BILL CONDO

A LOOK BEHIND RECENT WEBSITE SECURITY BREACHES

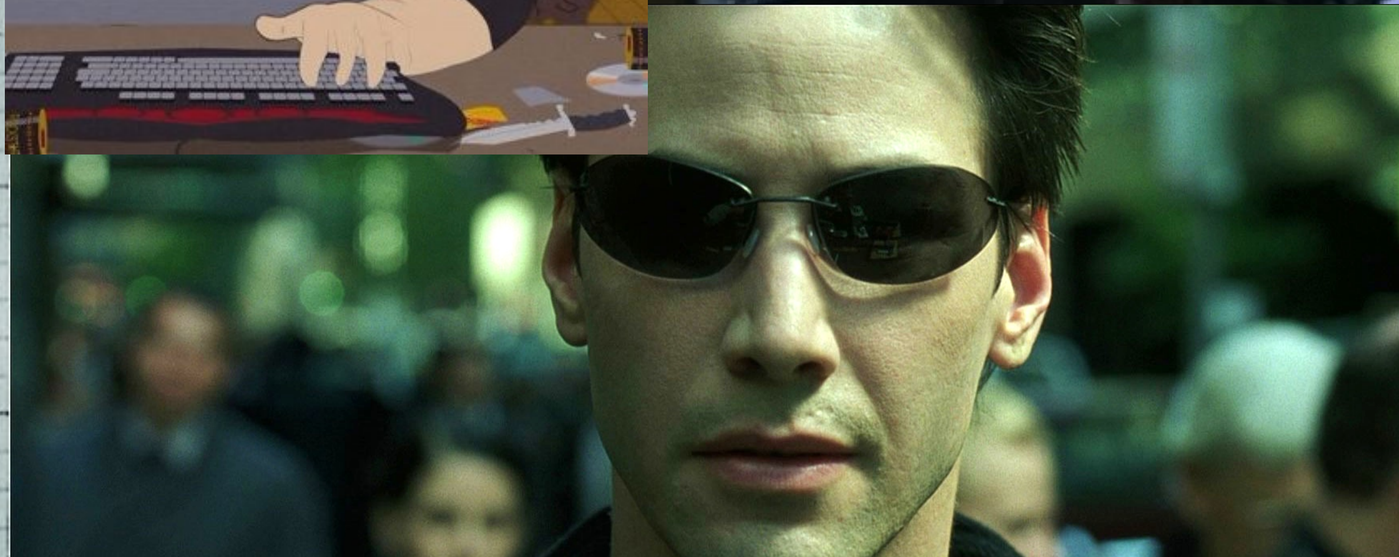
ABOUT ME

- I organize ColumbusPHP (Columbus, OH)
- I currently run my own agency, HustleWorks
- I love to talk security. Chat with me after my talk.

