

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 image shows a login interface with a light gray background. At the top center, the word "Login" is written in blue. Below it is a form with two input fields. The first field is labeled "Username" and contains the text "wiener". The second field is labeled "Password" and contains four dots ("...."). At the bottom of the form is a green button with the white text "Log in".

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.

The screenshot shows a web-based exploit editor interface. At the top, there is a code editor window with the following content:

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

Below the code editor are four orange buttons with white text:

- Store
- View exploit
- Deliver exploit to victim
- Access log

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

The screenshot shows a web browser displaying the URL <https://0aaf002c038e89f88796d9bc0080002d.web-security-academy.net/my-account/qwerty1.png>. The page title is "Exploiting path mapping for web cache deception". The main content area is titled "My Account". It displays two pieces of information: "Your username is: carlos" and "Your API Key is: Meo0a1cnN8kE65i8UsnAg9DbfwQEPbel". Below this, there is a form field labeled "Email" with a placeholder "Email" and a green "Update email" button.

Как можно заметить сервер действительно сохранил динамичный ответ в КЭШ.

Ответ: «Meo0a1cnN8kE65i8UsnAg9DbfwQEPbel»