Black Magic

brought to you by:
Denise, Luca and Colin

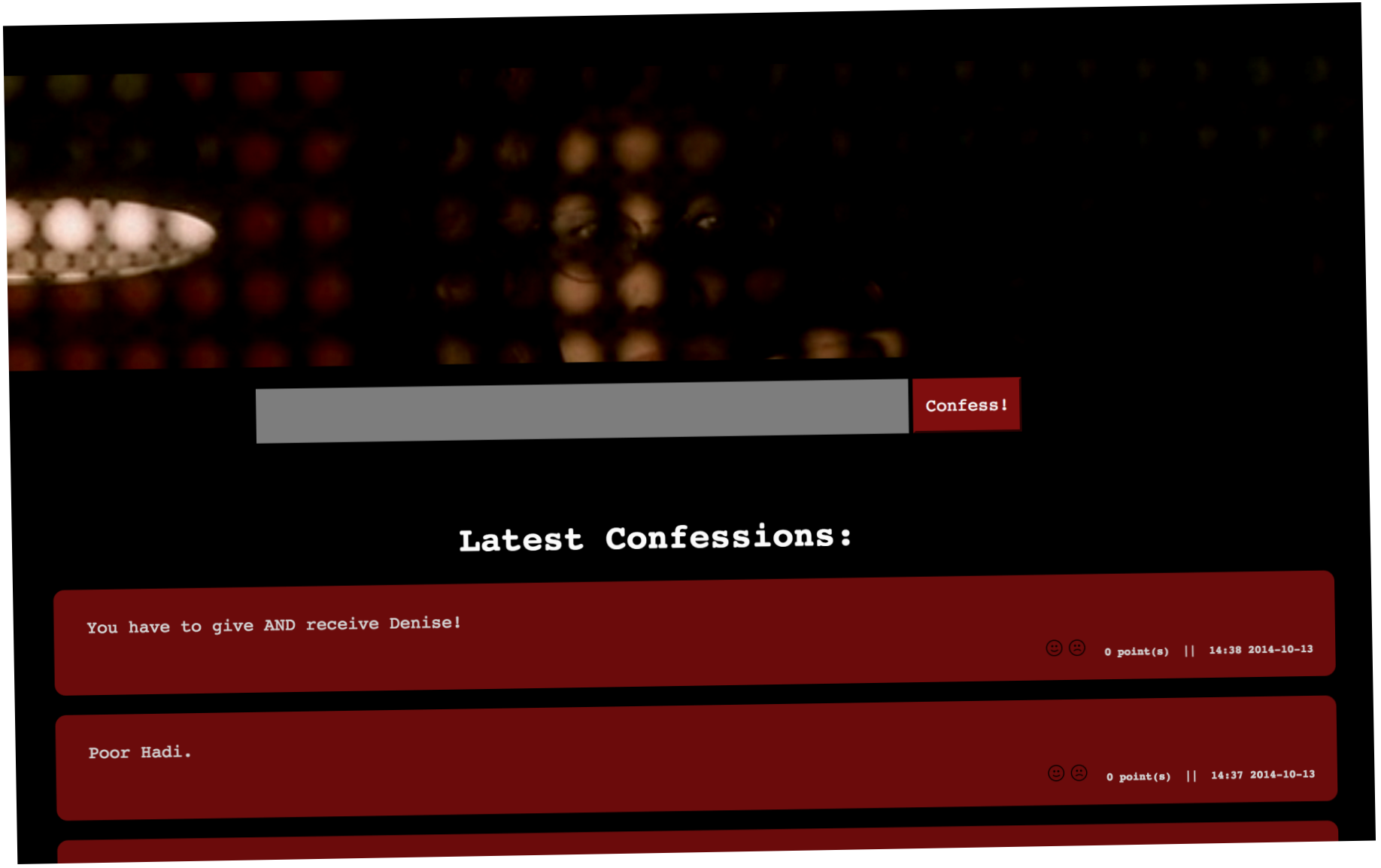
~~Black~~ ~~Magic~~

Cross Site-Scripting Attacks

brought to you by:
Denise, Luca and Colin

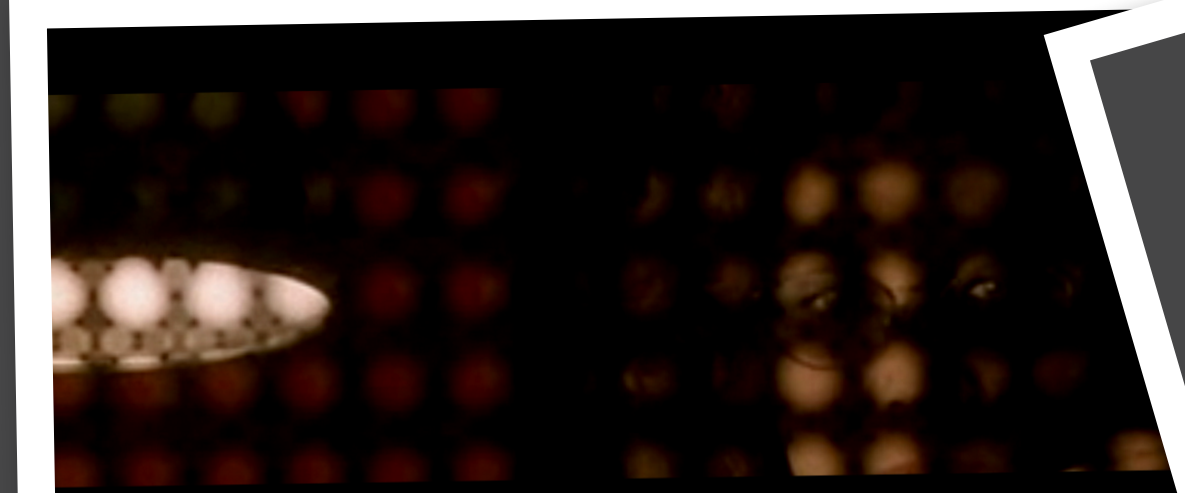
Overview

- Reality check