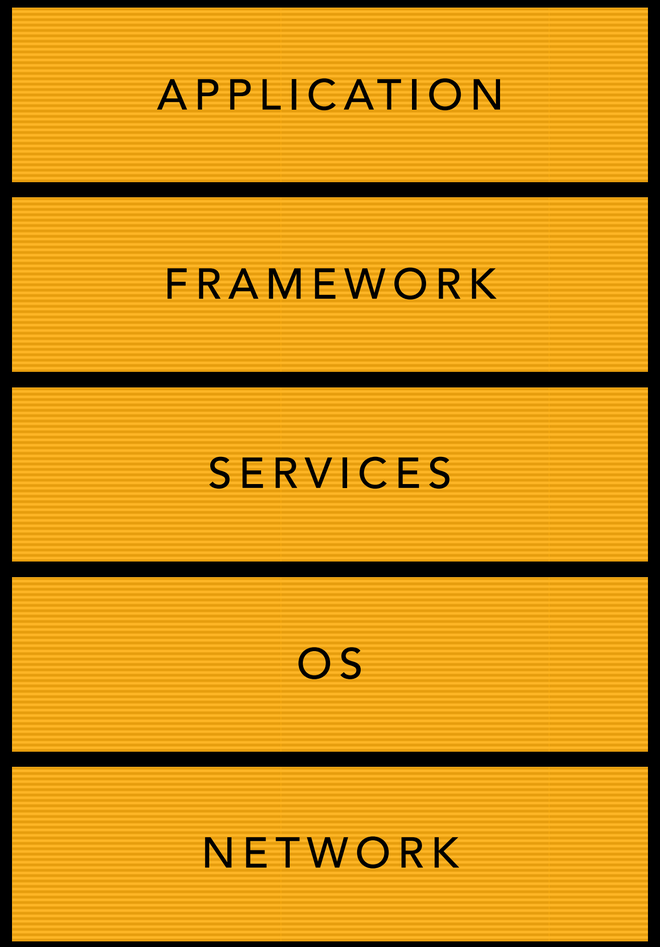
THE AGENDA

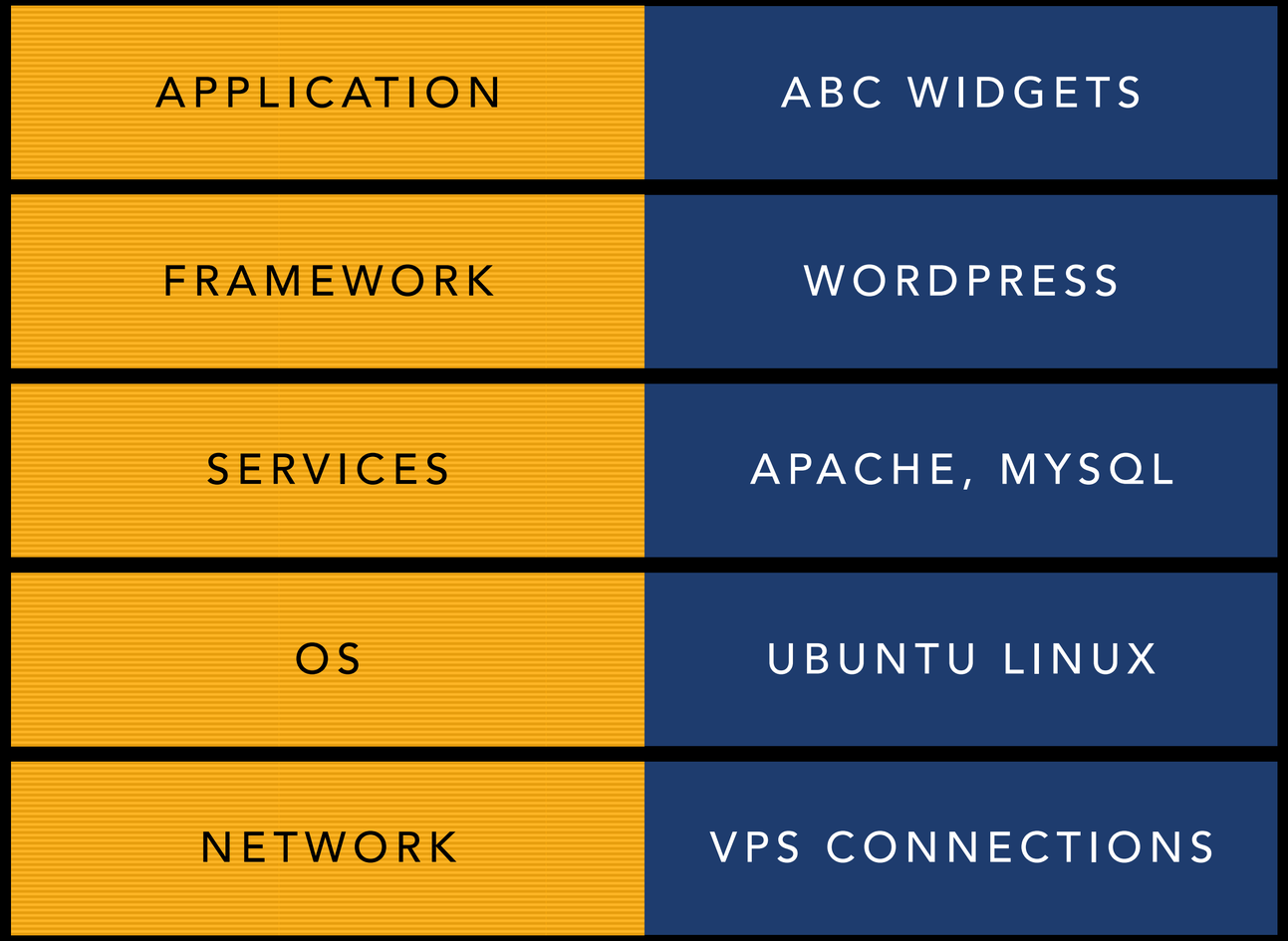
- Getting into the mindset
- A look at selected breaches
- Take aways

MINDSET




SECURITY


APPLICATION
FRAMEWORK
SERVICES
OS
NETWORK


APPLICATION
ABC WIDGETS
FRAMEWORK
WORDPRESS
SERVICES
APACHE, MYSQL
OS
UBUNTU LINUX
NETWORK
VPS CONNECTIONS

Apache™ HTTP SERVER PROJECT

Essentials

- About
- License
- FAQ
- Security Reports

Download!

- From a Mirror

Documentation

- Version 2.4
- Version 2.2
- Version 2.0
- Trunk (dev)
- Wiki

Get Support

- Support

Get Involved

- Mailing Lists
- Bug Reports
- Developer Info

Subprojects

- Docs
- Test
- Flood
- libapreq
- Modules
- mod_fcgid
- mod_ftp

Miscellaneous

- Contributors
- Sponsors
- Sponsorship

Apache httpd 2.4 vulnerabilities

This page lists all security vulnerabilities fixed in released versions of Apache httpd 2.4. Each vulnerability is given a security impact rating by the Apache security team - please note that this rating may well vary from platform to platform. We also list the versions of Apache httpd the flaw is known to affect, and where a flaw has not been verified list the version with a question mark.

Please note that if a vulnerability is shown below as being fixed in a "-dev" release then this means that a fix has been applied to the development source tree and will be part of an upcoming full release.

