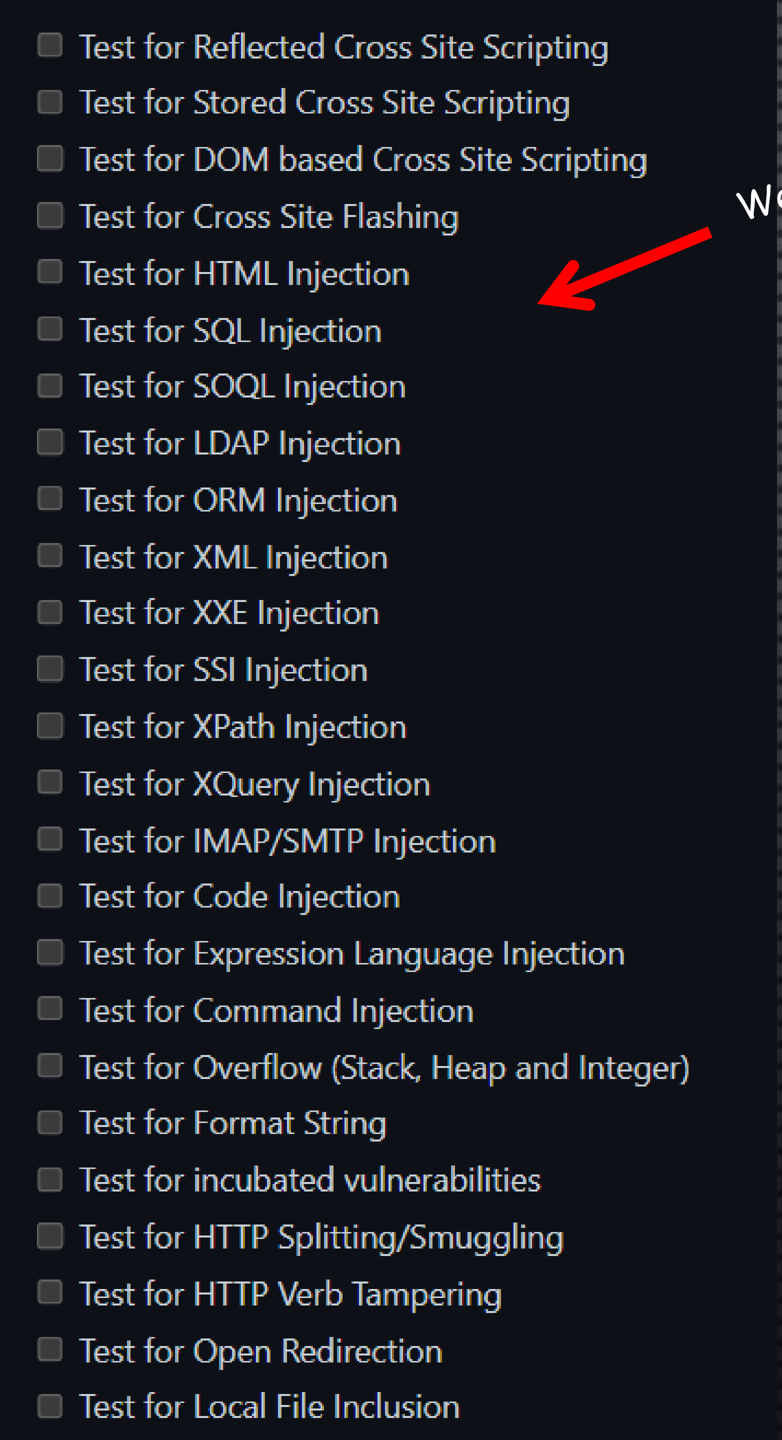


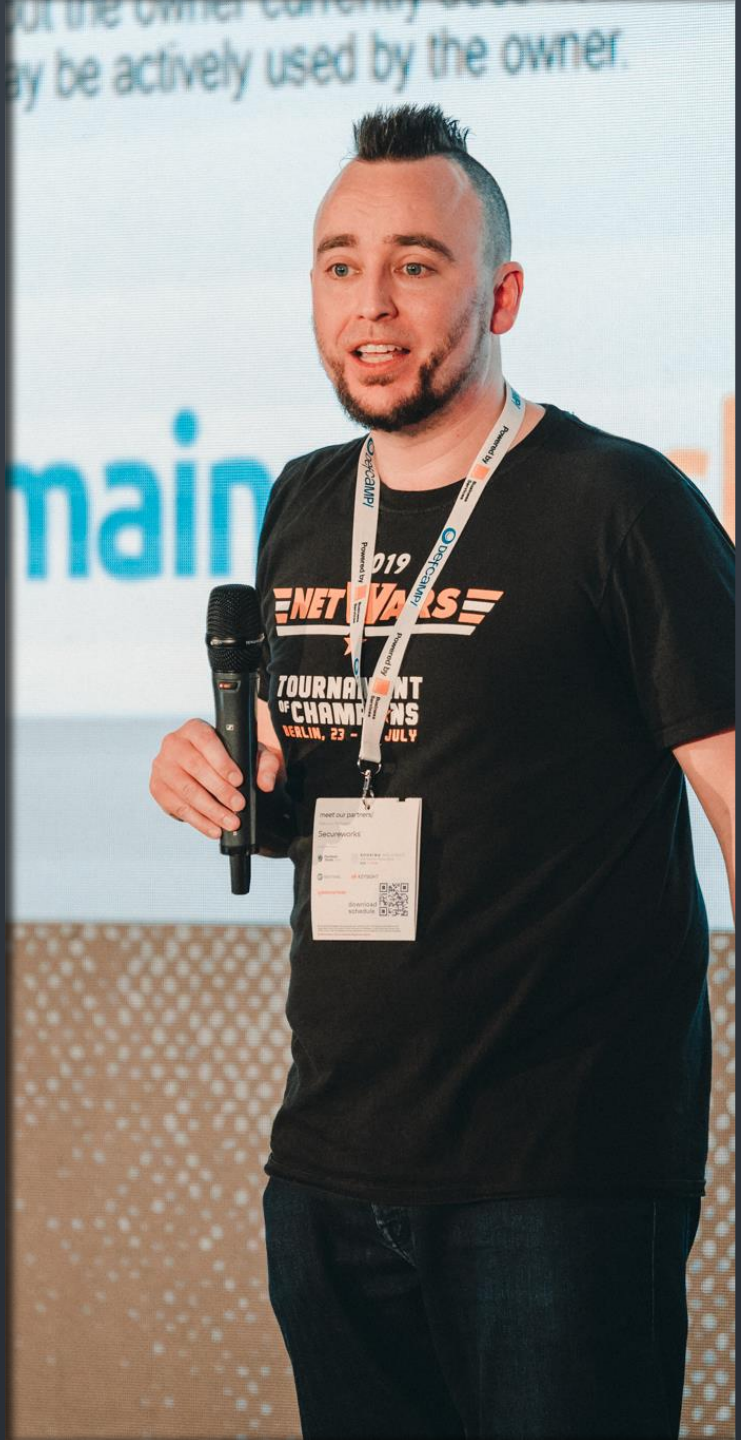
- ☐ Test for Reflected Cross Site Scripting
- ☐ Test for Stored Cross Site Scripting
- ☐ Test for DOM based Cross Site Scripting
- ☐ Test for Cross Site Flashing
- ☐ Test for HTML Injection
- ☐ Test for SQL Injection
- ☐ Test for SOQL Injection
- ☐ Test for LDAP Injection
- ☐ Test for ORM Injection
- ☐ Test for XML Injection
- ☐ Test for XXE Injection
- ☐ Test for SSI Injection
- ☐ Test for XPath Injection
- ☐ Test for XQuery Injection
- ☐ Test for IMAP/SMTP Injection
- ☐ Test for Code Injection
- ☐ Test for Expression Language Injection
- ☐ Test for Command Injection
- ☐ Test for Overflow (Stack, Heap and Integer)
- ☐ Test for Format String
- ☐ Test for incubated vulnerabilities
- ☐ Test for HTTP Splitting/Smuggling
- ☐ Test for HTTP Verb Tampering
- ☐ Test for Open Redirection
- ☐ Test for Local File Inclusion

We won't be talking about this!

RIVER SECURITY

WEB APPLICATION PENTESTING

Practical Methodology for Finding Bugs and Vulnerabilities



Chris Dale

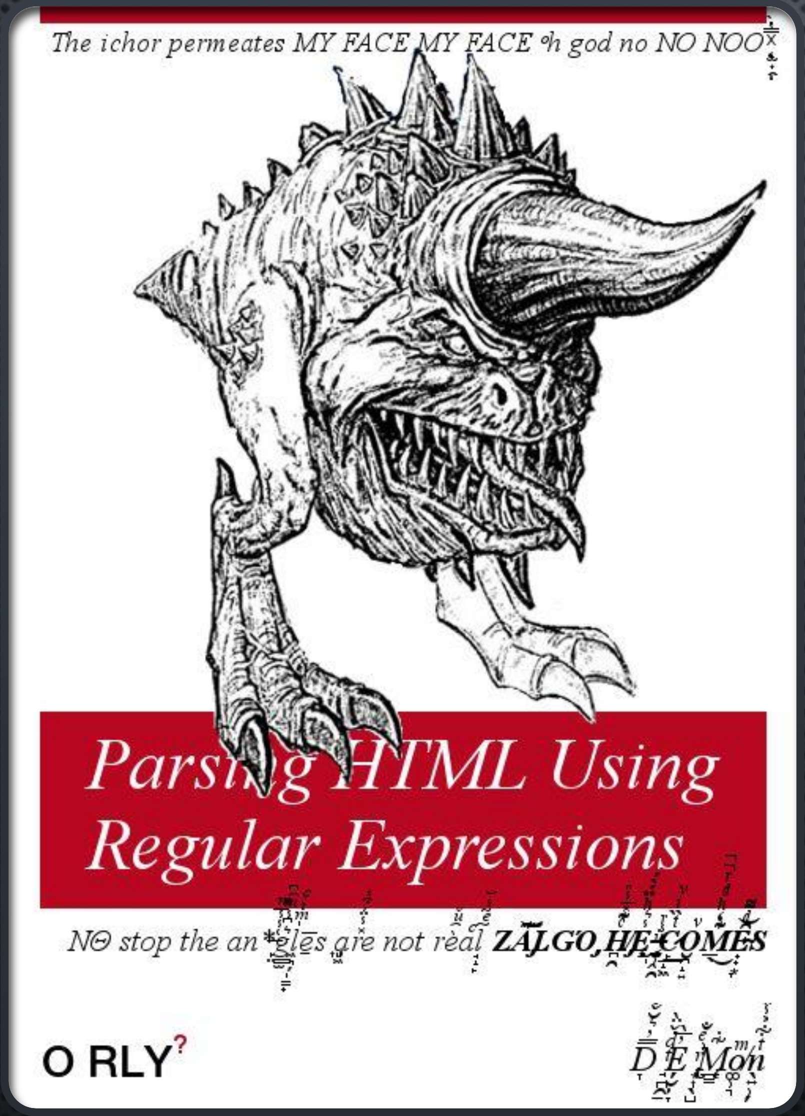
- COO, Principal and Founder at River Security
- Principal Instructor at SANS
- Co-Author – Cyber Deception, Attack Detection, Disruption and Active Defense

- Short summary:

I show how criminals break-in,
and I help throw them back out…

Certs

GCIH	GIAC Certified Incident Handler
GPEN	GIAC Certified Penetration Tester
GSLC	GIAC Security Leadership
GIAC	GIAC Mobile Device Security Analyst
GDAT	GIAC Defending Advanced Adversaries
GCTI	GIAC Cyber Threat Intelligence
GCFA	GIAC Certified Forensic Analyst
GXIH	GIAC Experienced Incident Handler
GXPT	GIAC Experience Penetration Tester
GSP	GIAC Security Professional


The ichor permeates MY FACE MY FACE ᵒh god no NO NOO
Parsing HTML Using Regular Expressions
NΘ stop the an*gles are not real ZALGO HE COMES
O RLY?
DE Mon

WHY THIS TALK?

- WEB IS UBIQUITOUS
- CONSIDERED BORING BY MANY
- NOT THE HIGHEST OF LEARNING CURVES.
  - YOU CAN PROVIDE VALUE FAST
- DUNNING KRUGER EFFECT
  - NOT JUST CHECKLIST, I.E. FRAMEWORKS , OWASP TOP10 , ETC.
- WEB IS REALLY A GREAT PLACE TO RESEARCH, BOUNTY AND GIVE YOUR CUSTOMERS VALUE.

