THINGS NOT TO DO IN A PENTEST REPORT

Tips, Tricks, And Traps In Report Writing

BRONWEN AKER | CORVUS

BR0NW3N.COM

WHAT THIS TALK IS ABOUT...

- Hacking is fun, but the report is the product!
- A good report tells a story
  - What was found
  - How was it found
  - How what was found can be fixed!

Bad Reports Do Harm

At Best

- They are Ignored
- Your customer will make no changes
- Business as usual…
  - Until they get hacked.

At Worst

- They tarnish your cred as a tester
- They tarnish your company's reputation
- They sour the customer on the value of security in general

Communication Is CRITICAL

An adequate hacker who writes well is more useful to a customer than a l33t hacker who writes poorly.

HOW CAN I SAY ALL THIS?!?!?

- Decades of Experience in Communications
  - Public Speaking, Writing, Teaching, Web Development, UI/UX Design
- BHIS Technical Editor since 2018
  - Read/edit 200+ pentest reports PER YEAR

There is Good News & Bad News

Bad News

- There are a lot of bad reports being written
- Vulnerability scans sold as pentest reports have soured business to infosec
- Small boutique shops are closing

Good News

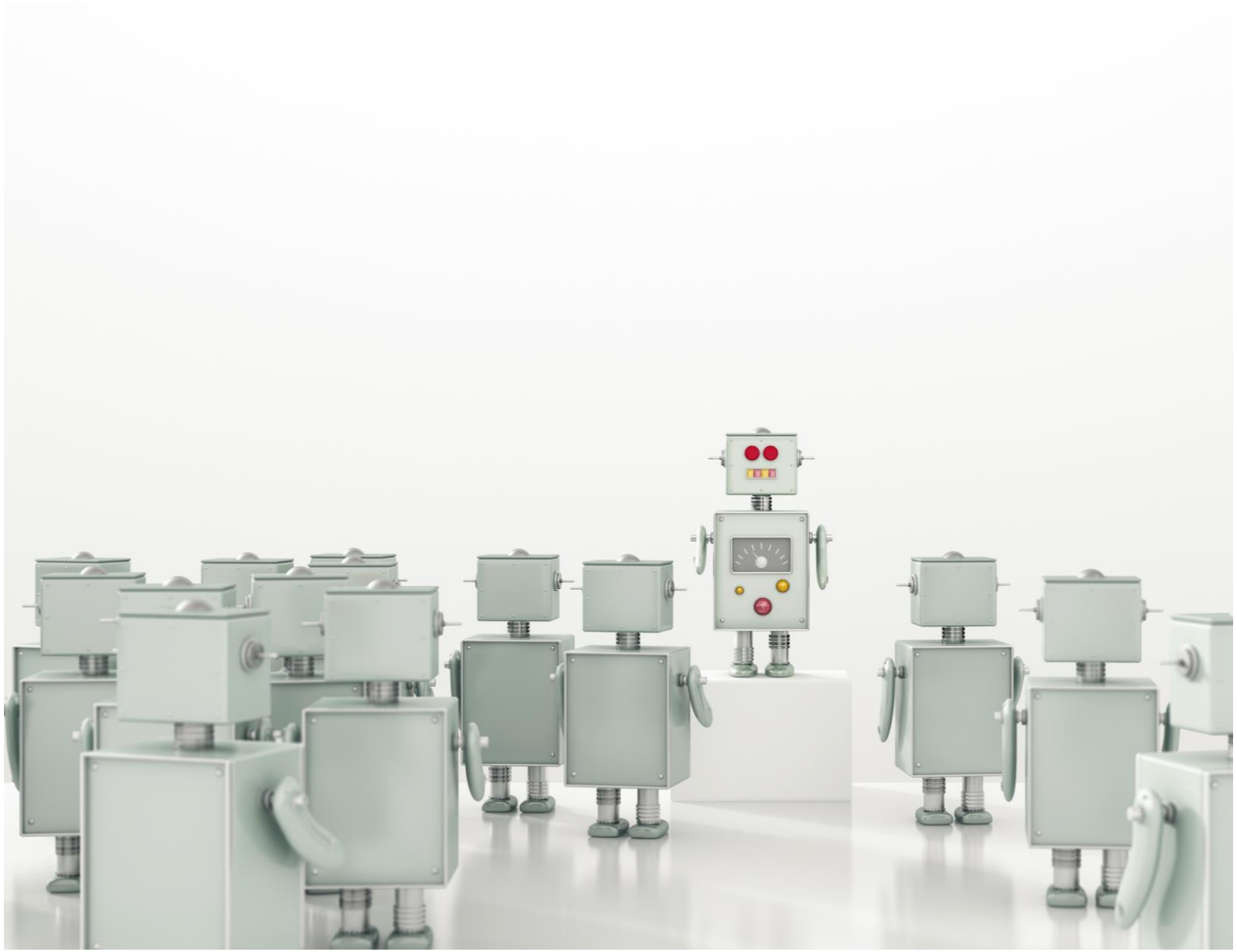
- Writing good reports is a skill that can be learned
- Good writing/communication is a valuable and transferrable skill
- Good reports provide value to your customers

7 DEADLY SINS OF REPORT WRITING

- Bad Writing
- Condescending Tone
- Bad Screenshots
- Inconsistent Formatting
- Randomized Lists
- Irrelevant Guidance
- Info from Another Customer

1. BAD WRITING

- Typos/Mispelllings
- Poor grammar
- Too much jargon
- Convoluted sentences
- No clear narrative



GOOD REPORT WRITING…

- Tells a story
- Is easy to follow
- Explains why things matter
- Is accessible to the reader

Ways to Improve Your Writing Skillz

- Take writing classes
  - Basic, Technical, or News writing
- Join Toastmasters
  - Improved public speaking helps with writing skills
  - Immediate feedback
- Use a writing aid
  - ⚠ Some have security issues
  - No Red Ink, ~~Grammarly~~
- Writing in a non-native language?
  - Use Duolingo, Babbel, etc., to improve your language skills

2. CONDESCENDING TONE

- Don’t brag in your report
  - Bragging about pwnage is petty
  - No one cares how l33t you are
  - The more brazenly you shame the customer, the less likely that they will become a client

Keep It Professional & Objective

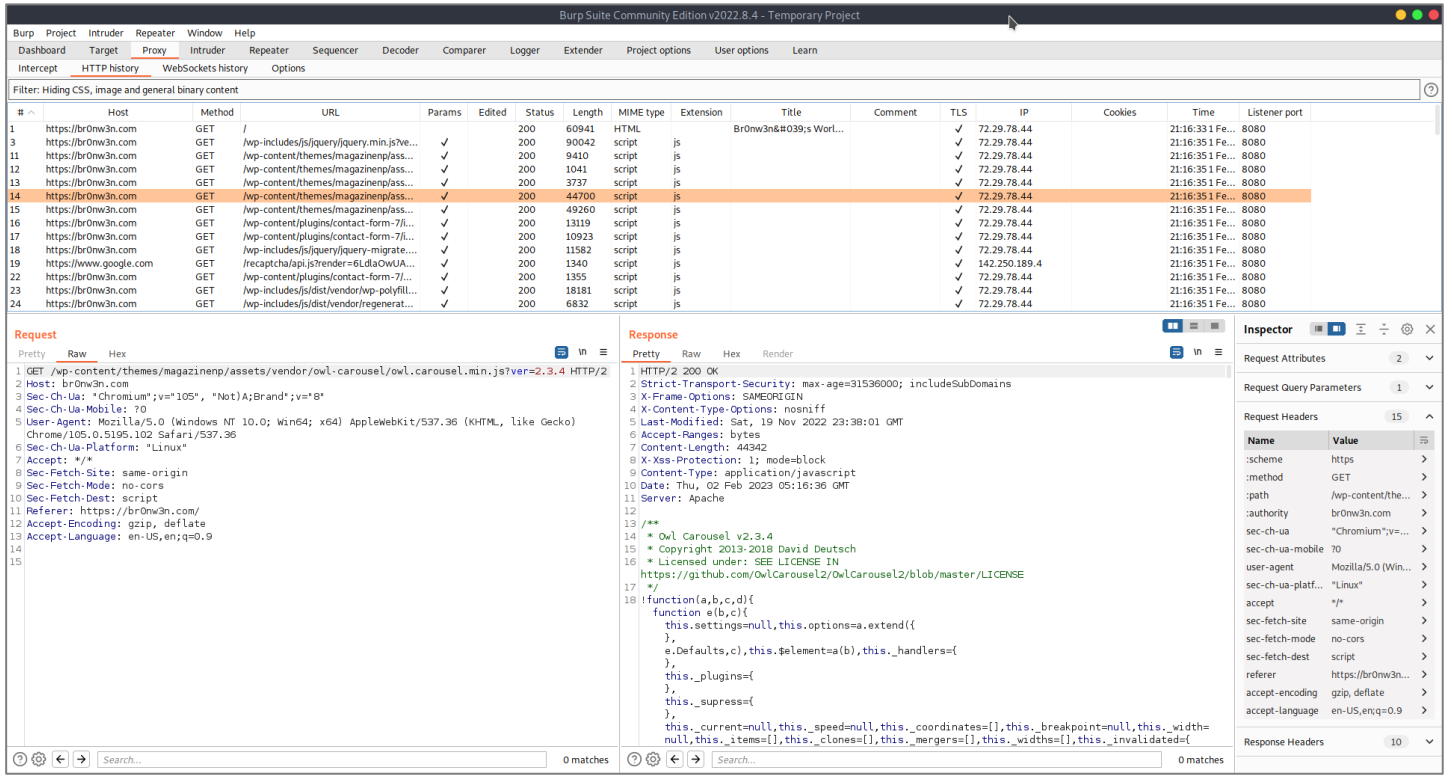
- Report may be read by executives, managers, consultants
- Avoid emotionally loaded terms
  - Drastic, awful, bad, good, etc.
- Use academic writing styles as examples to follow
- Use formal tone (not stilted)
- Specify and quantify whenever possible
  - Objectivity is your friend
  - Enhances cred
- Focus on what was found
  - Not on who found it

