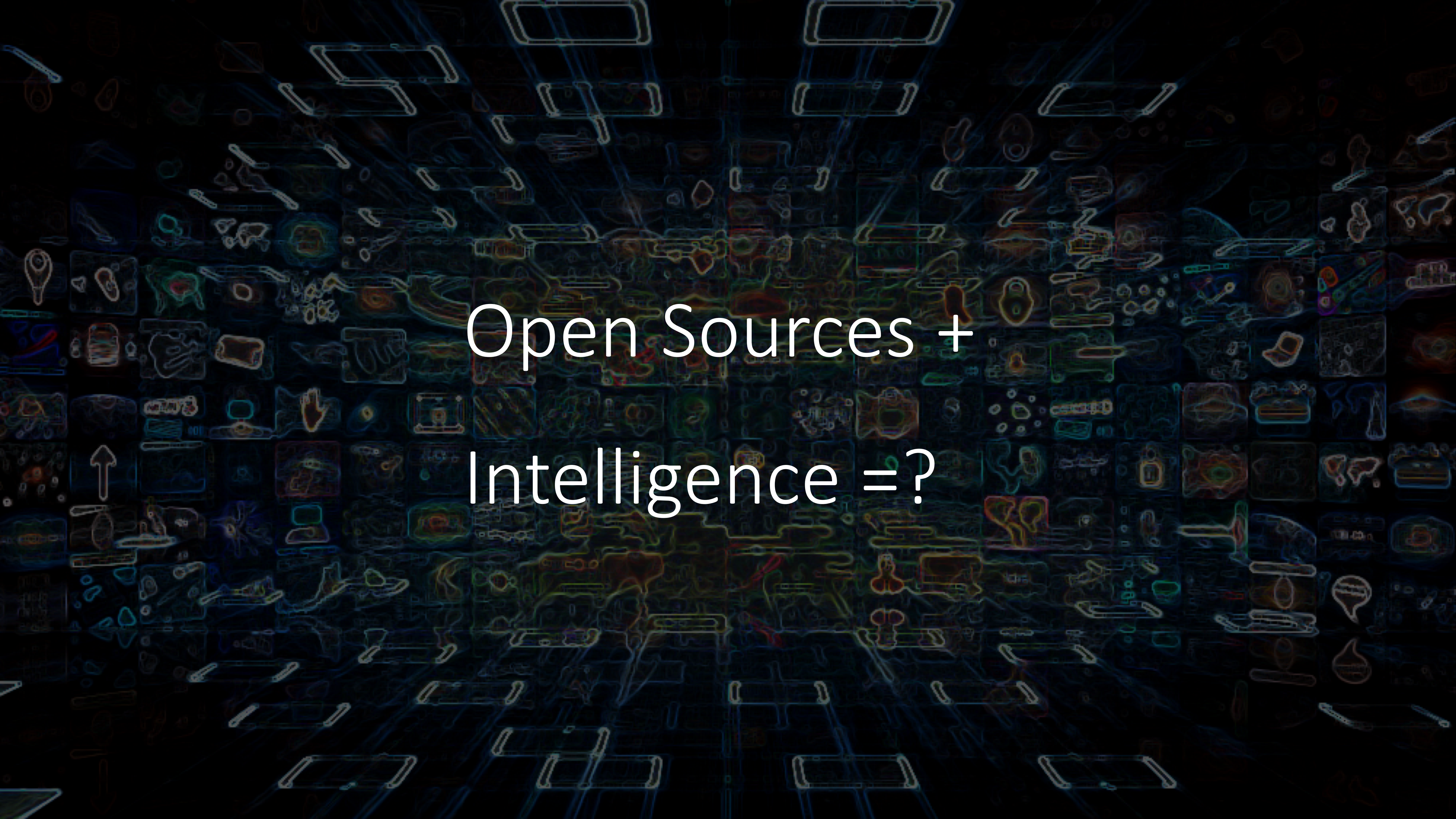
Open Source Intelligence in Cybersecurity

