HERA LAB

LAB 3: SQLI LABS

LAB 3 <#CODENAME: WHAT'S YOUR BROWSER?>

WAPTX

eLearn Security
AN iNE COMPANY

Sqli Injection will contain 10 challenging labs:

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

1. DESCRIPTION

You are a pentester, and "Web statistics" hired you to pentest their browsers statistic application. The application stores information about browsers in a DB.

Each level wrongly escape inputs, and you have to bypass some server-side PHP/MySQL 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.sqli.labs/

eLearn Security
AN iNE COMPANY

2. GOAL

You will need to reach different goals at every level.

3. TOOL

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

- Web Browser
- HTTP Proxy
- SQLMap

4. SOLUTIONS

The techniques used during this lab are better explained in the study material. You should refer to it for further details.

You can find the solutions at:
`http://info.sqli.labs/solutions.html`