Ways to Improve Your Writing Skillz

- Read your report out loud
  - Activates different part of your brain
  - Helps you find rough spots
- Imagine how different people would react
- Try to match the “language” used by the target audience

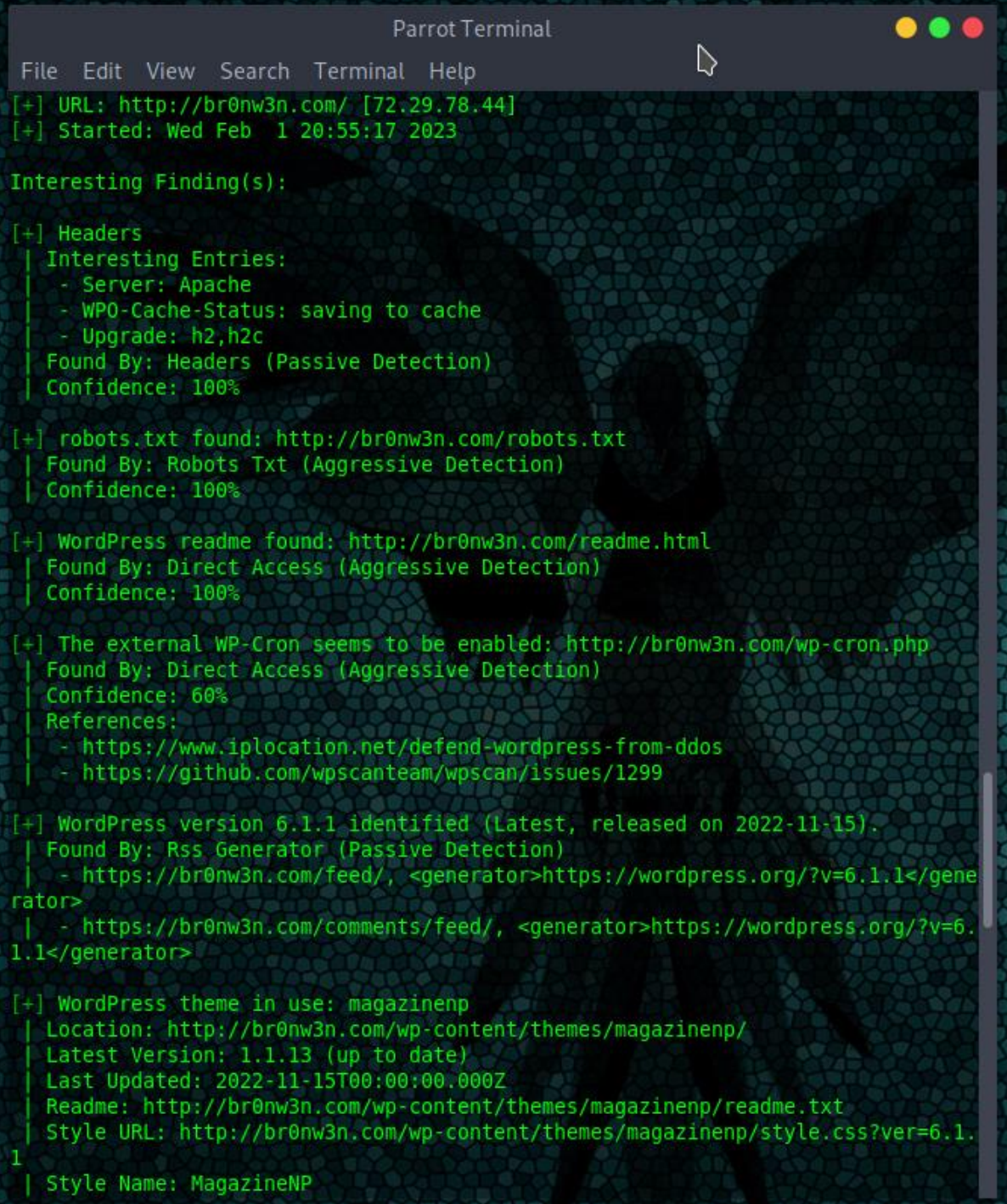
3. UNREADABLE SCREENSHOTS

- Tend to be too much or too little
- Unreadable text is useless text
  - Reduces or eliminates value as evidence of findings



Common Screenshot Problems

- Dark mode
  - Easy on eyes while working
  - Not so easy to read in reports
- Shell or browser window too wide/maxed
  - Makes text too small to be readable when placed in a report
- Transparency
  - Just don't
- No callouts or Highlighting
  - "Wall of Code" effect



Parrot Terminal

File Edit View Search Terminal Help

```
[+] URL: http://br0nw3n.com/ [72.29.78.44]
[+] Started: Wed Feb  1 20:55:17 2023

Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 |  - Server: Apache
 |  - WPO-Cache-Status: saving to cache
 |  - Upgrade: h2,h2c
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] robots.txt found: http://br0nw3n.com/robots.txt
 | Found By: Robots Txt (Aggressive Detection)
 | Confidence: 100%

[+] WordPress readme found: http://br0nw3n.com/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://br0nw3n.com/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 6.1.1 identified (Latest, released on 2022-11-15).
 | Found By: Rss Generator (Passive Detection)
 |  - https://br0nw3n.com/feed/, <generator>https://wordpress.org/?v=6.1.1</gene
rator>
 |  - https://br0nw3n.com/comments/feed/, <generator>https://wordpress.org/?v=6.
1.1</generator>

[+] WordPress theme in use: magazinenp
 | Location: http://br0nw3n.com/wp-content/themes/magazinenp/
 | Latest Version: 1.1.13 (up to date)
 | Last Updated: 2022-11-15T00:00:00.000Z
 | Readme: http://br0nw3n.com/wp-content/themes/magazinenp/readme.txt
 | Style URL: http://br0nw3n.com/wp-content/themes/magazinenp/style.css?ver=6.1.
1
 | Style Name: MagazineNP
```

