## WEB SECURITY #2

Slides at: github.com/bitskriegofficial/web-security-2







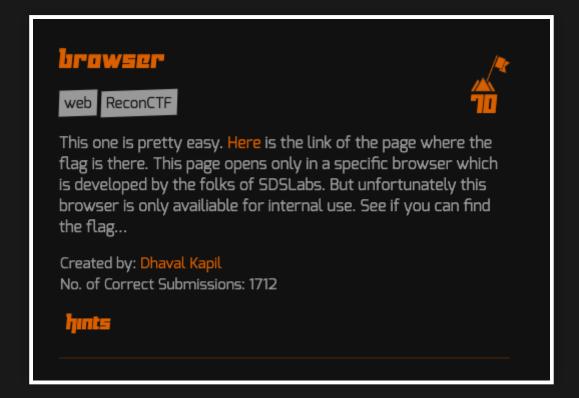
H4xOr, in his early days, made an authentication system. He obviously felt that he had the made the most cutting-edge system but we know how brilliant he actually is. Show him just how easy it is to become the admin. You can visit this link to get the flag once you become admin.

Created by: Ravi Kishore R

No. of Correct Submissions: 3251

hints

http://hack.bckdr.in:10003/



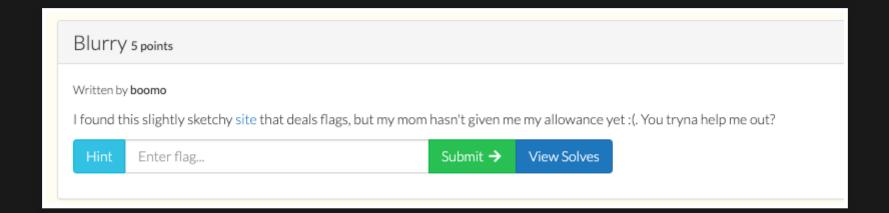
http://hack.bckdr.in:11010/



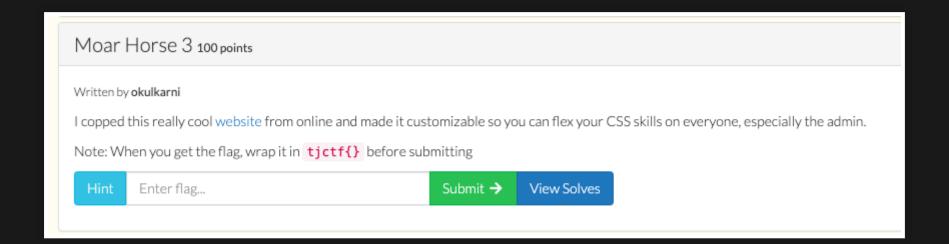
http://2018shell.picoctf.com:52135/



http://hack.bckdr.in:13005/



https://blurry.tjctf.org/



https://moar\_horse\_3.tjctf.org/

## XSS CHALLENGES

JavaScript Basics/Advanced things

Regular Expressions

DOM

## alert(1) to win

The code below generates HTML in an unsafe way. Prove it by calling alert(1).

```
function escape(s) {
   // Slightly too lazy to make two input fields.
   // Pass in something like "TextNode#foo"
   var m = s.split(/#/);

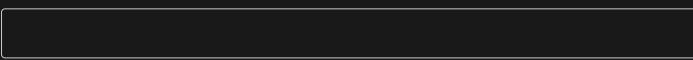
   // Only slightly contrived at this point.
   var a = document.createElement('div');
   a.appendChild(document['create'+m[0]].apply(document, m.slice(1)));
   return a.innerHTML;
}
```

Inpu

type here			
			//

Outpu

Test iframe



Warmup

## NOTE

- Keep practicing wasting hours
- Apart from CTFs, try to exploit in real world for fun and rewards
- You need to know how a lock works before picking it