

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.

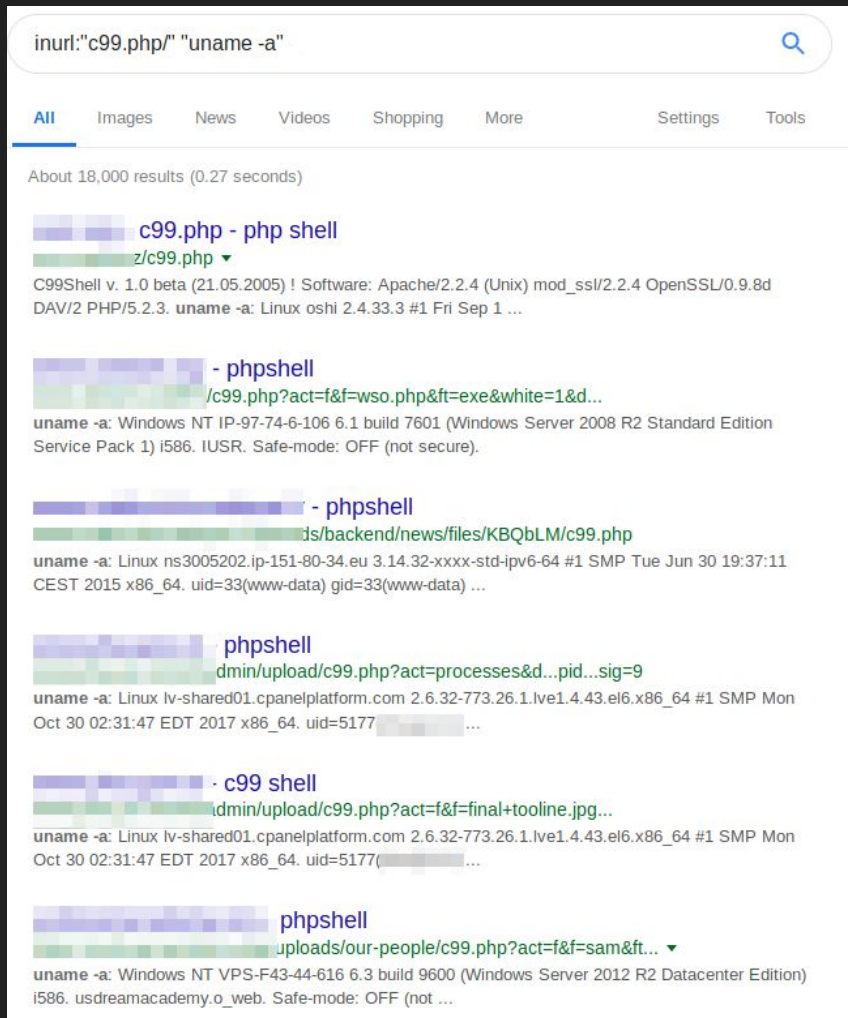
Untargeted Reconnaissance

- 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?!



inurl:"c99.php/" "uname -a"

All Images News Videos Shopping More Settings Tools

About 18,000 results (0.27 seconds)

c99.php - php shell
z/c99.php ▼
C99Shell v. 1.0 beta (21.05.2005) ! Software: Apache/2.2.4 (Unix) mod_ssl/2.2.4 OpenSSL/0.9.8d DAV/2 PHP/5.2.3. **uname -a:** Linux oshi 2.4.33.3 #1 Fri Sep 1 ...

- phpshell
/c99.php?act=f&f=wso.php&ft=exe&white=1&d...
uname -a: Windows NT IP-97-74-6-106 6.1 build 7601 (Windows Server 2008 R2 Standard Edition Service Pack 1) i586. IUSR. Safe-mode: OFF (not secure).

- phpshell
ds/backend/news/files/KBQbLM/c99.php
uname -a: Linux ns3005202.ip-151-80-34.eu 3.14.32-xxxx-std-ipv6-64 #1 SMP Tue Jun 30 19:37:11 CEST 2015 x86_64. uid=33(www-data) gid=33(www-data) ...

phpshell
admin/upload/c99.php?act=processes&d...pid...sig=9
uname -a: Linux lv-shared01.cpanelplatform.com 2.6.32-773.26.1.lve1.4.43.el6.x86_64 #1 SMP Mon Oct 30 02:31:47 EDT 2017 x86_64. uid=5177 ...

- c99 shell
admin/upload/c99.php?act=f&f=final+tooline.jpg...
uname -a: Linux lv-shared01.cpanelplatform.com 2.6.32-773.26.1.lve1.4.43.el6.x86_64 #1 SMP Mon Oct 30 02:31:47 EDT 2017 x86_64. uid=5177 ...

phpshell
uploads/our-people/c99.php?act=f&f=sam&ft... ▼
uname -a: Windows NT VPS-F43-44-616 6.3 build 9600 (Windows Server 2012 R2 Datacenter Edition) i586. usdreamacademy.o_web. Safe-mode: OFF (not ...

PublicWWW and Project Sonar

PublicWWW | Examples | Pricing | Sign Up | Log In

Source Code Search Engine

Find any alphanumeric snippet, signature or keyword in the web pages HTML, JS and CSS code.

