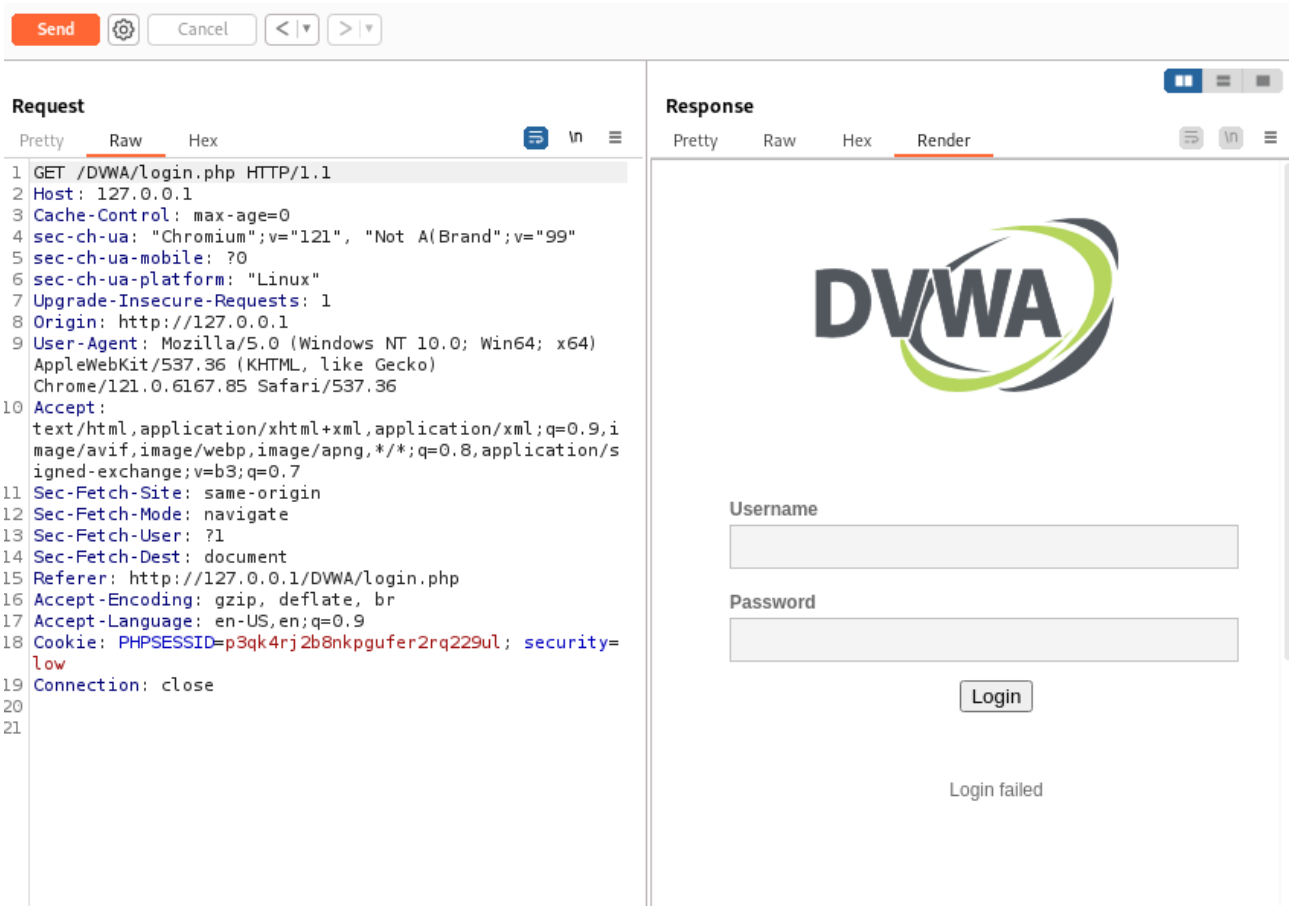

root@kali: /var/www/html/DVWA/config
File Actions Edit View Help
┌──(root㉿kali)-[/var/www/html]
└─# git clone https://github.com/digininja/DVWA
Cloning into 'DVWA'...
remote: Enumerating objects: 4580, done.
remote: Counting objects: 100% (130/130), done.
remote: Compressing objects: 100% (96/96), done.
remote: Total 4580 (delta 52), reused 94 (delta 33), pack-reused 4450
Receiving objects: 100% (4580/4580), 2.34 MiB | 1.96 MiB/s, done.
Resolving deltas: 100% (2147/2147), done.
┌──(root㉿kali)-[/var/www/html]
└─# chmod -R 777 DVWA/
┌──(root㉿kali)-[/var/www/html]
└─# cd DVWA/config
┌──(root㉿kali)-[/var/www/html/DVWA/config]
└─# cp config.inc.php.dist config.inc.php
┌──(root㉿kali)-[/var/www/html/DVWA/config]
└─# nano config.inc.php
┌──(root㉿kali)-[/var/www/html/DVWA/config]
└─# service mysql start
┌──(root㉿kali)-[/var/www/html/DVWA/config]
└─# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 39
Server version: 10.11.8-MariaDB-1 Debian n/a
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.
Support MariaDB developers by giving a star at https://github.com/MariaDB/server
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.