Parrot Terminal

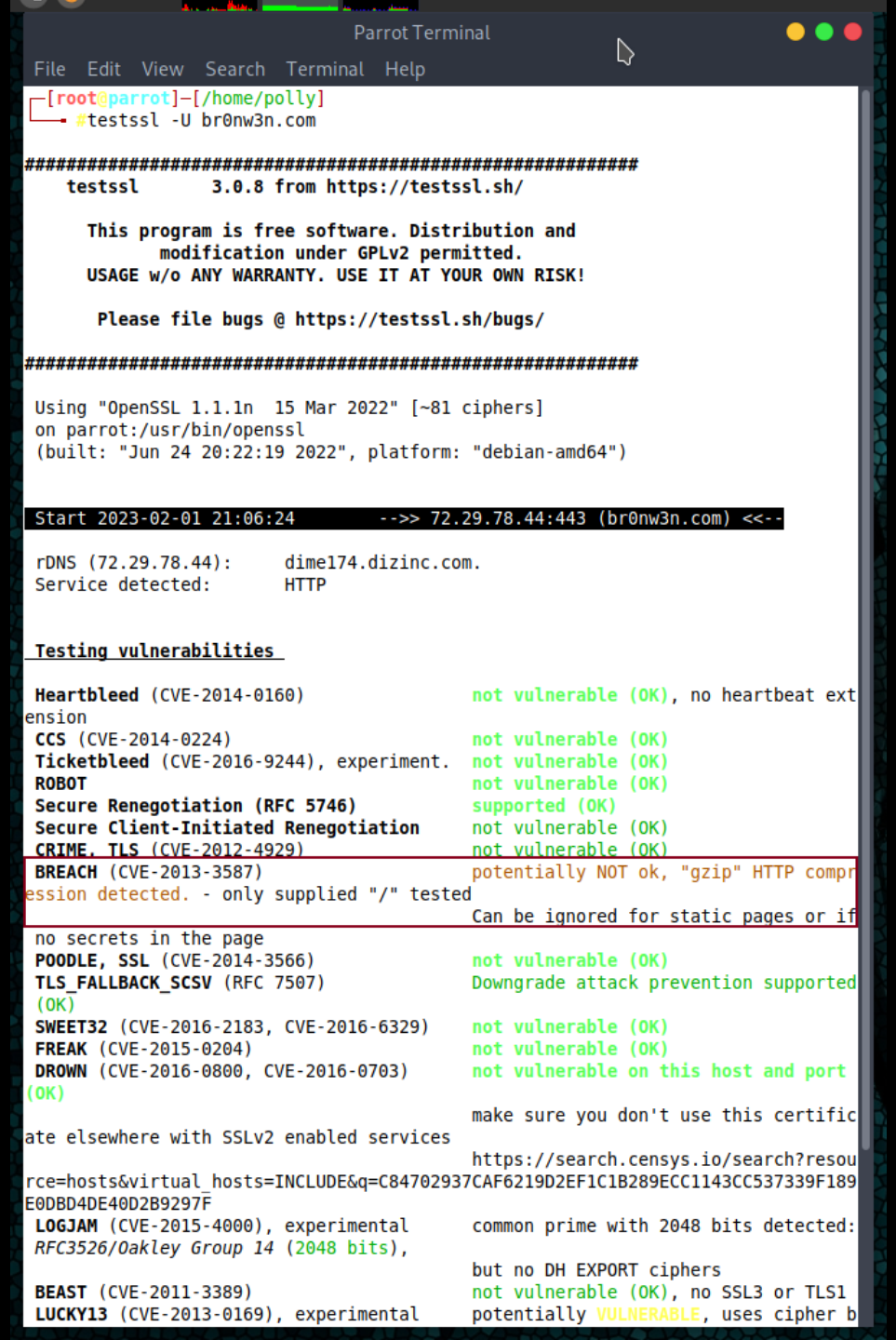
File Edit View Search Terminal Help

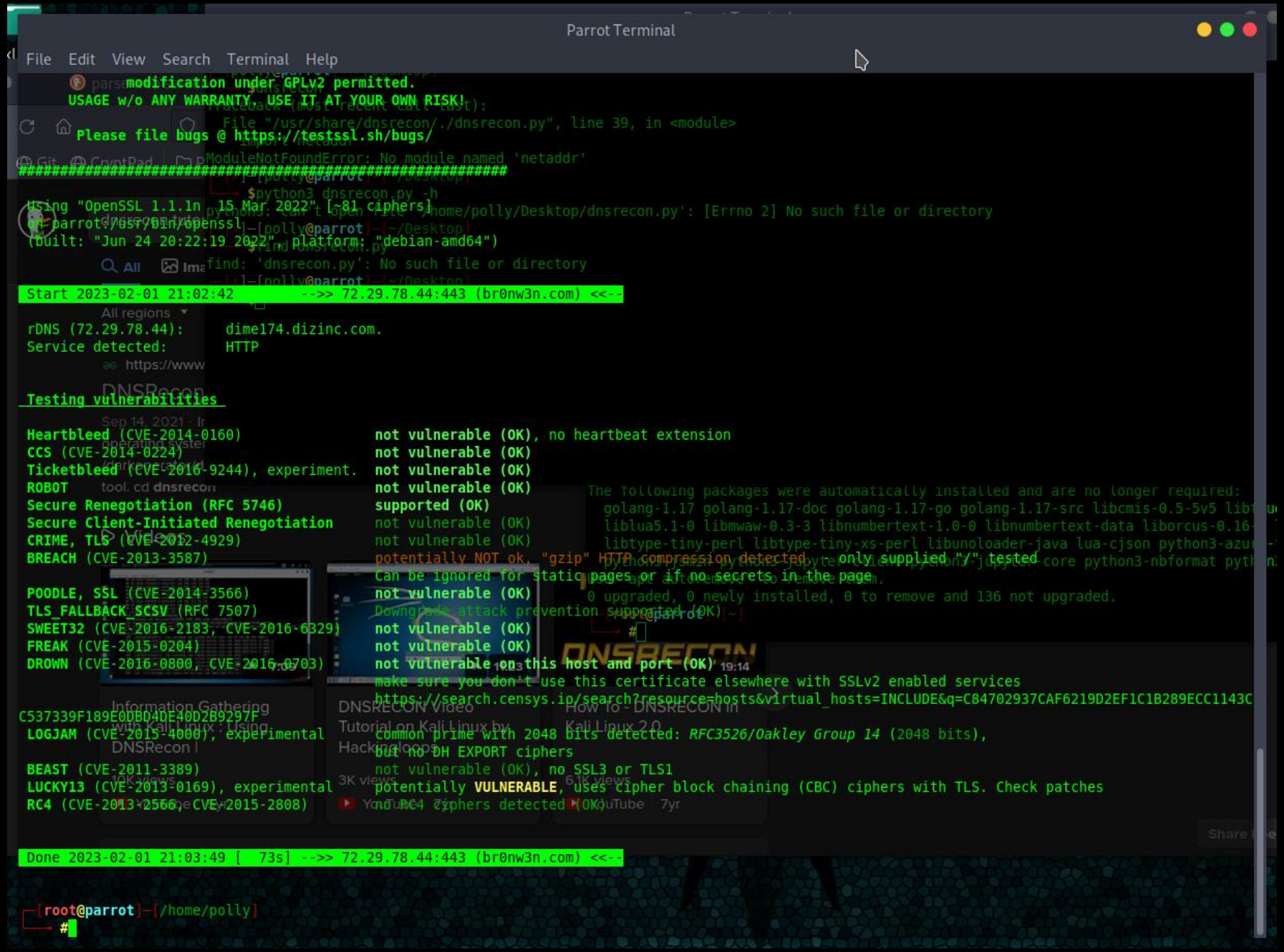
```
[+] URL: http://br0nw3n.com/ [72.29.78.44]
[+] Started: Wed Feb  1 20:55:17 2023

Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 |  - Server: Apache
 |  - WPO-Cache-Status: saving to cache
 |  - Upgrade: h2,h2c
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] robots.txt found: http://br0nw3n.com/robots.txt
 | Found By: Robots Txt (Aggressive Detection)
 | Confidence: 100%

[+] WordPress readme found: http://br0nw3n.com/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://br0nw3n.com/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 6.1.1 identified (Latest, released on 2022-11-15).
 | Found By: Rss Generator (Passive Detection)
 |  - https://br0nw3n.com/feed/, <generator>https://wordpress.org/?v=6.1.1</gene
rator>
 |  - https://br0nw3n.com/comments/feed/, <generator>https://wordpress.org/?v=6.
1.1</generator>

[+] WordPress theme in use: magazinenp
 | Location: http://br0nw3n.com/wp-content/themes/magazinenp/
 | Latest Version: 1.1.13 (up to date)
 | Last Updated: 2022-11-15T00:00:00.000Z
 | Readme: http://br0nw3n.com/wp-content/themes/magazinenp/readme.txt
 | Style URL: http://br0nw3n.com/wp-content/themes/magazinenp/style.css?ver=6.1.
1
 | Style Name: MagazineNP
```