Anastacia Webster

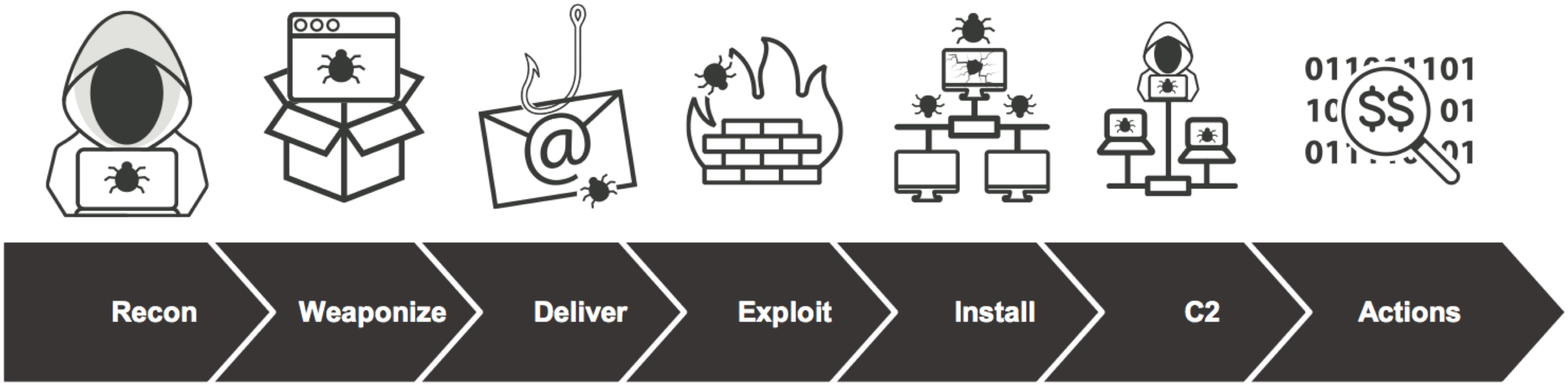
Overview

- 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

Gather data and intelligence on target organization

Weaponize

Craft malicious payload, use exploits for vulnerabilities

Deliver

Payload sent to target (phishing)

Exploit

Compromise system

Install

Install malware, obtain credentials and establish backdoors.

