TIC4304 Project Shadow Daemon

- Name: Ke Yule
- Student Number: A0211495H E0493826

View the markdown version for better formatting at:
https://github.com/keyule/4304-project/blob/main/report.md

Setting up Shadowd

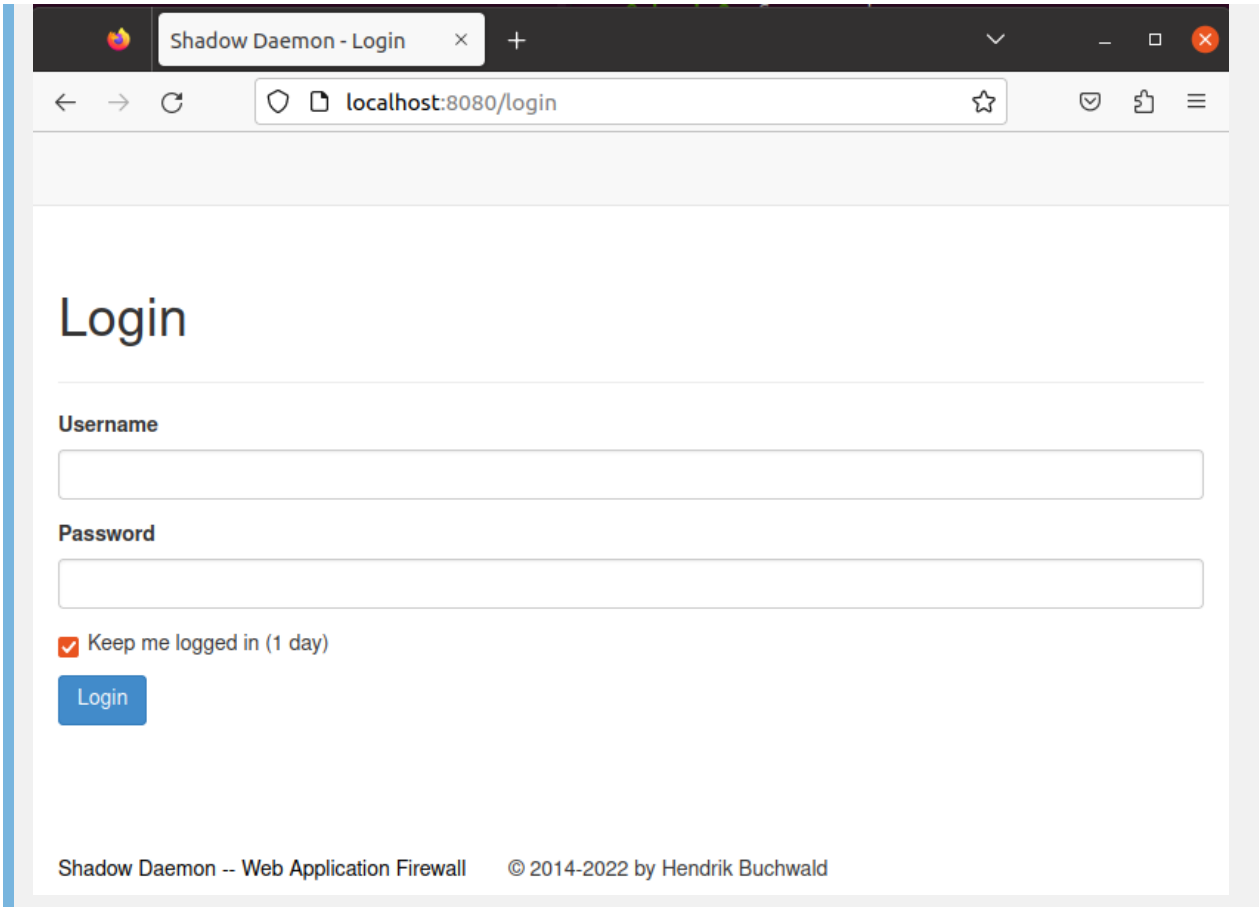
1. Installing Docker

```
curl -fsSL https://get.docker.com -o get-docker.sh
sudo sh get-docker.sh
sudo apt install docker-compose
```

2. Installing shadowd

```
git clone https://github.com/zecure/shadowdctl.git
cd shadowdctl
sudo ./shadowdctl up -d
sudo ./shadowdctl exec web ./app/console swd:register --admin --name=test
```

