De-Railing: Smashing the Rails Stack

Aaron Bedra
Relevance, Inc.

Just so you know...

There's more to life than being really really ridiculously good looking.

On Pirates and Ninjas

Pirates are cool, but anyone can be a pirate. That, and you can see them a mile away.

You might not even know a Ninja is around, at least until he's gone and you are laying in a pool of your own code...

Most of us are prepared for a pirate attack, but can you survive the Ninjas?

SQL Injection

Asset.find params[:id]

Asset.find(:all, :limit => "#{params}")

Asset.find(:all, :limit => "#{params}")

10 procedure help()

Methods to be careful of

- find_by_sql
- execute
- limit -- (fixed in Rails 2.1)
- offset -- (fixed in Rails 2.1)
- group_by
- order

What should I do to fix it?

- Only drop to raw SQL when absolutely necessary.
- Take advantage of built in Active Record methods such as quote() when applicable.
- Write tests.
- Use analysis tools that help you look for possible attack vectors.

Cross Site Scripting

<%= @asset.text %>

<%= @asset.text %>

<%= h @asset.text %>

Preventative Measures

- SafeERB
- XSS Shield
- Manual Escaping (Not Recommended)

Tarantula

Eight Legs, Two Fangs, and an Attitude

http://opensource.thinkrelevance.com/wiki/tarantula

- Crawls every available link reporting the http status
- Checks every rendered page for bad html
- Fuzzes every encountered form with garbage data
- Produces detailed reports of every action that include the html rendered along with the logs from the rendering methods