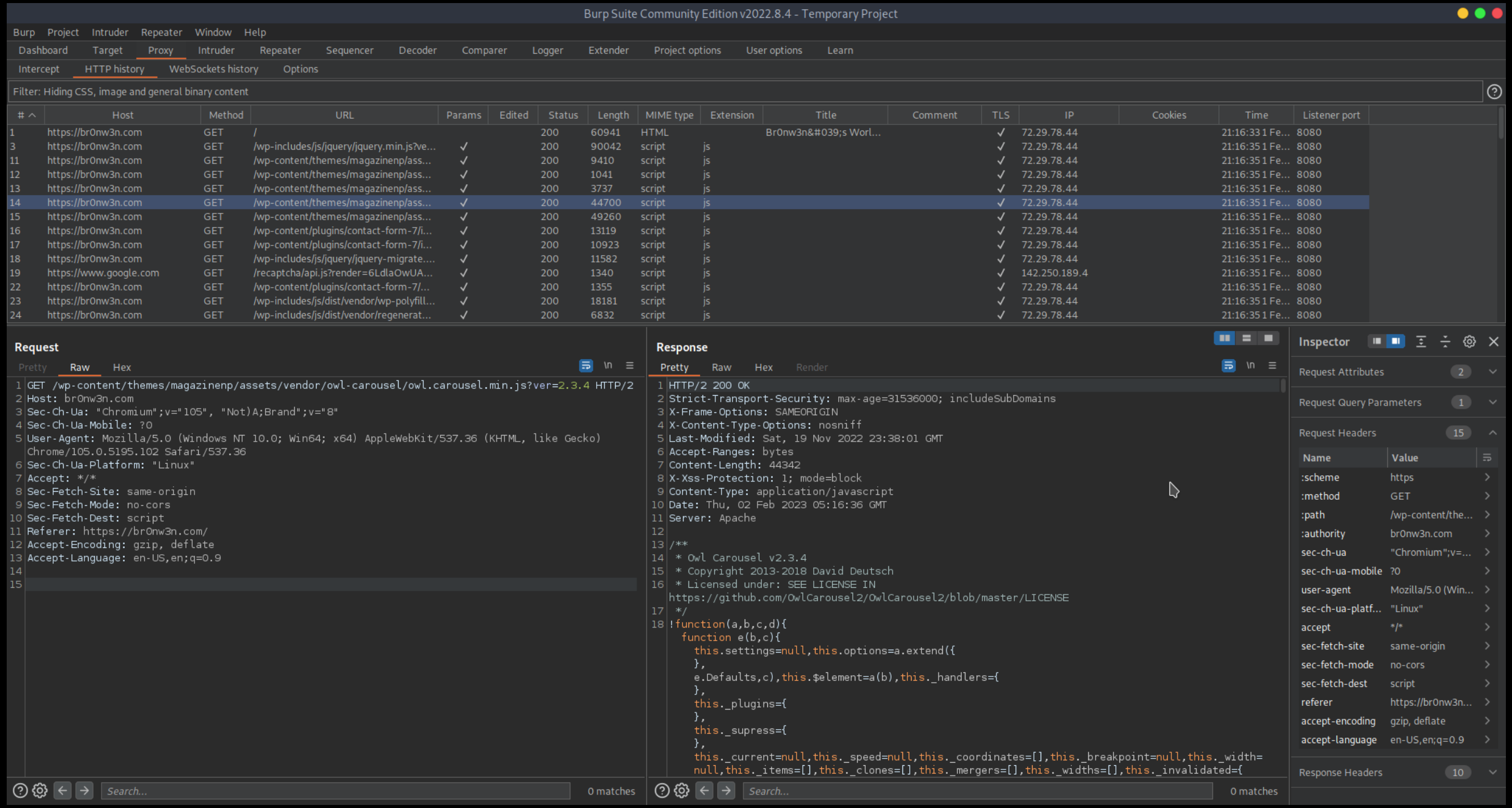
Parrot Terminal

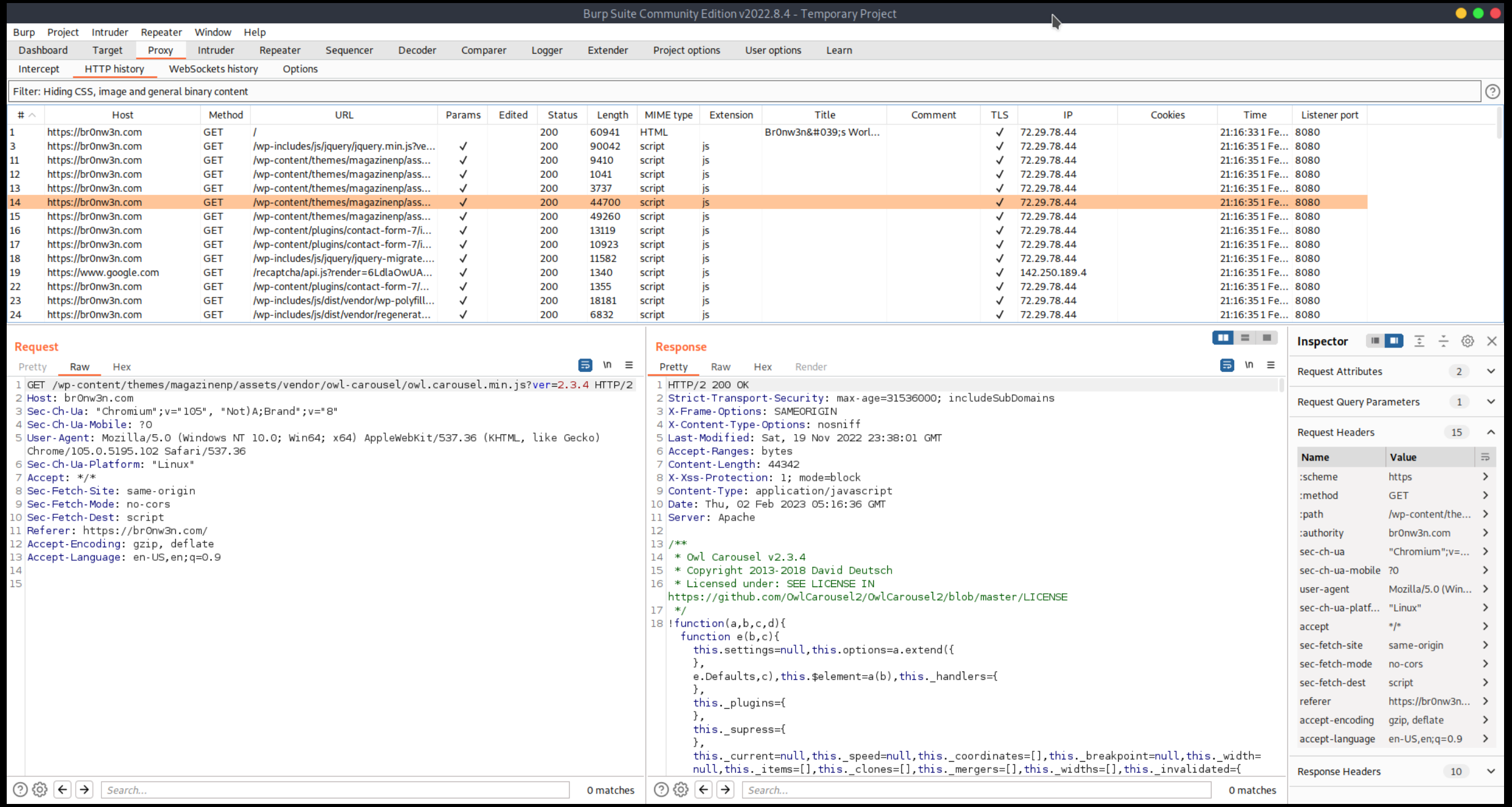
File Edit View Search Terminal Help

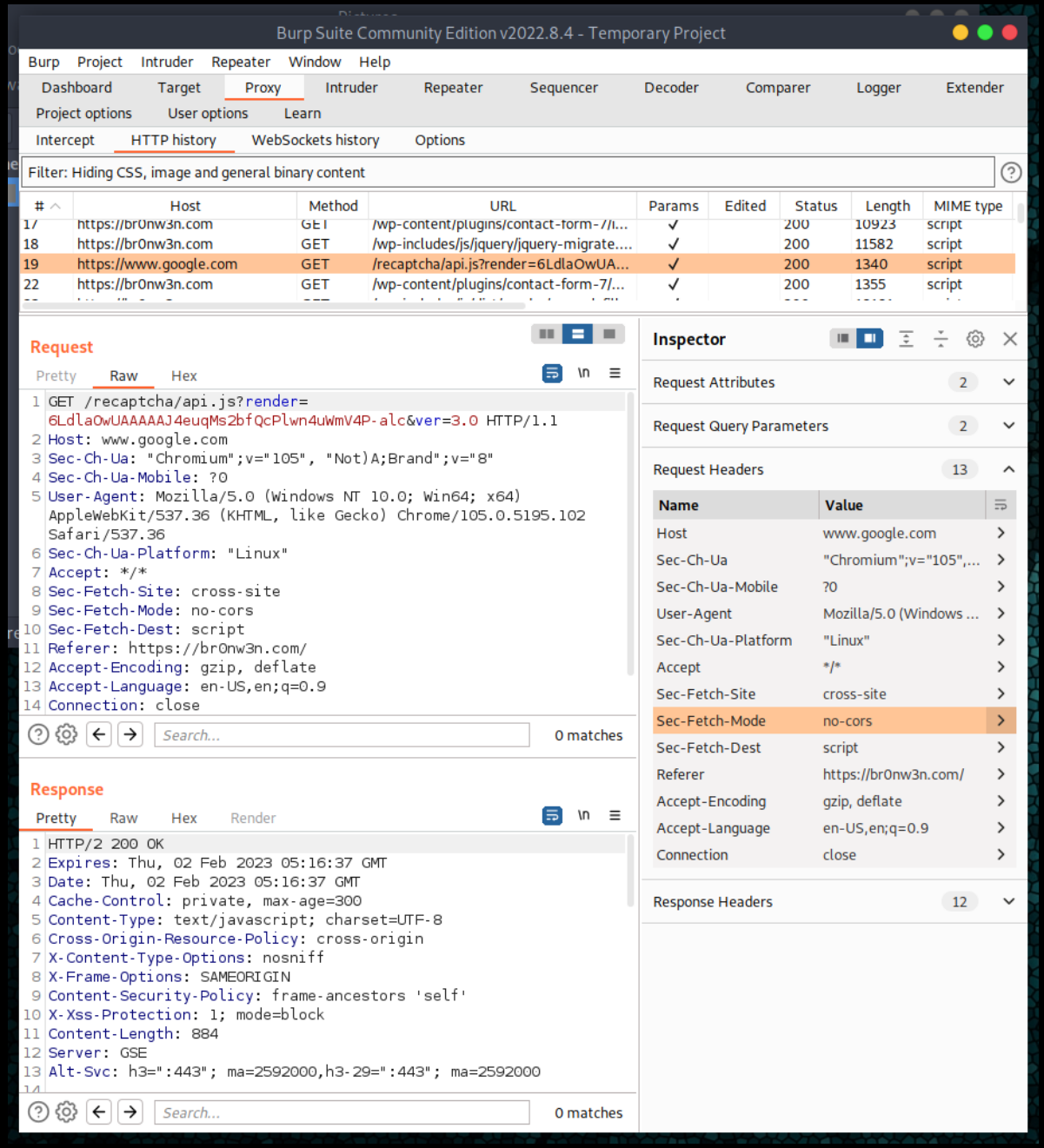
```
[+] URL: http://br0nw3n.com/ [72.29.78.44]
[+] Started: Wed Feb  1 20:55:17 2023

Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 |  - Server: Apache
 |  - WPO-Cache-Status: saving to cache
 |  - Upgrade: h2,h2c
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] robots.txt found: http://br0nw3n.com/robots.txt
 | Found By: Robots Txt (Aggressive Detection)
 | Confidence: 100%

[+] WordPress readme found: http://br0nw3n.com/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://br0nw3n.com/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 6.1.1 identified (Latest, released on 2022-11-15).
 | Found By: Rss Generator (Passive Detection)
 |  - https://br0nw3n.com/feed/, <generator>https://wordpress.org/?v=6.1.1</gene
rator>
 |  - https://br0nw3n.com/comments/feed/, <generator>https://wordpress.org/?v=6.
1.1</generator>

[+] WordPress theme in use: magazinenp
 | Location: http://br0nw3n.com/wp-content/themes/magazinenp/
 | Latest Version: 1.1.13 (up to date)
 | Last Updated: 2022-11-15T00:00:00.000Z
 | Readme: http://br0nw3n.com/wp-content/themes/magazinenp/readme.txt
 | Style URL: http://br0nw3n.com/wp-content/themes/magazinenp/style.css?ver=6.1.
1
 | Style Name: MagazineNP
```




