Forum:Hack Forums

Thread: Found this interesting in a website

Rukkas - *September 15, 2014, 3:32 pm*

So. I was looking into a website, and found that I can post HTML to the page. Now, I know its like HTMLi which is only for guestbooks and such, but is there a way I can use this to leverage access to anything else? Like the Admin panel?

The code used to get it to post to the website is as follows:

Code www.website.com/index.php?p="> <h1>Rukkas - Now What??</h1>
Is there anything else that could be done with something like this?

[img]http://s13.postimg.org/fpe6u1nwz/uploadtohf_0.jpg[/img]

Chax. - *September 15, 2014, 8:52 pm*

If you send me the website URL and your Jabber I will do some digging and show you what you would like to know. (If it can be done)

sp3ctrum - *September 15, 2014, 10:08 pm*

Possibly could be used to craft a xss attack. Check to see if some JS discloses cookies.
<script>alert(document.cookie)</script>

Frosteh - *September 16, 2014, 12:39 am*

See if you can get scripts running in the page, if you can do that then potentially you could use a XSS attack on the admin/webmaster/webdevelopers.

A theoretical attack would be to link them to a page on their site saying you think there's errors in the page (that you've planted yourself, e.g a broken image) and also there's javascript in the background that sends their cookies to a remote server where you can read them. You'll then be able to log into the site as the admin, change their creds or whatever.