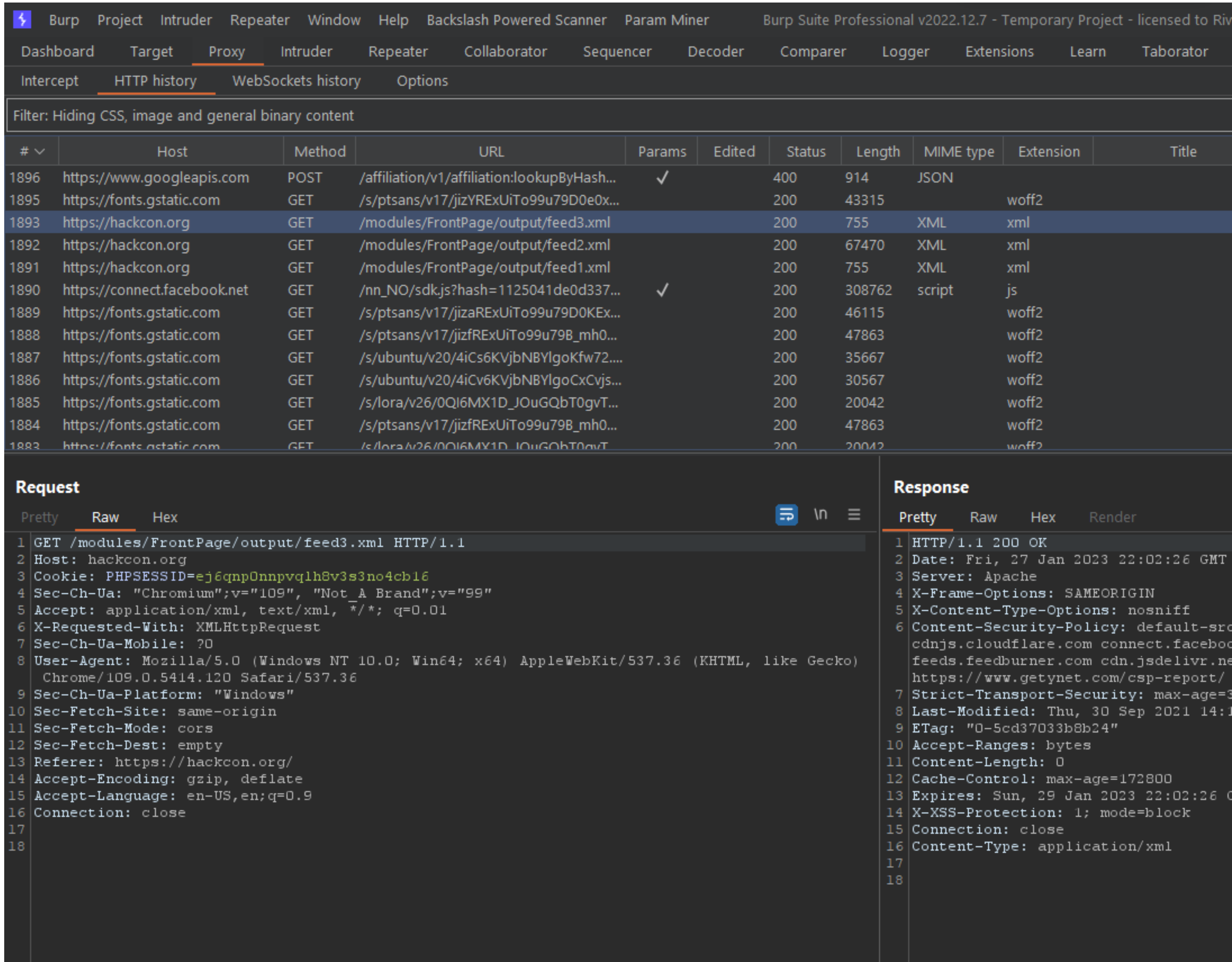
PORTSWIGGER TOP 10 ATTACKS

- 1 - Account hijacking using dirty dancing in sign-in OAuth-flows
- 2 - Browser-Powered Desync Attacks: A New Frontier in HTTP Request Smuggling
- 3 - Zimbra Email - Stealing Clear-Text Credentials via Memcache injection
- 4 - Hacking the Cloud with SAML
- 5 - Bypassing .NET Serialization Binders
- 6 - Making HTTP header injection critical via response queue poisoning
- 7 - Worldwide Server-side Cache Poisoning on All Akamai Edge Nodes
- 8 - Psychic Signatures in Java
- 9 - Practical client-side path-traversal attacks
- 10 - Exploiting Web3's Hidden Attack Surface: Universal XSS on Netlify's Next.js Library

https://portswigger.net/research/top-10-web-hacking-techniques-of-2022

Burp Suite – Tool of Choice

- Defacto tool by pentester
- Strong fuzzing capabilities
- Extension support
- Very flexible and robust
- Well developed scanner
- Spidering engine with decent SPA support
- Cheat sheet: https://www.sans.org/posters/burp-suite-cheat-sheet/



Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title
1896	https://www.googleapis.com	POST	/affiliation/v1/affiliation:lookupByHash...	✓		400	914	JSON		
1895	https://fonts.gstatic.com	GET	/s/ptsans/v17/jizYRExUiTo99u79D0e0x...			200	43315		woff2	
1893	https://hackcon.org	GET	/modules/FrontPage/output/feed3.xml			200	755	XML	xml	
1892	https://hackcon.org	GET	/modules/FrontPage/output/feed2.xml			200	67470	XML	xml	
1891	https://hackcon.org	GET	/modules/FrontPage/output/feed1.xml			200	755	XML	xml	
1890	https://connect.facebook.net	GET	/nn_NO/sdk.js?hash=1125041de0d337...	✓		200	308762	script	js	
1889	https://fonts.gstatic.com	GET	/s/ptsans/v17/jizaRExUiTo99u79D0KEx...			200	46115		woff2	
1888	https://fonts.gstatic.com	GET	/s/ptsans/v17/jizfRExUiTo99u79B_mh0...			200	47863		woff2	
1887	https://fonts.gstatic.com	GET	/s/ubuntu/v20/4iCs6KVjbNBYlgoKfw72....			200	35667		woff2	
1886	https://fonts.gstatic.com	GET	/s/ubuntu/v20/4iCv6KVjbNBYlgoCxCvjs...			200	30567		woff2	
1885	https://fonts.gstatic.com	GET	/s/lora/v26/0QI6MX1D_JOuGQbT0gvT...			200	20042		woff2	
1884	https://fonts.gstatic.com	GET	/s/ptsans/v17/jizfRExUiTo99u79B_mh0...			200	47863		woff2	
1883	https://fonts.gstatic.com	GET	/s/lora/v26/0QI6MX1D_JOuGQbT0gvT			200	20042		woff2	

Request

```
GET /modules/FrontPage/output/feed3.xml HTTP/1.1
Host: hackcon.org
Cookie: PHPSESSID=ej6qnp0nnpvqlh8v3s3no4cb16
Sec-Ch-Ua: "Chromium";v="109", "Not_A Brand";v="99"
Accept: application/xml, text/xml, */*; q=0.01
X-Requested-With: XMLHttpRequest
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
 Chrome/109.0.5414.120 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://hackcon.org/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close


```

Response

```
HTTP/1.1 200 OK
Date: Fri, 27 Jan 2023 22:02:26 GMT
Server: Apache
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Content-Security-Policy: default-src
cdnjs.cloudflare.com connect.faceboo
feeds.feedburner.com cdn.jsdelivr.ne
https://www.getynet.com/csp-report/
Strict-Transport-Security: max-age=3
Last-Modified: Thu, 30 Sep 2021 14:1
ETag: "0-5cd37033b8b24"
Accept-Ranges: bytes
Content-Length: 0
Cache-Control: max-age=172800
Expires: Sun, 29 Jan 2023 22:02:26 G
X-XSS-Protection: 1; mode=block
Connection: close
Content-Type: application/xml


```

Burp Extensions

Must have

- Active Scan ++
- Backslash Powered Scanner
- Param Miner
- Taborator

Nice to have

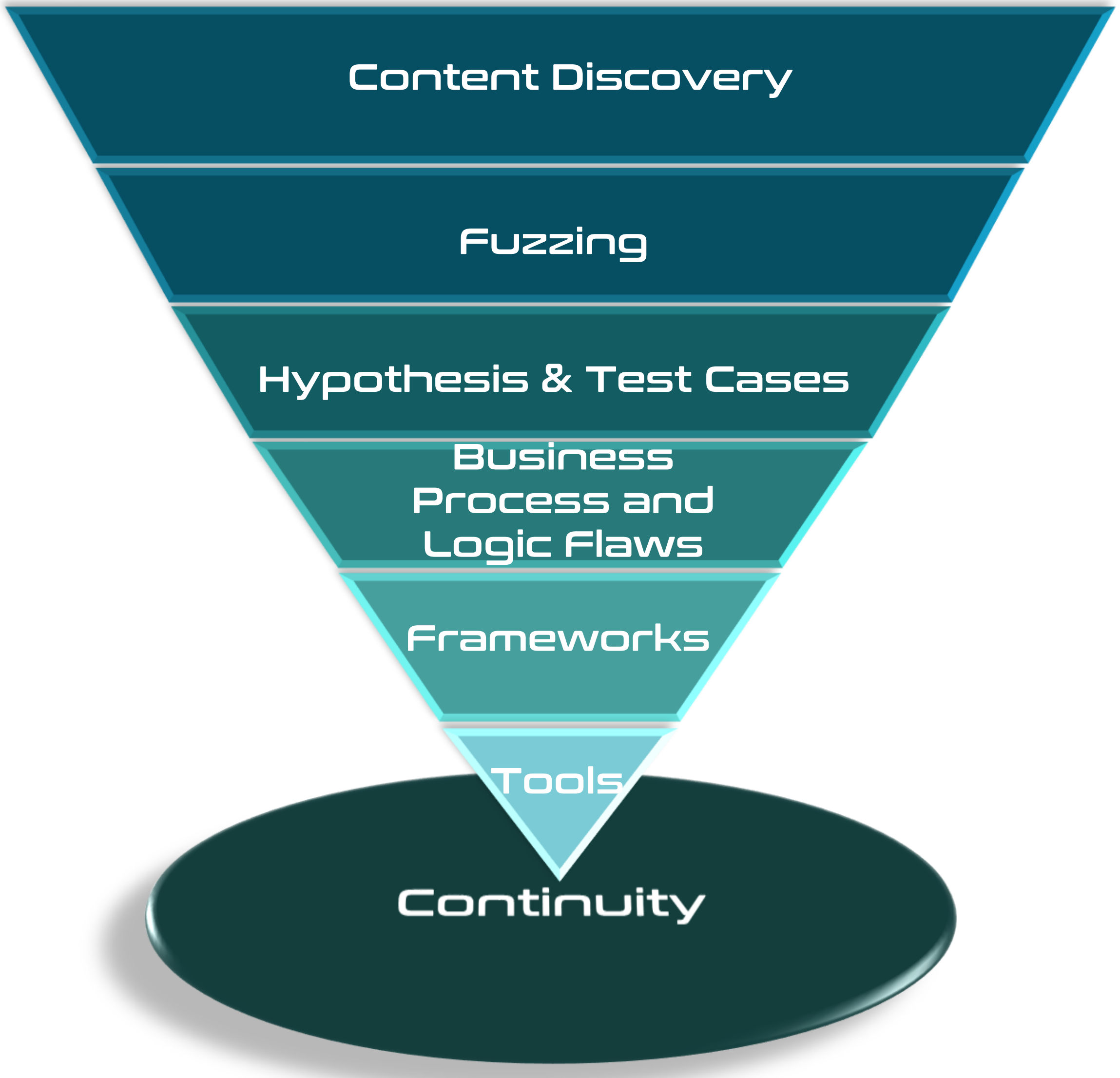
- Turbo Intruder
- Autorize
- Software Vulnerability Scanner
- Collaborator Everywhere

Honorable Mentions

- Freddy, deserialization scanner
- GraphQL raider
- JSON Web Tokens
- NTLM Challenge Decoder
- Retire.js
- Additional Scanner Checks

Finding Vulnerabilities Process Pyramid

Fully test the scope, every script and input



Content Discovery

Fuzzing

Hypothesis & Test Cases

Business Process and Logic Flaws

Frameworks

Tools

Continuity

Producing High Value Penetration Tests

Reliable and consistent testing is important, and not relying on a single individuals' skills and efforts to complete a penetration test helps ensure the highest levels of standards.

Team Based Effort

Penetration Testing is a team effort, not an individual effort. Utilize a team to maximize the penetration test efforts.

Thoroughly Map Attack Surface

Leave no stone untouched. Many vulnerabilities are found in the "paths least travelled". Fully explore!

Reporting

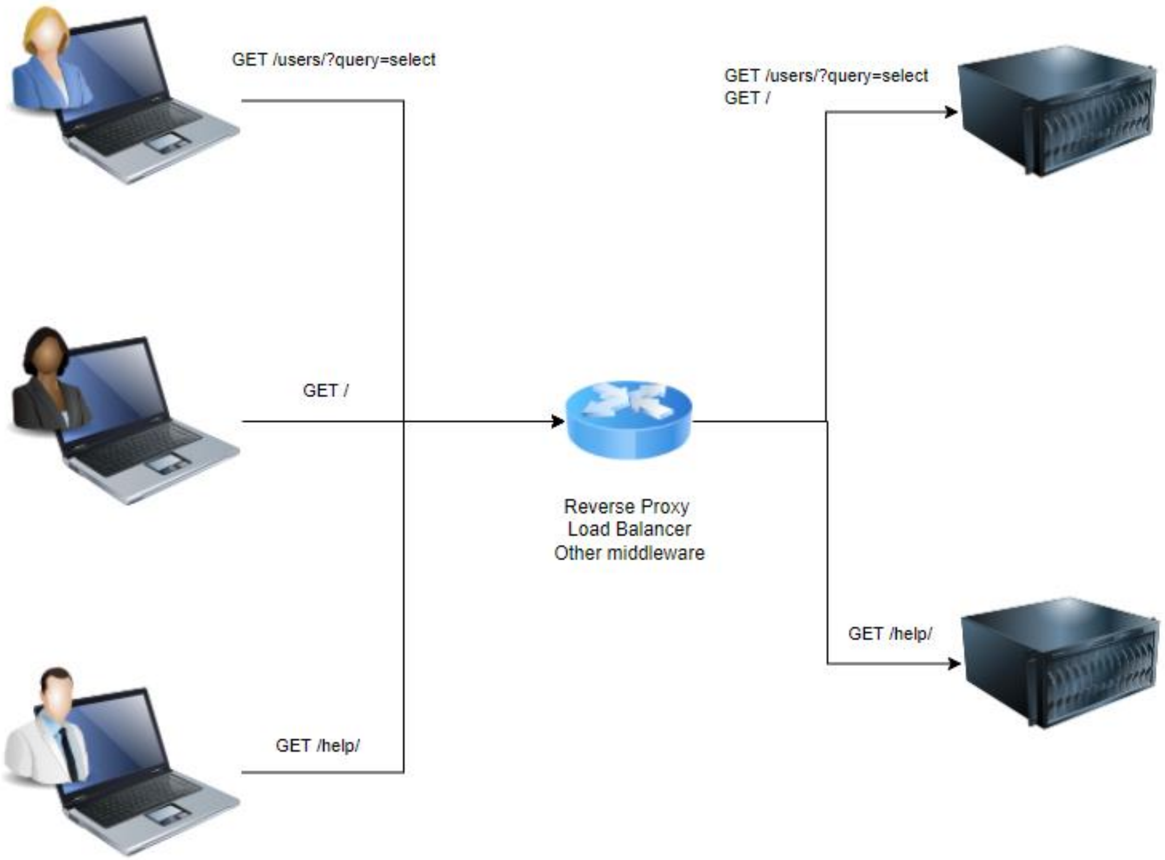
Document findings, process, discrepancies and hypothesis. It will be useful now and later.

Hypothesis and Knowledge Sharing

A team is stronger. Produce hypothesis to uncover potential attacks across all layers. Strengthen the team knowledge by working as one.