3. Shadowd should be up now and when we navigate to 127.0.0.1:8080 we can see the login page for shadowd



4. Login and create new Profle with `Server ip: *`

Setting up Apache webserver

1. Install Apache

```
sudo apt install apache2 php libapache2-mod-php
```

2. Download php connector

```
wget https://shadowd.zecure.org/files/shadowd_php-2.2.0.tar.gz
tar -xvf shadowd_php-2.2.0.tar.gz
sudo mkdir /usr/share/shadowd
sudo mv shadowd_php-2.2.0 /usr/share/shadowd/php
sudo chown -R root:root /usr/share/shadowd/php
```

3. Add auto prepend

   - File: `/etc/apache2/sites-available/000-default.conf`
   - Just add the following line anywhere in the file

```
php_value auto_prepend_file /usr/share/shadowd/php/shadowd.php
```

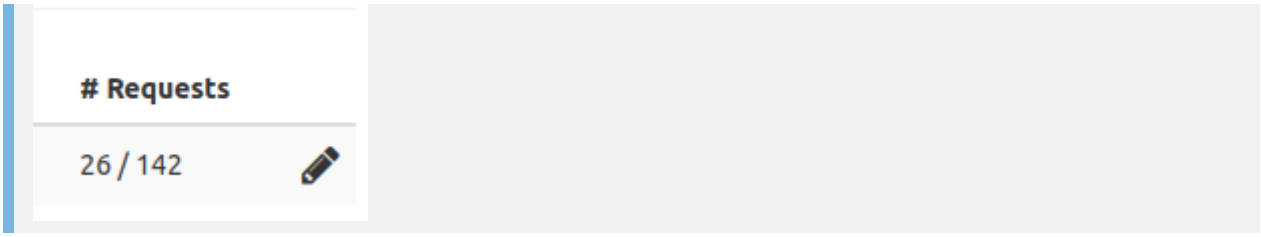
4. Set up settings for connector.ini

```
sudo mkdir /etc/shadowd
sudo cp /usr/share/shadowd/php/misc/examples/connectors.ini /etc/shadowd
sudo chown root:www-data /etc/shadowd/connectors.ini
sudo chmod 640 /etc/shadowd/connectors.ini
```

   - connector.ini:

```
[shadowd_php]
profile=1
key=12345
debug=1
```

5. After this we should be able to see requests come in onto profile 1 on the dashboard for shadowd



Setting up a php page thats vulnerable to xss

```
- I just stole the code from homework2 warmup.php and warmup_server.php and added
it into `var/www/html`
- code can be found in Appendix
```

Adding a whitelist to only enable Special Characters

```
```
Profile: 1 (Test)
Caller: /var/www/html/warmup_server.php
Path: POST|content
Min. length: 1
Max. length: 100
Filter: Special Characters
Status: Activated
```

- Change the profile from passive to active
```

Done!

XSS is now blocked! I dont know how to add a screenshot for it as theres no popup to show its blocked. It just doesnt send the request, and stays on the same page. So there isnt really anything to show.

Appendix

warmup.php:

```
<!DOCTYPE html>
<html lang="en">
<head></head>
<body>
    <script>
        function logoutclick() {
            window.location.href = "logout.php";
        }
        function checkpost() {
            if (myform.content.value=="") {
                alert("Please input xss attack code!");
            }
        }
    </script>
    <div class="page-header">
        <h1>Hi, This Page Is for Warmup Task.</h1>
    </div>
    <form action="./warmup_server.php" name="myform" method="POST"
onsubmit="return checkpost();">
        <legend>Please Insert Your Attack Code:</legend>
        <br>
        <input value="" name="content" style="width:300px; height:20px;"/>
        <button value="submit" name="submit" class="button">Submit</button>
    </form>
    <br>
    <br>
    <button name="logout" class="button" onclick = "logoutclick()">Sign
out</button>
</body>
</html>
```

warmup_server.php

```
<?php
    $content = $_POST["content"];
    if ($content == '') {
        header("location: warmup.php");
    }
    echo "The last xss code: [" . $content ."]";
?>

<!DOCTYPE html>
<html lang="en">
```

```
<head></head>
<body>
    <script>
        function backclick() {
            window.location.href = "warmup.php";
        }
        function logoutclick() {
            window.location.href = "logout.php";
        }
    </script>
    <p>
        <button name="back" class="button" onclick = "backclick()">Back</button>

            
             
        <button name="logout" class="button" onclick = "logoutclick()">Sign
out</button>
    </p>
</body>
</html>
```