

## WRITE UPs CTF #2

CTF.INFOSECINSTITUTE.COM

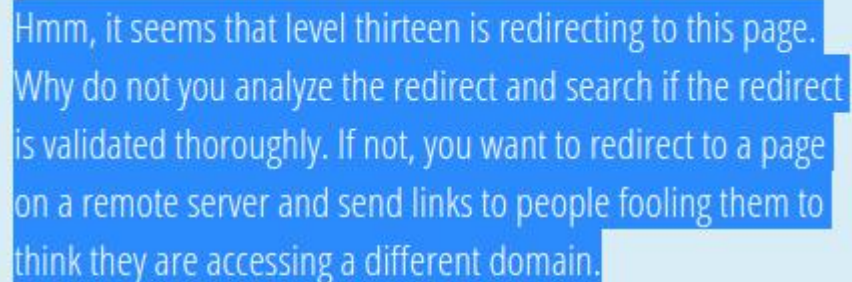
Nama : -McMillan

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

### 1.1 LEVEL 13

### 1.2 Vulnerability: A10 Unvalidated Redirects and Forwards

### 1.3 Screenshot soal :



Hmm, it seems that level thirteen is redirecting to this page. Why do not you analyze the redirect and search if the redirect is validated thoroughly. If not, you want to redirect to a page on a remote server and send links to people fooling them to think they are accessing a different domain.

 Get a Hint

### 1.4 Deskripsi soal

Hmm, sepertinya level tiga belas mengarahkan ke halaman ini. Mengapa Anda tidak menganalisa redirect dan mencari jika redirect divalidasi secara menyeluruh. Jika tidak, Anda ingin mengalihkan ke halaman di server jauh dan mengirim tautan ke orang-orang yang membodohi mereka untuk berpikir mereka mengakses domain yang berbeda. (translate.google.com)

## 1.5 Write-up :



*Coba tambahkan URL jarak jauh dalam parameter GET yang sesuai  
Sepertinya menambahkan protokol atau www. tidak berfungsi dan halaman melakukan pemeriksaan  
peka huruf besar kecil. Anda perlu mencari cara lain untuk mengalihkan.  
Tidak ada lagi petunjuk!*

Ref :

[https://www.owasp.org/index.php/Top\\_10\\_2010-A10-Unvalidated\\_Redirects\\_and\\_Fo](https://www.owasp.org/index.php/Top_10_2010-A10-Unvalidated_Redirects_and_Fo)  
[rwards](#)

saya menemukan petunjuk di source code nya.

```
...<li><a class="exPending" href="http://localhost/exercises/ex13.php?redirect=hTTP://google.com">Level 13</a></li>

<li><a class="exPending" href="http://localhost/exercises/ex13.php?redirect=ex13-task.php">Level 13</a></li>

/" id="brand" >Practical Website Hacking</a>
```

Dan buatlah seperti ini.

<http://ctf.infosecinstitute.com/ctf2/exercises/ex13.php?redirect=hTTP://google.com>

## Website Hacking

Bad Redirect Parameter

 Get a Hint

Ref : <https://www.drupal.org/project/redirect/issues/1451868>

Dalam refrensi diatas untuk redirect bisa juga menggunakan spasi atau unicode %20

<http://ctf.infosecinstitute.com/ctf2/exercises/ex13.php?redirect=%20hTtp://google.co>

[m](#)

Dan ternyata benar,, kita langsung dilempar ke web google.

Saya rasa level 13 sudah kita lalui dan berjalan lancar.

Muliate.