Platform Distinctions

- A web application may have several "platform distinctions"
  - Load-balancers may balance on an endpoint
  - Reverse proxies does the same
- Do your best if the target is split into different platforms
  - Each platform distinction should receive full test process



Goal: Find Everything

i. Map Browsable Attack Surface

ii. Find Unlinked Content & Params

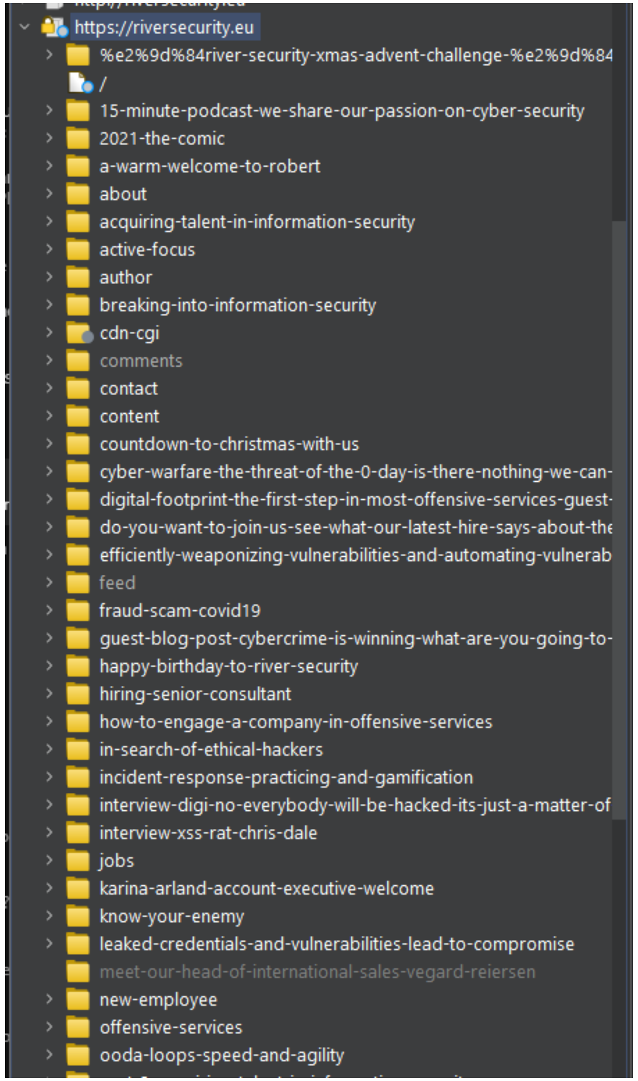
iii. Repeat for each `Platform Distinctions` of the application

Leave no stone unturned. Many vulnerabilities are found in the "paths least travelled". Fully explore!

Map Browsable Attack Surface

Content Discovery

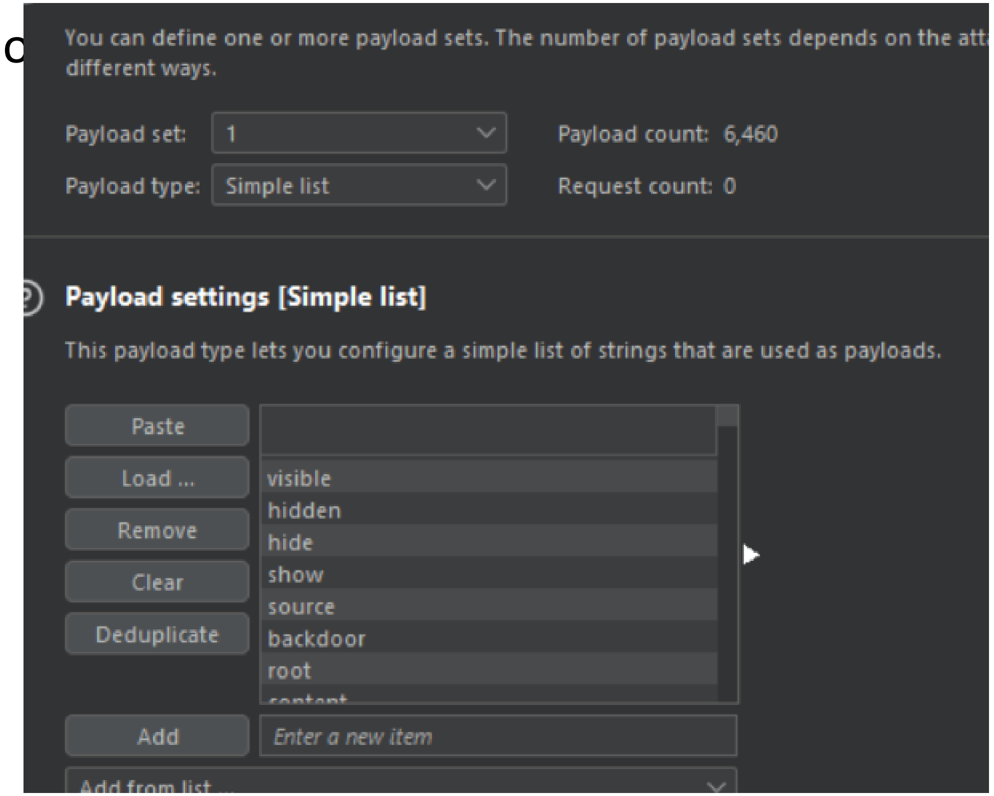
- Browse the entire application, discover all browsable content
  - Click
  - Use
  - Learn
- Use the Burp Suite Crawl feature on the top level of the application.
  - Has decent support for SPA as of Burp Suite v. >2
  - Helps build a complete sitemap
  - Use most complete configuration, which is the slowest
- For JavaScript, extract file paths and references.
  - CyberChef extract file paths module
  - GAP Burp Plugin
  - JSParser



```
http://riversecurity.eu
https://riversecurity.eu
  %e2%9d%84river-security-xmas-advent-challenge-%e2%9d%84
  /
  15-minute-podcast-we-share-our-passion-on-cyber-security
  2021-the-comic
  a-warm-welcome-to-robert
  about
  acquiring-talent-in-information-security
  active-focus
  author
  breaking-into-information-security
  cdn-cgi
  comments
  contact
  content
  countdown-to-christmas-with-us
  cyber-warfare-the-threat-of-the-0-day-is-there-nothing-we-can-
  digital-footprint-the-first-step-in-most-offensive-services-guest-
  do-you-want-to-join-us-see-what-our-latest-hire-says-about-the
  efficiently-weaponizing-vulnerabilities-and-automating-vulnerab
  feed
  fraud-scam-covid19
  guest-blog-post-cybercrime-is-winning-what-are-you-going-to-
  happy-birthday-to-river-security
  hiring-senior-consultant
  how-to-engage-a-company-in-offensive-services
  in-search-of-ethical-hackers
  incident-response-practicing-and-gamification
  interview-digi-no-everybody-will-be-hacked-its-just-a-matter-of
  interview-xss-rat-chris-dale
  jobs
  karina-arland-account-executive-welcome
  know-your-enemy
  leaked-credentials-and-vulnerabilities-lead-to-compromise
  meet-our-head-of-international-sales-vegard-reiersen
  new-employee
  offensive-services
  ooda-loops-speed-and-agility
```

Find Unlinked Content

- Fuzz **verbs** and **functionality**, find more content
  - For functionality such as e.g. **/?action=showUser&id=123** , try fuzzing the verb (i.e. show) with words like:
    - Add, delete, update and so on… i.e. making actio
  - Useful wordlists inside of Burp:
    - Server-side variable names
    - Form Field values
    - Form Field names



You can define one or more payload sets. The number of payload sets depends on the att
different ways.

Payload set: 1 Payload count: 6,460

Payload type: Simple list Request count: 0

Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

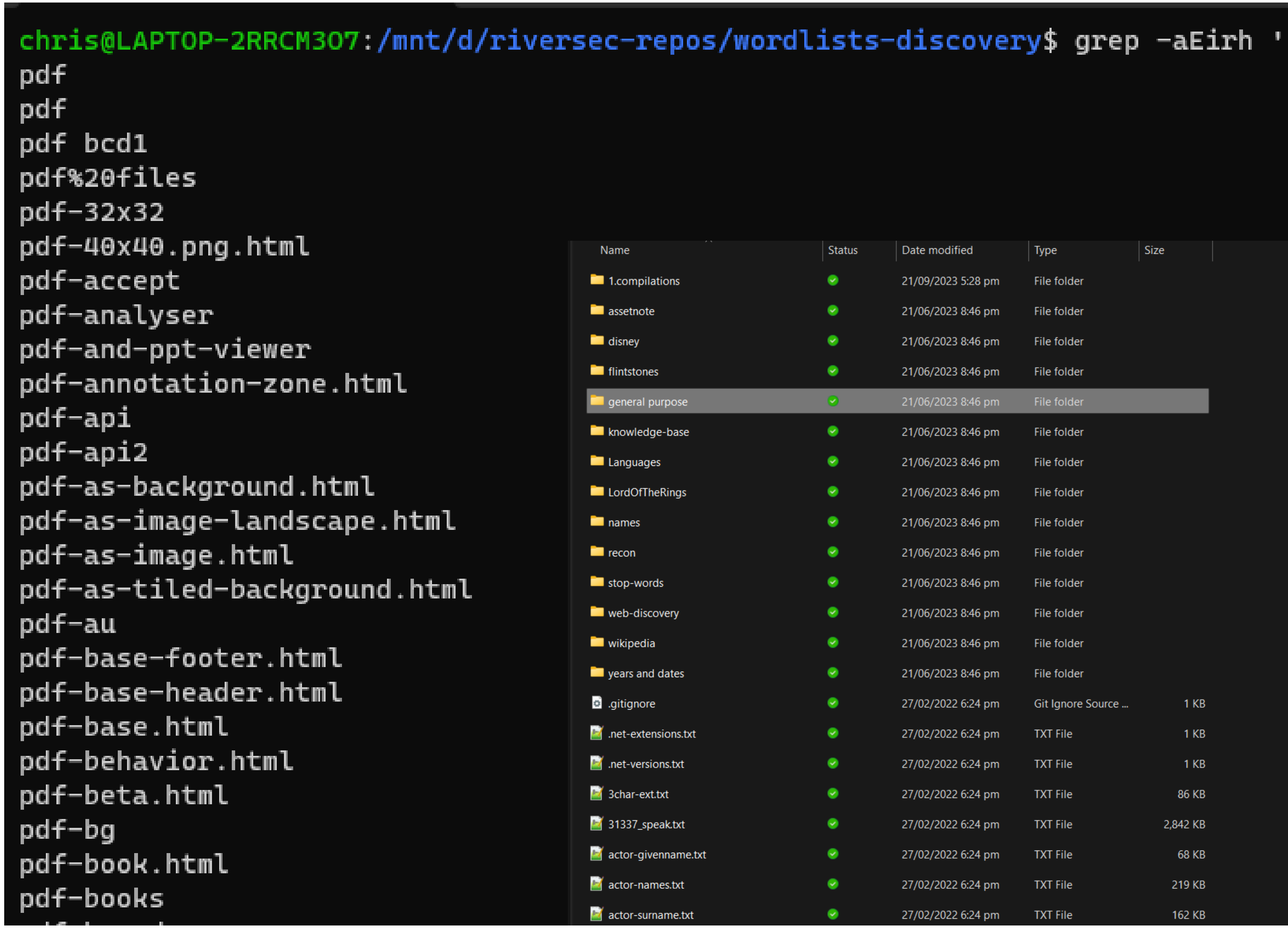
visible
hidden
hide
show
source
backdoor
root
content

Enter a new item

Find Unlinked Content

Content Discovery

- Use and create wordlists based on target functionality
  - Example: A website relevant to *PDF's*
- `grep -aEirh '^pdf.*' * | sort | uniq`

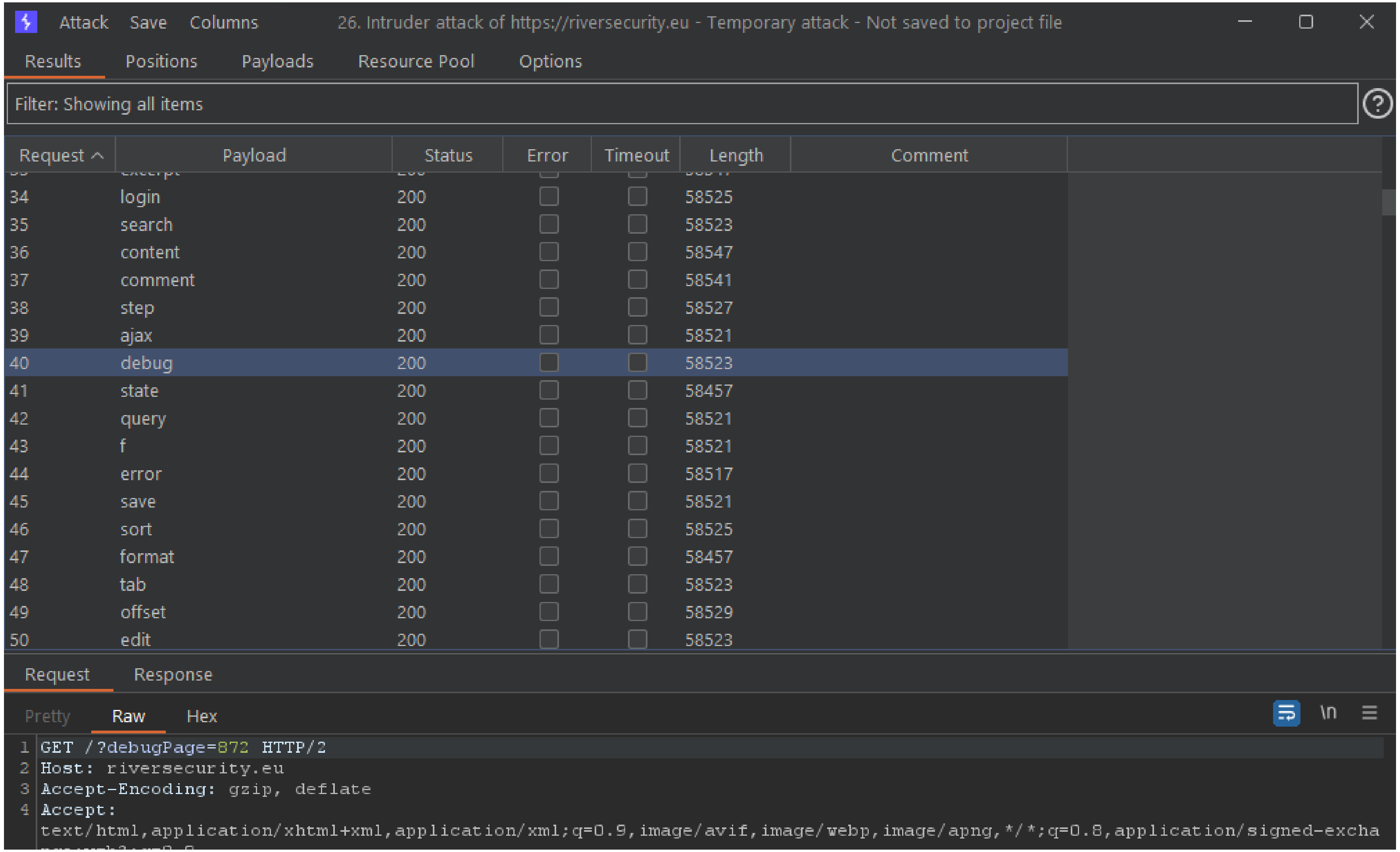


```
chris@LAPTOP-2RRCM3O7:/mnt/d/riversec-repos/wordlists-discovery$ grep -aEirh '
pdf
pdf
pdf bcd1
pdf%20files
pdf-32x32
pdf-40x40.png.html
pdf-accept
pdf-analyser
pdf-and-ppt-viewer
pdf-annotation-zone.html
pdf-api
pdf-api2
pdf-as-background.html
pdf-as-image-landscape.html
pdf-as-image.html
pdf-as-tiled-background.html
pdf-au
pdf-base-footer.html
pdf-base-header.html
pdf-base.html
pdf-behavior.html
pdf-beta.html
pdf-bg
pdf-book.html
pdf-books
```

