De-Railing: Smashing the Rails Stack

Aaron Bedra
Relevance, Inc.
http://thinkrelevance.com

1

Overview

- SQL Injection
- XSS (Cross Site Scripting)
- CSRF (Cross Site Request Forgery)
- Server Security
- Demo (fixing an insecure app with Tarantula)

Tarantula
Eight Legs, Two Fangs, and an Attitude

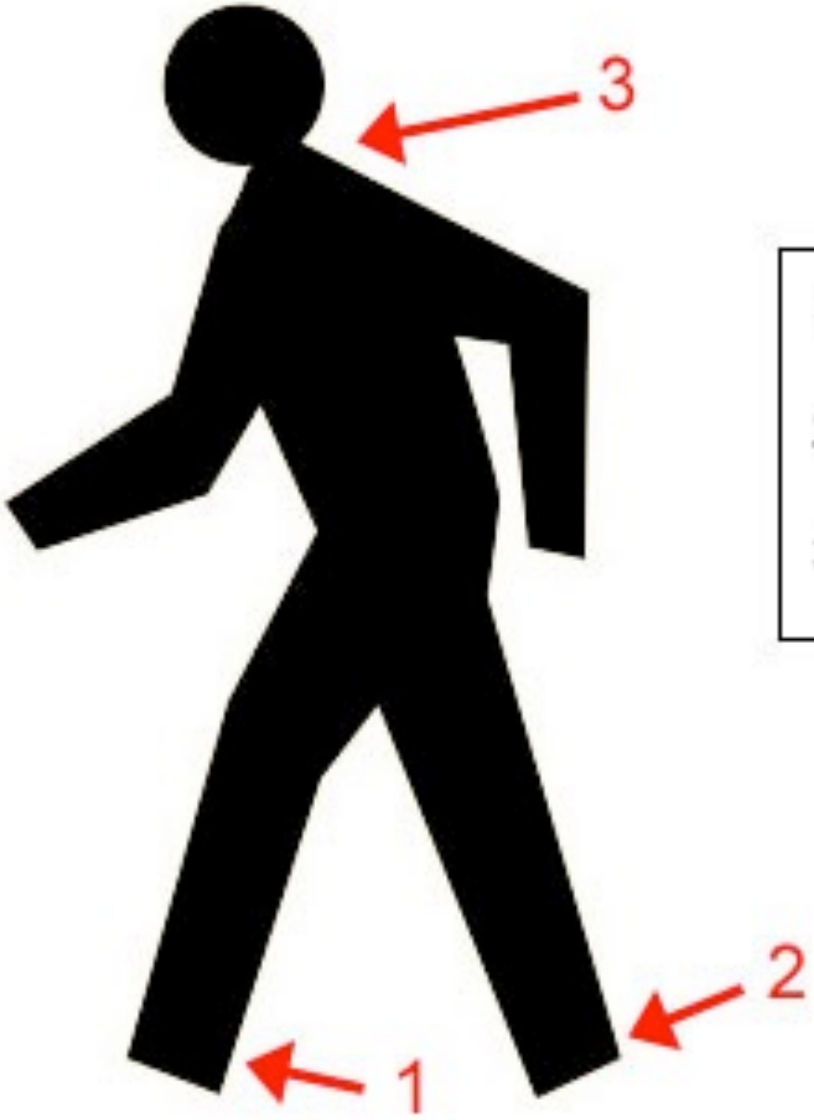
DEMO

XSS Tools

- SafeERB
- XSS Shield
- Cross Site Sniper

Fig. 3c: When Dealing With a Killa Bee Swarm in the Lands of Shaolin

Courtesey of the Wu-Tang Institute, Dr. Robert Digital



1. Watch Your Step, Kid
2. Watch Your Step, Kid
3. Protect Your Neck

What should you take away from this?

- Keep your framework up to date!
- Take advantage of plugins when you can.
- Think security from the ground up.
- Audit your applications for security holes.

Audit Planning

- Make plans with your project manager to incorporate audits.
- Put together an audit checklist so any member of your team can do it.
- Preach security awareness within your organization.
- Just do it!

PeepCode press

$9

Security Audit

Building safe applications

by Aaron Bedra

Valuable Links

- github.com/relevance/tarantula/tree/master
- rorsecurity.info
- owasp.org
- aaronbedra.com
- workingwithrails.com/person/5499-aaron-bedra

Questions?