

A dark, stylized image showing a person's silhouette in profile, looking at a computer monitor. The monitor displays a complex network diagram with various nodes and connections. The overall color palette is dark with some blue and green highlights.

# Open Source Intelligence in Cybersecurity

Anastacia Webster

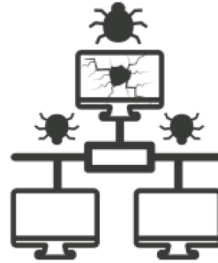
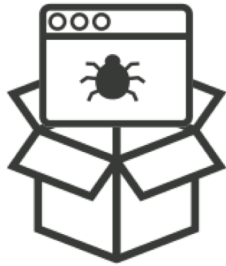
# Overview

- Open Sources + Intelligence = ?
- Open Source Intelligence in Cybersecurity?
- Finding Tools to Use
- Non Technical Tools/ Skills
- Technical Tools/ Skills
- Demonstration Tools
- Demonstration



Open Sources +  
Intelligence =?

# Open Source Intelligence in Cybersecurity



**Recon**

**Weaponize**

**Deliver**

**Exploit**

**Install**

**C2**

**Actions**

Gather data and intelligence on target organization

Craft malicious payload, use exploits for vulnerabilities

Payload sent to target (phishing)

Compromise system

Install malware, obtain credentials and establish backdoors.

Navigate internal network and setup command and control

Ultimate goals achieved

# PHASE 1: RECON

- Research the target
- Collect/Analyze information about online actives/public presence
  - Social Media
  - Harvest Email Addresses
  - Government Records
  - Public News
  - Scan internet facing systems and applications
- Build Profile

# RECON ACTORS



Criminals



Hacktivists



Criminal  
hackers



Competitors



Foreign  
nations



Disgruntled  
employees

← Mass untargeted

Targets individuals →

# Finding Tools to Use

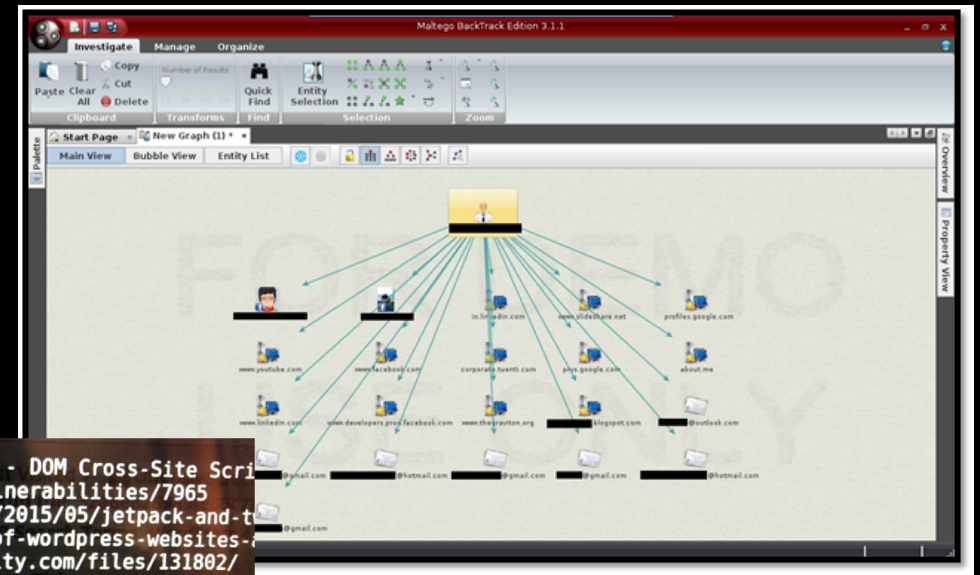
- Tons of FREE Tools out there for you to use...
  - <https://osintframework.com/>
  - <https://inteltechniques.com/menu.html>
  - <https://www.i-intelligence.eu/osint-tools-and-resources-handbook-2018/>
  - <http://reconvillage.org>
  - Search GitHub...





