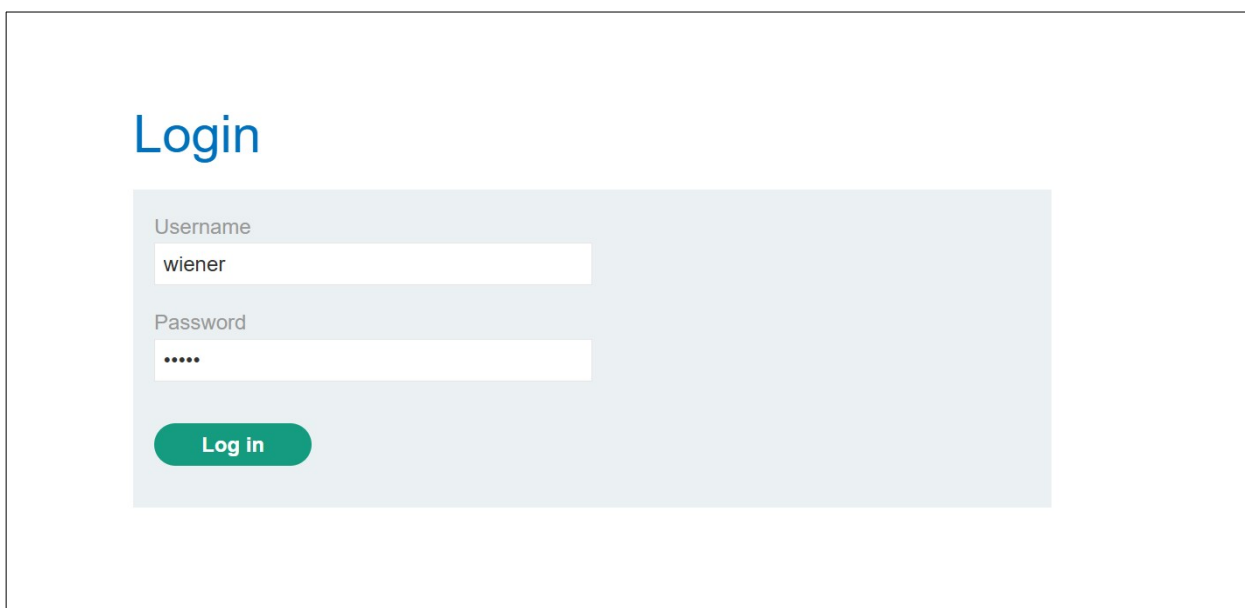


Lab: Exploiting path mapping for web cache deception

Задача:

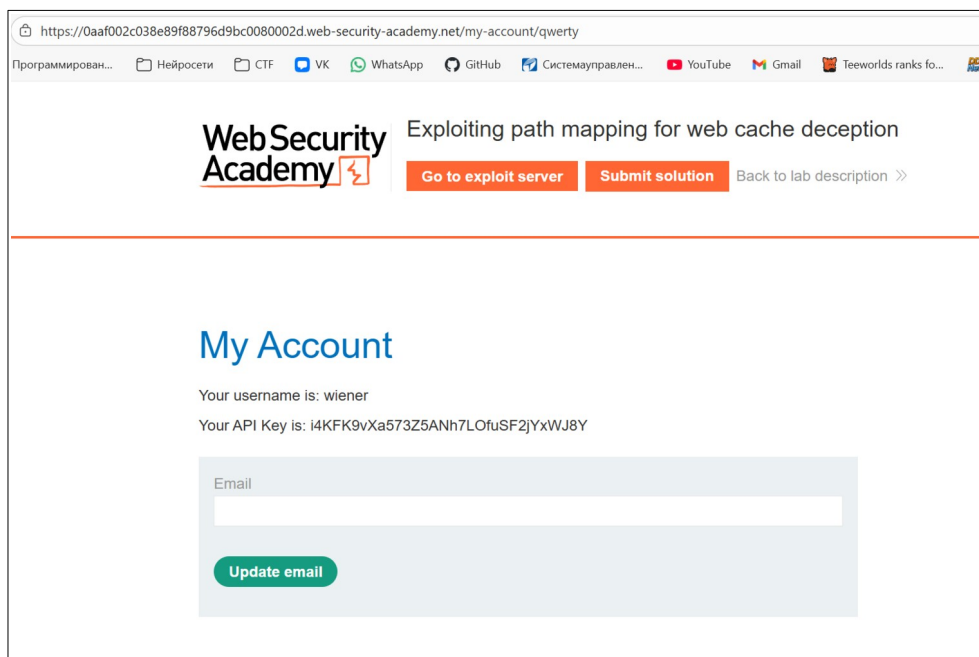
To solve the lab, find the API key for the user carlos. You can log in to your own account using the following credentials: wiener:peter.

