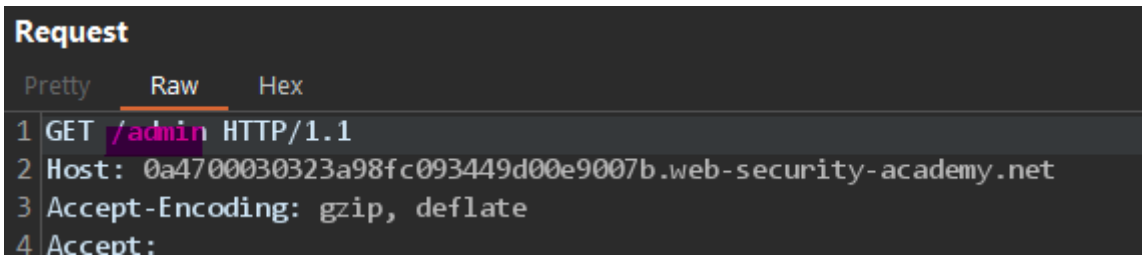
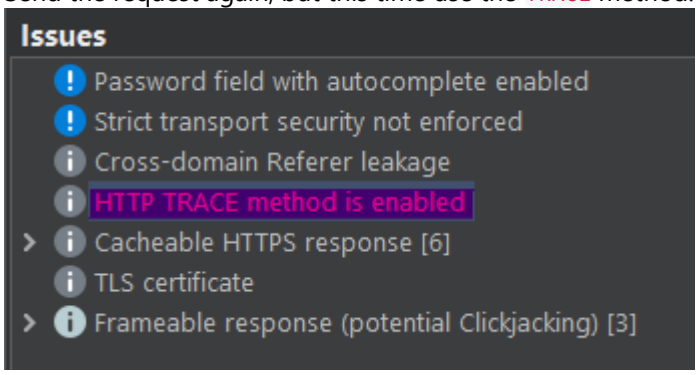
Lab: Authentication bypass via information disclosure

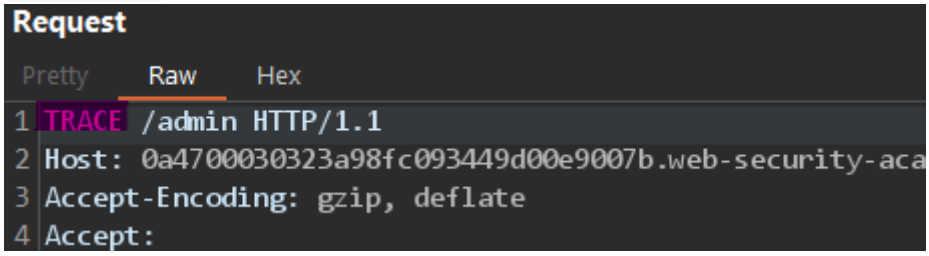
In Burp Repeater, browse to `GET /admin`. The response discloses that the admin panel is only accessible if logged in as an administrator, or if requested from a local IP.



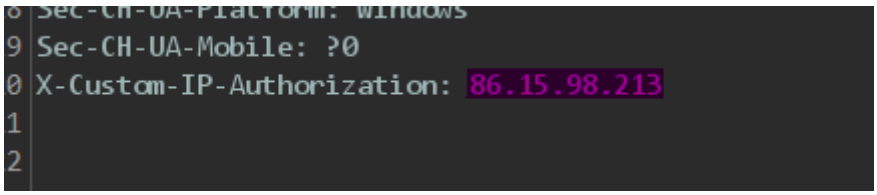
Send the request again, but this time use the `TRACE` method:



`TRACE /admin`



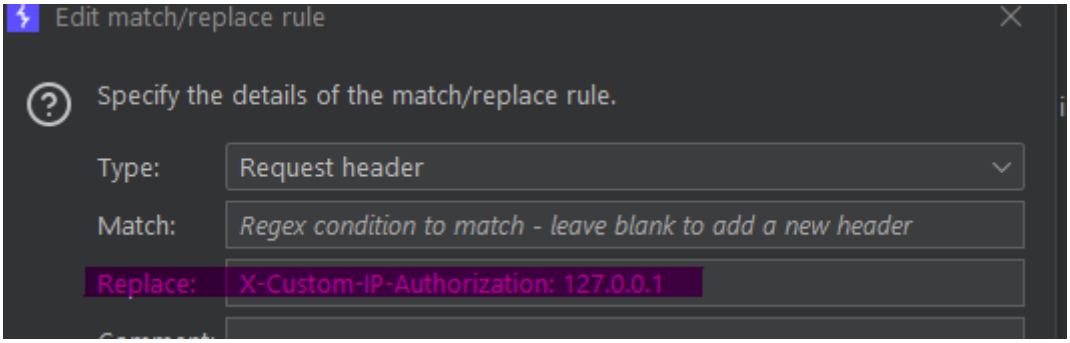
Study the response. Notice that the `X-Custom-IP-Authorization` header, containing your IP address, was automatically appended to your request. This is used to determine whether or not the request came from the `localhost` IP address.



Go to "Proxy" > "Options", scroll down to the "Match and Replace" section, and click "Add". Leave the match condition blank, but in the "Replace" field, enter:

```
X-Custom-IP-Authorization: 127.0.0.1

Burp Proxy will now add this header to every request you send.
```



Browse to the home page. Notice that you now have access to the admin panel, where you can delete Carlos.