- Technical background
- Live demo
- Q&A



Intro > **Reality check** > Technical Background > Live Demo > Q & A


Confess!
Latest Confessions:
You have to give AND receive Denise!
Poor Hadi.



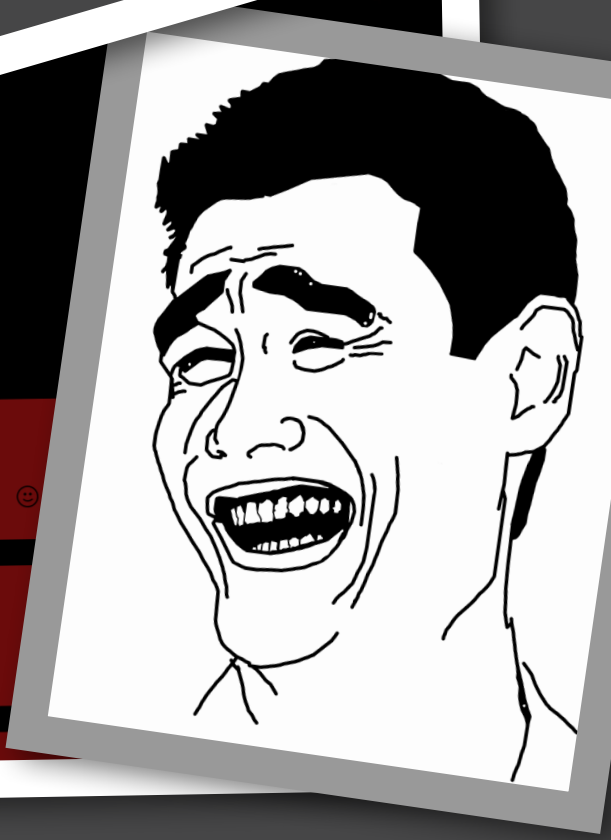
Confess!

