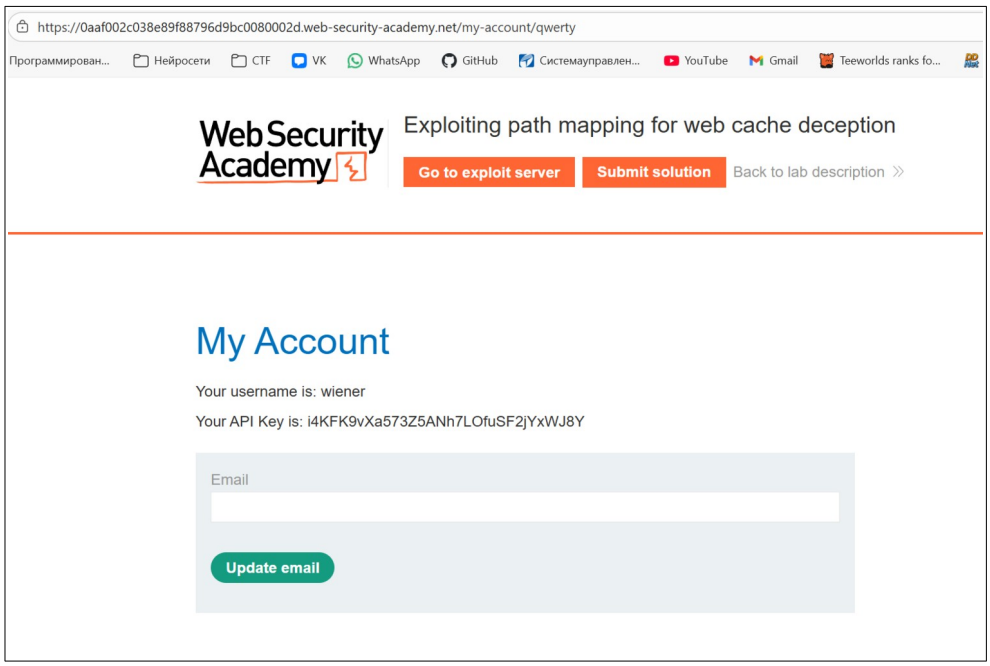
Lab: Exploiting path mapping for web cache deception

Задача:

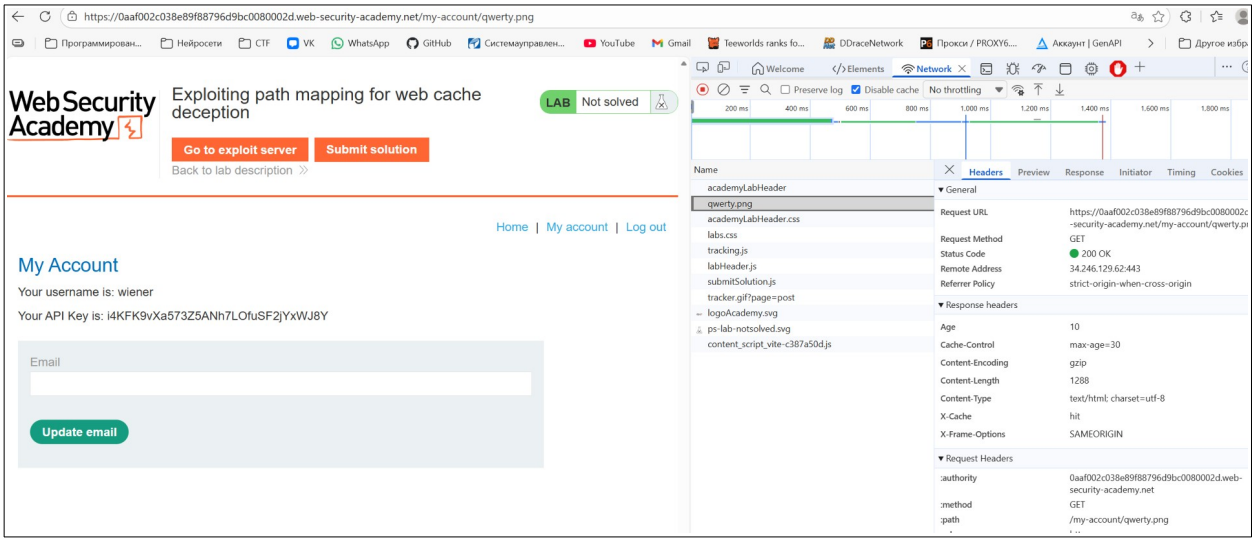
To solve the lab, find the API key for the user carlos. You can log in to your own account using the following credentials: wiener:peter.