Name	Status	Date modified	Type	Size
1.compilations	✓	21/09/2023 5:28 pm	File folder	
assetnote	✓	21/06/2023 8:46 pm	File folder	
disney	✓	21/06/2023 8:46 pm	File folder	
flintstones	✓	21/06/2023 8:46 pm	File folder	
general purpose	✓	21/06/2023 8:46 pm	File folder	
knowledge-base	✓	21/06/2023 8:46 pm	File folder	
Languages	✓	21/06/2023 8:46 pm	File folder	
LordOfTheRings	✓	21/06/2023 8:46 pm	File folder	
names	✓	21/06/2023 8:46 pm	File folder	
recon	✓	21/06/2023 8:46 pm	File folder	
stop-words	✓	21/06/2023 8:46 pm	File folder	
web-discovery	✓	21/06/2023 8:46 pm	File folder	
wikipedia	✓	21/06/2023 8:46 pm	File folder	
years and dates	✓	21/06/2023 8:46 pm	File folder	
.gitignore	✓	27/02/2022 6:24 pm	Git Ignore Source ...	1 KB
.net-extensions.txt	✓	27/02/2022 6:24 pm	TXT File	1 KB
.net-versions.txt	✓	27/02/2022 6:24 pm	TXT File	1 KB
3char-ext.txt	✓	27/02/2022 6:24 pm	TXT File	86 KB
31337_speak.txt	✓	27/02/2022 6:24 pm	TXT File	2,842 KB
actor-givenname.txt	✓	27/02/2022 6:24 pm	TXT File	68 KB
actor-names.txt	✓	27/02/2022 6:24 pm	TXT File	219 KB
actor-surname.txt	✓	27/02/2022 6:24 pm	TXT File	162 KB

Verb Example /?page=872

Content Discovery

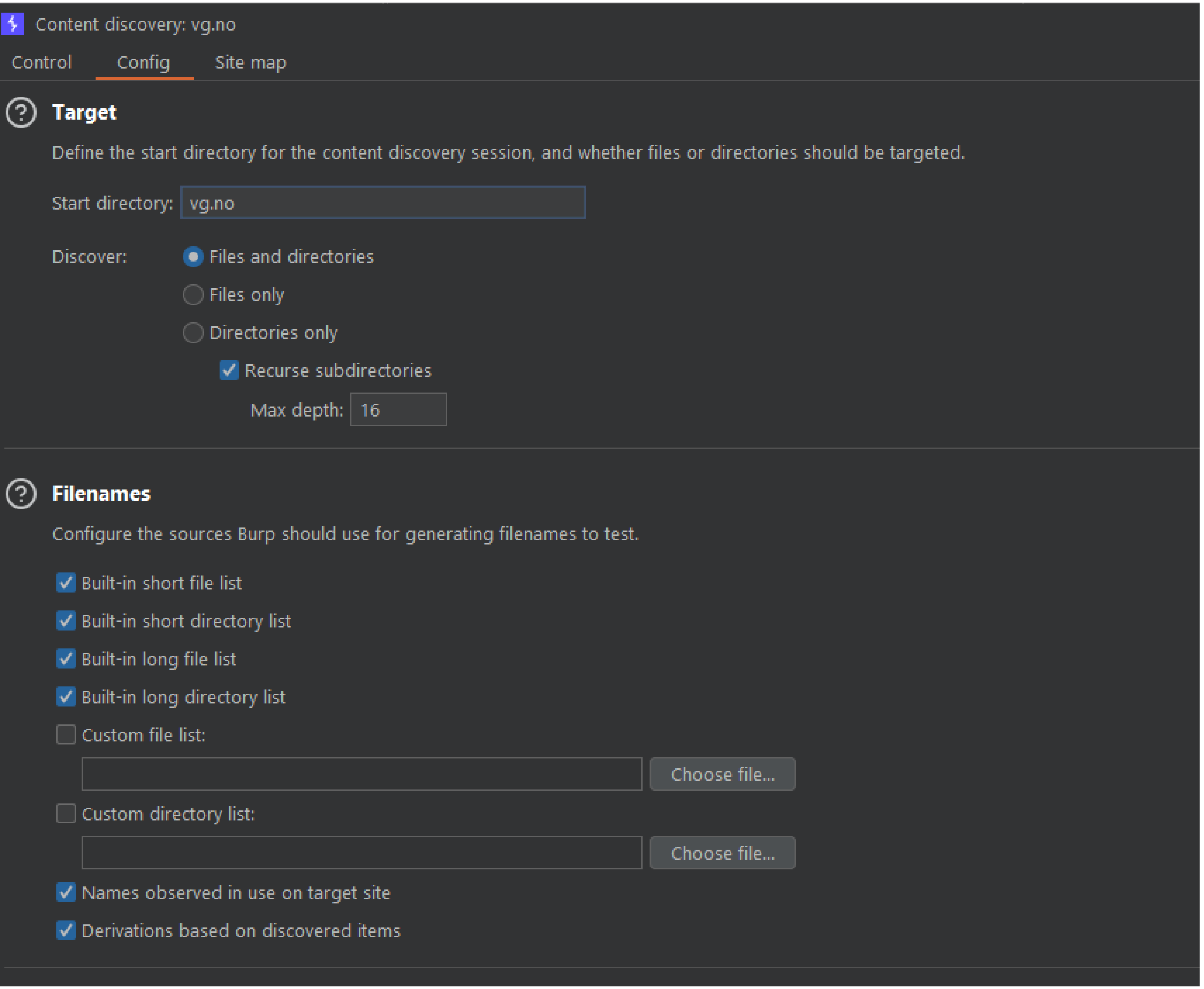

Attack
Save
Columns
26. Intruder attack of https://riversecurity.eu - Temporary attack - Not saved to project file
Results
Positions
Payloads
Resource Pool
Options
Filter: Showing all items
Request
Response
Pretty
Raw
Hex
\n

Request	Payload	Status	Error	Timeout	Length	Comment
34	login	200	□	□	58525	
35	search	200	□	□	58523	
36	content	200	□	□	58547	
37	comment	200	□	□	58541	
38	step	200	□	□	58527	
39	ajax	200	□	□	58521	
40	debug	200	□	□	58523	
41	state	200	□	□	58457	
42	query	200	□	□	58521	
43	f	200	□	□	58521	
44	error	200	□	□	58517	
45	save	200	□	□	58521	
46	sort	200	□	□	58525	
47	format	200	□	□	58457	
48	tab	200	□	□	58523	
49	offset	200	□	□	58529	
50	edit	200	□	□	58523	

```
GET /?debugPage=872 HTTP/2
Host: riversecurity.eu
Accept-Encoding: gzip, deflate
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-excha
```

Content Discovery

Content Discovery



Content discovery: vg.no

Target

Define the start directory for the content discovery session, and whether files or directories should be targeted.

Start directory: vg.no

Discover:
● Files and directories
○ Files only
○ Directories only
☑ Recurse subdirectories
Max depth: 16

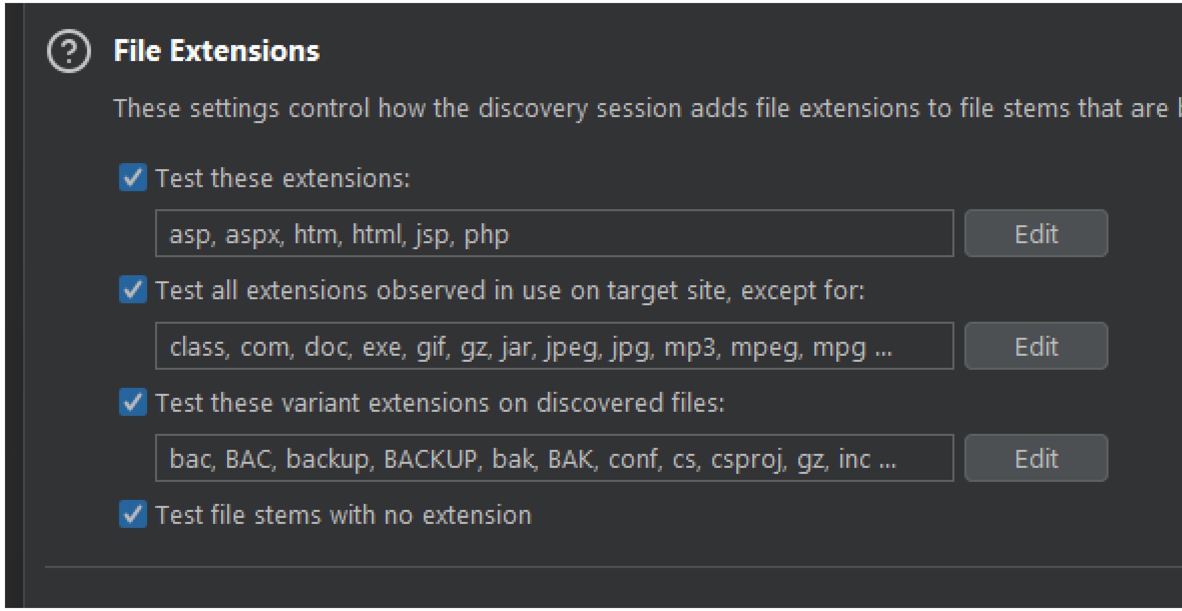
Filenames

Configure the sources Burp should use for generating filenames to test.

☑ Built-in short file list
☑ Built-in short directory list
☑ Built-in long file list
☑ Built-in long directory list
□ Custom file list:

□ Custom directory list:

☑ Names observed in use on target site
☑ Derivations based on discovered items



File Extensions

These settings control how the discovery session adds file extensions to file stems that are l

☑ Test these extensions:
asp, aspx, htm, html, jsp, php

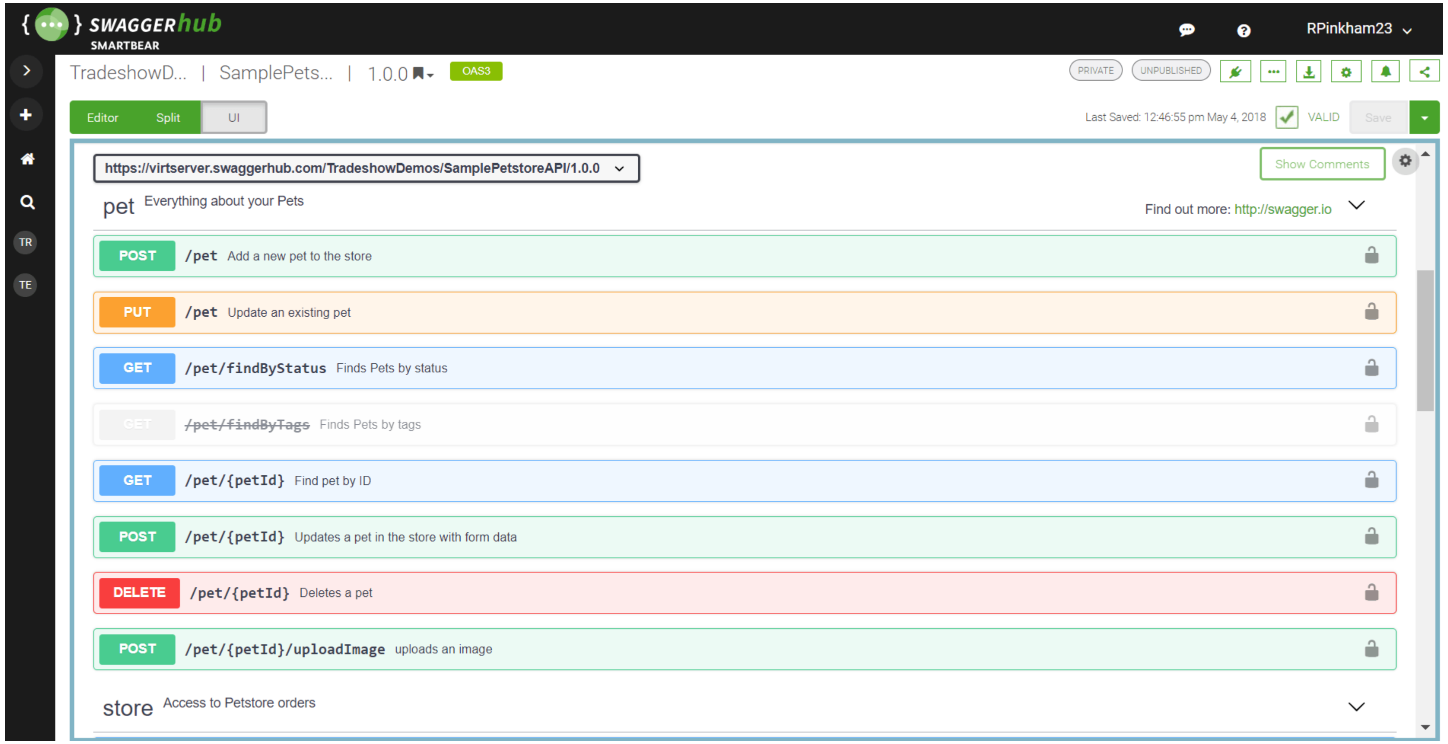
☑ Test all extensions observed in use on target site, except for:
class, com, doc, exe, gif, gz, jar, jpeg, jpg, mp3, mpeg, mpg ...

☑ Test these variant extensions on discovered files:
bac, BAC, backup, BACKUP, bak, BAK, conf, cs, csproj, gz, inc ...

