

master

...

cve / bug_e / edoc-doctor-appointment-system / Stored Cross Site Scripting (XSS).md



onEpAth936 add

History

1 contributor

31 lines (13 sloc) | 1013 Bytes

...

Stored Cross Site Scripting (XSS)
vulnerability exists in edoc-doctor-appointment-system v1.0.1. A successful exploit could allow the attacker to execute arbitrary script code which could lead to stealing or modifying of authentication information of the user, such as data relating to his or her current session.

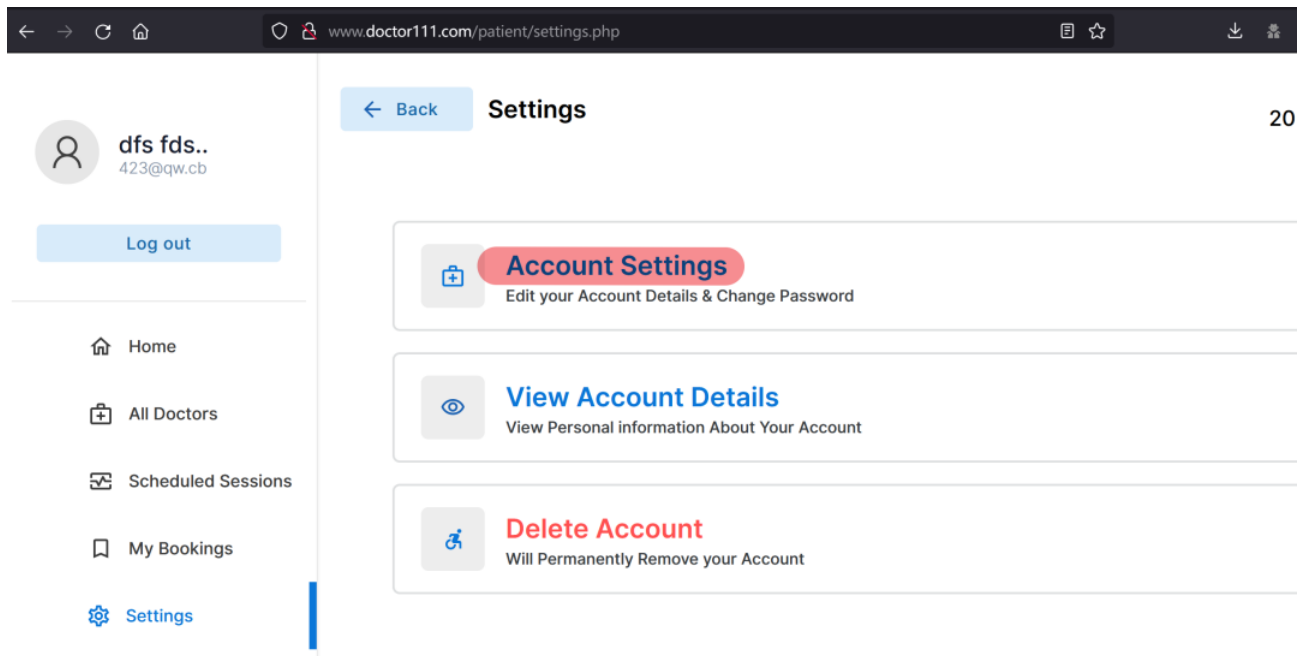
vendor : <https://github.com/HashenUdara/edoc-doctor-appointment-system>

Vulnerability Position : <http://ip/patient/settings.php>

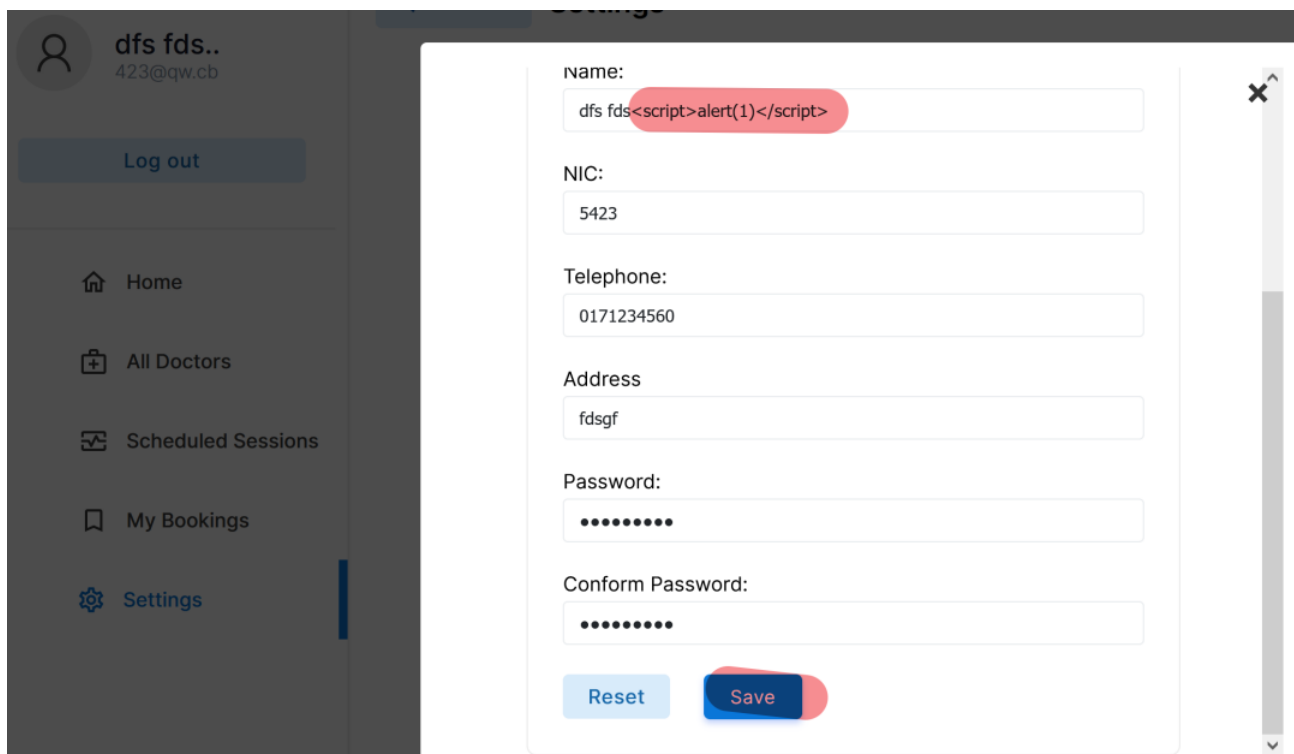
Log in to the <http://ip/login.php>

Visit <http://ip/patient/settings.php> , will access the page of the module.

Click Account Setting.



And then insert `<script>alert(1)</script>` at the name box.



At last click the save button.

When you click View Account Details button , you will see the pop -up window.



dfs fds
423@qw.cb

Log out

Home

All Doctors

Scheduled Sessions

My Bookings

Settings

← Back

Settings



Account Settings

Edit your Account Details & Change Password



View Account Details

View Personal information About Your Account



Delete Account

Will Permanently Remove your Account

