In ur s3rvs
h4k1ng ur c0dez

IN UR S3VRS

*cute animal tax

H4K1NG UR C0DEZ

Introductions

Jack Skinner	@developerjack
Katie McLaughlin	@glasnt

And what about you?

(not your employer)

What the CVE?

Definitions

CVE

- "**C**ommon **V**ulnerabilities and **E**xposures"
- Unique database of vulnerabilities
- Identified by ID `CVE-YYYY-NNNNNN`
- https://cve.mitre.org

Definitions

OWASP

- “**O**pen **W**eb **A**pplication **S**ecurity **P**roject”
- https://www.owasp.org

OWASP Top 10

- Most common attack vectors for Web

OWASP Top 10

- Injection
- Cross-Site Scripting
- Cross-Site Request Forgery

(broken authentication, vuln. components, exposing internals, exposing data, security misconfig, unvalidated redirects, missing access control)

The State of Play

Security in 2014

In the last 12 months…

CVEs against common PHP CMSs

- Wordpress - 29
- Drupal - 14
- and many more...

http://www.cvedetails.com

In the last 12 months…

32 new CVEs in PHP itself

Major Vectors:

- Denial of Service
- Overflow

http://www.cvedetails.com

PHP Versions

What version are you running?

PHP 5.0, 5.1, 5.2, 5.3

- No longer supported
- No security patches
- Do not use

PHP 5.0, 5.1, 5.2, 5.3

- No longer supported
- No security patches
- Do not use

Did you know?

 - PHP 5.1 has not been supported since 2006

(That’s 9 years, guys)

But, PHP 5.3!

- Don’t use it
- Upgrade
- Please, for the love of god, upgrade.

Even Microsoft Azure no longer supports 5.3

http://www.microsofttrends.com/2015/01/27/warning-azure-web-sites-turning-off-php-5-3-support-on-january-31-2015/

So what PHP versions can I use?

- 5.4 - Security Fixes, Supported til Sep 2015
- 5.5 - Bug & Security Fixes, til mid 2016
- 5.6 - Bug & Security Fixes, til mid 2017

- 7.0 - Shiny, coming “Real Soon Now” ™

In the last 12 months…

Multiple Operating System CVEs

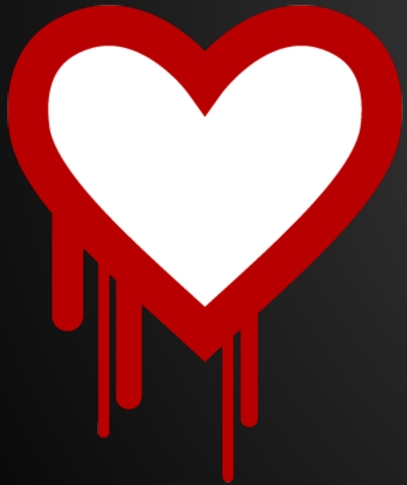
CVE-2014-0160

CVE-2014-6271

CVE-2014-0235

In the last 12 months…

Multiple Operating System CVEs better known as



In the last 12 months...

- Possibly even more issues

- “Responsible Disclosure” may not be enacted by all parties.

In the last 12 months...

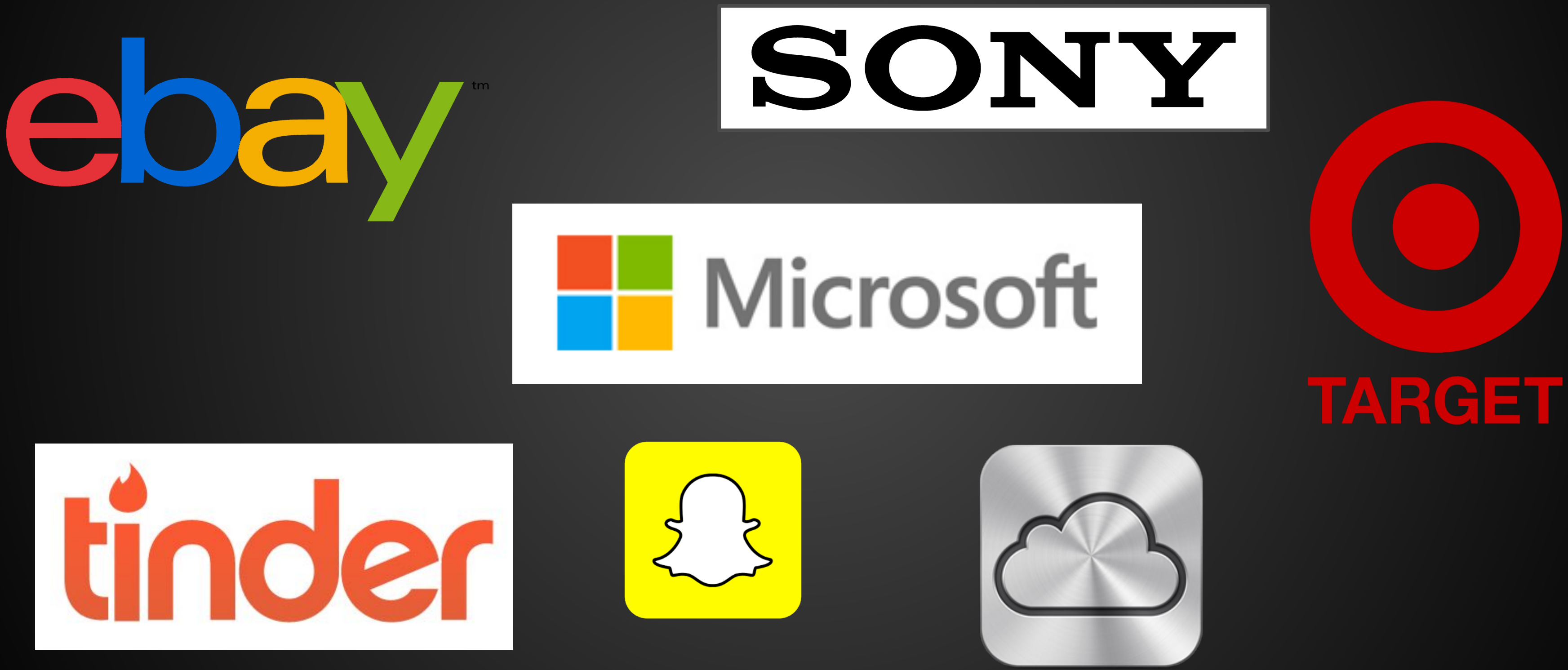
- Possibly even more issues

- “Responsible Disclosure” may not be enacted by all parties.

“It seems I am not the only spy!” - Spy

“That won’t happen to me”

In the last 12 months…



http://www.androidauthority.com/hacks-security-breaches-2014-577255/

“I’m not big enough to be a target”

“

‘Security through Obscurity’
in the real world of professional IT
is over

”

- Eben Moglen, January 13, 2015

https://www.youtube.com/watch?v=OAKRdZLU7AU

TL;DR

Internets be crazy

What can you do?

Know the enemy

Let’s Demo.

Demo:
Logic Issues

Demo:
SQL Injection

Demo:
Cross Site Scripting

(XSS)

D

Demo:
Cross Site Request Forgery

(CSRF)

Review

Review

- Don’t trust user input
- Keep your system patched
- Keep your application patched
- Don’t trust machine input
- Keep your every patched
- Don’t trust input

Overtime Bonus Demo:
PHP 5.3

Questions?

IIn

The End.

Beer time! <3