Latest Confessions:

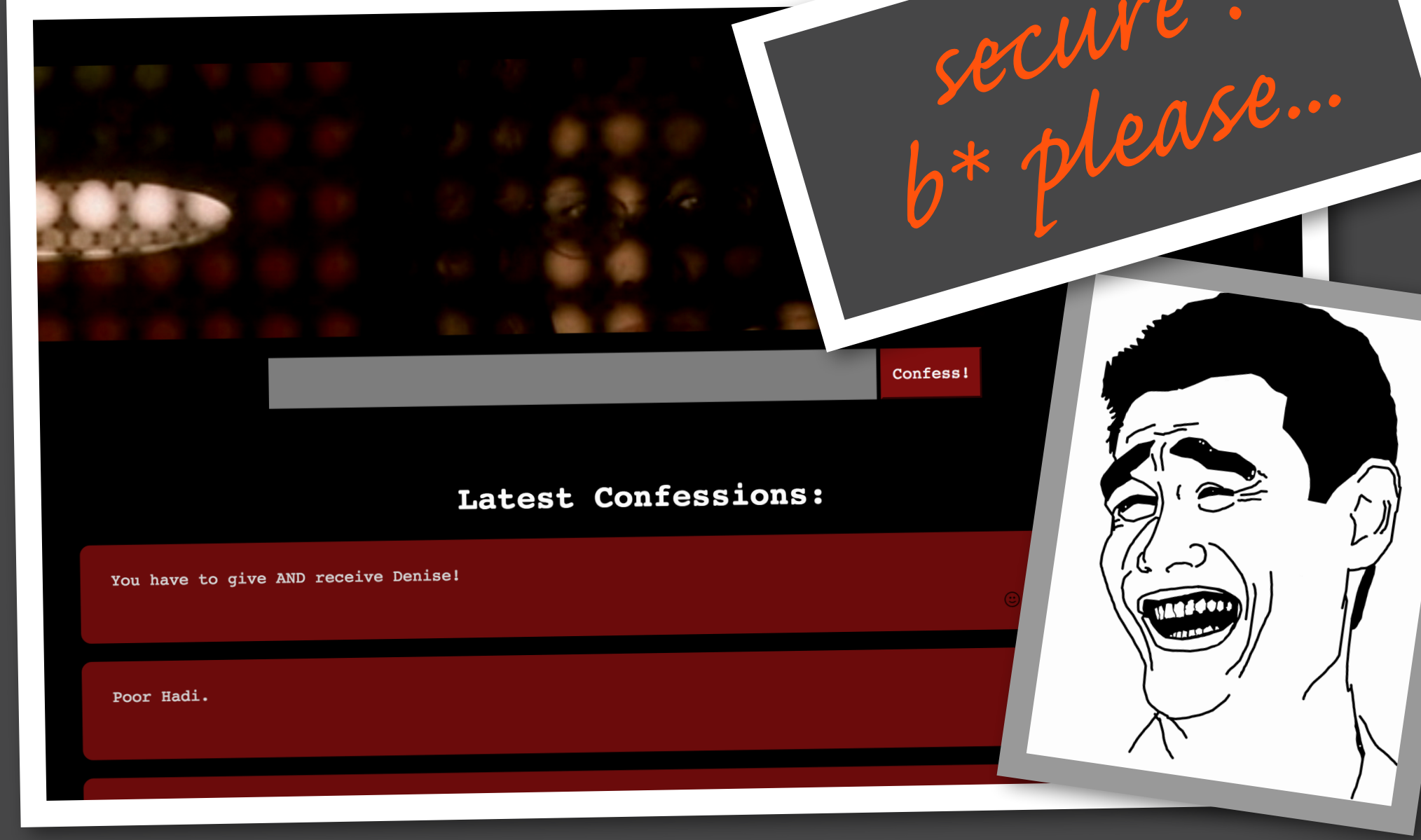
You have to give AND receive Denise!

