What the Hack?

Fortifying your security by understanding your adversary

Mikey Veenstra
@heyitsmikeyv
WordCamp Phoenix 2019

Who’s Mikey?

- Threat Analyst at Wordfence
- GIAC Advisory Board Member
- Ethical Hacker
- Typical Geek Dad

this slide deck was PWNED!!!!

by: W0rdC4mp Cr3w

Greetz to: TowKey01 &&
Mas0nDoRN &&
Teh_FEEBZ

Put your hacker hat on.

Reconnaissance:

Knowledge is power.

Two angles, one goal.

“I want to open this door. Where can I find a key?”
vs
“I’ve got some keys. What doors can I open?”

Questions They’re Asking

“What types of keys might work on this door?”

“How do I narrow down which doors to try?”

Targeted or not, they’re all still threats.

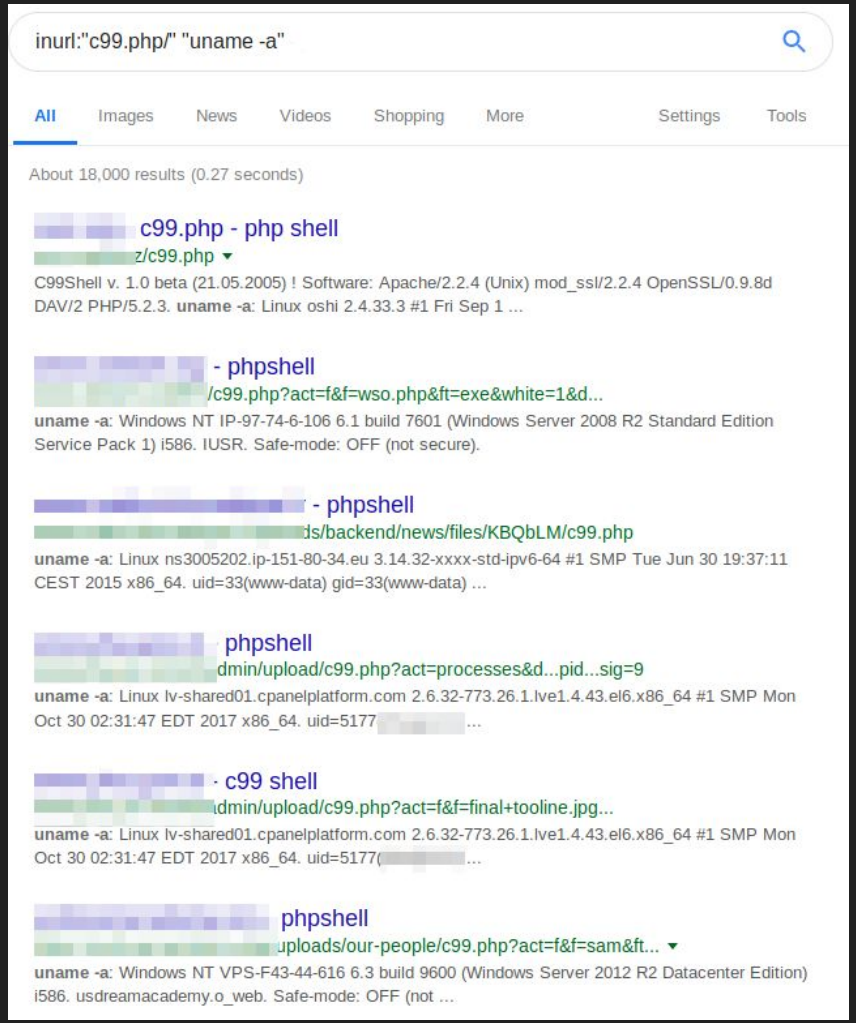
Untargeted Reconnaissance

I. Google Dorks
II. PublicWWW
III. Project Sonar

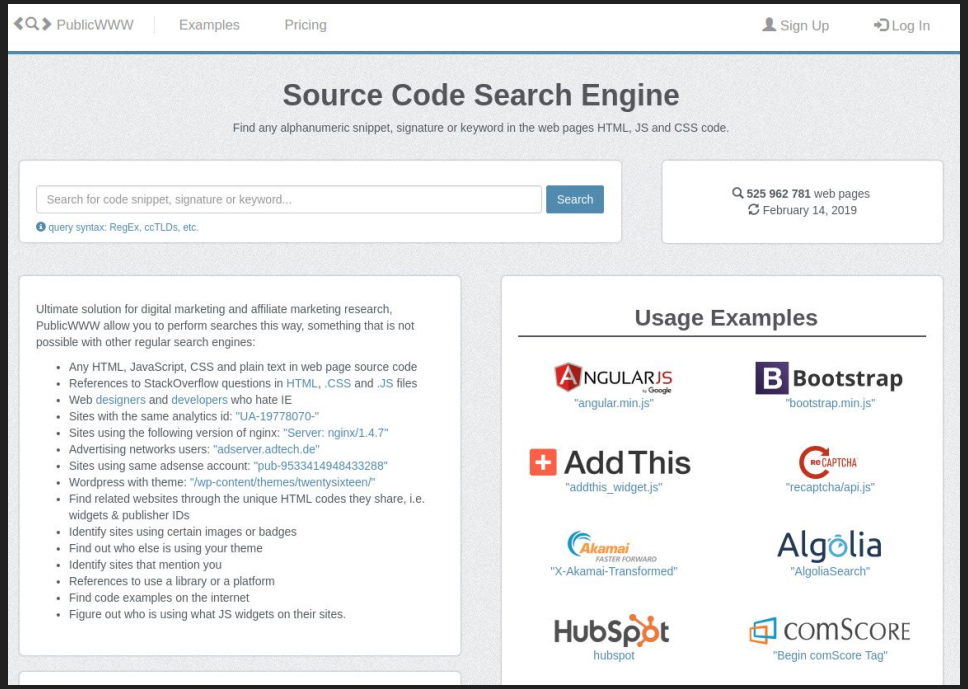
The Art of the Google Dork

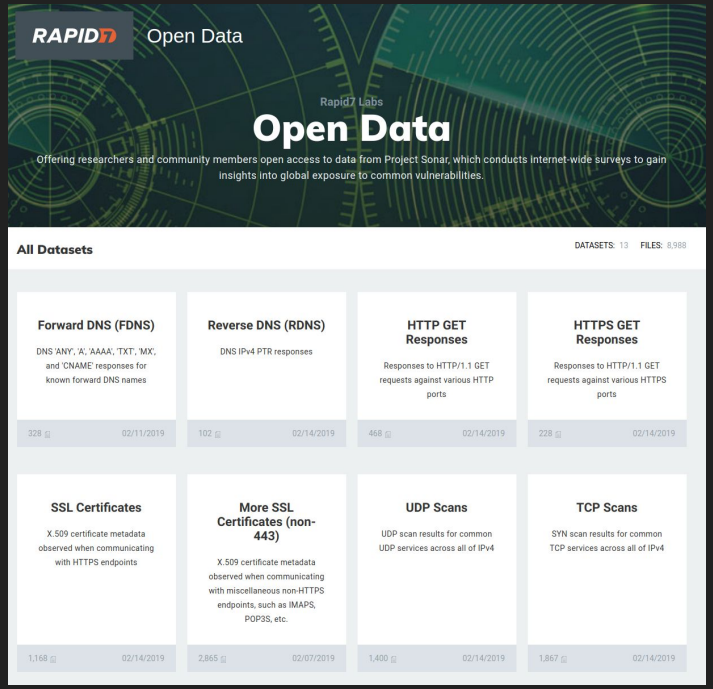
Find all sorts of cool stuff:

- Indicators of vulnerability
- Unexpected files
- Another hacker's shells?!



PublicWWW and Project Sonar





Assume the internet knows everything about your site.