☑ Test file stems with no extension

OpenAPI / Swagger Specs

- If we can cheat, we should!
- Paints a picture of what the developers **intended** to include
- Still requires us to do content discovery



https://virtserver.swaggerhub.com/TradeshowDemos/SamplePetstoreAPI/1.0.0

pet Everything about your Pets

Find out more: http://swagger.io

POST /pet Add a new pet to the store

PUT /pet Update an existing pet

GET /pet/findByStatus Finds Pets by status

GET ~~/pet/findByTags~~ Finds Pets by tags

GET /pet/{petId} Find pet by ID

POST /pet/{petId} Updates a pet in the store with form data

DELETE /pet/{petId} Deletes a pet

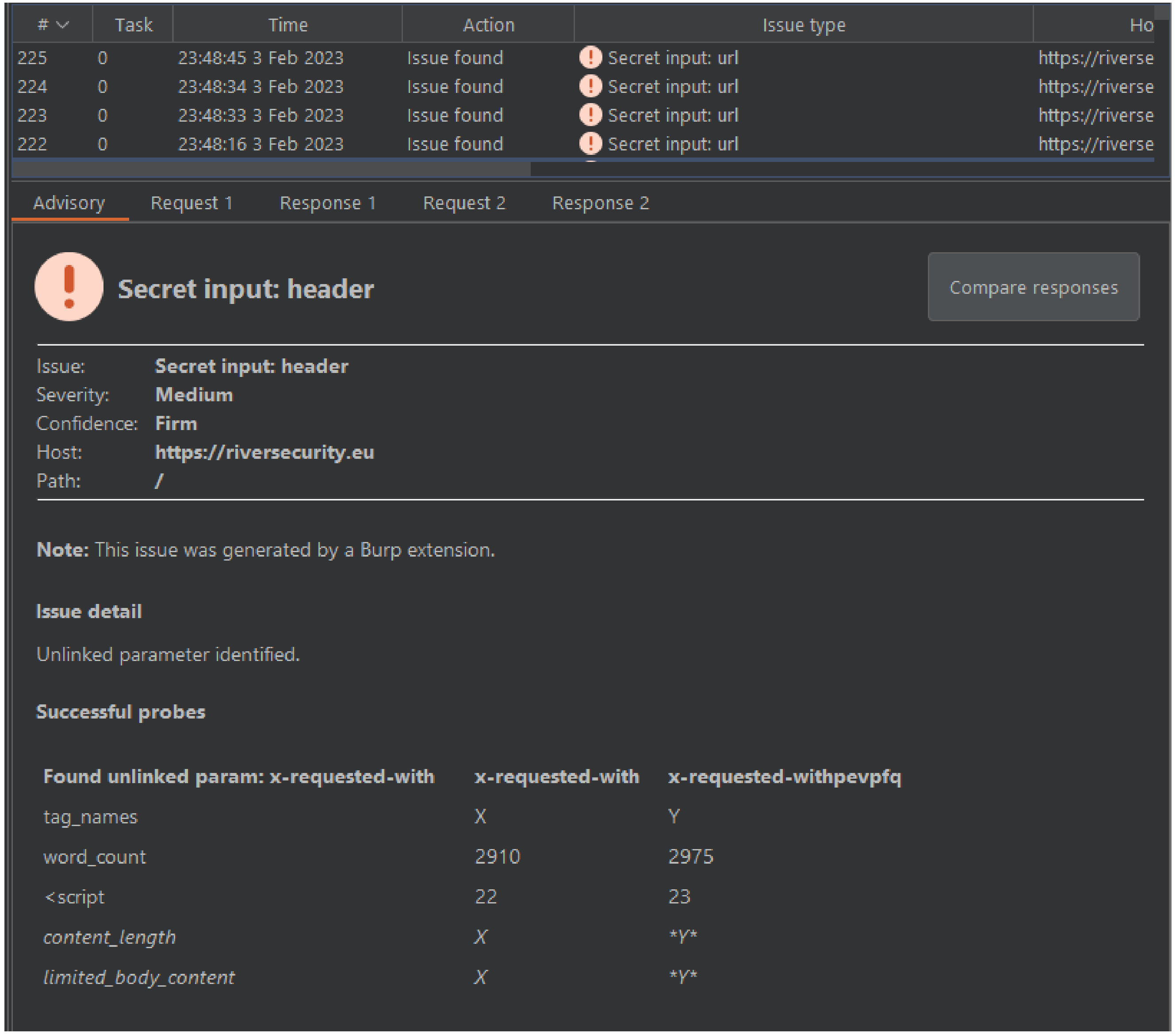
POST /pet/{petId}/uploadImage uploads an image

store Access to Petstore orders

Unlinked Parameters

Content Discovery

- Discover if there are any unlinked parameters
  - Particularly important on all Platform Distinctions
  - Any change based on a new parameter is interesting
  - GET, POST, Cookies, Headers
- Headers might bypass authentication
- Might find attack surface
- **Param miner extension!**



#	Task	Time	Action	Issue type	Ho
225	0	23:48:45 3 Feb 2023	Issue found	! Secret input: url	https://riverse
224	0	23:48:34 3 Feb 2023	Issue found	! Secret input: url	https://riverse
223	0	23:48:33 3 Feb 2023	Issue found	! Secret input: url	https://riverse
222	0	23:48:16 3 Feb 2023	Issue found	! Secret input: url	https://riverse

Secret input: header

Issue:	**Secret input: header**
Severity:	**Medium**
Confidence:	**Firm**
Host:	**https://riversecurity.eu**
Path:	**/**

Note: This issue was generated by a Burp extension.

Issue detail

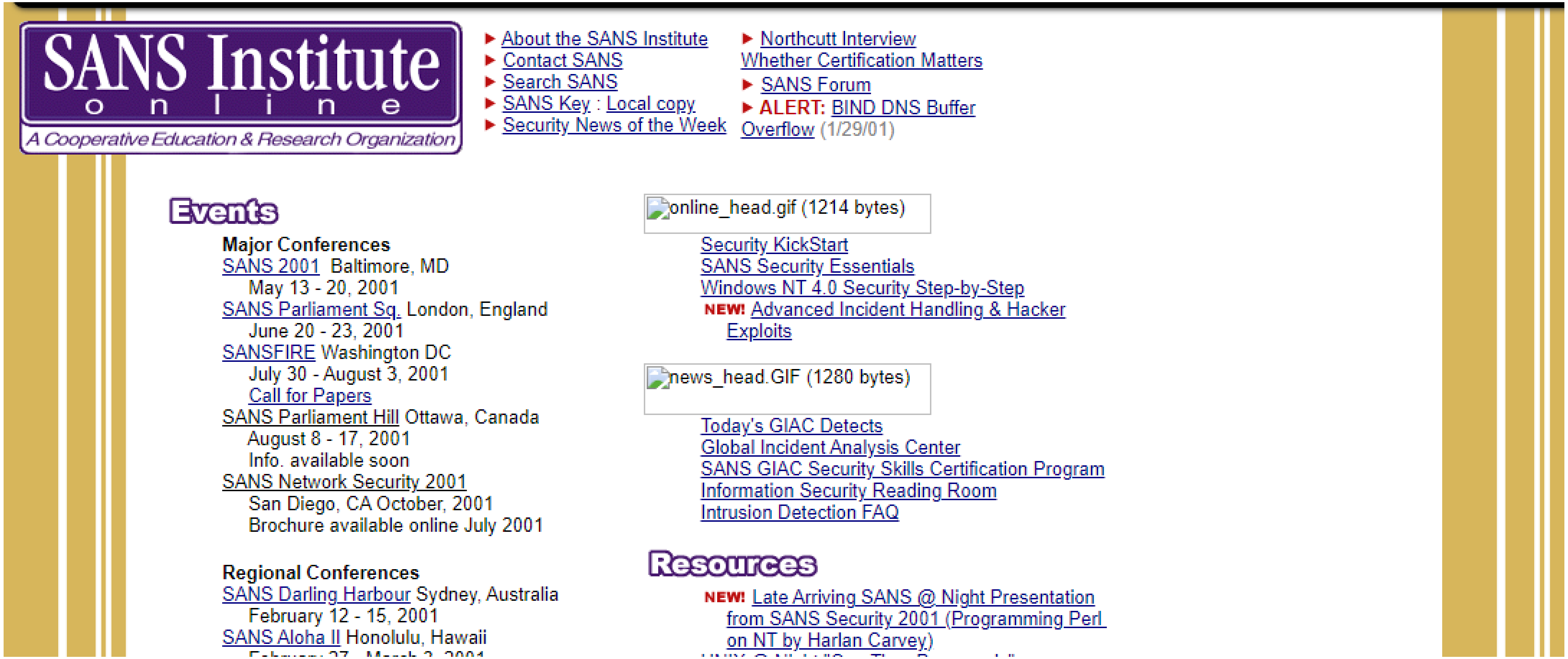
Unlinked parameter identified.

Successful probes

Found unlinked param: x-requested-with	x-requested-with	x-requested-withpevpfq
tag_names	X	Y
word_count	2910	2975
<script	22	23
content_length	*X*	**Y**
limited_body_content	*X*	**Y**

OSINT to Support

- WaybackRobots.py
- WaybackURLs.py
- Dorking
- Other OSINT sources



SANS Institute online

A Cooperative Education & Research Organization

- About the SANS Institute
- Contact SANS
- Search SANS
- SANS Key : Local copy
- Security News of the Week
- Northcutt Interview Whether Certification Matters
- SANS Forum
- ALERT: BIND DNS Buffer Overflow (1/29/01)

Events

Major Conferences
SANS 2001 Baltimore, MD
May 13 - 20, 2001
SANS Parliament Sq. London, England
June 20 - 23, 2001
SANSFIRE Washington DC
July 30 - August 3, 2001
Call for Papers
SANS Parliament Hill Ottawa, Canada
August 8 - 17, 2001
Info. available soon
SANS Network Security 2001
San Diego, CA October, 2001
Brochure available online July 2001

Regional Conferences
SANS Darling Harbour Sydney, Australia
February 12 - 15, 2001
SANS Aloha II Honolulu, Hawaii
February 27 - March 2, 2001

online_head.gif (1214 bytes)

Security KickStart
SANS Security Essentials
Windows NT 4.0 Security Step-by-Step
NEW! Advanced Incident Handling & Hacker Exploits

news_head.GIF (1280 bytes)

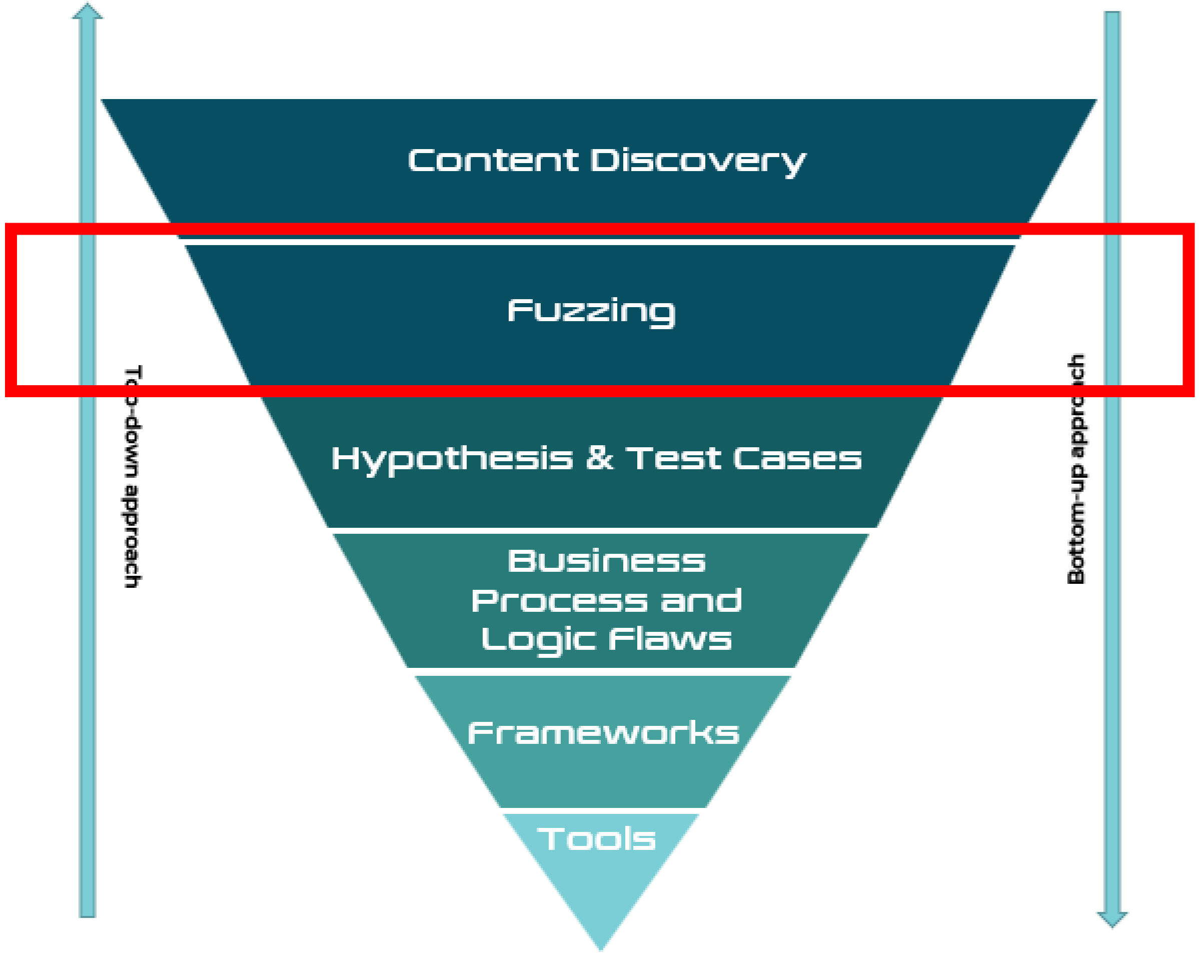
Today's GIAC Detects
Global Incident Analysis Center
SANS GIAC Security Skills Certification Program
Information Security Reading Room
Intrusion Detection FAQ

Resources

NEW! Late Arriving SANS @ Night Presentation from SANS Security 2001 (Programming Perl on NT by Harlan Carvey)

