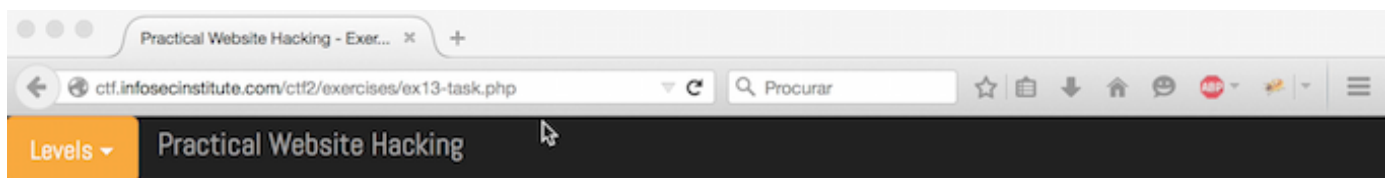


Infosecinstitute CTF 2 - LEVEL 13


This will be solution for Level 13 [Practical Web Hacking](#) CTF #2.

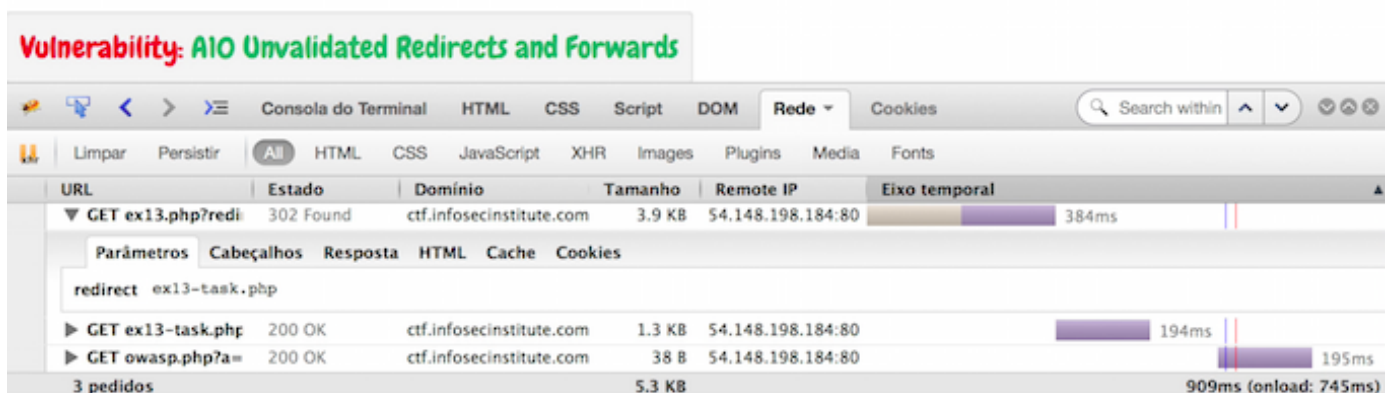
This level we are told that we have to find a way to redirect our selfs to other domain, this means that we need to exploit a [Unvalidated Redirect or Forward](#).

The the information we need is given to us after the last level as seen in the picture.



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



We can try to execute a direct redirect with the same parameter and the url that we want.

Practical Website Hacking - Exer... ✕

secinstitute.com/ctf2/exercises/ex13.php?redirect=//www.google.com

Procurar

Levels ▾ Practical Website Hacking

Bad Redirect Parameter

Get a Hint

Vulnerability: AIO Unvalidated Redirects and Forwards

Consola do Terminal HTML CSS Script DOM Rede Cookies

Limpar Persistir All HTML CSS JavaScript XHR Images Plugins Media Fonts

| URL | Estado | Dominio | Tamanho | Remote IP | Eixo temporal |
|---------------------|--------|--------------------------|---------|-------------------|-----------------------|
| ▶ GET ex13.php?redi | 200 OK | ctf.infosecinstitute.com | 1.2 KB | 54.148.198.184:80 | 379ms |
| ▶ GET owasp.php?a= | 200 OK | ctf.infosecinstitute.com | 38 B | 54.148.198.184:80 | 185ms |
| 2 pedidos | | | 1.2 KB | | 702ms (onload: 543ms) |

This shows us that we have some protection in place, and we are left with the flowing options.

1. Find out if the protection is case sensitive.
2. Find if the protocol is actually mandatory.

And by the picture below we can see that the last option is actually the correct one might seem remote by their are some markup formats that use this syntax to represent external domains :)

The screenshot shows a web browser window with the address bar displaying `ctf.infosecinstitute.com/ctf2/exercises/ex13.php?redirect=//www.google.com`. The page has a dark header with "Levels" and "Practical Website Hacking". The main content area displays a green message: "Congratulations, you just completed the last level. You are a true Ninja warrior now." Below this is a button labeled "Get a Hint".

A network log is visible at the bottom, titled "Vulnerability: AIO Unvalidated Redirects and Forwards". The log shows three requests:

| URL | Estado | Dominio | Tamanho | Remote IP | Eixo temporal |
|-------------------|--------|--------------------------|---------|-------------------|-----------------------|
| GET ex13.php?redi | 200 OK | ctf.infosecinstitute.com | 1.3 KB | 54.148.198.184:80 | 384ms |
| POST scores.php | 200 OK | ctf.infosecinstitute.com | 4 B | 54.148.198.184:80 | 187ms |
| GET owasp.php?a= | 200 OK | ctf.infosecinstitute.com | 38 B | 54.148.198.184:80 | 372ms |
| 3 pedidos | | | 1.3 KB | | 928ms (onload: 587ms) |

Video

infosecinstitute.com ctf2 Level 13



So we are done, most of the levels have a direct mapping with owasp top 10, and most of them a representation of some of the weak links in web development.

 [0x4E0x650x6F](#)

 [0x4E0x650x6F](#)