For server side help, type 'help contents'
MariaDB [(none)]> delete user 'kali'@'127.0.0.1' identified by 'kali' ;
ERROR 1046 (3D000): No database selected
MariaDB [(none)]> create user 'kaly'@'127.0.0.1' identified by 'kaly' ;
Query OK, 0 rows affected (0.003 sec)
MariaDB [(none)]> grant all privileges on dvwa.* to 'kaly'@'127.0.0.1' identified by 'kaly' ;
Query OK, 0 rows affected (0.019 sec)
MariaDB [(none)]> exit
Bye
┌──(root㉿kali)-[/var/www/html/DVWA/config]
└─# service apache2 start
┌──(root㉿kali)-[/var/www/html/DVWA/config]
└─# cd /etc/php/8.1/apache2
cd: no such file or directory: /etc/php/8.1/apache2
┌──(root㉿kali)-[/var/www/html/DVWA/config]
└─# cd /etc/php/8.2/apache2
┌──(root㉿kali)-[/etc/php/8.2/apache2]
└─# service apache2 start


Burp Suite Community Edition v2023.12.1.3 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Ext
2 ×
Send Cancel Follow redirection
Request
Pretty Raw Hex
1 POST /DVWA/login.php HTTP/1.1
2 Host: 127.0.0.1
3 Content-Length: 88
4 Cache-Control: max-age=0
5 sec-ch-ua: "Chromium";v="121", "Not A(Brand";v="99"
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "Linux"
8 Upgrade-Insecure-Requests: 1
9 Origin: http://127.0.0.1
10 Content-Type: application/x-www-form-urlencoded
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.85 Safari/537.36
12 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Referer: http://127.0.0.1/DVWA/login.php
18 Accept-Encoding: gzip, deflate, br
19 Accept-Language: en-US,en;q=0.9
20 Cookie: security=impossible; PHPSESSID=4kspjv4uevgq4pchr95gjgbvdn
21 Connection: close
22
23 username=adone&password=pastore&Login=Login&user_token=18dec6cd1a3663cfbd2b9d95e187f00a
Search 0 highlights
Response
Pretty Raw Hex Render
1 HTTP/1.1 302 Found
2 Date: Tue, 11 Jun 2024 13:26:49 GMT
3 Server: Apache/2.4.58 (Debian)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, must-revalidate
6 Pragma: no-cache
7 Set-Cookie: PHPSESSID=rtaha22r98aame6i30s7hk54t2; expires=Wed, 12 Jun 2024 13:26:49 GMT; Max-Age=86400; path=/; HttpOnly; SameSite=Strict
8 Location: login.php
9 Content-Length: 0
10 Connection: close
11 Content-Type: text/html; charset=UTF-8
12
13
Search 0 highlights


Send
Cancel
Request
Pretty
Raw
Hex
GET /DVWA/login.php HTTP/1.1
Host: 127.0.0.1
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="121", "Not A(Brand";v="99"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
Origin: http://127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.85 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://127.0.0.1/DVWA/login.php
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=p3qk4rj2b8nkpgufer2rq229ul; security=low
Connection: close
Search
0 highlights
Response
Pretty
Raw
Hex
Render
HTTP/1.1 200 OK
Date: Tue, 11 Jun 2024 13:39:12 GMT
Server: Apache/2.4.58 (Debian)
Expires: Tue, 23 Jun 2009 12:00:00 GMT
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 1381
Connection: close
Content-Type: text/html;charset=utf-8
<!DOCTYPE html>
<html lang="en-GB">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<title>
Login :: Damn Vulnerable Web Application (DVWA)
</title>
<link rel="stylesheet" type="text/css" href="dvwa/css/login.css" />
</head>
<body>

Search
0 highlights


Send
Cancel
Request
Pretty
Raw
Hex
GET /DVWA/login.php HTTP/1.1
Host: 127.0.0.1
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="121", "Not A(Brand";v="99"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
Origin: http://127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.85 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://127.0.0.1/DVWA/login.php
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=p3qk4rj2b8nkpgufer2rq229ul; security=low
Connection: close
Response
Pretty
Raw
Hex
Render
DVWA
Username
Password
Login
Login failed