Первым делом вошёл в аккаунт, данные от которого прикреплены к лабораторной работе.

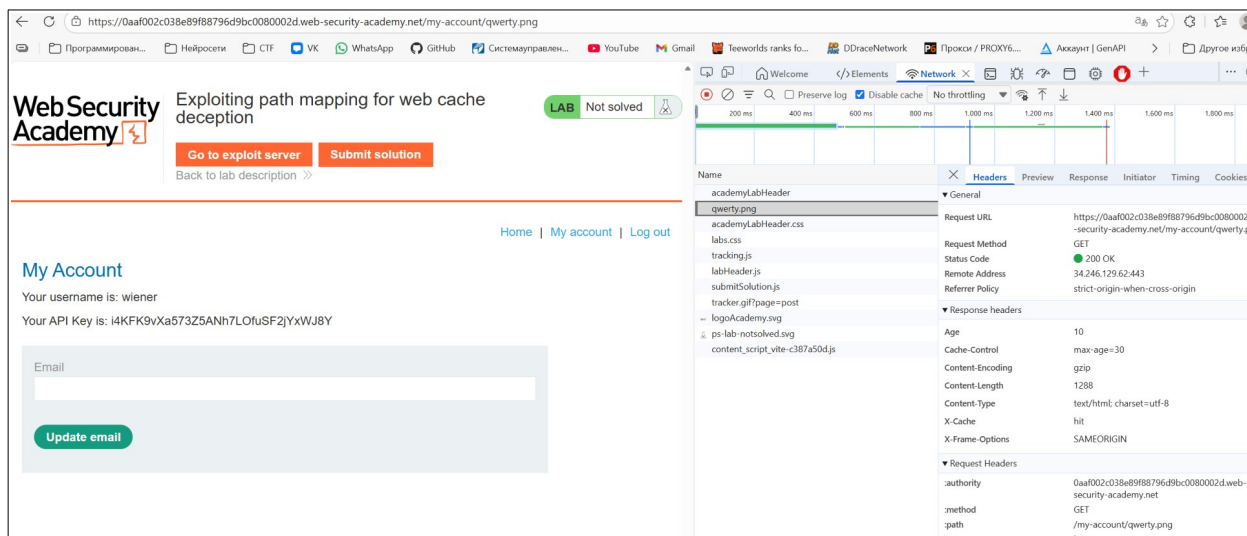


The screenshot shows a web login interface. At the top, the word "Login" is displayed in a blue font. Below it, there is a light blue rectangular box containing the login fields. Inside this box, the label "Username" is above a text input field containing the text "wiener". Below that, the label "Password" is above a text input field containing five dots. At the bottom of the box is a green rounded button with the text "Log in" in white.

Поменял endpoint и заметил, что результат получается точно такой же, что и был.



Приписал к endpoint расширение, которое предположительно могло являться статическим и после двух перезагрузок в средствах разработчика вижу, что X-Cache: hit, значит, что страница действительно попадает в кэш при добавлении .png.



Далее перехожу во вкладку «Go to exploit server» и пишу скрипт для перехода на endpoint, который будет закэширован.

Body:

```
<script>document.location="https://0aaf002c038e89f88796d9bc0080002d.web-security-academy.net/my-account/qwerty1.png"</script>
```

Store

View exploit

Deliver exploit to victim

Access log

Нажимаю на кнопку «Deliver exploit to victim», а затем перехожу по этой ссылке.

0aaf002c038e89f88796d9bc0080002d.web-security-academy.net/my-account/qwerty1.png

Web Security Academy

Exploiting path mapping for web cache deception

Go to exploit server

Submit solution

Back to lab description >>

My Account

Your username is: carlos

Your API Key is: Meo0a1cnN8kE65i8UsnAg9DbfwQEPbel

Email

Update email

Как можно заметить сервер действительно сохранил динамичный ответ в КЭШ.

Ответ: «Meo0a1cnN8kE65i8UsnAg9DbfwQEPbel»