# Technical Tools/ Skills

- Maltego
- Burp
- WPScan
- Wireshark
- Dirbuster
- Creepy
- Buscador
- Email/Username/Password Generators



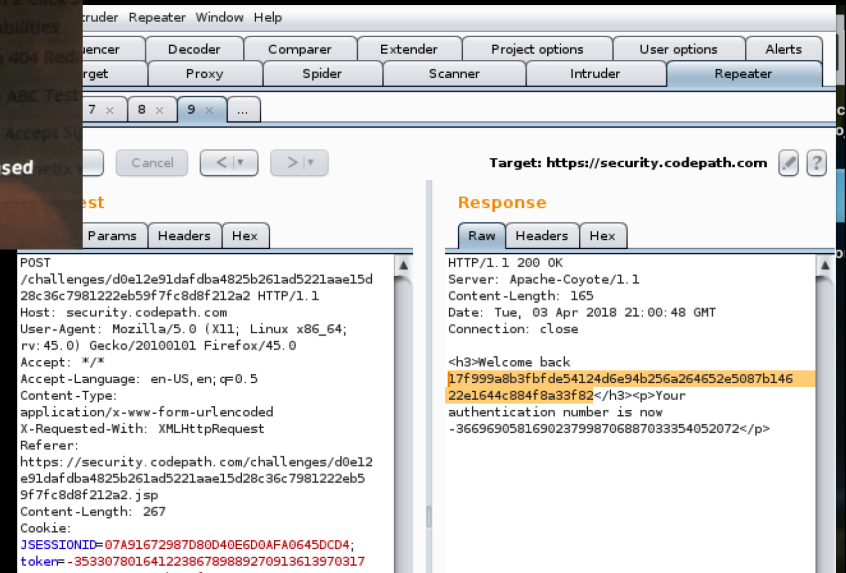
```
Title: Twenty Fifteen Theme <= 1.1 - DOM Cross-Site Scri
Reference: https://wpvulndb.com/vulnerabilities/7965
Reference: https://blog.sucuri.net/2015/05/jetpack-and-t
WordPress-websites-affected-millions-of-wordpress-websites-
Reference: http://packetstormsecurity.com/files/131802/
Reference: http://seclists.org/fulldisclosure/2015/May/41
Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name
Fixed in: 1.2

Enumerating plugins from passive detection ... Plugin 1 Rask
No plugins found

Enumerating usernames ...
Identified the following 1 user/s:
+-----+-----+-----+
| Id | Login | Name |
+-----+-----+-----+
| 1 | admin | 404 Not |
+-----+-----+-----+

Default first WordPress username 'admin' is still used

Finished: Tue May 15 10:26:24 2018
Requests Done: 57
```





# Demonstration Tools

# More Technical: DirBuster

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

Target URL (eg http://example.com:80/)

Work Method  Use GET requests only  Auto Switch (HEAD and GET)

Number Of Threads  10 Threads  Go Faster

Select scanning type:  List based brute force  Pure Brute Force

File with list of dirs/files

Char set  Min length  Max Length

Select starting options:  Standard start point  URL Fuzz

Brute Force Dirs  Be Recursive Dir to start with

Brute Force Files  Use Blank Extension File extension

URL to fuzz - /test.html?url={dir}.asp

Please complete the test details

# More Technical: WPScan

[!] Title: WordPress <= 4.2 - Unauthenticated Stored Cross-Site Scripting (XSS)

Reference: <https://wpvulndb.com/vulnerabilities/7945>

Reference: <http://klikki.fi/adv/wordpress2.html>

Reference: <http://packetstormsecurity.com/files/131644/>

Reference: <https://www.exploit-db.com/exploits/36844/>

[i] Fixed in: 4.2.1

[!] Title: WordPress 4.1-4.2.1 - Unauthenticated Generic Cross-Site Scripting (XSS)

Reference: <https://wpvulndb.com/vulnerabilities/7979>

Reference: [https://codex.wordpress.org/Version\\_4.2.2](https://codex.wordpress.org/Version_4.2.2)

[i] Fixed in: 4.2.2

[!] Title: WordPress <= 4.2.2 - Authenticated Stored Cross-Site Scripting (XSS)

Reference: <https://wpvulndb.com/vulnerabilities/8111>

Reference: <https://wordpress.org/news/2015/07/wordpress-4-2-3/>

Reference: <https://twitter.com/klikkiy/status/624264122570526720>

Reference: <https://klikki.fi/adv/wordpress3.html>

Reference: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5622>

Reference: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5623>

[i] Fixed in: 4.2.3

[!] Title: WordPress <=

Reference: <https://wp>

Reference:

<https://github.com/Wor>

5

Reference: <https://cv>

[i] Fixed in: 4.2.4

[!] Title: WordPress <=

```
[+] Enumerating usernames ...
[+] Identified the following 2 user/s:
+-----+-----+-----+
| Id | Login | Name |
+-----+-----+-----+
| 1 | admin | admin |
| 2 | k_77j0y | Kill Joy |
+-----+-----+-----+
[!] Default first WordPress username 'admin'
```

```
type="text/javascript" defer></script>
<style type="text/css">...</style>
<link rel="stylesheet" id="contact-form-7-css" href="https://gencybercards.com/wp-content
plugins/contact-form-7/includes/css/styles.css?ver=5.0.2" type="text/css" media="all">
<link rel="stylesheet" id="rgs-css" href="https://gencybercards.com/wp-content/themes/
salient/css/rgs.css?ver=8.0" type="text/css" media="all">
<link rel="stylesheet" id="font-awesome-css" href="https://gencyberca
themes/salient/css/font-awesome.min.css?ver=4.6.3" type="text/css" me
<link rel="stylesheet" id="main-styles-css" href="https://gencybercar
themes/salient/style.css?ver=8.0.1" type="text/css" media="all">
<style id="main-styles-inline-css" type="text/css">
html:not(.page-trans-loaded) { background-color: #588bcc; }
</style>
<link rel="stylesheet" id="pretty_photo-css" href="https://gencyberca
themes/salient/css/prettyPhoto.css?ver=7.0.1" type="text/css" media="all">
```

✓ Success

k-77j0y.com uses  
WordPress

Help Us Improve These Results

```
<link rel="alternate" type="application/rss+xml" title="Cyber Realm raquo; Comments feed" href="https://gencybercards.com/comments/feed/" />
<link rel="alternate" type="application/rss+xml" title="Cyber Realm raquo; Home Comments Feed" href="https://gencybercards.com/main/feed/" />
<meta property="og:site_name" content="Cyber Realm"/><meta property="og:url" content="https://gencybercards.com/" /><meta
property="og:title" content="Home"/><meta property="og:type" content="article"/>
<script type="text/javascript">
window._wpemojiSettings =
{"baseUrl": "https://s.w.org/images/core/emoji/2.4.7/72x72/", "ext": ".png", "svgUrl": "https://s.w.org/images/core/emoji/2.4.7/72x72/2.4.7-emoji.png", "source": {"concatemoji": "https://gencybercards.com/wp-includes/js/wp-emoji-release.min.js?ver=4.9.6"}};
function(a,b,c){function d(a,b){var
c=String.fromCharCode;l.clearRect(0,0,k.width,k.height),l.fillText(c.apply(this,a),0,0);var
d=k.toDataURL();l.clearRect(0,0,k.width,k.height),l.fillText(c.apply(this,b),0,0);var e=k.toDataURL();return d===e}function e(a){var
b;if(!l||!l.fillText)return!1;switch(l.textBaseline="top",l.font="600 32px Arial",a){case"flag":return!(b=d("55356,56826,55356,56819"),
[55356,56826,8203,55356,56819])&&(b=d("55356,57332,56128,56423,56128,56418,56128,56421,56128,56430,56128,56423,56128,56447),
[55356,57332,8203,56128,56423,8203,56128,56418,8203,56128,56421,8203,56128,56430,8203,56128,56423,8203,56128,56447]),!b);case"emoji":
b=d("55357,56692,8205,9792,65039"),[55357,56692,8203,9792,65039]),!b)return!1}function f(a){var
c=b.createElement("script");c.src=a,c.defer=c.type="text/javascript",b.getElementsByTagName("head")[0].appendChild(c);var
g,h,i,j,k=b.createElement("canvas"),l=k.getContext("2d");for(j=Array("flag","emoji"),c.supports=
{everything:!0,everythingExceptFlag:!0},i=0;i<j.length;i++){c.supports[j[i]]=e(j[i]),c.supports.everything&c.supports[j[i]],"flag"===j[i]&&
(c.supports.everythingExceptFlag&c.supports.everythingExceptFlag&c.supports[j[i]])};c.supports.everythingExceptFlag=c.supports.everyth
ceptFlag&c.supports.flag,c.DOMReady=!1,c.readyCallback=function(){c.DOMReady=!0},c.supports.everything||(function(){
[c.readyCallback()],b.addEventListener(b.addEventListener("DOMContentLoaded",h,!1),a.addEventListener("load",h,!1));
(a.attachEvent("onload",h),b.attachEvent("onreadystatechange",function(){"complete"===b.readyState&c.readyCallback()})),g=c.source||
{}),g.concatemoji?f(g.concatemoji):g.wpemoji&&g.tweetemoji&&(f(g.tweetemoji),f(g.wpemoji))})(window,document,window._wpemojiSettings);
</script>
<style type="text/css">
img.wp-smiley,
img.emoji {
display: inline !important;
border: none !important;
}
```

Non Technical:  
CMS/View  
Source/Inspect

# Questions/Comments?

Email me at [anastacia.webster@csusb.edu](mailto:anastacia.webster@csusb.edu).