

## WRITE UPS CTF #2

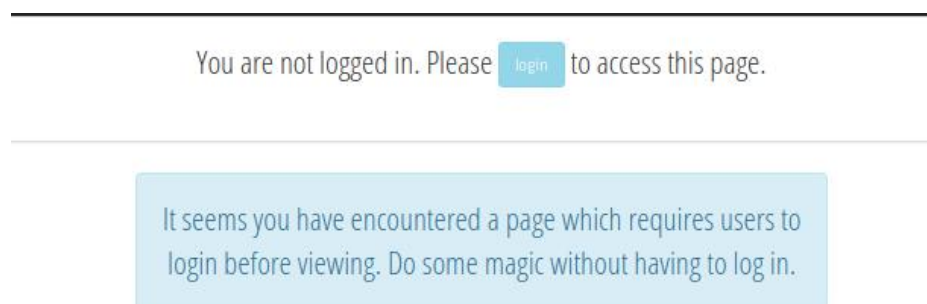
### CTF.INFOSECINSTITUTE.COM

Nama : -Marsekal

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

#### 1.1 LEVEL 05

Screenshot Soal :



Deskripsi soal :

Sepertinya Anda telah menemukan halaman yang mengharuskan pengguna untuk login sebelum melihat. Lakukan sihir tanpa harus masuk.

Write-up :

Terlihat bahwa *button* nya tidak bisa ditekan, Mari kita coba *inspect* lagi. Yang mana ada syntax disable disana, dan kita hanya menghapus nya saja.

```
<p class="lead">  
  "You are not logged in. Please "  
  <a class="btn btn-sm btn-info" href="login.html">login</a> == $0  
  " to access this page."  
</p>
```

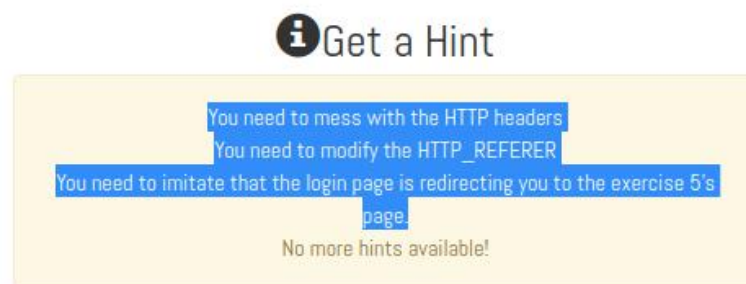
Dan taraaaa....

File not found :3

<http://ctf.infosecinstitute.com/ctf2/exercises/login.html>



Jika kita perhatikan lagi soalnya kita disuruh menjadi pesulap xD. Kekekeeekeh



Anda perlu mengacaukan header HTTP

Anda perlu memodifikasi HTTP\_REFERER

Anda perlu menirukan bahwa halaman login mengarahkan Anda ke halaman latihan 5 itu.

Sepertinya kita hanya melakukan hal yang simple.

Ref : <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referer>

Kali ini saya menggunakan salah satu add ons chrome untuk referer yaitu *referer control*.

# Referer Control



You can set the referer to be sent on a per-site basis. Each filter comes with four options:

- to** If you do not want to let this site know where you are coming from.
- from** To hide that you are originating from this site.
- 3rd** Only requests from third parties are filtered.  
google.com requesting google.com/calendar → first party request  
google.com requesting bing.com → third party request  
google.com requesting maps.google.com → third party request
- RegEx** Interprets your filter as a regular expression. For advanced users.

There are three referer options:

- Normal** do not change referer - use this to whitelist sites when using the default action
- Custom** set up a custom referer to send
- Block** do not send any referer at all

Referer Control status: ☐ active ☒ inactive

Block Javascript Referer: ☐ active ☒ inactive

Referer Control status: ☒ active ☐ inactive

Block Javascript Referer: ☐ active ☒ inactive

RegEx: google.com requesting bing.com → third party request  
google.com requesting maps.google.com → third party request  
Interprets your filter as a regular expression. For advanced users.

There are three referer options:

- Normal** do not change referer - use this to whitelist sites when using the default action
- Custom** set up a custom referer to send
- Block** do not send any referer at all

site filter				referer setting			
enter site	to	from	3rd	RegEx	Normal	Custom	Block
✗ http://ctf.infosecinstitute.com/ctf2/exercises/ex5.php	to	from	3rd	RegEx	Normal	Custom	Block
http://ctf.infosecinstitute.com/ctf2/exercises/login.html				url	target host	referer host	random

You can use \* in a site filter as a wildcard (if RegEx is disabled).  
Caution: http://bnnnle.com does not match http://www.bnnnle.com (and vice versa).

Pertama masukkan dahulu *site* nya di *textbox enter site* jika sudah memasukkan site nya matikan button *from* dan *3rd* yang berada di sebelah kanan dan klik *custom* dan masukkan site yang ingin kita referer.

Referer Control status: ☒ active ☐ inactive

Block Javascript Referer: ☐ active ☒ inactive

RegEx: google.com requesting bing.com → third party request  
google.com requesting maps.google.com → third party request  
Interprets your filter as a regular expression. For advanced users.

There are three referer options:

- Normal** do not change referer - use this to whitelist sites when using the default action
- Custom** set up a custom referer to send
- Block** do not send any referer at all

site filter				referer setting			
enter site	to	from	3rd	RegEx	Normal	Custom	Block
✗ http://ctf.infosecinstitute.com/ctf2/exercises/ex5.php	to	from	3rd	RegEx	Normal	Custom	Block
http://ctf.infosecinstitute.com/ctf2/exercises/login.html				url	target host	referer host	random

You can use \* in a site filter as a wildcard (if RegEx is disabled).  
Caution: http://google.com does not match http://www.google.com (and vice versa).

Gosh, you were fast. You completed Level 5. You will be redirected to level 6 in 10 seconds.

 Get a Hint