Fuzzing

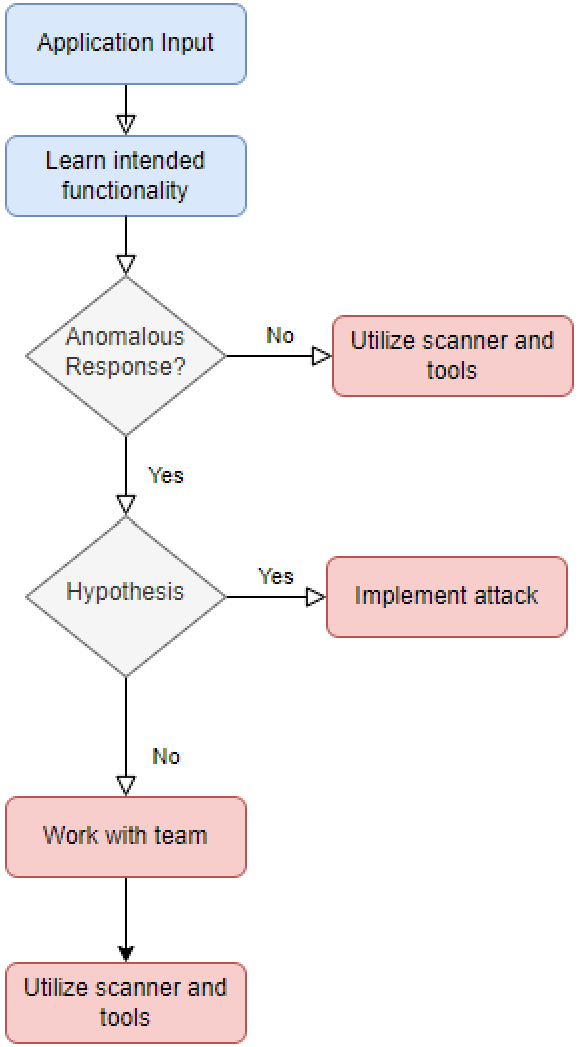
Find bytes and input producing different/unexpected results



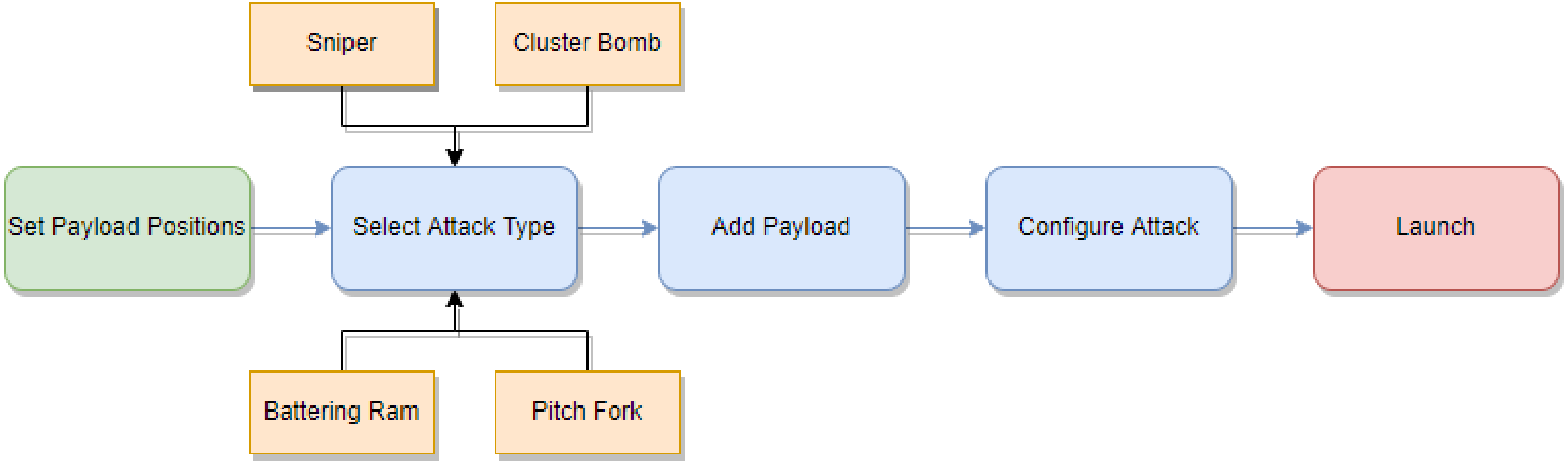
Fuzzing Bytes 101

Fuzzing

1. For-each script and input
2. Send their script to repeater / play with it in browser
   - Determine properly how the functionality works and try related attack
3. Send to intruder and fuzz
   - %00 to %FF
     - URL Decode targets Middleware
     - URL Encode targets App
   - Anomalies, discrepancies, interesting results?
     - Create Hypothesis
     - Work with team if you cannot produce hypothesis
   - Use wordlists
4. Utilize vulnerability scanner
   - Backslash Powered Scanner and other extensions will also aid here.
5. Scanner results? Update methodology



Fuzzing



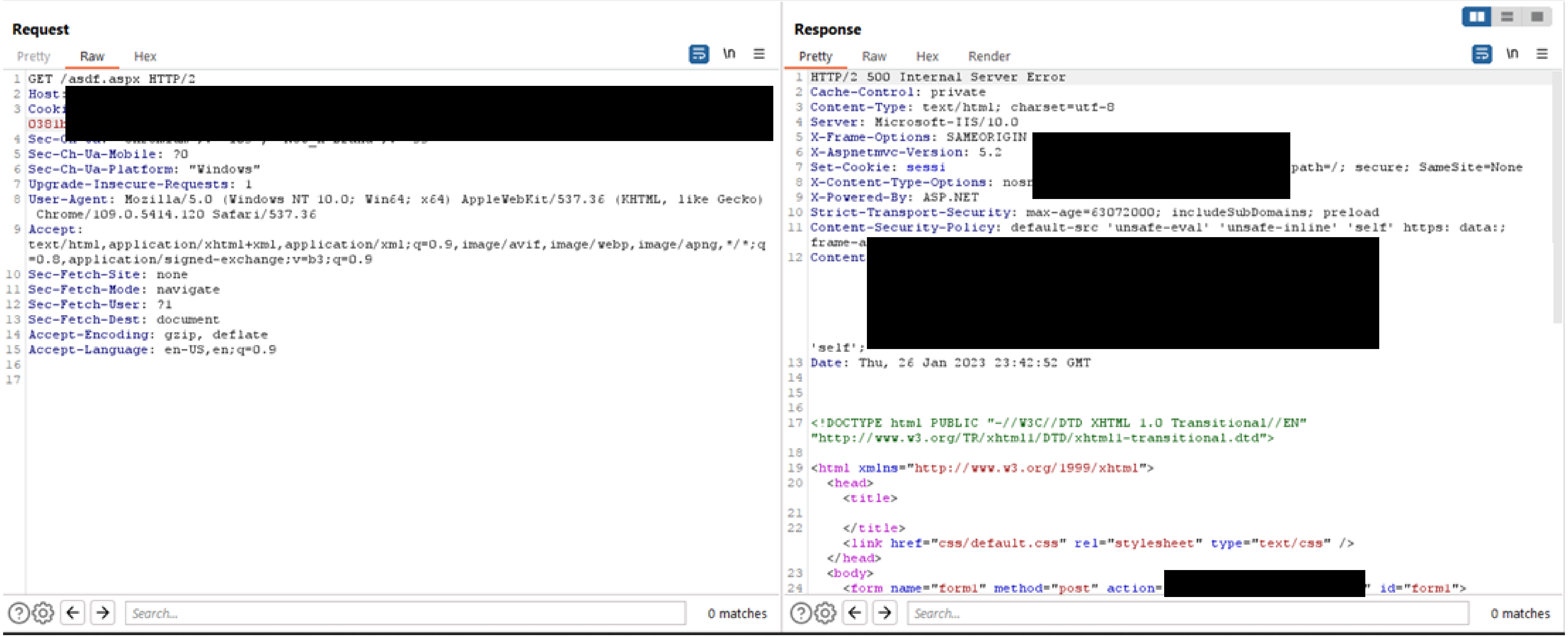
Fuzzing is not one size fits all, our goal is to produce interesting results. Be creative!

Attack Types

- Position – This is a variable where you want to inject a payload of a certain kind, e.g. a word a wordlist.
- Sniper – Loop a payload through all positions
- Cluster Bomb – Loop through multiple payloads through all positions, like nested for loops.
- Battering Jam – Push through one payload into each position at the same time.
- Pitch Fork – Apply a set of payloads for each position which is iterated at the same time

Asdf.aspx produces 500 server error

Fuzzing



Request

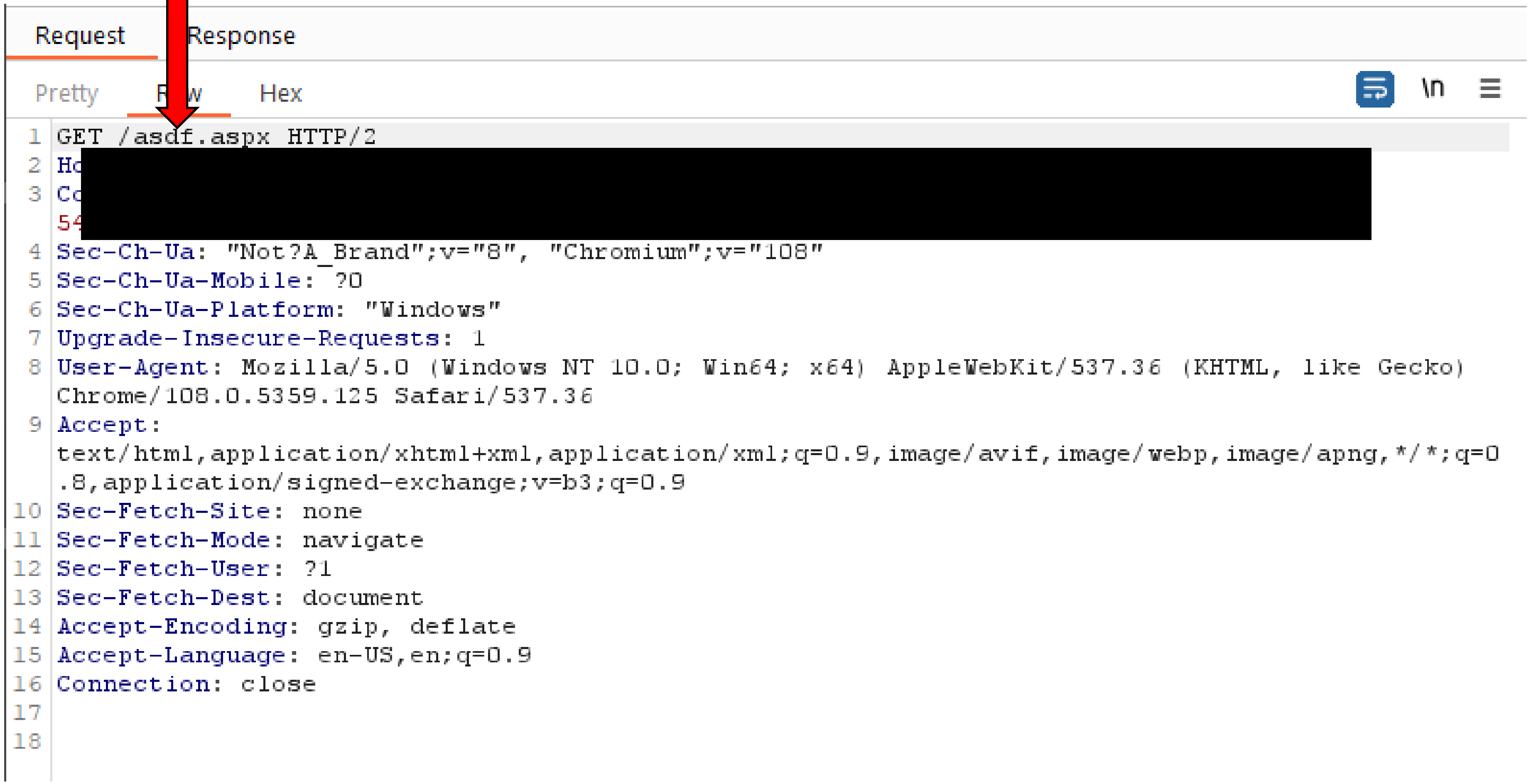
```
GET /asdf.aspx HTTP/2
Host[redacted]
Cooki
0381b
Sec-C
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
 Chrome/109.0.5414.120 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q
=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9


```

Response

```
HTTP/2 500 Internal Server Error
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/10.0
X-Frame-Options: SAMEORIGIN [redacted]
X-Aspnetmvc-Version: 5.2
Set-Cookie: sessi path=/; secure; SameSite=None
X-Content-Type-Options: nosn
X-Powered-By: ASP.NET
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
Content-Security-Policy: default-src 'unsafe-eval' 'unsafe-inline' 'self' https: data:;
frame-a[redacted]
Content



'self';
Date: Thu, 26 Jan 2023 23:42:52 GMT



<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <title>

    </title>
    <link href="css/default.css" rel="stylesheet" type="text/css" />
  </head>
  <body>
    <form name="form1" method="post" action=[redacted]" id="form1">
```

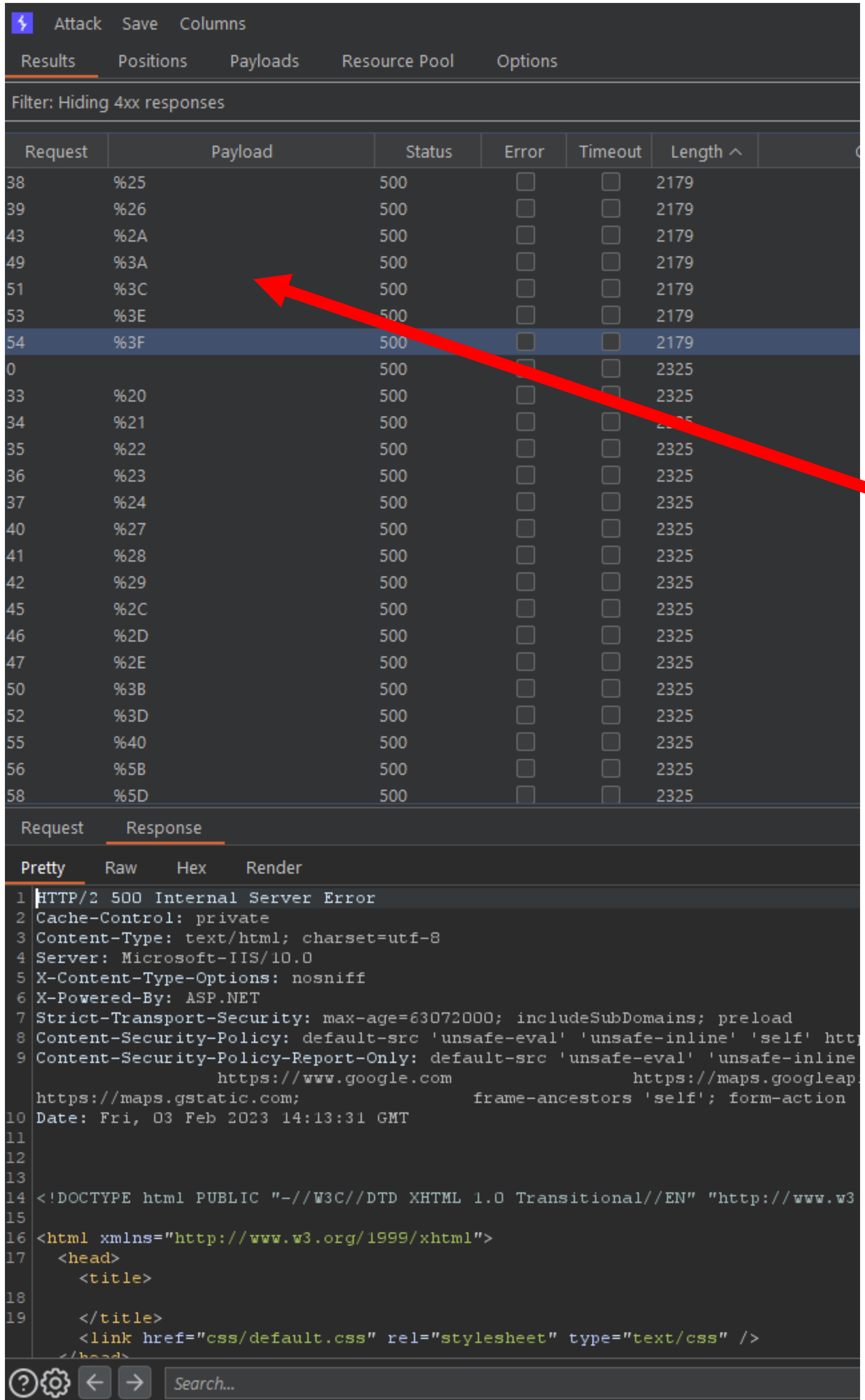
Bytes Examples

Payload here



```
GET /asdf.aspx HTTP/2
[redacted]
Sec-Ch-Ua: "Not?A_Brand";v="8", "Chromium";v="108"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.125 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close