C2

Navigate internal network and setup command and control

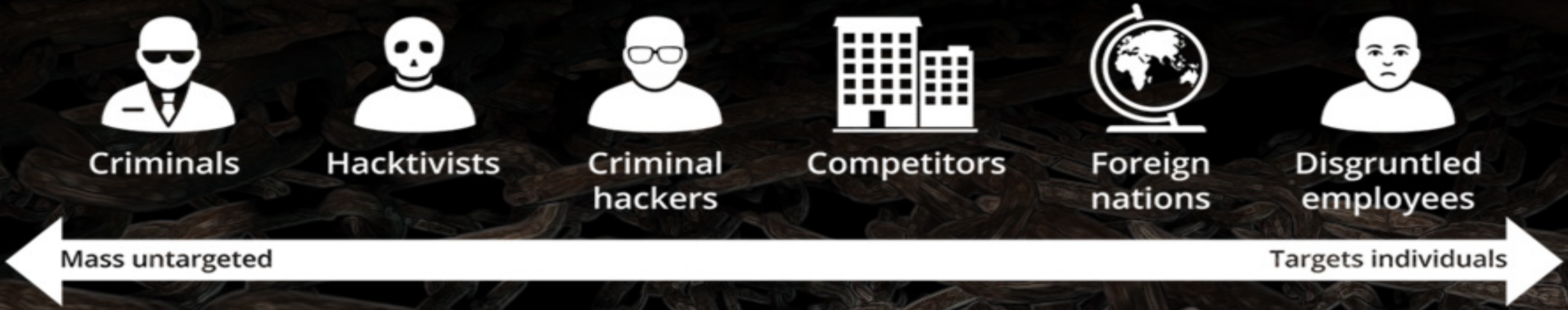
Actions

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

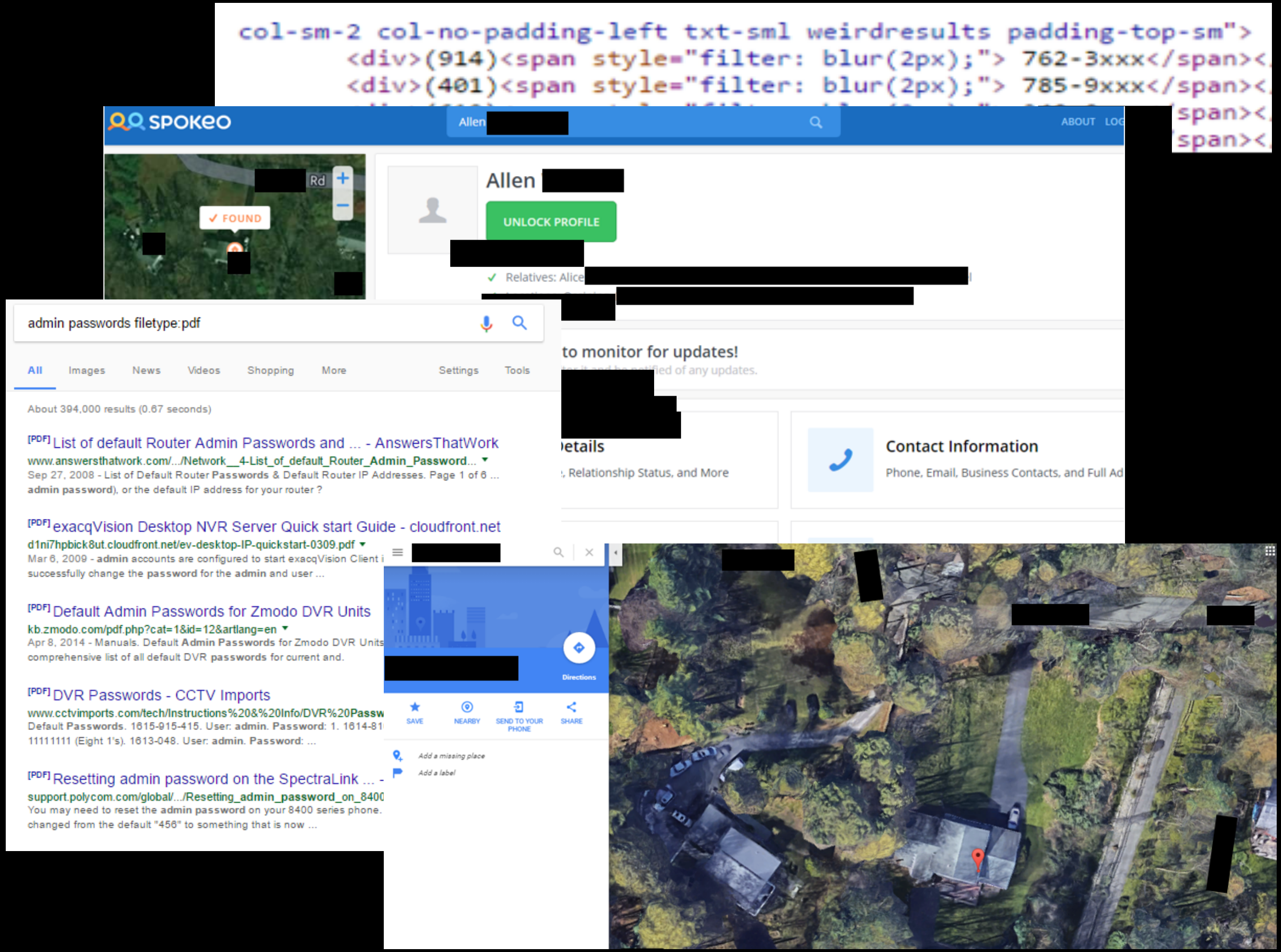


Finding Tools to Use

- 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…

Non Technical Tools/ Skills

- Google Booleans
- View Source/ Inspect
- People Search Engines
- Social Media
- Browser Extensions
- Mapping/ Surveillance TV
- Reverse Phone Look Ups
- CMS Look Ups



```
col-sm-2 col-no-padding-left txt-sml weirdresults padding-top-sm">
     <div>(914)<span style="filter: blur(2px);"> 762-3xxx</span><
     <div>(401)<span style="filter: blur(2px);"> 785-9xxx</span><
                                                              span><
                                                              span><
```

Allen [redacted]

[redacted]

✓ Relatives: Alice [redacted]

[redacted]

to monitor for updates!

