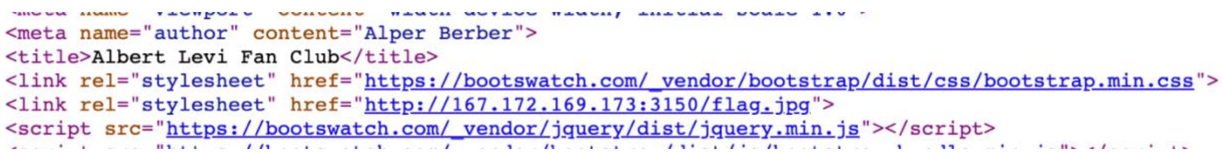
Category: Web
Challenge: Albert Levi Fan Club

When examining the source code of the page, we see an unusual stylesheet reference to a file called "flag.jpg".

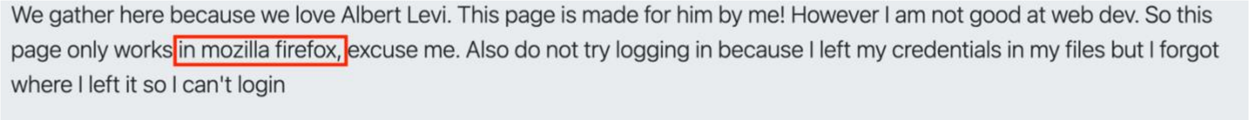


```
<meta name="author" content="Alper Berber">
<title>Albert Levi Fan Club</title>
<link rel="stylesheet" href="https://bootswatch.com/_vendor/bootstrap/dist/css/bootstrap.min.css">
<link rel="stylesheet" href="http://167.172.169.173:3150/flag.jpg">
<script src="https://bootswatch.com/_vendor/jquery/dist/jquery.min.js"></script>
```

When we see its contents, we find out the comment section in the css file. It says, he left his password in plaintext.

```
" /* I am not sure if I left my credentials here, but I am pretty sure that I
left them in PLAINTEXT! */ "
```

When considering the User-Agent reference here;

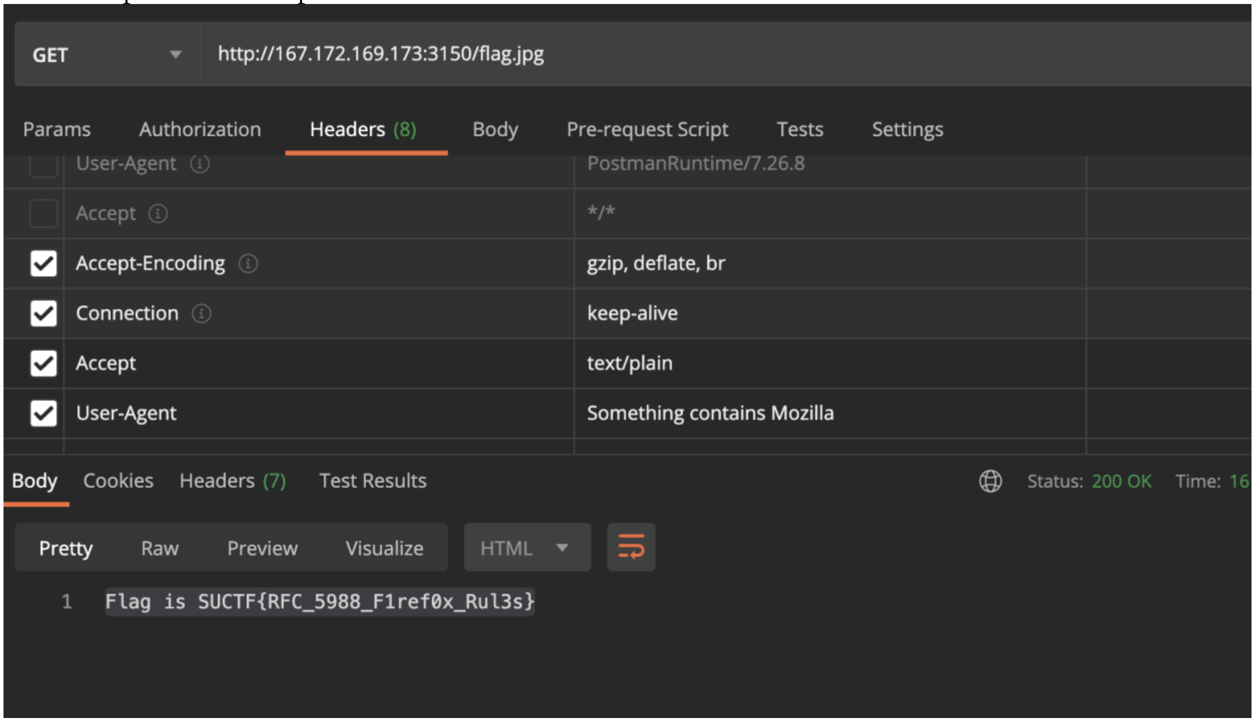


We gather here because we love Albert Levi. This page is made for him by me! However I am not good at web dev. So this page only works in mozilla firefox, excuse me. Also do not try logging in because I left my credentials in my files but I forgot where I left it so I can't login

And the plain text reference in the CSS file's comment section. We create a request to the flag.jpg with the following headers:

```
Accept: "text/plain"
User-Agent: "Something contains Mozilla"
Host: 167.172.169.173:3150
Accept-Encoding: gzip, deflate, br
```

We end up with this response:



GET http://167.172.169.173:3150/flag.jpg

□	User-Agent	PostmanRuntime/7.26.8
□	Accept	*/*
☑	Accept-Encoding	gzip, deflate, br
☑	Connection	keep-alive
☑	Accept	text/plain
☑	User-Agent	Something contains Mozilla

Status: 200 OK Time: 16

```
Flag is SUCTF{RFC_5988_F1ref0x_Rul3s}
```