Search for code snippet, signature or keyword...









🔍 525 962 781 web pages
🔄 February 14, 2019

🔗 query syntax: RegEx, ccTLDs, etc.

Ultimate solution for digital marketing and affiliate marketing research, PublicWWW allow you to perform searches this way, something that is not possible with other regular search engines:

- Any HTML, JavaScript, CSS and plain text in web page source code
- References to StackOverflow questions in HTML, .CSS and .JS files
- Web designers and developers who hate IE
- Sites with the same analytics id: "UA-19778070-"
- Sites using the following version of nginx: "Server: nginx/1.4.7"
- Advertising networks users: "adserver.adtech.de"
- Sites using same adsense account: "pub-9533414948433288"
- Wordpress with theme: "wp-content/themes/wentysixteen/"
- Find related websites through the unique HTML codes they share, i.e. widgets & publisher IDs
- Identify sites using certain images or badges
- Find out who else is using your theme
- Identify sites that mention you
- References to use a library or a platform
- Find code examples on the internet
- Figure out who is using what JS widgets on their sites.

Usage Examples

-  **ANGULARJS**
"angular.min.js"
-  **Bootstrap**
"bootstrap.min.js"
-  **Add This**
"addthis_widget.js"
-  **reCAPTCHA**
"recaptcha/api.js"
-  **Akamai**
"X-Akamai-Transformed"
-  **Algolia**
"AlgoliaSearch"
-  **HubSpot**
hubspot
-  **COMSCORE**
"Begin comScore Tag"

RAPID7 Open Data

Rapid7 Labs

Open Data

Offering researchers and community members open access to data from Project Sonar, which conducts Internet-wide surveys to gain insights into global exposure to common vulnerabilities.

All Datasets

DATASETS: 13 | FILES: 8,988

Dataset Name	Description	Count	Last Updated
Forward DNS (FDNS)	DNS ANY, A, AAAA, TXT, MX, and CNAME responses for known forward DNS names	328	02/11/2019
Reverse DNS (RDNS)	DNS IPv4 PTR responses	102	02/14/2019
HTTP GET Responses	Responses to HTTP/1.1 GET requests against various HTTP ports	468	02/14/2019
HTTPS GET Responses	Responses to HTTP/1.1 GET requests against various HTTPS ports	228	02/14/2019
SSL Certificates	X.509 certificate metadata observed when communicating with HTTPS endpoints	1,168	02/14/2019
More SSL Certificates (non-443)	X.509 certificate metadata observed when communicating with miscellaneous non-HTTPS endpoints, such as IMAPS, POP3S, etc.	2,865	02/07/2019
UDP Scans	UDP scan results for common UDP services across all of IPv4	1,400	02/14/2019
TCP Scans	SYN scan results for common TCP services across all of IPv4	1,867	02/14/2019

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
```

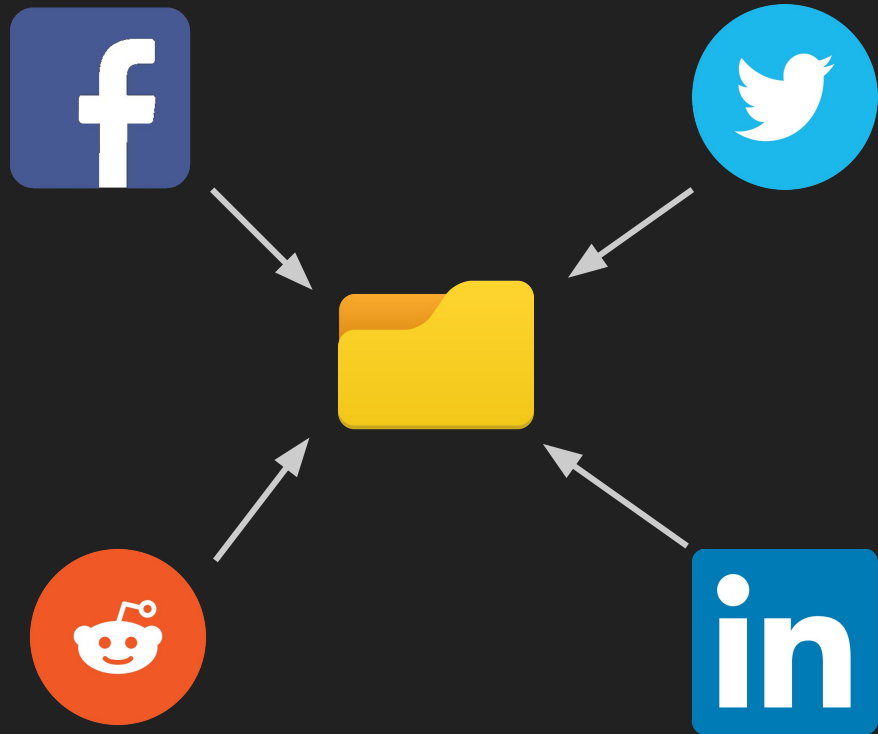
```
Reference: http://www.vapidlabs.com/advisory.php?v=190
```

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 \neq 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