[redacted]

etails

, Relationship Status, and More

Contact Information

Phone, Email, Business Contacts, and Full Ad

admin passwords filetype:pdf

About 394,000 results (0.67 seconds)

[PDF] List of default Router Admin Passwords and ... - AnswersThatWork
www.answersthatwork.com/.../Network__4-List_of_default_Router_Admin_Password... ▾
Sep 27, 2008 - List of Default Router Passwords & Default Router IP Addresses. Page 1 of 6 ... admin password), or the default IP address for your router ?

[PDF] exacqVision Desktop NVR Server Quick start Guide - cloudfront.net
d1ni7hpbick8ut.cloudfront.net/ev-desktop-IP-quickstart-0309.pdf ▾
Mar 6, 2009 - admin accounts are configured to start exacqVision Client i
successfully change the password for the admin and user ...

[PDF] Default Admin Passwords for Zmodo DVR Units
kb.zmodo.com/pdf.php?cat=1&id=12&artlang=en ▾
Apr 8, 2014 - Manuals. Default Admin Passwords for Zmodo DVR Units
comprehensive list of all default DVR passwords for current and.

[PDF] DVR Passwords - CCTV Imports
www.cctvimports.com/tech/Instructions%20&%20Info/DVR%20Passw
Default Passwords. 1615-915-415. User: admin. Password: 1. 1614-81
11111111 (Eight 1's). 1613-048. User: admin. Password: ...

[PDF] Resetting admin password on the SpectraLink ... -
support.polycom.com/global/.../Resetting_admin_password_on_8400
You may need to reset the admin password on your 8400 series phone.
changed from the default "456" to something that is now ...

[redacted]

[redacted]

[redacted]

[redacted]

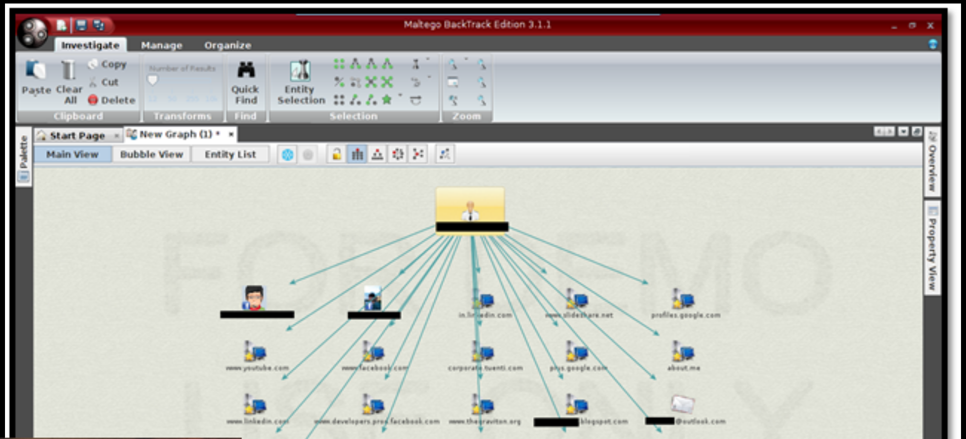
[redacted]

