

HERA LAB

LAB 1: XSS LABS

LAB 1 <#CODENAME: FIND ME!>



eLearnSecurity has been chosen by students in 140 countries in the world
and by leading organizations such as:



CSRF LABS WILL CONTAIN 11 CHALLENGING LABS:

1. **Warm-up:** XSS level 1
2. **Easy:** XSS level 2
3. **Easy:** XSS level 3
4. **Easy:** XSS level 4
5. **Medium:** XSS level 5
6. **Medium:** XSS level 6
7. **Medium:** XSS level 7
8. **Hard:** XSS level 8
9. **Hard:** XSS level 9
10. **Hard:** XSS level 10
11. **Hard:** XSS level 11

1. DESCRIPTION

The **Find Me!** labs do not need any introduction!

Each level generates HTML in an unsafe way, and you have to bypass some server-side PHP filters.

The solutions you will see are just a few of the many you can have.

As a suggestion, once you will finish these labs, you can try to solve them again using your way and alternative techniques.

The full list of all the labs and the related descriptions are available at:

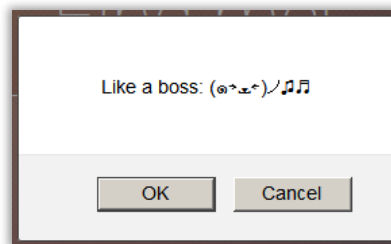
<http://info.xss.labs/>

2. GOAL

The main goal of these labs is to create a PoC triggering an alert box like this one:

```
alert('l33t');
```

If the exploitation has performed successfully, you'll see something like this:



Of course, it must be executed **without user interaction**.

3. TOOL

The best tool is, as usual, your **brain**. You may also need:

- Web Browser
- HTTP Proxy
- Local/Remote server web

4. SOLUTIONS

The techniques to use during this lab are better explained in the study material. You should refer to it for further details. These solutions are provided here only to verify the correctness.

The solution files are available at <http://info.xss.labs/solutions>.