This page is created from a database of vulnerabilities originally populated by Apache Week. Please send comments or corrections for these vulnerabilities to the Security Team.

The initial GA release, Apache httpd 2.4.1, includes fixes for all vulnerabilities which have been resolved in Apache httpd 2.2.22 and all older releases. Consult the Apache httpd 2.2 vulnerabilities list for more information.

Fixed in Apache httpd 2.4.24-dev

n/a: HTTP_PROXY environment variable "httpoxy" mitigation CVE-2016-5387

HTTP_PROXY is a well-defined environment variable in a CGI process, which collided with a number of libraries which failed to avoid colliding with this CGI namespace. A mitigation is provided for the httpd CGI environment to avoid populating the "HTTP_PROXY" variable from a "Proxy:" header, which has never been registered by IANA.

This workaround and patch are documented in the ASF Advisory at https://www.apache.org/security/asf-httpoxy-response.txt

Acknowledgements: We would like to thank Dominic Scheirlinck and Scott Geary of Vend for reporting and proposing a fix for this issue.

Reported to security team: 2nd July 2016
Issue public: 18th July 2016
Update Released: 18th July 2016
Affects: 2.4.23, 2.4.20, 2.4.18, 2.4.17, 2.4.16, 2.4.12, 2.4.10, 2.4.9, 2.4.7, 2.4.6, 2.4.4, 2.4.3, 2.4.2, 2.4.1

Fixed in Apache httpd 2.4.23

important: TLS/SSL X.509 client certificate auth bypass with HTTP/2 CVE-2016-4979

For configurations enabling support for HTTP/2, SSL client certificate validation was not enforced if configured, allowing clients unauthorized access to protected resources over HTTP/2. This issue affected releases 2.4.18 and 2.4.20 only.

Acknowledgements: This issue was reported by Erki Aring.

Reported to security team: 30th June 2016

SMART TRADEOFFS

SUMMARIZE, NOTIFY

BREACHES


TechCrunch

TECHCRUNCH

- WordPress.com VIP
- OurMine posted publicly to the site
- Weak staff password

TECHCRUNCH LESSONS

- Set a password policy
- Turn on second factor auth for high value targets
- Consider authentication gates such location, browser user agent


ClixSense

CLIXSENCE

- 6.6 million accounts
- 2.2 million records released so far
- Plaintext passwords, usernames, email addresses, and other personal info
- After gaining access, the hacker was able "to copy most, if not all" of the ClixSense users table, ran SQL code to change account names to "hacked account," deleted several forum posts, as well as set account balances of users to $0.00.

CLIXSENCE LESSONS

- Hash Passwords
- Reconsider if you truly need all of the info that you’re requesting
- Limit access across systems


ASHLEY
MADISON®.COM
Life is Short. Have an Affair.®


37m account dump
DMCA
$578m lawsuit
Two suicides
8/2015

ASHLEYMADISON

- Real names, home addresses, search history and credit card transactions
- Attempts to use DCMA to hide breach and data dumps
- Lawsuits, Suicides
- Avid Life Media CEO Noel Biderman Resigns
- Passwords hashed with bcrypt, some with MD5
- CynoSure Prime cracked 11.2 million Ashley Madison users’ passwords

ASHLEYMADISON LESSONS

- Don’t keep legacy MD5 passwords. Wrap them in bcrypt.
- Be aware of dictionary based attacks (RockYou, etc)


last.fm


Hacked
“Some” accounts
43.5 million accounts
2012
2016

LAST.FM

- 43.5 million accounts
- Usernames, email addresses, join date, and other internal records
- Passwords hashed with MD5
- 96 percent of passwords decrypted in two hours


Linked in


Hacked
6.5m accounts
117m accounts
2012
2016

LINKEDIN

- 117 million users
- Passwords were stored as SHA1 w/o salt
- 90% of the passwords in 72 hours
- For sale on a marketplace
- LinkedIn since invalidated some of the passwords
- Check your email at “Have I Been Pwned”

LINKEDIN LESSONS

- Strong Hashes
- Banned Password List
- Have a plan to invalidate passwords
- Keep an eye on available data dumps


YAHOO!

Hacked

2014

500m+ accounts

2016

YAHOO

- 500 million users, largest of all time
- Yahoo believes it was a state sponsored act
- Hackers have sold the entire Yahoo database at least three times
- Data: Emails, telephone numbers, dates of birth, hashed passwords, plain text security questions and answers
- Most passwords were stored bcrypt
- SEC, FTC Disclosure Issues

YAHOO LESSONS

- Security answers should be encrypted
- Security questions should be invalidated after a breach
- Disclose quickly, responsibly
- With scale, comes attention

MANY OTHERS


eHarmony®


Adobe


Dropbox

PRACTICES

USE LOGGING SERVICES TO REVIEW AND NOTIFY

DOCUMENT WHAT YOU'RE PROTECTING

SANE PASSWORDS

GET EXTERNAL INPUT

BE AWARE OF OUTSIDE EVENTS

THANKS

@mavrck

mavrck.com