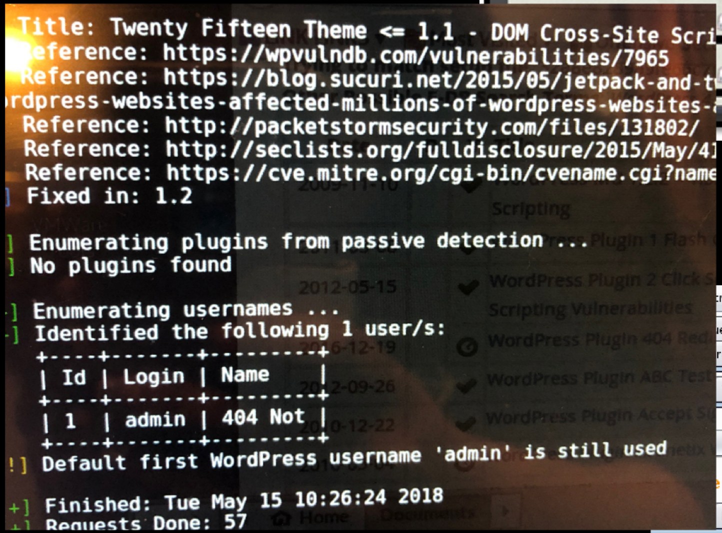
[redacted]

[redacted]

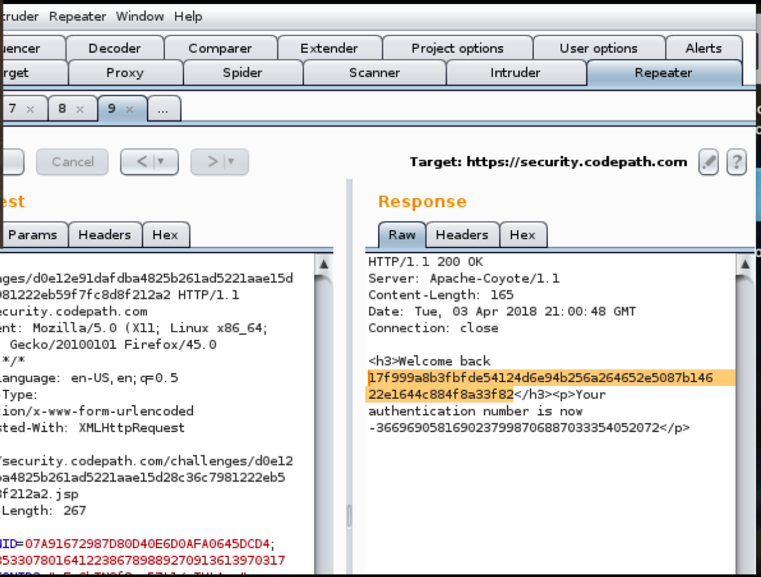
Technical Tools/ Skills

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





```
Title: Twenty Fifteen Theme <= 1.1 - DOM Cross-Site Scri
eference: https://wpvulndb.com/vulnerabilities/7965
Reference: https://blog.sucuri.net/2015/05/jetpack-and-t
rdpress-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 ...
] 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
```

