WRITE UPs CTF #2

CTF.INFOSECINSTITUTE.COM

Nama : -Marsekal

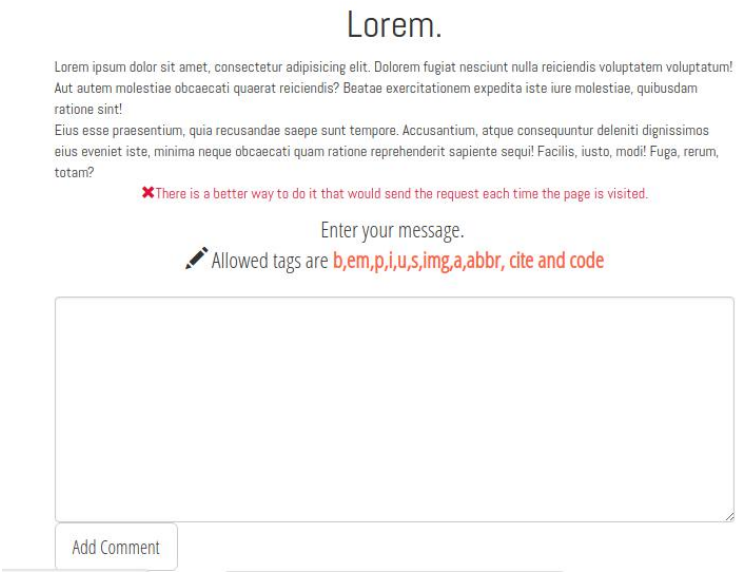
Team : **iL7Team, Sulawesi I.T Security, & Medan Cyber Security**

1.1 LEVEL 06

Vulnerability:

A8 Cross-Site Request Forgery (CSRF)

Screenshot Soal :



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 :

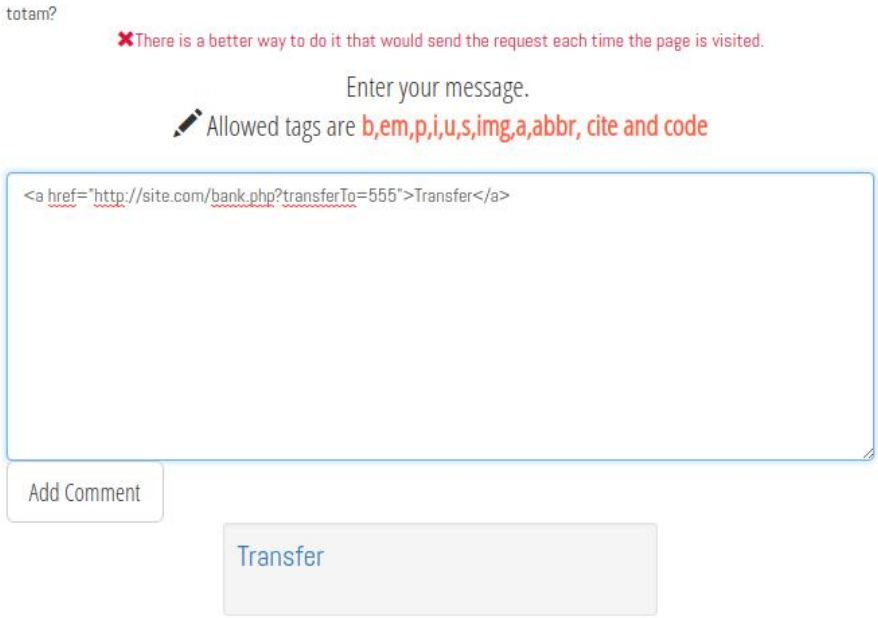
Kita disuruh untuk melakukan CSRF yang mana ada sebuah *textarea* untuk kita

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*

Transfer



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.

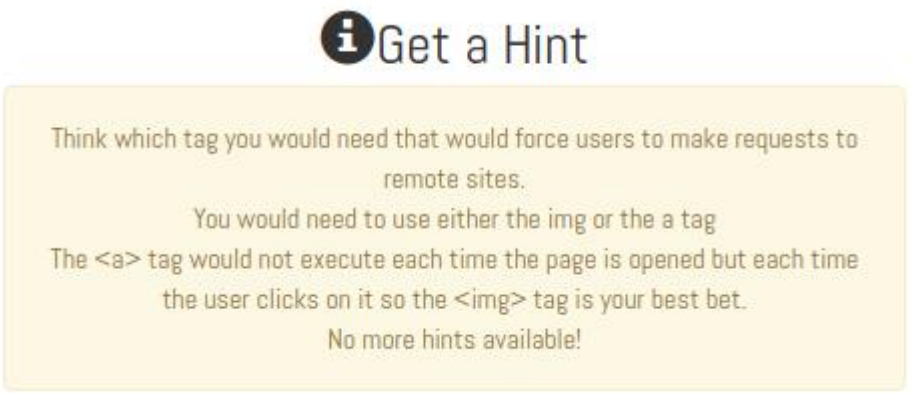
Dan ternyata ini benar-benar salah.

mari kita coba dengan tag yang lainnya.

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

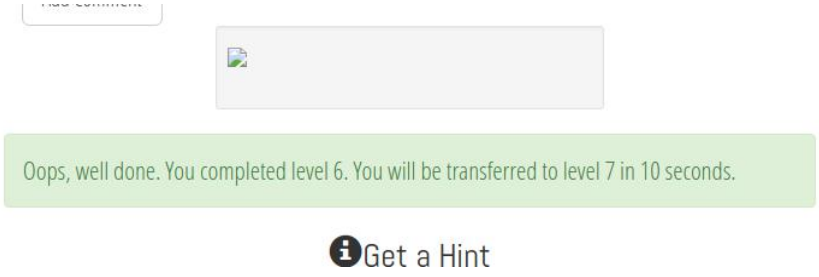
:v

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



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.



Dan taraa.. Selesai

Saya memasukkan request seperti ini

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