Poor Hadi.

secure ?
b* please...



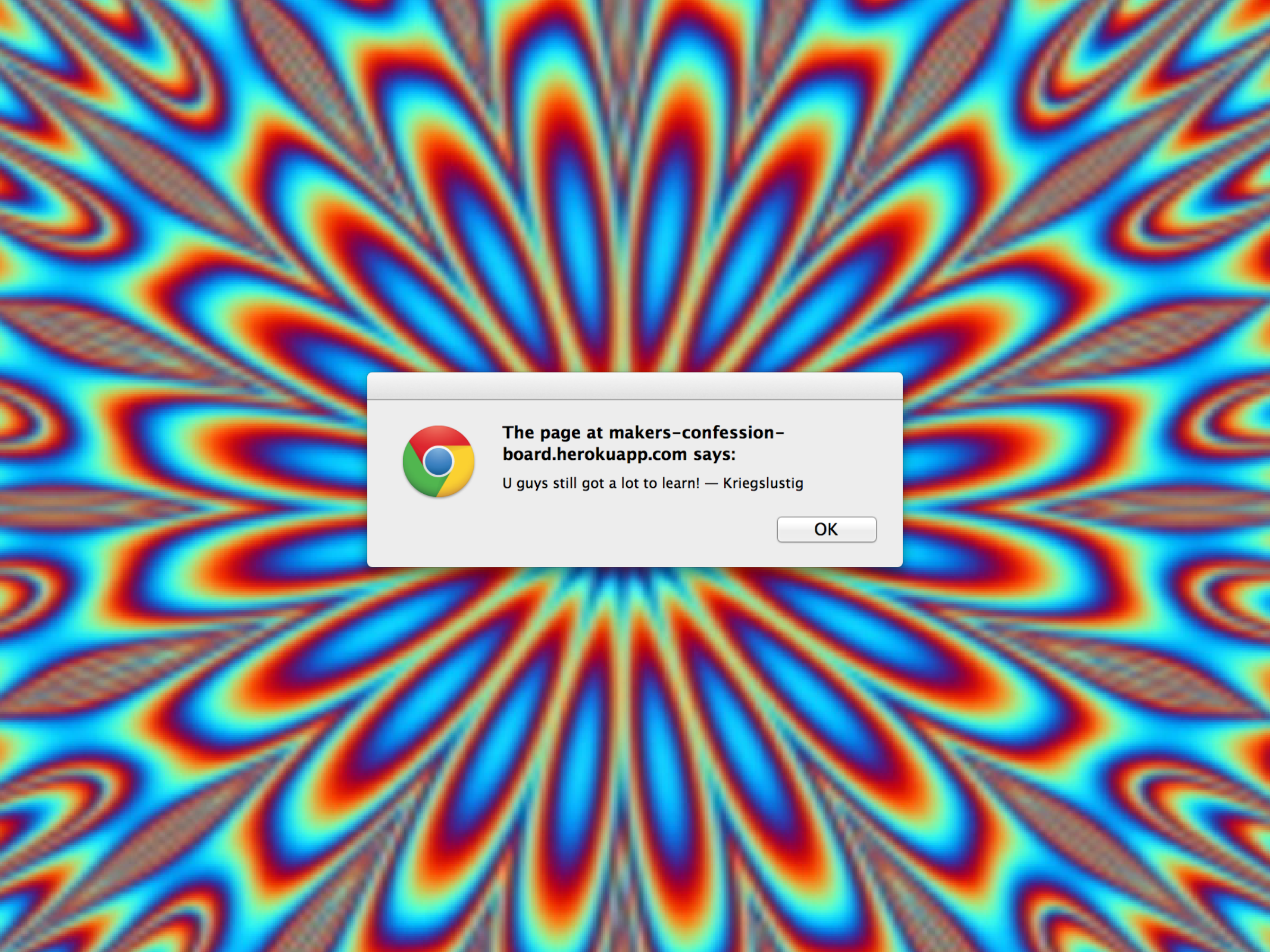
Intro > **Reality check** > Technical Background > Live Demo > Q & A



