Security Matters: Getting Started with Security Scanners

Dale Clarke - Digitaria

Who Am I?

Former Drupal developer (6 yrs)

Security interest going back to running honey pots in college

Security architect at Digitaria

Obligatory Disclaimer

Please only run scanners on your own sites

Only run scanners against non-prod environments

If you find security issues with core, contributed modules, libraries, etc., please disclose those findings to the author/creator in a responsible way.

Overview

Why security?

Intro to security basics

Configuring and running a scanner

Interpreting results

Issues with scanners

Q&A

Why Security

It’s the responsible thing to do

It protects your brand / reputation

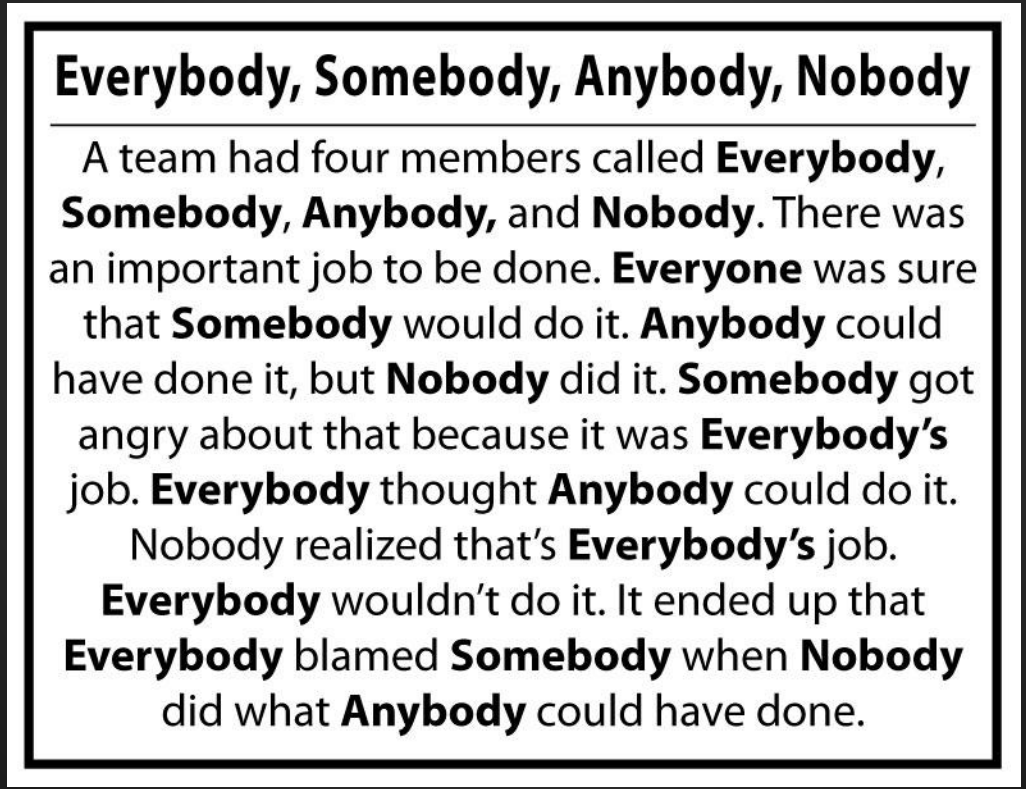
It’s a relatively small expense upfront that is much less than the cost of dealing with getting hacked

Estimated costs of cybercrime and hacking in 2013 around $100 billion USD! [http://on.wsj.com/1rbWa7n]

Why Security

A little story about **Everybody**, **Somebody**, **Anybody**, and **Nobody**...

Why Security



Everybody, Somebody, Anybody, Nobody

A team had four members called **Everybody**, **Somebody**, **Anybody,** and **Nobody**. There was an important job to be done. **Everyone** was sure that **Somebody** would do it. **Anybody** could have done it, but **Nobody** did it. **Somebody** got angry about that because it was **Everybody's** job. **Everybody** thought **Anybody** could do it. Nobody realized that's **Everybody's** job. **Everybody** wouldn't do it. It ended up that **Everybody** blamed **Somebody** when **Nobody** did what **Anybody** could have done.

Security Basics

OWASP - Open Web Application Security Project

Created in 2004 with the goal “... to make software security visible, so that individuals and organizations worldwide can make informed decisions about true software security risks.”

To help they publish a top 10 threats list

OWASP Top 10

A1 Injection

A2 Broken Authentication and Session Management

A3 Cross-Site Scripting (XSS)

A4 Insecure Direct Object References

A5 Security Misconfiguration

A6 Sensitive Data Exposure

A7 Missing Function Level Access Control

A8 Cross-Site Request Forgery (CSRF)

A9 Using Components with Known Vulnerabilities

A10 Unvalidated Redirects and Forwards

How to comply?

Write 100% perfect bug free code

Hire a pentester

Crowdsource it

Automate it

Introducing Security Scanners

Many options but they all essentially

- Spider the site
- Attempt known attacks
- Fuzz inputs
- Generate a report

Lots of options… Qualys, HP, Acunetix, Skipfish, IronWASP, etc

Skipfish

Maintained by Google

Released in 2010 under the Apache Licence 2.0

Written in C++

Cost: FREE!!!

Live Demo

Install

Config and run

Review results

Live Demo - Install

sudo apt-get install build-essential libssl-dev libpcre-ocaml-dev libidn11-dev

wget https://skipfish.googlecode.com/files/skipfish-2.10b.tgz

tar zxvf skipfish-2.10b.tgz

make

Live Demo - Config and Run

mkdir wordlists

mkdir reports

touch wordlists/drupal7

./skipfish -W wordlists/drupal7 -o reports/drupal7_01 http://drupal7/

Live Demo - Review

Let’s look at some examples

Limitations of Scanners

Lots of false positives

Unable to scan JS heavy sites

Limited to certain types of vulnerabilities

Just because the scanner doesn’t report it doesn’t mean it isn’t there

Responsible Disclosure

If you find an issue in core, a contrib module, 3rd party library/script, etc please report it through the proper channels.

http://drupal.org/node/101494

Questions?