Parrot Terminal
File Edit View Search Terminal Help
modification under GPLv2 permitted.
USAGE w/o ANY WARRANTY. USE IT AT YOUR OWN RISK!
Please file bugs @ https://testssl.sh/bugs/
Using "OpenSSL 1.1.1n 15 Mar 2022" [~81 ciphers]
on parrot:/usr/bin/openssl
(built: "Jun 24 20:22:19 2022", platform: "debian-amd64")
Start 2023-02-01 21:02:42 -->> 72.29.78.44:443 (br0nw3n.com) <<--
rDNS (72.29.78.44): dime174.dizinc.com.
Service detected: HTTP
Testing vulnerabilities
Heartbleed (CVE-2014-0160) not vulnerable (OK), no heartbeat extension
CCS (CVE-2014-0224) not vulnerable (OK)
Ticketbleed (CVE-2016-9244), experiment. not vulnerable (OK)
ROBOT not vulnerable (OK)
Secure Renegotiation (RFC 5746) supported (OK)
Secure Client-Initiated Renegotiation not vulnerable (OK)
CRIME, TLS (CVE-2012-4929) not vulnerable (OK)
BREACH (CVE-2013-3587) potentially NOT ok, "gzip" HTTP compression detected - only supplied "/" tested
Can be ignored for static pages or if no secrets in the page
POODLE, SSL (CVE-2014-3566) not vulnerable (OK)
TLS_FALLBACK_SCSV (RFC 7507) not vulnerable (OK)
SWEET32 (CVE-2016-2183, CVE-2016-6329) not vulnerable (OK)
FREAK (CVE-2015-0204) not vulnerable (OK)
DROWN (CVE-2016-0800, CVE-2016-0703) not vulnerable on this host and port (OK)
make sure you don't use this certificate elsewhere with SSLv2 enabled services
https://search.censys.io/search?resource=hosts&virtual_hosts=INCLUDE&q=C84702937CAF6219D2EF1C1B289ECC1143C
C537339F189E0DBD4DE40D2B9297F
LOGJAM (CVE-2015-4000), experimental common prime with 2048 bits detected: RFC3526/Oakley Group 14 (2048 bits),
but no DH EXPORT ciphers
BEAST (CVE-2011-3389) not vulnerable (OK), no SSL3 or TLS1
LUCKY13 (CVE-2013-0169), experimental potentially VULNERABLE, uses cipher block chaining (CBC) ciphers with TLS. Check patches
RC4 (CVE-2013-2566, CVE-2015-2808) no RC4 ciphers detected (OK)
Done 2023-02-01 21:03:49 [73s] -->> 72.29.78.44:443 (br0nw3n.com) <<--
[root@parrot]-[/home/polly]
#

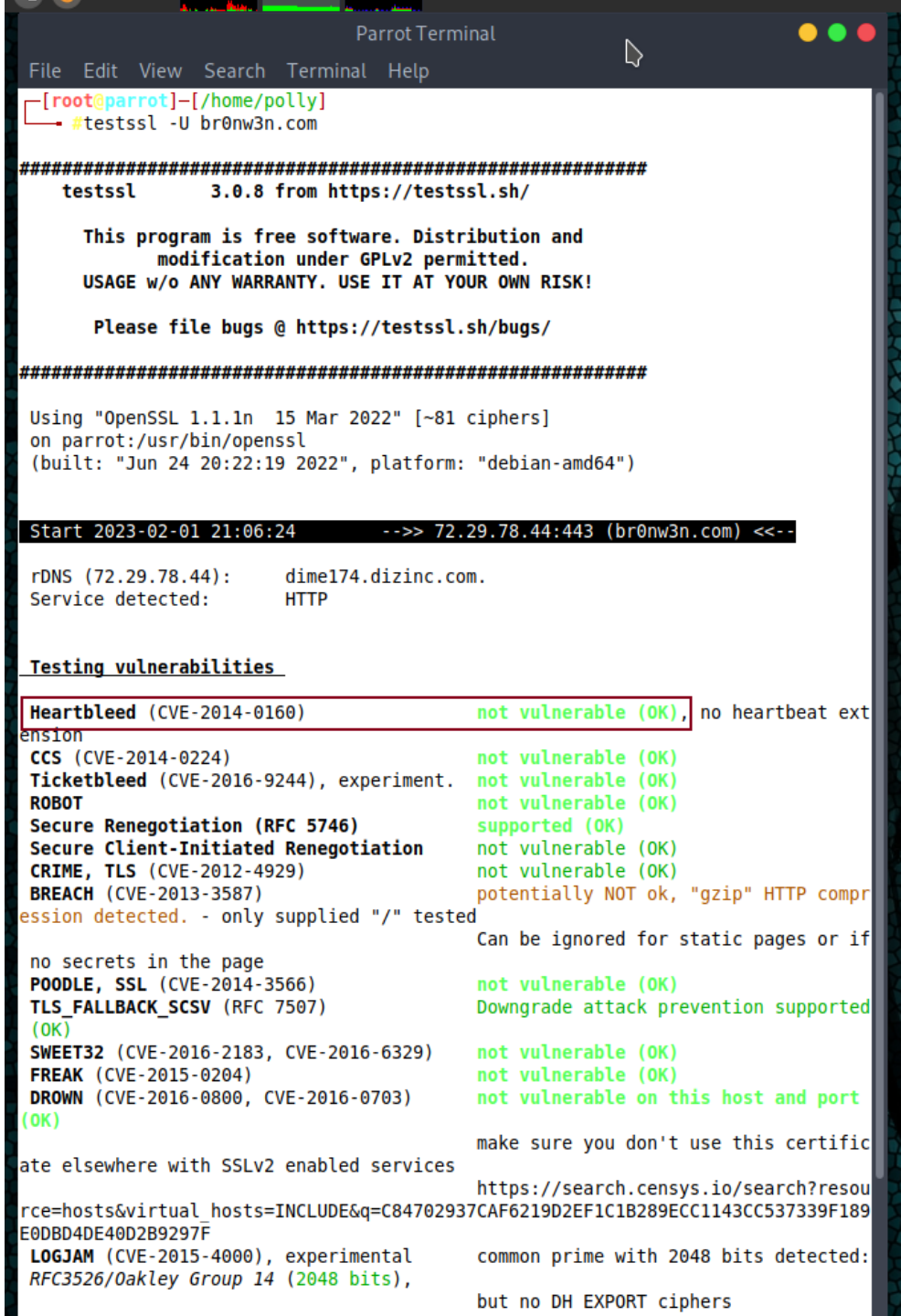

Burp Suite Community Edition v2022.8.4 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Intercept HTTP history WebSockets history Options
Filter: Hiding CSS, image and general binary content
Host Method URL Params Edited Status Length MIME type Extension Title Comment TLS IP Cookies Time Listener port
1 https://br0nw3n.com GET / 200 60941 HTML Br0nw3n's Worl... 72.29.78.44 21:16:33 1 Fe... 8080
3 https://br0nw3n.com GET /wp-includes/js/jquery/jquery.min.js?ve... 200 90042 script js 72.29.78.44 21:16:35 1 Fe... 8080
11 https://br0nw3n.com GET /wp-content/themes/magazinenp/ass... 200 9410 script js 72.29.78.44 21:16:35 1 Fe... 8080
12 https://br0nw3n.com GET /wp-content/themes/magazinenp/ass... 200 1041 script js 72.29.78.44 21:16:35 1 Fe... 8080
13 https://br0nw3n.com GET /wp-content/themes/magazinenp/ass... 200 3737 script js 72.29.78.44 21:16:35 1 Fe... 8080
14 https://br0nw3n.com GET /wp-content/themes/magazinenp/ass... 200 44700 script js 72.29.78.44 21:16:35 1 Fe... 8080
15 https://br0nw3n.com GET /wp-content/themes/magazinenp/ass... 200 49260 script js 72.29.78.44 21:16:35 1 Fe... 8080
16 https://br0nw3n.com GET /wp-content/plugins/contact-form-7/i... 200 13119 script js 72.29.78.44 21:16:35 1 Fe... 8080
17 https://br0nw3n.com GET /wp-content/plugins/contact-form-7/i... 200 10923 script js 72.29.78.44 21:16:35 1 Fe... 8080
18 https://br0nw3n.com GET /wp-includes/js/jquery/jquery-migrate.... 200 11582 script js 72.29.78.44 21:16:35 1 Fe... 8080
19 https://www.google.com GET /recaptcha/api.js?render=6LdlaOwUA... 200 1340 script js 142.250.189.4 21:16:35 1 Fe... 8080
22 https://br0nw3n.com GET /wp-content/plugins/contact-form-7/... 200 1355 script js 72.29.78.44 21:16:35 1 Fe... 8080
23 https://br0nw3n.com GET /wp-includes/js/dist/vendor/wp-polyfill... 200 18181 script js 72.29.78.44 21:16:35 1 Fe... 8080
24 https://br0nw3n.com GET /wp-includes/js/dist/vendor/regenerat... 200 6832 script js 72.29.78.44 21:16:35 1 Fe... 8080
Request
Pretty Raw Hex
GET /wp-content/themes/magazinenp/assets/vendor/owl-carousel/owl.carousel.min.js?ver=2.3.4 HTTP/2
Host: br0nw3n.com
Sec-Ch-Ua: "Chromium";v="105", "Not)A;Brand";v="8"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.5195.102 Safari/537.36
Sec-Ch-Ua-Platform: "Linux"
Accept: */*
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://br0nw3n.com/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Search... 0 matches
Response
Pretty Raw Hex Render
HTTP/2 200 OK
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Last-Modified: Sat, 19 Nov 2022 23:38:01 GMT
Accept-Ranges: bytes
Content-Length: 44342
X-Xss-Protection: 1; mode=block
Content-Type: application/javascript
Date: Thu, 02 Feb 2023 05:16:36 GMT
Server: Apache
/**
* Owl Carousel v2.3.4
* Copyright 2013-2018 David Deutsch
* Licensed under: SEE LICENSE IN https://github.com/OwlCarousel2/OwlCarousel2/blob/master/LICENSE
*/
!function(a,b,c,d){
function e(b,c){
this.settings=null,this.options=a.extend({
},
e.Defaults,c),this.$element=a(b),this._handlers={
},
this._plugins={
},
this._supress={
},
this._current=null,this._speed=null,this._coordinates=[],this._breakpoint=null,this._width=
null,this._items=[],this._clones=[],this._mergers=[],this._widths=[],this._invalidated={
Search... 0 matches
Inspector
Request Attributes 2
Request Query Parameters 1
Request Headers 15
Name Value
:scheme https
:method GET
:path /wp-content/the...
:authority br0nw3n.com
sec-ch-ua "Chromium";v=...
sec-ch-ua-mobile ?0
user-agent Mozilla/5.0 (Win...
sec-ch-ua-platf... "Linux"
accept */*
sec-fetch-site same-origin
sec-fetch-mode no-cors
sec-fetch-dest script
referer https://br0nw3n...
accept-encoding gzip, deflate
accept-language en-US,en;q=0.9
Response Headers 10