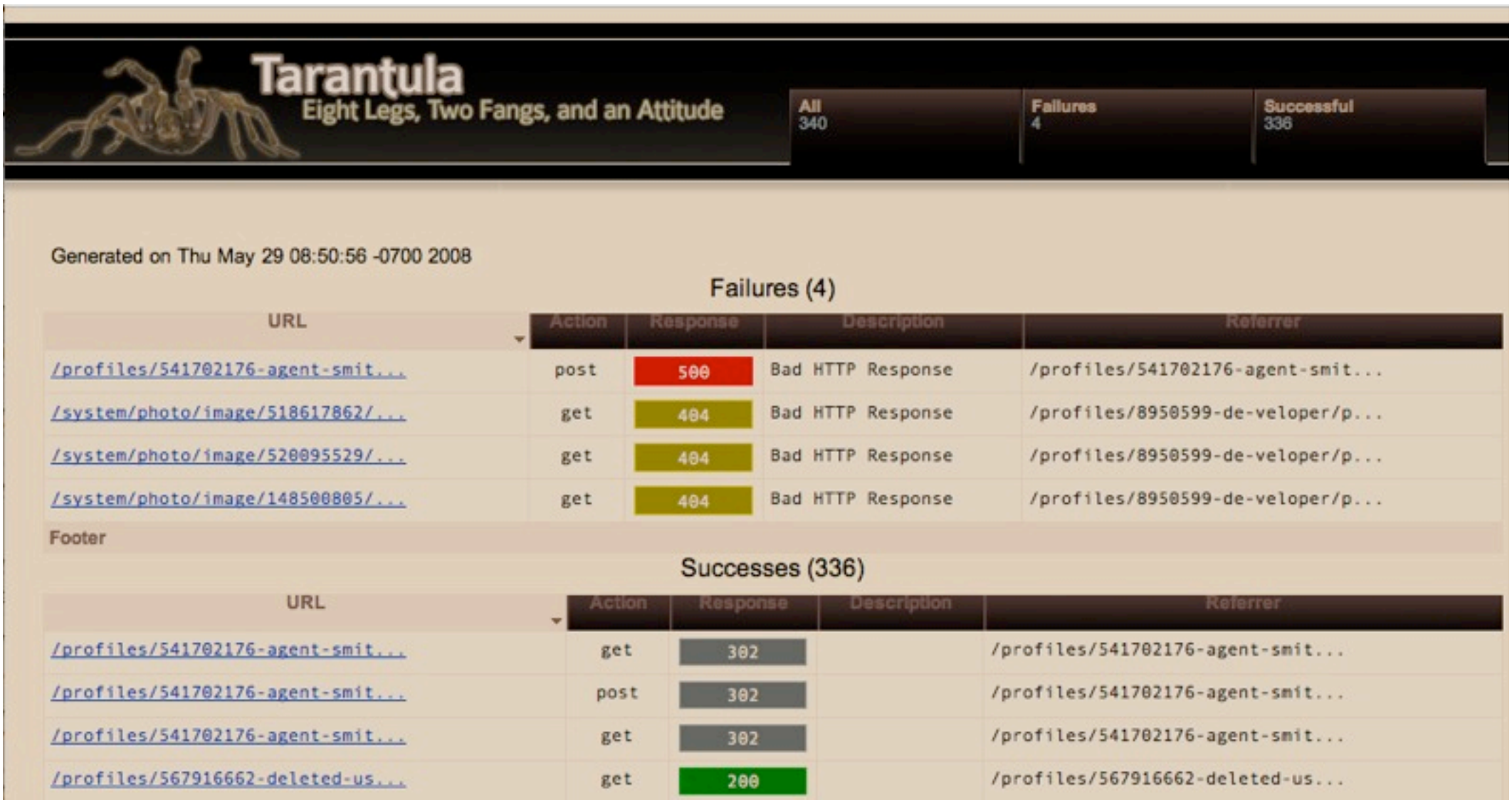
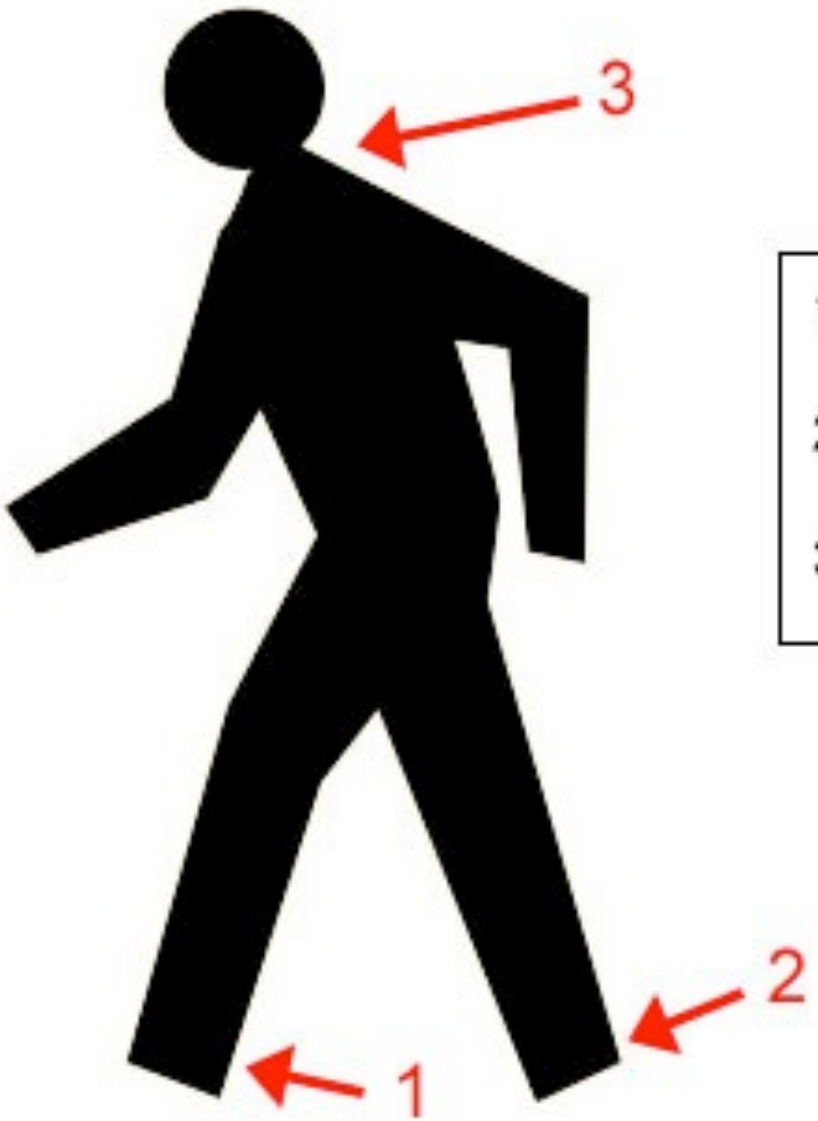


Fig. 3c: When Dealing With a Killa Bee Swarm in the Lands of Shaolin

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



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

Don’t let the Ninjas get your neck!

- Add a firewall script that blocks all non used ports.
- Don’t allow the root user to login remotely.
- Move your ssh port to a non-standard place.
- Demand strong passwords for all your users.
- Turn off password authentication entirely and use ssh keys.
- Monitor your server logs every now and then to make sure nobody is doing anything sneaky.

Now that you know some Ninja moves, let's put a plan into action.

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

- http://rorsecurity.info
- http://owasp.org
- http://www.quarkruby.com/2007/9/20/ruby-on-rails-security-guide
- http://rubythis.blogspot.com/2006/11/rails-security-checklist.html
- http://aaronbedra.com

Questions?

Aaron Bedra
Relevance, Inc.