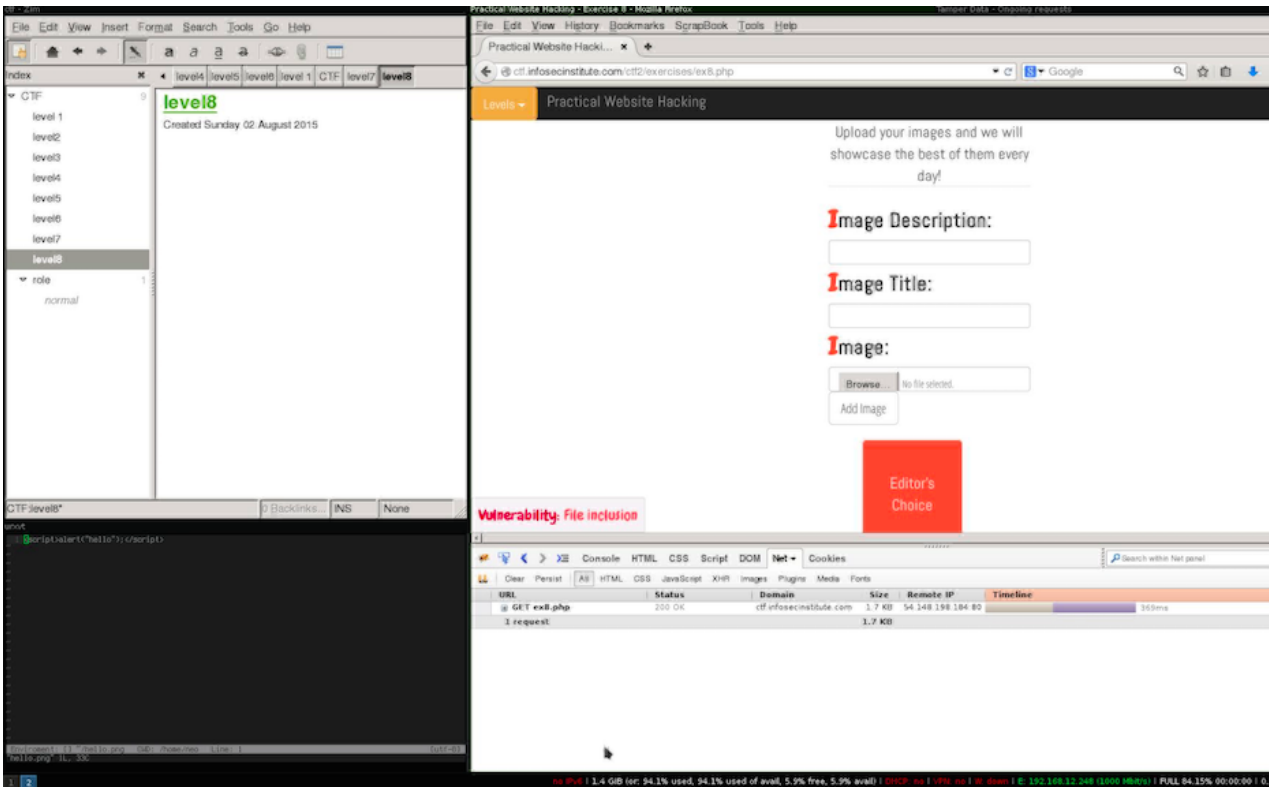
# Infosecinstitute CTF 2 - LEVEL 8

This will be solution for Level 8 Practical Web Hacking CTF #2.

This level we have file upload Unrestricted file uploads form, the objective is to bypass the protection in place and find a way to upload and execute our javascript payload.

The vulnerabilities are usualy about the detection of the file type, the usual implementations are:

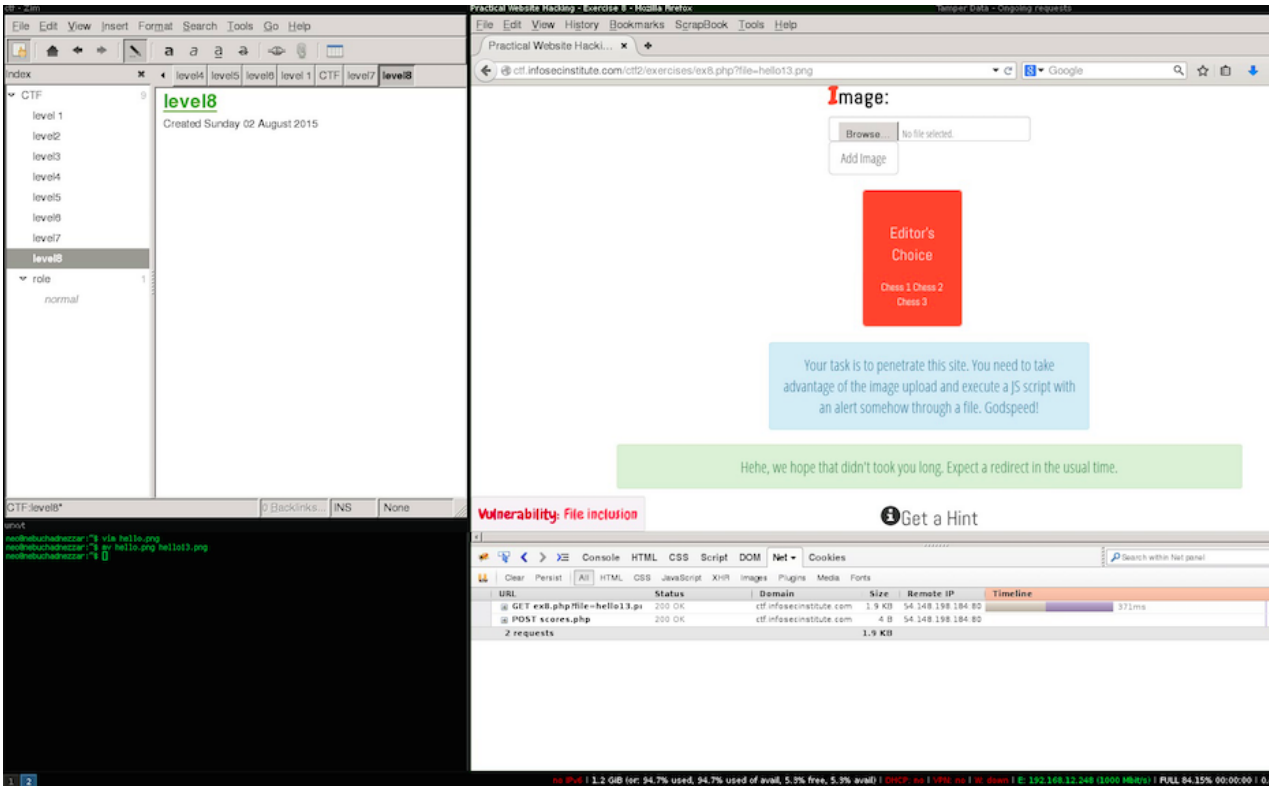
1. File type based on extention (the worst kind there is!) This is usualy a bad idea becuase from the System's prespective the extension doen't realy matter ;).
2. Mime type. This last one is common but hard to get it right and it can be changed\spoofed (like everything else that comes from the user).




After creating a file with wour payload with png extension.

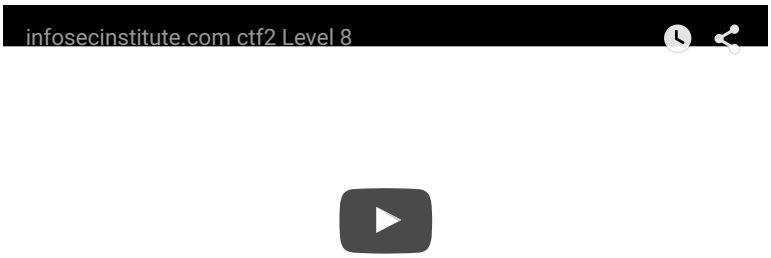
```
<script>alert("hello");</script>
```

I noticed that the upload needs review, this means that our image will not be avaliable using the attachment_id parameter, but also means that the moderators need a way to access the file to perform their operations. This means that might be other parameter that is not "moderated", flowing the common naming convetion we can find out that that parameters name is file.




This level was easy, but the truth is file uploads are hard to implement and the main reason why files uploaded by users should never be in web root, and \ or accessible by any means.

A bad implementation of a file upload can take a web site down, or slow down its performance significantly **(CVE-2014-0050, CVE-2013-0248)**, or even lead to remote code execution in the server.




0x4E0x650x6F
0x4E0x650x6F