Burp Suite Community Edition v2022.8.4 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Intercept HTTP history WebSockets history Options
Filter: Hiding CSS, image and general binary content
Host Method URL Params Edited Status Length MIME type Extension Title Comment TLS IP Cookies Time Listener port
1 https://br0nw3n.com GET / 200 60941 HTML Br0nw3n's Worl... 72.29.78.44 21:16:33 1 Fe... 8080
3 https://br0nw3n.com GET /wp-includes/js/jquery/jquery.min.js?ve... 200 90042 script js 72.29.78.44 21:16:35 1 Fe... 8080
11 https://br0nw3n.com GET /wp-content/themes/magazinenp/ass... 200 9410 script js 72.29.78.44 21:16:35 1 Fe... 8080
12 https://br0nw3n.com GET /wp-content/themes/magazinenp/ass... 200 1041 script js 72.29.78.44 21:16:35 1 Fe... 8080
13 https://br0nw3n.com GET /wp-content/themes/magazinenp/ass... 200 3737 script js 72.29.78.44 21:16:35 1 Fe... 8080
14 https://br0nw3n.com GET /wp-content/themes/magazinenp/ass... 200 44700 script js 72.29.78.44 21:16:35 1 Fe... 8080
15 https://br0nw3n.com GET /wp-content/themes/magazinenp/ass... 200 49260 script js 72.29.78.44 21:16:35 1 Fe... 8080
16 https://br0nw3n.com GET /wp-content/plugins/contact-form-7/i... 200 13119 script js 72.29.78.44 21:16:35 1 Fe... 8080
17 https://br0nw3n.com GET /wp-content/plugins/contact-form-7/i... 200 10923 script js 72.29.78.44 21:16:35 1 Fe... 8080
18 https://br0nw3n.com GET /wp-includes/js/jquery/jquery-migrate.... 200 11582 script js 72.29.78.44 21:16:35 1 Fe... 8080
19 https://www.google.com GET /recaptcha/api.js?render=6LdlaOwUA... 200 1340 script js 142.250.189.4 21:16:35 1 Fe... 8080
22 https://br0nw3n.com GET /wp-content/plugins/contact-form-7/... 200 1355 script js 72.29.78.44 21:16:35 1 Fe... 8080
23 https://br0nw3n.com GET /wp-includes/js/dist/vendor/wp-polyfill... 200 18181 script js 72.29.78.44 21:16:35 1 Fe... 8080
24 https://br0nw3n.com GET /wp-includes/js/dist/vendor/regenerat... 200 6832 script js 72.29.78.44 21:16:35 1 Fe... 8080
Request
Pretty Raw Hex
GET /wp-content/themes/magazinenp/assets/vendor/owl-carousel/owl.carousel.min.js?ver=2.3.4 HTTP/2
Host: br0nw3n.com
Sec-Ch-Ua: "Chromium";v="105", "Not)A;Brand";v="8"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.5195.102 Safari/537.36
Sec-Ch-Ua-Platform: "Linux"
Accept: */*
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://br0nw3n.com/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Search... 0 matches
Response
Pretty Raw Hex Render
HTTP/2 200 OK
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Last-Modified: Sat, 19 Nov 2022 23:38:01 GMT
Accept-Ranges: bytes
Content-Length: 44342
X-Xss-Protection: 1; mode=block
Content-Type: application/javascript
Date: Thu, 02 Feb 2023 05:16:36 GMT
Server: Apache
/**
* Owl Carousel v2.3.4
* Copyright 2013-2018 David Deutsch
* Licensed under: SEE LICENSE IN https://github.com/OwlCarousel2/OwlCarousel2/blob/master/LICENSE
*/
!function(a,b,c,d){
function e(b,c){
this.settings=null,this.options=a.extend({
},
e.Defaults,c),this.$element=a(b),this._handlers={
},
this._plugins={
},
this._supress={
},
this._current=null,this._speed=null,this._coordinates=[],this._breakpoint=null,this._width=
null,this._items=[],this._clones=[],this._mergers=[],this._widths=[],this._invalidated={
Search... 0 matches
Inspector
Request Attributes 2
Request Query Parameters 1
Request Headers 15
Name Value
:scheme https
:method GET
:path /wp-content/the...
:authority br0nw3n.com
sec-ch-ua "Chromium";v=...
sec-ch-ua-mobile ?0
user-agent Mozilla/5.0 (Win...
sec-ch-ua-platf... "Linux"
accept */*
sec-fetch-site same-origin
sec-fetch-mode no-cors
sec-fetch-dest script
referer https://br0nw3n...
accept-encoding gzip, deflate
accept-language en-US,en;q=0.9
Response Headers 10



WAYS TO IMPROVE YOUR SCREENSHOTS

- Switch to light mode before taking screenshot
- Make sure shell/browser window is narrow
- Use callouts/highlighting to draw the reader's eye to important bits
- When in doubt, go tall!
- Use captions – make them descriptive
- Avoid:
  - Drop shadows, other special effects
  - They only distract!



4. Inconsistent/Unprofessional Formatting

Avoid fancy, special fonts

Times New Roman may be boring, but it's readable!

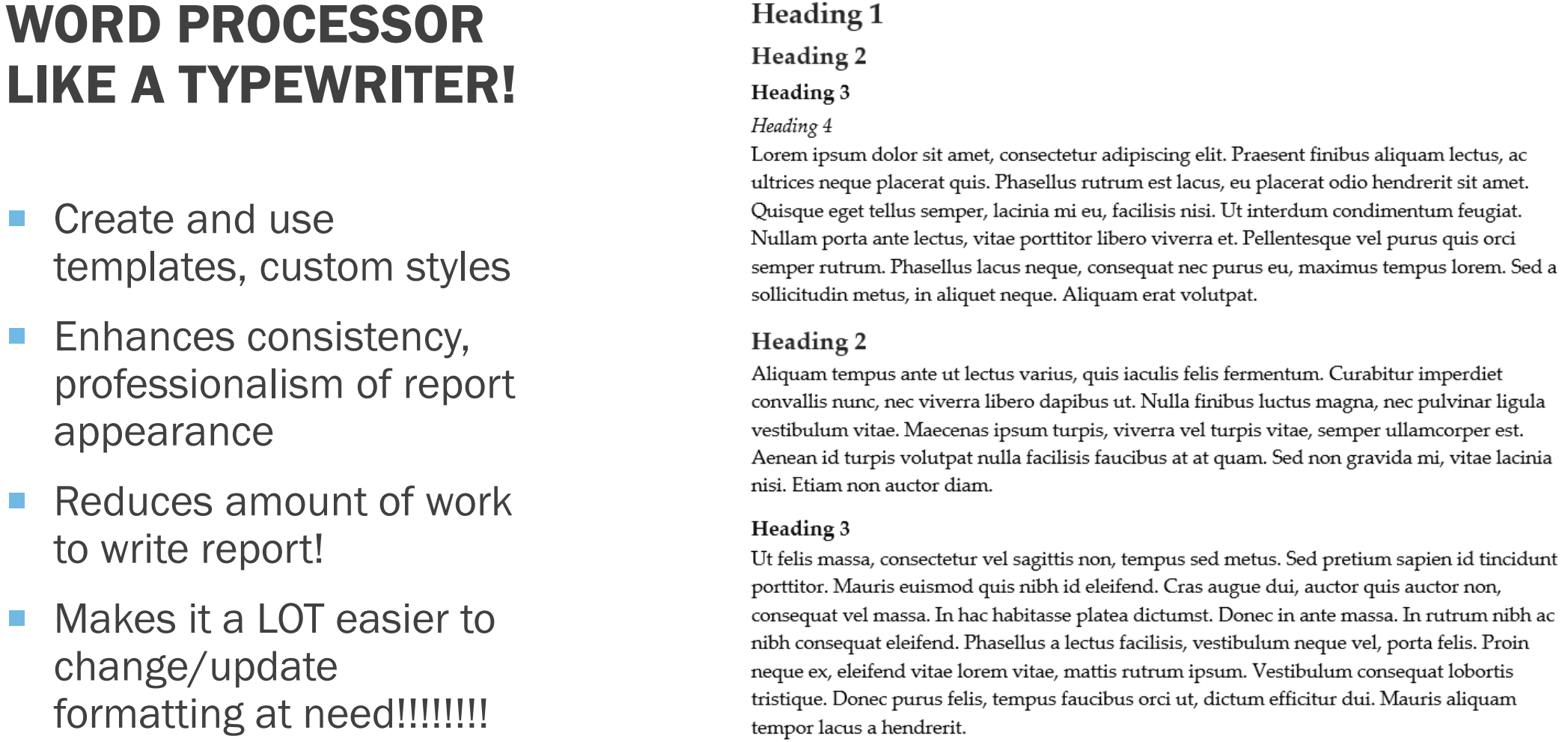
Use Styles to apply fonts, shading, etc., consistently

Also means less manual work for you

- Technical people prefer sans serif fonts
  - Arial, Calibri, Avenir, Trebuchet
- Business/Literary people prefer serif fonts
  - Times, Bookman, Palatino

DON'T USE YOUR WORD PROCESSOR LIKE A TYPEWRITER!