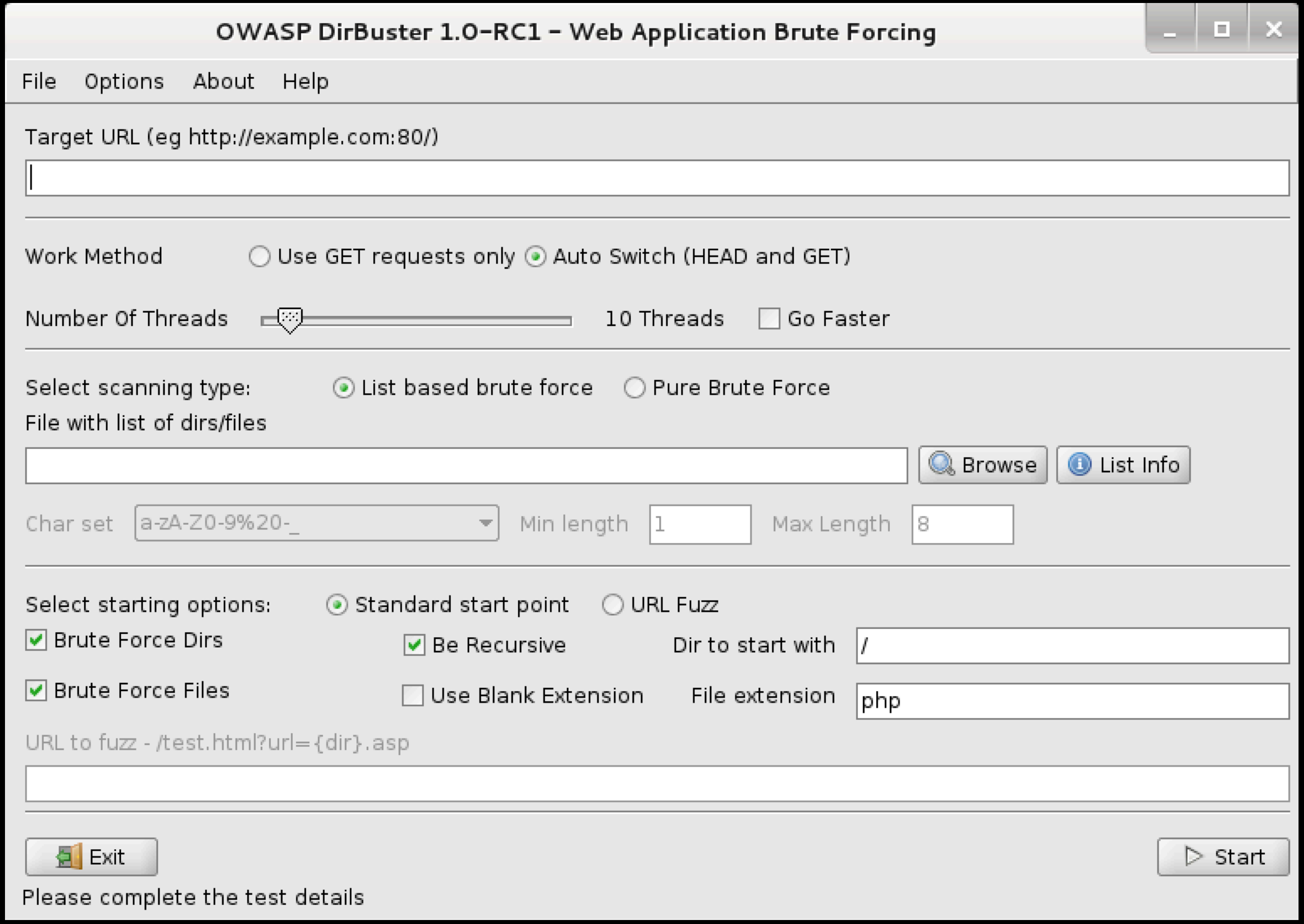


```
POST
/challenges/d0e12e91dafdba4825b261ad5221aae15d
28c36c7981222eb59f7fc8d8f212a2 HTTP/1.1
Host: security.codepath.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64;
rv:45.0) Gecko/20100101 Firefox/45.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Content-Type:
application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer:
https://security.codepath.com/challenges/d0e12
e91dafdba4825b261ad5221aae15d28c36c7981222eb5
9f7fc8d8f212a2.jsp
Content-Length: 267
Cookie:
JSESSIONID=07A91672987D80D40E6D0AFA0645DCD4;
token=-35330780164122386789889270913613970317
```

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Length: 165
Date: Tue, 03 Apr 2018 21:00:48 GMT
Connection: close

