# WRITE UPs CTF #2

# CTF.INFOSECINSTITUTE.COM

Nama: -Marsekal

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

### 1.1 LEVEL 06

Vulnerability:

A8 Cross-Site Request Forgery (CSRF)

Screenshot Soal:

# Lorem. Lorem ipsum dolor sit amet, consectetur adipisicing elit. Dolorem fugiat nesciunt nulla reiciendis voluptatem voluptatum! Aut autem molestiae obcaecati quaerat reiciendis? Beatae exercitationem expedita iste iure molestiae, quibusdam ratione sint! Eius esse praesentium, quia recusandae saepe sunt tempore. Accusantium, atque consequuntur deleniti dignissimos eius eveniet iste, minima neque obcaecati quam ratione reprehenderit sapiente sequi! Facilis, iusto, modi! Fuga, rerum, totam? \*\*There is a better way to do it that would send the request each time the page is visited. Enter your message. \*\*Allowed tags are b,em,p,i,u,s,img,a,abbr, cite and code Add Comment

Sepertinya Anda telah mendarat di situs yang menggunakan tag HTML untuk komentar artikel. Anda ingin memanfaatkan ini dengan membuat pengguna melakukan tindakan pada file bank.php di root site.com, jika mereka masuk di sana. Anda ingin browser pengguna memuat halaman itu dan mengeksekusi transfer string kueriTo dengan nomor 555 sebagai parameter.

## Deskripsi soal:

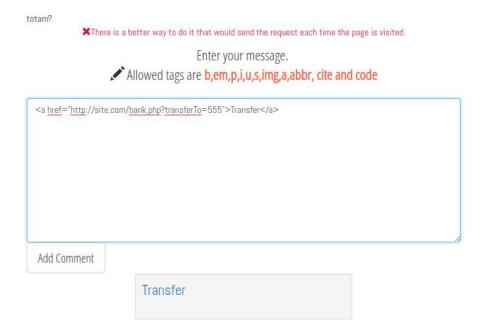
Kita disuruh untuk melakukan CSRF yang mana ada sebuah textarea untuk kita

exploitasi dengan tag diizinkan yaitu b,em,p,i,u,s,img,a,abbr, cite and code

# Write-up:

Mula mula Saya mencoba dengan tag a

<a href="http://site.com/bank.php?transferTo=555">Transfer</a>



Upss.. Sepertinya kita salah, terlihat ada notifikasi "Ada cara yang lebih baik untuk melakukannya yang akan mengirim permintaan setiap kali halaman tersebut dikunjungi." . Tapi apa salahnya kita coba.

Dan ternyata ini benar-benar salah.

mari kita coba dengan tag yang lainnya.

<img src="http://site.com/bank.php?transferTo=555" width="200px" height="200px"
alt="test">

\*Not quite right yet...

Enter your message.

Allowed tags are b,em,p,i,u,s,img,a,abbr, cite and code



Think which tag you would need that would force users to make requests to remote sites.

You would need to use either the img or the a tag

The <a> tag would not execute each time the page is opened but each time
the user clicks on it so the <img> tag is your best bet.

No more hints available!

Pikirkan tag mana yang Anda perlukan yang akan memaksa pengguna untuk membuat permintaan ke situs-situs terpencil.

Anda harus menggunakan img atau tag

Tag <a> tidak akan dieksekusi setiap kali halaman dibuka tetapi setiap kali pengguna mengkliknya sehingga tag <img> adalah pilihan terbaik Anda.

Tidak ada lagi petunjuk!

Kita sudah melakukan tag yang benar sebelumnya tapi masih ada kesalahan.

Oops, well done. Yo	u completed level 6. You will be tran	sferred to level 7 in 10 seconds.
	<b>€</b> Get a Hin	†

Dan taraa.. Selesai

Saya memasukkan request seperti ini

<img src="http://site.com/bank.php?transferTo=555">