- Create and use templates, custom styles
- Enhances consistency, professionalism of report appearance
- Reduces amount of work to write report!
- Makes it a LOT easier to change/update formatting at need!!!!!!!!



Heading 1

Heading 2

Heading 3

Heading 4

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Praesent finibus aliquam lectus, ac ultrices neque placerat quis. Phasellus rutrum est lacus, eu placerat odio hendrerit sit amet. Quisque eget tellus semper, lacinia mi eu, facilisis nisi. Ut interdum condimentum feugiat. Nullam porta ante lectus, vitae porttitor libero viverra et. Pellentesque vel purus quis orci semper rutrum. Phasellus lacus neque, consequat nec purus eu, maximus tempus lorem. Sed a sollicitudin metus, in aliquet neque. Aliquam erat volutpat.

Heading 2

Aliquam tempus ante ut lectus varius, quis iaculis felis fermentum. Curabitur imperdiet convallis nunc, nec viverra libero dapibus ut. Nulla finibus luctus magna, nec pulvinar ligula vestibulum vitae. Maecenas ipsum turpis, viverra vel turpis vitae, semper ullamcorper est. Aenean id turpis volutpat nulla facilisis faucibus at at quam. Sed non gravida mi, vitae lacinia nisi. Etiam non auctor diam.

Heading 3

Ut felis massa, consectetur vel sagittis non, tempus sed metus. Sed pretium sapien id tincidunt porttitor. Mauris euismod quis nibh id eleifend. Cras augue dui, auctor quis auctor non, consequat vel massa. In hac habitasse platea dictumst. Donec in ante massa. In rutrum nibh ac nibh consequat eleifend. Phasellus a lectus facilisis, vestibulum neque vel, porta felis. Proin neque ex, eleifend vitae lorem vitae, mattis rutrum ipsum. Vestibulum consequat lobortis tristique. Donec purus felis, tempus faucibus orci ut, dictum efficitur dui. Mauris aliquam tempor lacus a hendrerit.

5. RANDOM LISTS

- Many pentest reports include LOOOOONGGGG lists of IP addresses
- Some poor schmoe will likely have to use your list(s) to verify findings
- Same or other schmoe has to FIX all those systems!

- 39.1.203.23
- 226.107.98.122
- 6.223.229.133
- 3.246.72.237
- 10.198.242.26
- 62.231.169.31
- 141.116.122.58
- 98.240.116.85
- 148.249.68.130
- 167.11.222.164
- 223.49.237.228
- 227.90.5.226
- 105.134.81.174
- 11.97.207.124
- 206.136.253.65
- 195.60.32.1
- 65.232.212.214
- 196.29.118.108
- 187.255.30.211
- 126.236.87.157
- 55.92.126.39
- 6.219.199.176
- 215.206.142.242
- 61.81.12.8
- 223.117.90.149
- 188.2.49.68
- 0.168.7.40
- 218.54.14.211
- 207.3.118.205
- 151.104.243.37
- 169.99.94.75
- 51.246.124.31
- 162.52.229.69
- 87.228.108.237
- 108.19.178.131
- 104.36.167.84
- 19.227.128.128
- 67.87.254.53
- 30.196.60.36
- 10.228.181.113
- 119.183.202.66
- 26.109.223.149
- 199.239.96.120
- 228.135.99.125
- 93.11.197.52
- 39.21.96.119
- 58.212.232.240
- 4.1.160.28
- 251.2.127.228
- 200.108.70.84
- 12.87.143.4
- 36.158.149.26
- 151.22.220.229
- 155.215.216.114
- 175.30.222.128
- 58.202.174.34
- 197.168.131.48
- 160.106.62.57
- 138.220.89.186
- 128.133.111.4
- 82.198.167.130
- 225.249.100.100
- 169.195.132.237
- 139.81.195.1
- 149.111.57.220
- 185.98.86.98
- 14.236.206.2
- 118.57.162.36
- 155.13.168.100
- 167.18.219.99
- 245.22.187.187
- 39.42.86.179
- 57.80.245.122
- 94.62.144.95
- 192.69.210.99
- 21.79.64.171
- 177.215.2.253
- 199.15.82.28
- 48.201.33.251
- 231.198.26.50
- 71.219.30.66
- 133.238.213.45
- 60.28.195.36
- 89.171.230.23
- 229.43.65.167
- 168.190.133.143
- 34.75.188.84
- 178.250.166.82
- 181.209.89.115
- 208.183.25.224
- 194.48.168.218
- 181.72.30.254
- 37.9.252.209
- 225.34.61.209
- 103.206.66.148
- 59.8.173.251
- 150.244.114.217
- 112.134.87.229
- 108.141.206.48
- 8.215.142.160
- 227.153.124.104
- 235.12.190.157
- 109.220.68.112
- 198.100.44.227
- 113.86.6.253
- 170.125.125.67
- 1.228.203.130
- 96.180.46.214

WORD *SUCKS* AT SORTING

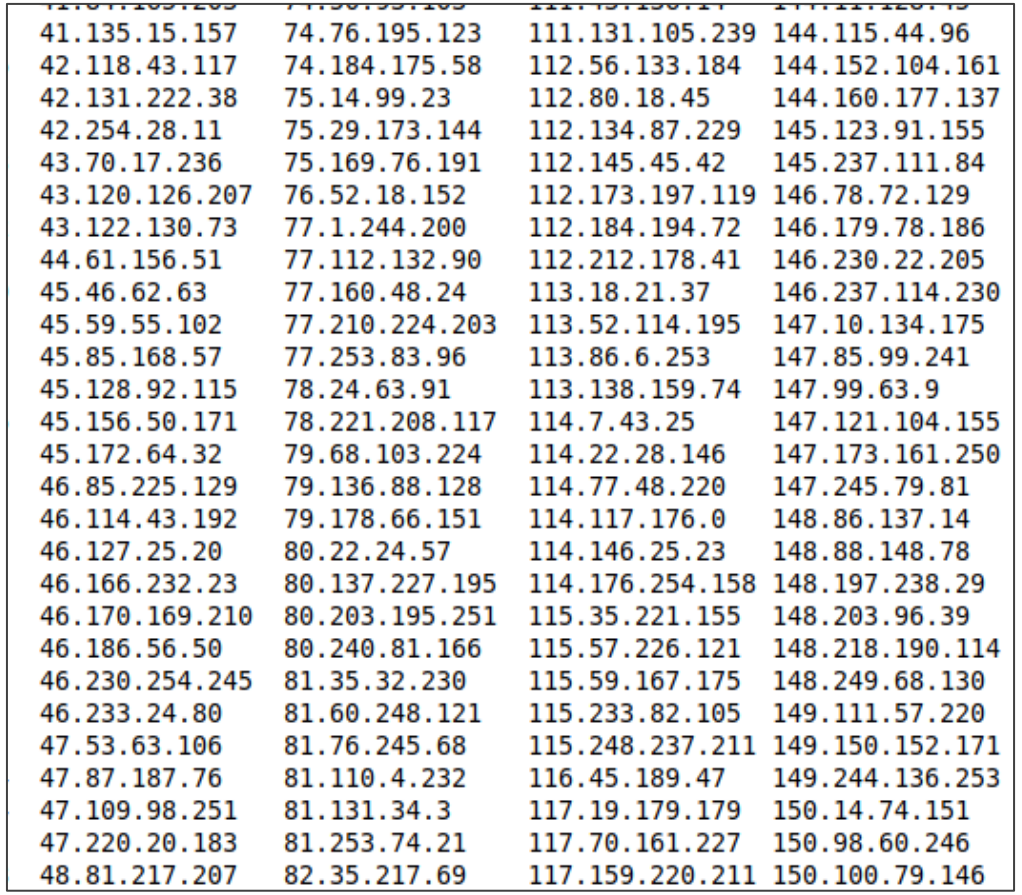
- Ideally, lists should be sorted:
  - Alphabetically
  - Numerically
  - By octet
  - By domain, then subdomain

Random/Original	Text	Number	Date*
34.122.53.113	14.144.148.126	3.163.2.85	34.122.53.113
48.9.97.140	3.163.2.85	14.144.148.126	48.9.97.140
90.102.190.159	34.122.53.113	34.122.53.113	90.102.190.159
56.160.162.175	36.91.53.247	36.91.53.247	56.160.162.175
90.93.203.147	44.15.174.252	44.15.174.252	90.93.203.147
64.232.50.221	44.36.62.196	44.36.62.196	64.232.50.221
67.68.74.212	48.9.97.140	48.9.97.140	67.68.74.212
14.144.148.126	53.133.207.183	53.133.207.183	14.144.148.126
73.245.109.235	56.160.162.175	56.160.162.175	73.245.109.235
44.36.62.196	64.232.50.221	64.232.50.221	44.36.62.196
3.163.2.85	67.68.74.212	67.68.74.212	3.163.2.85
53.133.207.183	73.245.109.235	73.245.109.235	53.133.207.183
44.15.174.252	75.225.28.49	75.225.28.49	44.15.174.252
75.225.28.49	90.102.190.159	90.102.190.159	75.225.28.49
36.91.53.247	90.93.203.147	90.93.203.147	36.91.53.247

*The date sort is kinda useless, tbh.