<h3>Welcome back
17f999a8b3fbfde54124d6e94b256a264652e5087b146
22e1644c884f8a33f82</h3><p>Your
authentication number is now
-3669690581690237998706887033354052072</p>
```

Demonstration Tools

More Technical: DirBuster



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 a-zA-Z0-9%20-_ Min length 1 Max Length 8

Select starting options: ● Standard start point ○ URL Fuzz

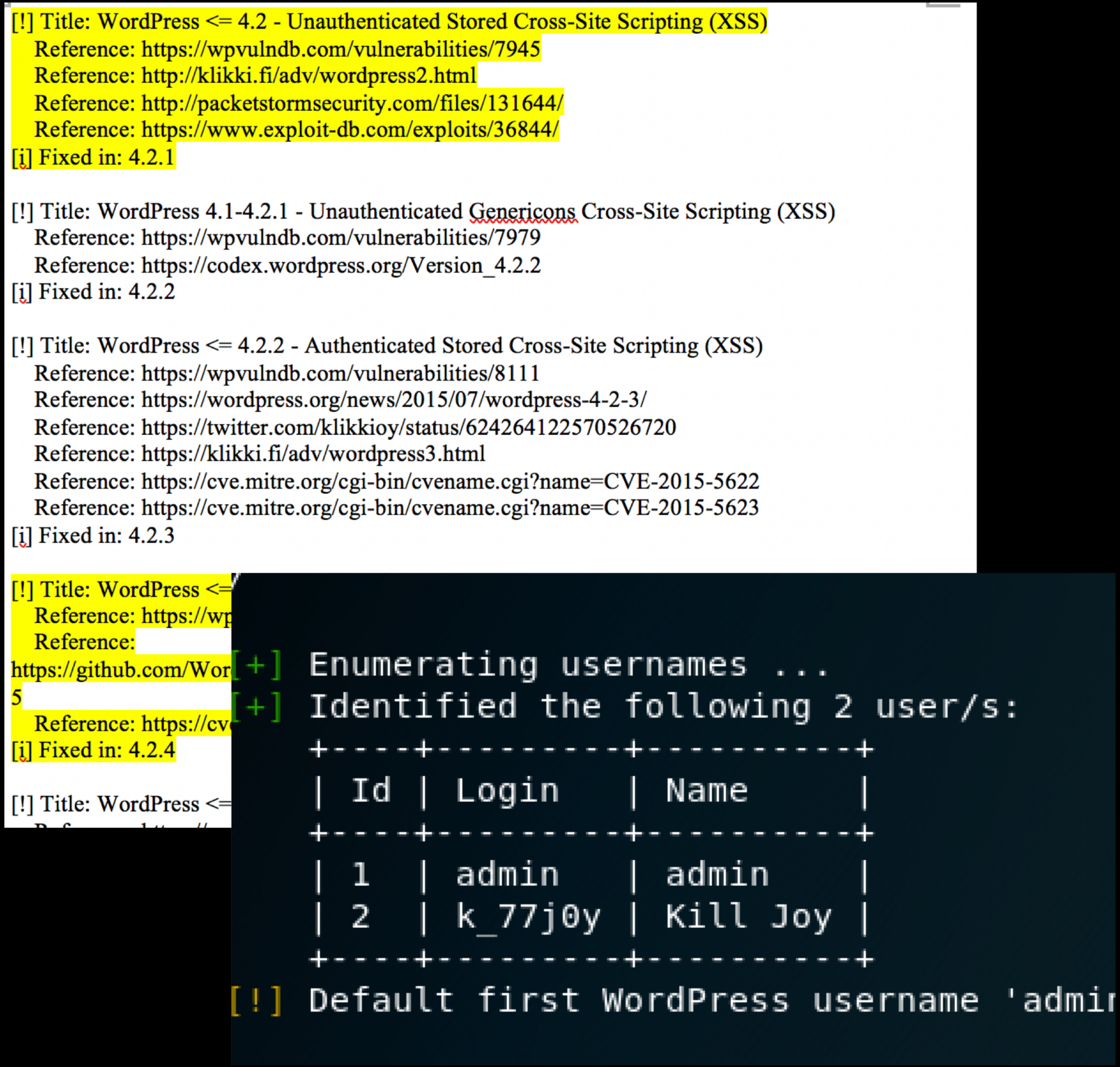
☑ Brute Force Dirs ☑ Be Recursive Dir to start with /

☑ Brute Force Files □ Use Blank Extension File extension php

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

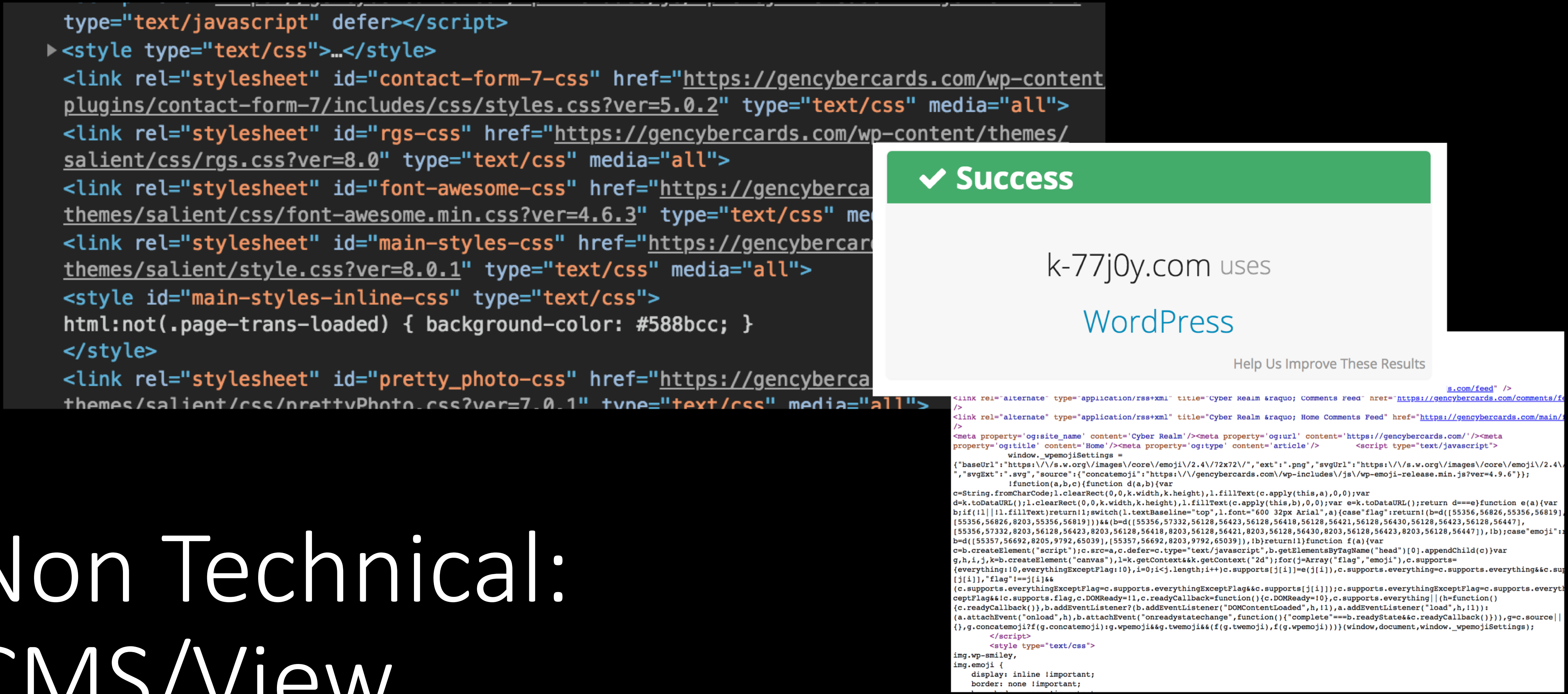
Please complete the test details

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 Genericons Cross-Site Scripting (XSS)
    Reference: https://wpvulndb.com/vulnerabilities/7979
    Reference: 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/klikkioy/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

```
s.com/feed" />
<link rel="alternate" type="application/rss+xml" title="Cyber Realm &raquo; Comments Feed" href="https://gencybercards.com/comments/fe
/>
<link rel="alternate" type="application/rss+xml" title="Cyber Realm &raquo; Home Comments Feed" href="https://gencybercards.com/main/f
/>
<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\/72x72\/","ext":".png","svgUrl":"https:\/\/s.w.org\/images\/core\/emoji\/2.4\/
","svgExt":".svg","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":r
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&&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.everything&&c.sup
[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||(h=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.twemoji&&(f(g.twemoji),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.