```

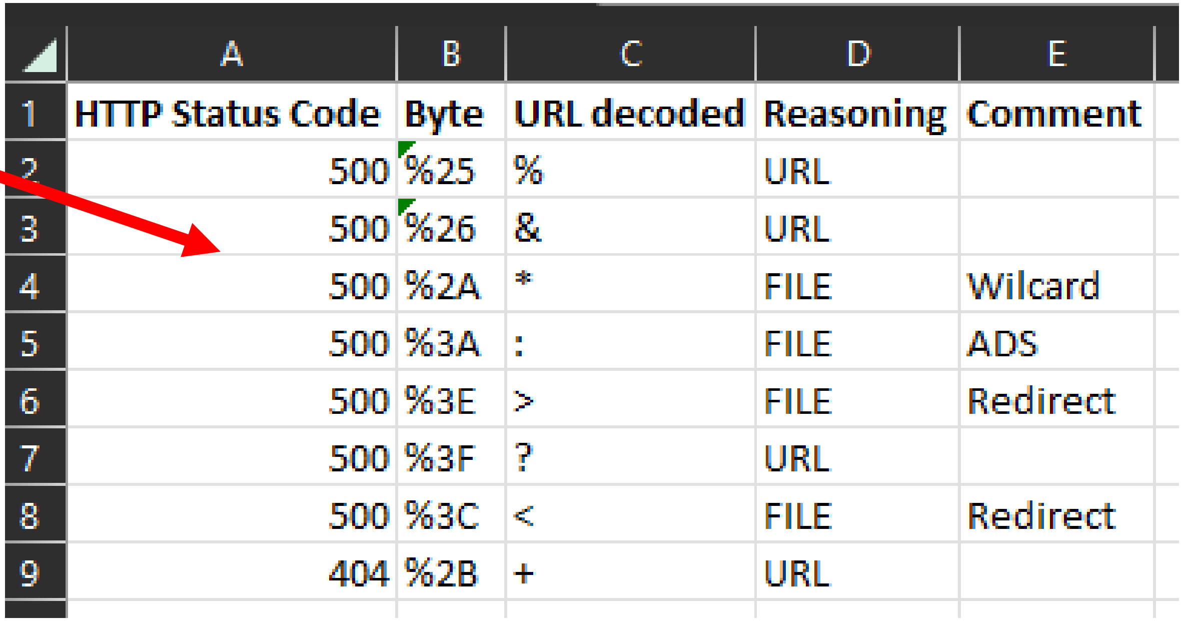
Fuzzing



Filter: Hiding 4xx responses

Request	Payload	Status	Error	Timeout	Length
38	%25	500	□	□	2179
39	%26	500	□	□	2179
43	%2A	500	□	□	2179
49	%3A	500	□	□	2179
51	%3C	500	□	□	2179
53	%3E	500	□	□	2179
54	%3F	500	□	□	2179
0		500	□	□	2325
33	%20	500	□	□	2325
34	%21	500	□	□	2325
35	%22	500	□	□	2325
36	%23	500	□	□	2325
37	%24	500	□	□	2325
40	%27	500	□	□	2325
41	%28	500	□	□	2325
42	%29	500	□	□	2325
45	%2C	500	□	□	2325
46	%2D	500	□	□	2325
47	%2E	500	□	□	2325
50	%3B	500	□	□	2325
52	%3D	500	□	□	2325
55	%40	500	□	□	2325
56	%5B	500	□	□	2325
58	%5D	500	□	□	2325

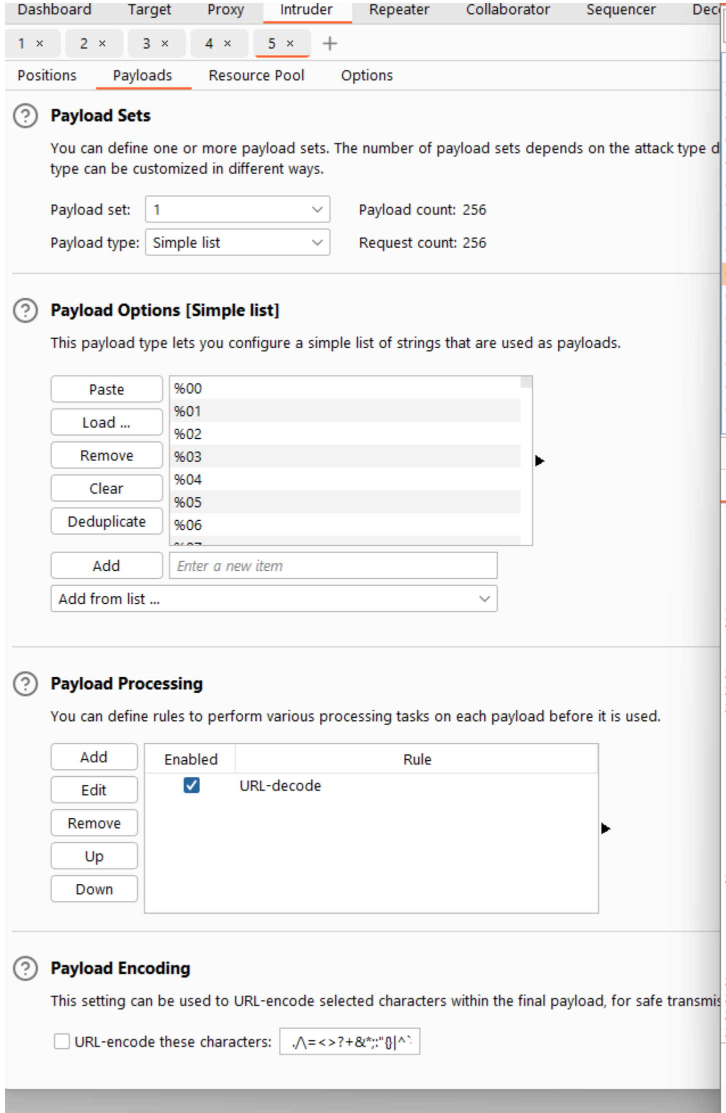
```
HTTP/2 500 Internal Server Error
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/10.0
X-Content-Type-Options: nosniff
X-Powered-By: ASP.NET
Strict-Transport-Security: max-age=63072000; includeSubDomains; preload
Content-Security-Policy: default-src 'unsafe-eval' 'unsafe-inline' 'self' htt
Content-Security-Policy-Report-Only: default-src 'unsafe-eval' 'unsafe-inline
                 https://www.google.com                 https://maps.googleap
https://maps.gstatic.com;                 frame-ancestors 'self'; form-action
Date: Fri, 03 Feb 2023 14:13:31 GMT



<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3

<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <title>

    </title>
    <link href="css/default.css" rel="stylesheet" type="text/css" />
```



	A	B	C	D	E
1	HTTP Status Code	Byte	URL decoded	Reasoning	Comment
2	500	%25	%	URL	
3	500	%26	&	URL	
4	500	%2A	*	FILE	Wilcard
5	500	%3A	:	FILE	ADS
6	500	%3E	>	FILE	Redirect
7	500	%3F	?	URL	
8	500	%3C	<	FILE	Redirect
9	404	%2B	+	URL	

Second example: A Single Character

Fuzzing



Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type d type can be customized in different ways.

Payload set: 1 Payload count: 256

Payload type: Simple list Request count: 256

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

```
%00
%01
%02
%03
%04
%05
%06
```

Payload Processing

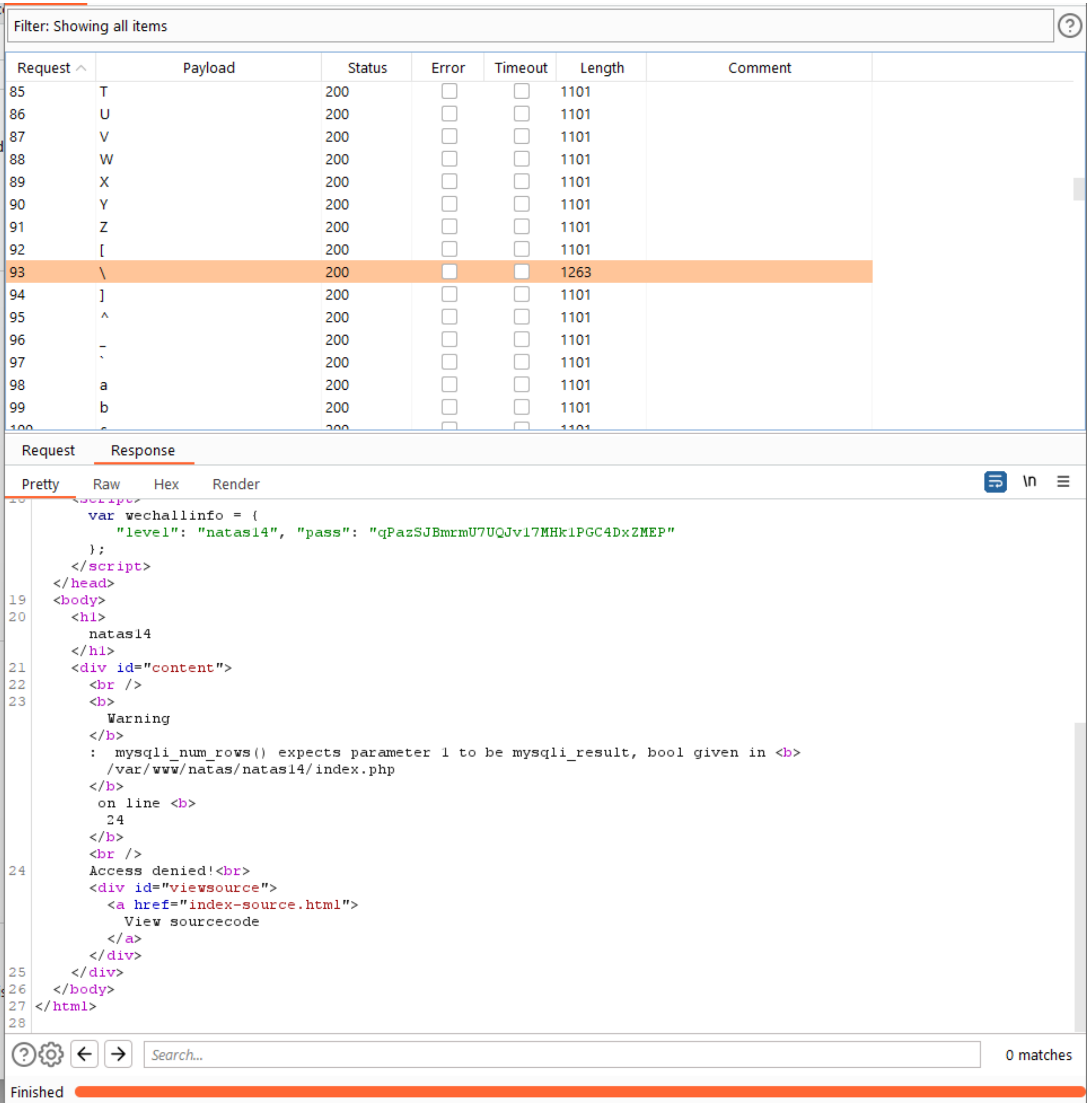
You can define rules to perform various processing tasks on each payload before it is used.

Enabled	Rule
☑	URL-decode

Payload Encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmis

□ URL-encode these characters: ./\=<>?+&*;:"{}|^`


Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
85	T	200	□	□	1101	
86	U	200	□	□	1101	
87	V	200	□	□	1101	
88	W	200	□	□	1101	
89	X	200	□	□	1101	
90	Y	200	□	□	1101	
91	Z	200	□	□	1101	
92	[	200	□	□	1101	
93	\	200	□	□	1263	
94	]	200	□	□	1101	
95	^	200	□	□	1101	
96	_	200	□	□	1101	
97	`	200	□	□	1101	
98	a	200	□	□	1101	
99	b	200	□	□	1101	

```
      var wechallinfo = {
        "level": "natas14", "pass": "qPazSJBmrmU7UQJv17MHk1PGC4DxZMEP"
      };
    </script>
  </head>
  <body>
    <h1>
      natas14
    </h1>
    <div id="content">
      <br />
      <b>
        Warning
      </b>
      :  mysqli_num_rows() expects parameter 1 to be mysqli_result, bool given in <b>
        /var/www/natas/natas14/index.php
      </b>
       on line <b>
        24
      </b>
      <br />
      Access denied!<br>
      <div id="viewsource">
        <a href="index-source.html">
          View sourcecode
        </a>
      </div>
    </div>
  </body>
</html>
```

Fuzzing

This Photo by Unknown Author is licensed under CC BY

Occam’s Razor

Among competing hypothesis, the one with the fewest hypothesis is often correct.