Ways to Improve Your Lists

- Linux is your friend!
  - `cat list.txt | sort -V | uniq`
  - `sort -uV list.txt`
- Sorting reduces the pain you inflict on others
- De-duping avoids damaging your cred
- https://br0nw3n.com/2022/08/sort-your-lists-penetration-test-reporting-tips/



41.135.15.157	74.76.195.123	111.131.105.239	144.115.44.96
42.118.43.117	74.184.175.58	112.56.133.184	144.152.104.161
42.131.222.38	75.14.99.23	112.80.18.45	144.160.177.137
42.254.28.11	75.29.173.144	112.134.87.229	145.123.91.155
43.70.17.236	75.169.76.191	112.145.45.42	145.237.111.84
43.120.126.207	76.52.18.152	112.173.197.119	146.78.72.129
43.122.130.73	77.1.244.200	112.184.194.72	146.179.78.186
44.61.156.51	77.112.132.90	112.212.178.41	146.230.22.205
45.46.62.63	77.160.48.24	113.18.21.37	146.237.114.230
45.59.55.102	77.210.224.203	113.52.114.195	147.10.134.175
45.85.168.57	77.253.83.96	113.86.6.253	147.85.99.241
45.128.92.115	78.24.63.91	113.138.159.74	147.99.63.9
45.156.50.171	78.221.208.117	114.7.43.25	147.121.104.155
45.172.64.32	79.68.103.224	114.22.28.146	147.173.161.250
46.85.225.129	79.136.88.128	114.77.48.220	147.245.79.81
46.114.43.192	79.178.66.151	114.117.176.0	148.86.137.14
46.127.25.20	80.22.24.57	114.146.25.23	148.88.148.78
46.166.232.23	80.137.227.195	114.176.254.158	148.197.238.29
46.170.169.210	80.203.195.251	115.35.221.155	148.203.96.39
46.186.56.50	80.240.81.166	115.57.226.121	148.218.190.114
46.230.254.245	81.35.32.230	115.59.167.175	148.249.68.130
46.233.24.80	81.60.248.121	115.233.82.105	149.111.57.220
47.53.63.106	81.76.245.68	115.248.237.211	149.150.152.171
47.87.187.76	81.110.4.232	116.45.189.47	149.244.136.253
47.109.98.251	81.131.34.3	117.19.179.179	150.14.74.151
47.220.20.183	81.253.74.21	117.70.161.227	150.98.60.246
48.81.217.207	82.35.217.69	117.159.220.211	150.100.79.146

6. IRRELEVANT GUIDANCE

- You are supposed to be the subject matter expert
- Your guidance needs to be:
  - Meaningful
  - Relevant
  - Practical
- Anyone can run scripts
- Your guidance is what your customers need most!

7. INFO FROM ANOTHER CUSTOMER

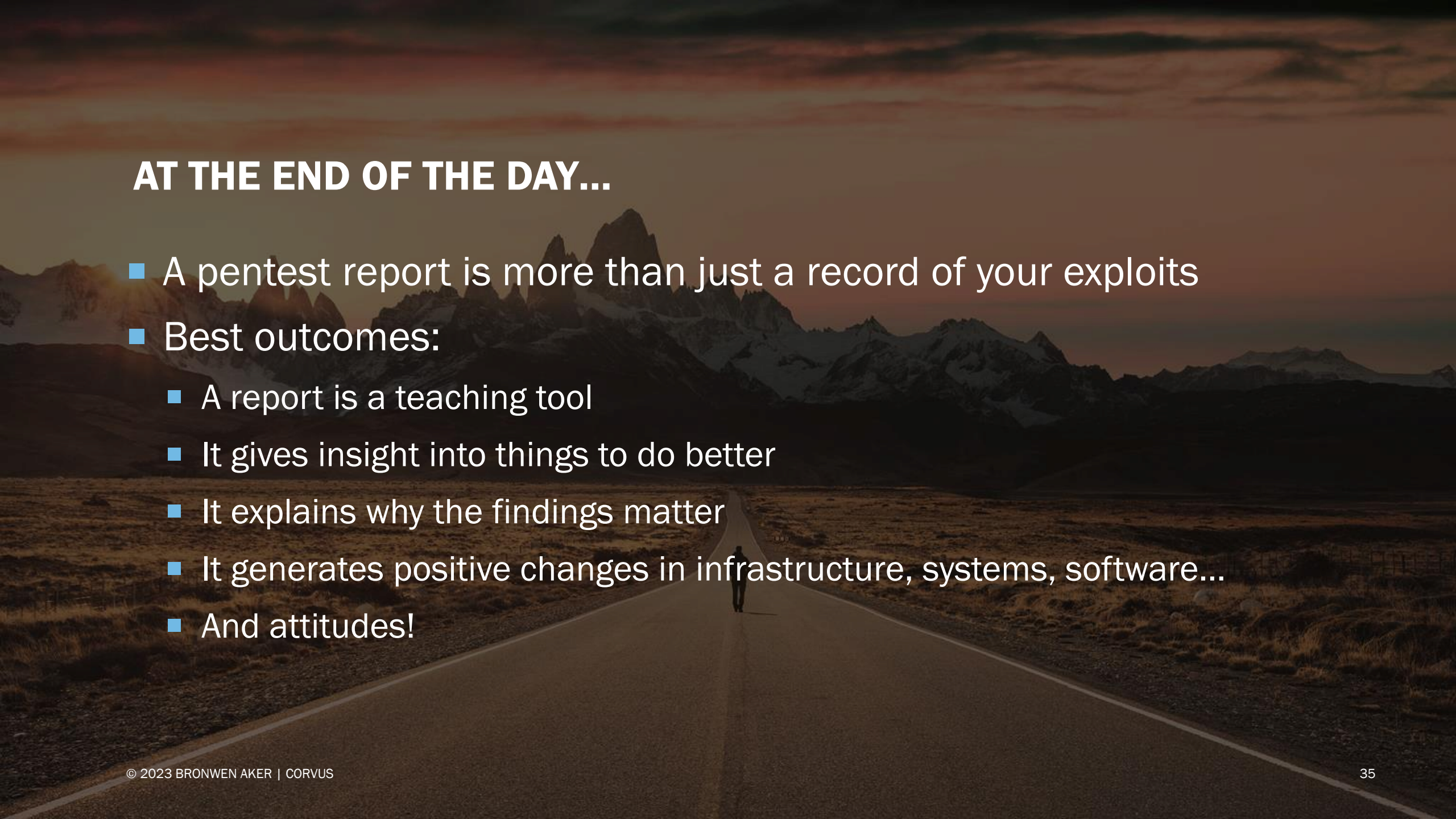
- DO NOT COPY/PASTE FROM ANOTHER REPORT
- Contamination with another client's info has SERIOUS repercussions
- At BHIS, copy/pasting between reports is a *fireable* offense

Other Tips & Tricks

- Have someone else read your report (if possible and you can get them to sign an NDA)
  - Really. Anyone.
- Leave yourself time to make edits/revisions
- If the client does something well, mention it
- GET SOME SLEEP!
- Print Preview is your friend!
- Include the exact commands you used
- Include links to tools
  - Footnotes work well for this

But wait! There's more!

- Fundamentals
  - Report As You Go
  - Sort Your Lists
  - Include Command Strings
  - Learn to Use Word
  - Include a Data Archive
  - Check Your Spelling
  - Include Links to Cool Tools
  - Take a Writing Class
- Writing Style Issues
  - Watch Your Tone
  - Remember Your Audience
  - Use Inclusive Language
  - Use the Past Tense
  - Don't Start Sentences with Numerals
  - Spell Out Numbers < 10
- All About Screenshots
  - Don't Use Dark Mode
  - Make Shell Windows Opaque
  - Browser Setting Tweaks
  - Use Callouts and Highlighting
  - Drop Shadows Are Not Your Friends
  - Make Image Captions Descriptive
- Proofreading
  - Hire an Editor
  - Get Some Sleep
  - Give It A Rest
- Final Touches
  - Print Preview is Your Friend
  - Sanitize Before You Send



AT THE END OF THE DAY…

- A pentest report is more than just a record of your exploits
- Best outcomes:
  - A report is a teaching tool
  - It gives insight into things to do better
  - It explains why the findings matter
  - It generates positive changes in infrastructure, systems, software…
  - And attitudes!

REMEMBER…

- Hacking is fun, but the report is the product!
- A good report tells a story
  - What was found
  - How was it found
  - How what was found can be fixed!
- You don’t have to be a l33t haxor to write reports well
- Keep your focus on helping your customer understand
- Great reports EMPOWER

THINGS NOT TO DO IN A PENTEST REPORT

Tips, Tricks, And Traps In Report Writing

BRONWEN AKER | CORVUS

BR0NW3N.COM

Bronwen Aker | GSEC, GCIH, GCFE

- Website: `https://br0nw3n.com/`
- LinkedIn: `https://www.linkedin.com/in/bronwenaker/`
- Discord: `Corvus#5800`

(Do your OSINT. I'm online.)