Intro > **Reality check** > Technical Background > Live Demo > Q & A

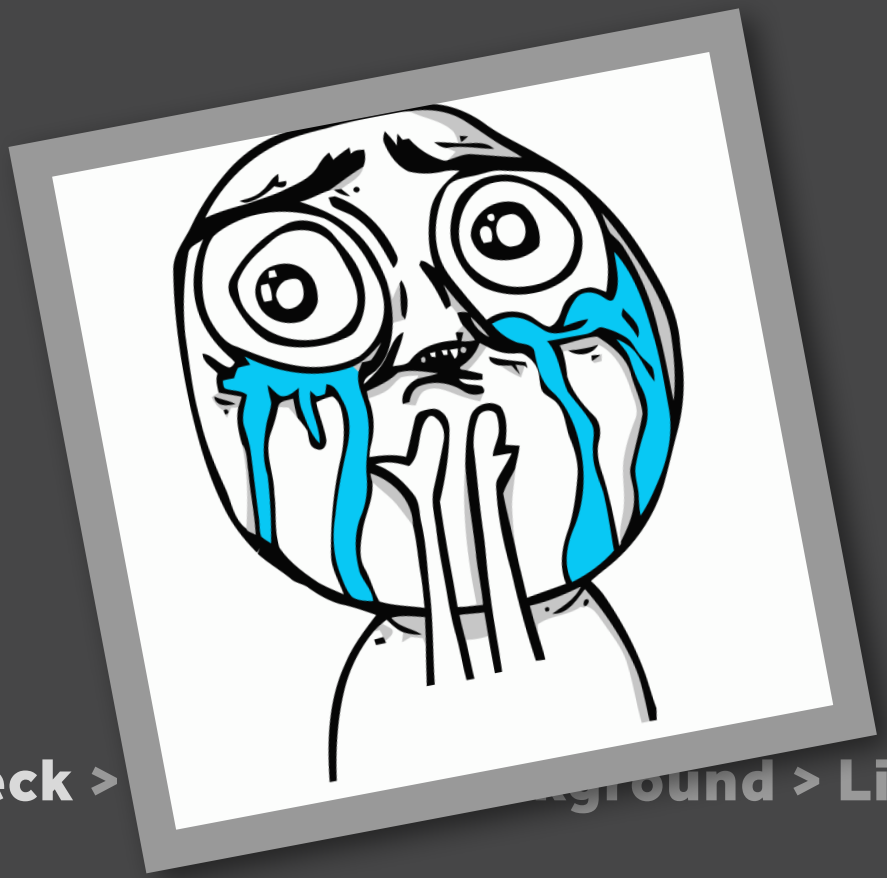
Oopsy daisie...

or, straight outta swiss alps brah!


The page at makers-confession-board.herokuapp.com says:
U guys still got a lot to learn! — Kriegslustig
OK

WTF ???

confessions board is down...



type = Stored

- persistent
- stored on the server (db...)
- what u want as a «hacker»

type = Reflected

- non persistent
- manipulated URIs (queries)
- not so cool

type = type-0

- persistent
- coolest-sounding (but really not so cool)
- client side executed (virus)
- cannot be prevented by dev

conclusion

- never trust user input
- protect your forms
- escape 'em
- protect your databases

known victims of XSS:

Orkut

YouTube

Intro > Reality check > **Technical Background** > Live Demo > Q & A

Any
questions?

Links:

bit.ly/owasp_xss

bit.ly/sinatradoc_escapehtml

(will be completed within the next few hours)

Intro > Reality check > Technical Background > Live Demo > Q & A

Scripts used:

netzkinder.cc/yolo/nice.js

Thanks for your attention