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

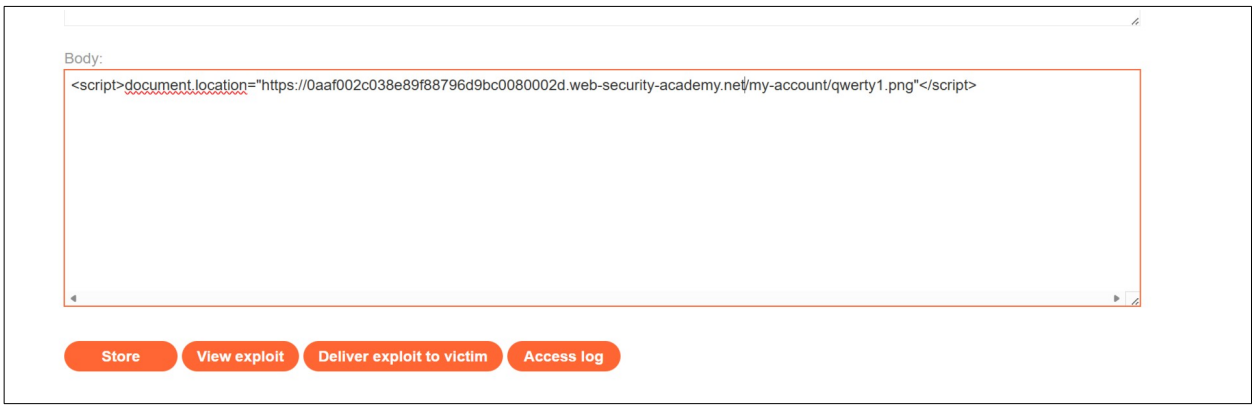
Поменял endpoint и заметил, что результат получается точно такой же, что и был.



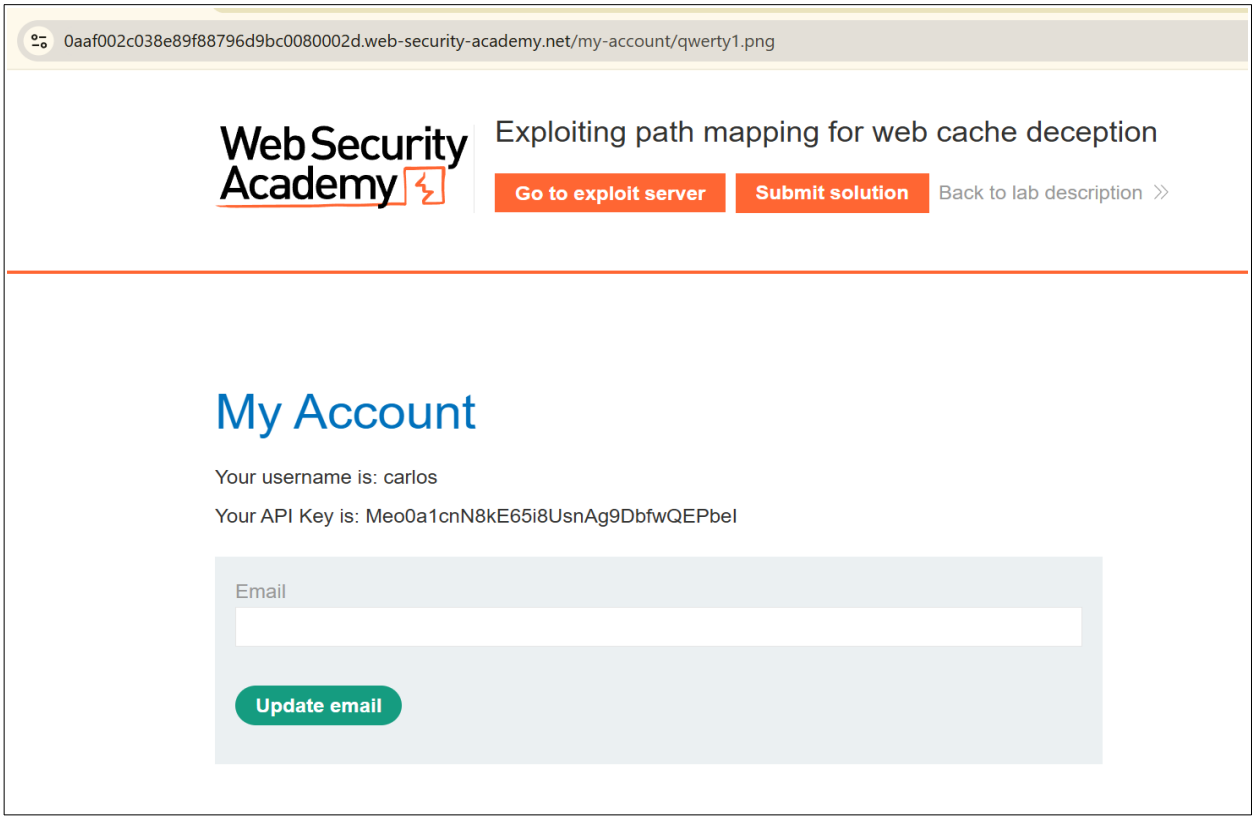
Приписал к endpoint расширение, которое предположительно могло являться статическим и после двух перезагрузок в средствах разработчика вижу, что X-Cache: hit, значит, что страница действительно попадает в кэш при добавлении .png.



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



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



Как можно заметить сервер действительно сохранил динамичный ответ в кэш.

Ответ: «Meo0a1cnN8kE65i8UsnAg9DbfwQEPbeI»