Targeted Reconnaissance

I. Application Scanners
II. Forced Browsing
III. OSINT

Application Scanners

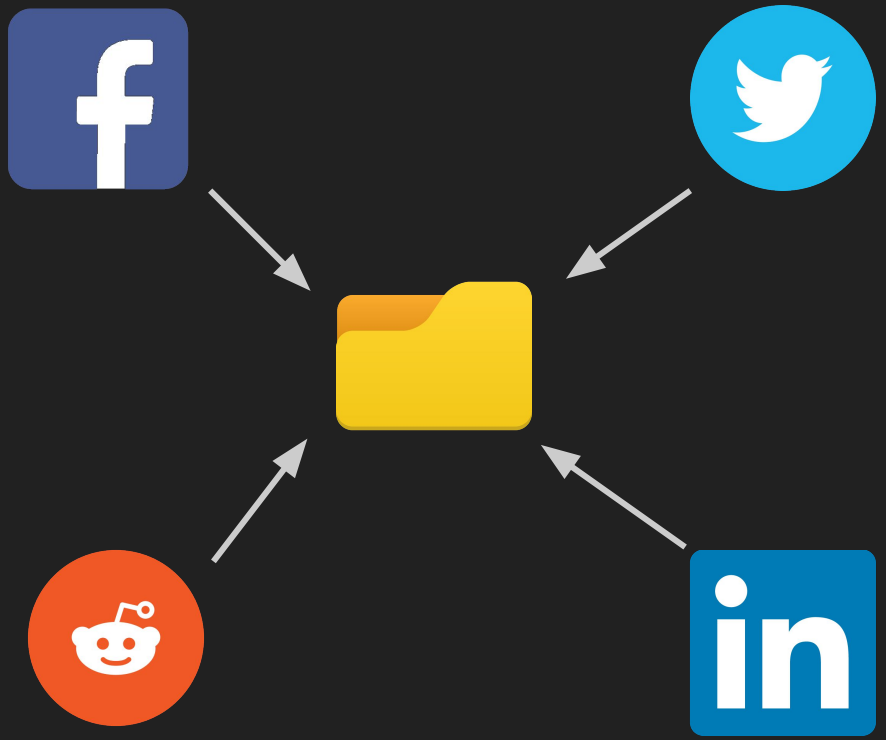
```
[+] Enumerating installed plugins (only ones with known vulnerabilities) ...

   Time: 00:00:05 <=========================================================================

[+] We found 1 plugin:

[+] Name: flickr-picture-backup - v0.7
 |  Latest version: 0.7 (up to date)
 |  Last updated: 2014-09-03T09:47:00.000Z
 |  Location: http://localhost/wp0/wp-content/plugins/flickr-picture-backup/
 |  Readme: http://localhost/wp0/wp-content/plugins/flickr-picture-backup/readme.txt
[!] Directory listing is enabled: http://localhost/wp0/wp-content/plugins/flickr-picture-backup/

[!] Title: flickr-picture-backup <= 0.7 - Unauthenticated File Upload
    Reference: https://wpvulndb.com/vulnerabilities/8803
    Reference: http://www.vapidlabs.com/advisory.php?v=190
```

Forced Browsing

“It’s like a bruteforce attack,
but for file paths!”

Open Source Intelligence (OSINT)

- Email Addresses
- Infrastructure Knowledge
- Exploitable Personnel
- Wordlist Generation



Recon Takeaways

1. Data can’t be both public and secret.
2. Obscurity != Security
3. The internet is watching.

Bypassing Security

Cloud WAFs & CDNs

Finding An Origin IP

- Outgoing Email Headers
- Common Subdomains
- Reverse DNS (PTR) Records

File Upload Restrictions

Blacklisting “.php” files?

.php5 .phtml .PhP .pht .phar

Do this instead:

- Whitelist, don’t blacklist.
- If possible, ditch the uploaded filename.
- Disable code execution in uploads

“What do I have, and who might want it?”

Assume breach.

What the Hack?

Fortifying your security by understanding your adversary

Mikey Veenstra
@heyitsmikeyv
WordCamp Phoenix 2019