Avoiding Rabbit Holes

- A rabbit hole is: A potential exploit condition which will take up a lot of time to research.
- Prioritize “**width**” rather than “**depth**”
  - Focus on rabbit holes with the time left after the scope is covered
- Structure your work and scope
  - Duration of the engagement vs. How much time do we have left?
  - Hours spent – Work left
    - Each hour spent impacts the total value spent on the engagement
  - How many scripts, functions and other things do we have left to test?
  - **Do we need to get someone else to help us conclude a rabbit hole?**
- Large applications: split into smaller parts to help team prioritize

Using Wordlists

With our fuzzing efforts, wordlists can help produce valuable results, e.g., anomalies in cases of:

- Different HTML or HTTP results
- Timing differences
- External server interaction

Use wordlists that help you target different technology and hypothesis.

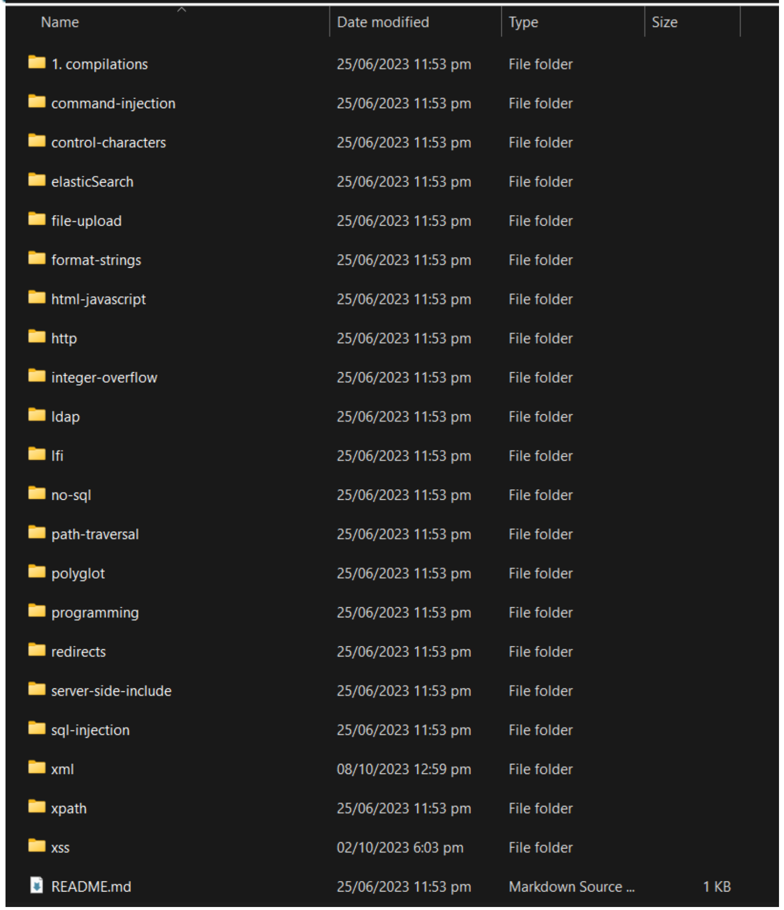
Great starting points:

- SecLists: https://github.com/danielmiessler/SecLists
- AssetNote: https://wordlists.assetnote.io/

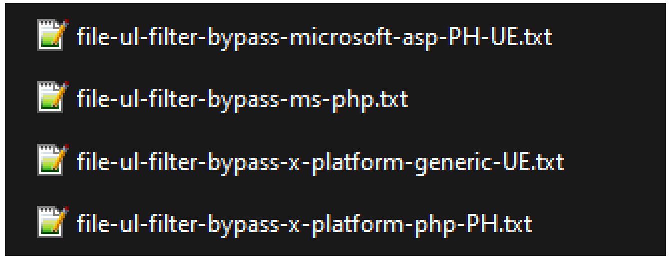
Take time to learn what these wordlists contain; it will help you learn when to apply them

- Which wordlists requires placeholders?
- Which ones are already URL encoded?

Fuzzing



Name	Date modified	Type	Size
1. compilations	25/06/2023 11:53 pm	File folder	
command-injection	25/06/2023 11:53 pm	File folder	
control-characters	25/06/2023 11:53 pm	File folder	
elasticSearch	25/06/2023 11:53 pm	File folder	
file-upload	25/06/2023 11:53 pm	File folder	
format-strings	25/06/2023 11:53 pm	File folder	
html-javascript	25/06/2023 11:53 pm	File folder	
http	25/06/2023 11:53 pm	File folder	
integer-overflow	25/06/2023 11:53 pm	File folder	
ldap	25/06/2023 11:53 pm	File folder	
lfi	25/06/2023 11:53 pm	File folder	
no-sql	25/06/2023 11:53 pm	File folder	
path-traversal	25/06/2023 11:53 pm	File folder	
polyglot	25/06/2023 11:53 pm	File folder	
programming	25/06/2023 11:53 pm	File folder	
redirects	25/06/2023 11:53 pm	File folder	
server-side-include	25/06/2023 11:53 pm	File folder	
sql-injection	25/06/2023 11:53 pm	File folder	
xml	08/10/2023 12:59 pm	File folder	
xpath	25/06/2023 11:53 pm	File folder	
xss	02/10/2023 6:03 pm	File folder	
README.md	25/06/2023 11:53 pm	Markdown Source ...	1 KB



file-ul-filter-bypass-microsoft-asp-PH-UE.txt

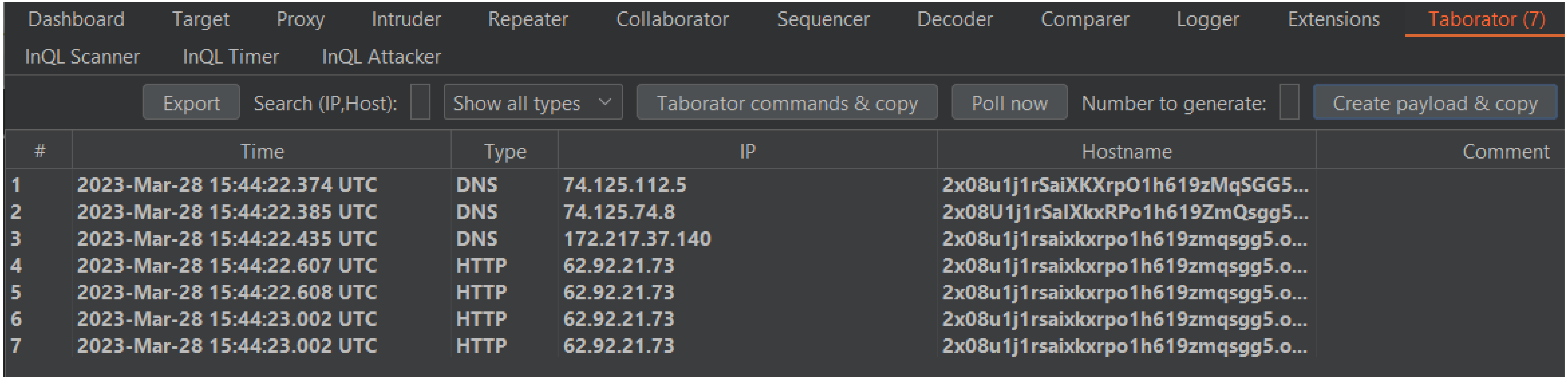
file-ul-filter-bypass-ms-php.txt

file-ul-filter-bypass-x-platform-generic-UE.txt

file-ul-filter-bypass-x-platform-php-PH.txt

Use Collaborator with placeholders

- Many wordlists rely on external server interaction.
- Burp Suite has a built in external interaction monitor
- Taborator plugin makes for quick access to Collaborator
  - Or use interactsh https://github.com/projectdiscovery/interactsh

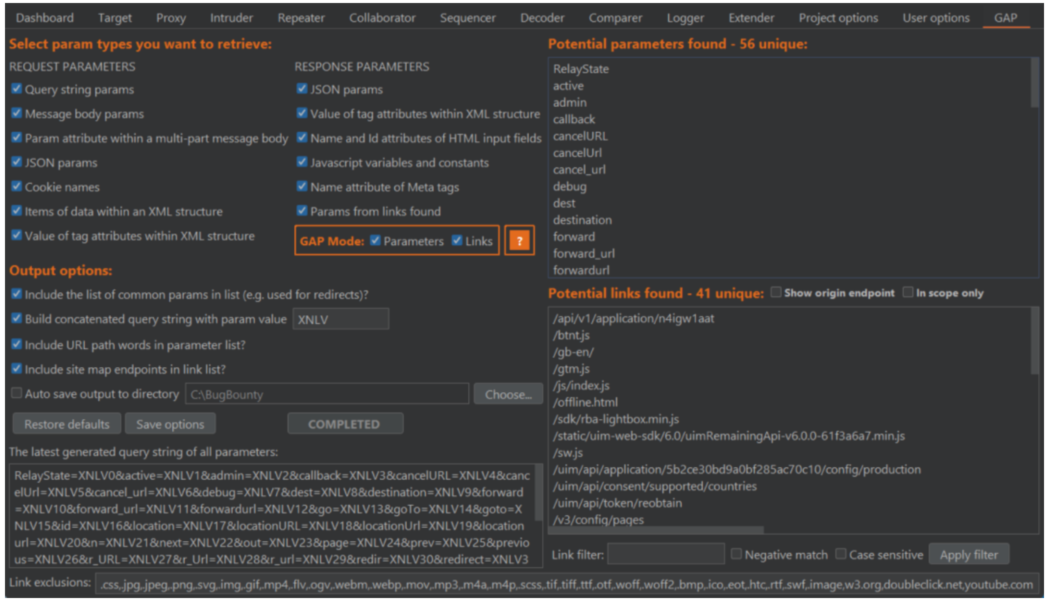


#	Time	Type	IP	Hostname	Comment
1	2023-Mar-28 15:44:22.374 UTC	DNS	74.125.112.5	2x08u1j1rSaiXKXrpO1h619zMqSGG5...	
2	2023-Mar-28 15:44:22.385 UTC	DNS	74.125.74.8	2x08U1j1rSaIXkxRPo1h619ZmQsgg5...	
3	2023-Mar-28 15:44:22.435 UTC	DNS	172.217.37.140	2x08u1j1rsaixkxrpo1h619zmqsgg5.o...	
4	2023-Mar-28 15:44:22.607 UTC	HTTP	62.92.21.73	2x08u1j1rsaixkxrpo1h619zmqsgg5.o...	
5	2023-Mar-28 15:44:22.608 UTC	HTTP	62.92.21.73	2x08u1j1rsaixkxrpo1h619zmqsgg5.o...	
6	2023-Mar-28 15:44:23.002 UTC	HTTP	62.92.21.73	2x08u1j1rsaixkxrpo1h619zmqsgg5.o...	
7	2023-Mar-28 15:44:23.002 UTC	HTTP	62.92.21.73	2x08u1j1rsaixkxrpo1h619zmqsgg5.o...	

Building Good Wordlists

Fuzzing

- Roy Solberg's CeWLer
  - Filter away stop-words
- Burp Suite GAP extension
- URL Shorteners bruteforce results
- http_disallowed_entries_CiscoTopMillion
- Wiki’s are a good source of wordlist



Select param types you want to retrieve:

REQUEST PARAMETERS

- ☑ Query string params
- ☑ Message body params
- ☑ Param attribute within a multi-part message body
- ☑ JSON params
- ☑ Cookie names
- ☑ Items of data within an XML structure
- ☑ Value of tag attributes within XML structure

RESPONSE PARAMETERS

- ☑ JSON params
- ☑ Value of tag attributes within XML structure
- ☑ Name and Id attributes of HTML input fields
- ☑ Javascript variables and constants
- ☑ Name attribute of Meta tags
- ☑ Params from links found

GAP Mode: ☑ Parameters ☑ Links ?

Output options:

- ☑ Include the list of common params in list (e.g. used for redirects)?
- ☑ Build concatenated query string with param value XNLV
- ☑ Include URL path words in parameter list?
- ☑ Include site map endpoints in link list?
- □ Auto save output to directory C:\BugBounty Choose...

Restore defaults | Save options | COMPLETED

The latest generated query string of all parameters:

```
RelayState=XNLV0&active=XNLV1&admin=XNLV2&callback=XNLV3&cancelURL=XNLV4&canc
elUrl=XNLV5&cancel_url=XNLV6&debug=XNLV7&dest=XNLV8&destination=XNLV9&forward
=XNLV10&forward_url=XNLV11&forwardurl=XNLV12&go=XNLV13&goTo=XNLV14&goto=X
NLV15&id=XNLV16&location=XNLV17&locationURL=XNLV18&locationUrl=XNLV19&location
url=XNLV20&n=XNLV21&next=XNLV22&out=XNLV23&page=XNLV24&prev=XNLV25&previo
us=XNLV26&r_URL=XNLV27&r_Url=XNLV28&r_url=XNLV29&redir=XNLV30&redirect=XNLV3
```

Potential parameters found - 56 unique:

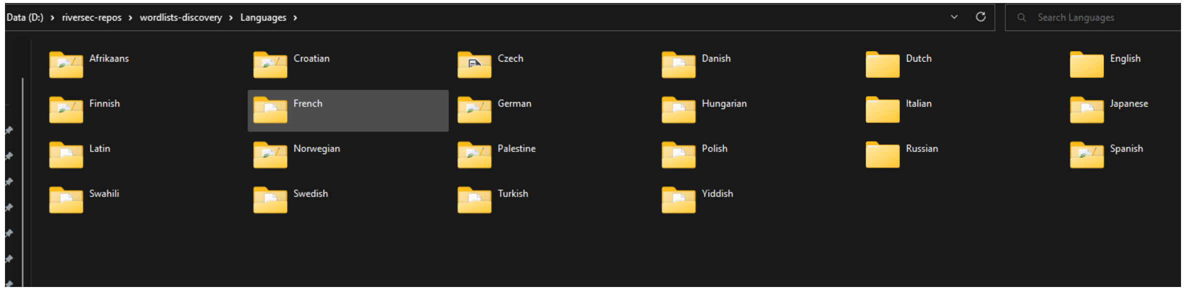
```
RelayState
active
admin
callback
cancelURL
cancelUrl
cancel_url
debug
dest
destination
forward
forward_url
forwardurl
```

Potential links found - 41 unique: □ Show origin endpoint □ In scope only

```
/api/v1/application/n4igw1aat
/btnt.js
/gb-en/
/gtm.js
/js/index.js
/offline.html
/sdk/rba-lightbox.min.js
/static/uim-web-sdk/6.0/uimRemainingApi-v6.0.0-61f3a6a7.min.js
/sw.js
/uim/api/application/5b2ce30bd9a0bf285ac70c10/config/production
/uim/api/consent/supported/countries
/uim/api/token/reobtain
/v3/config/pages
```

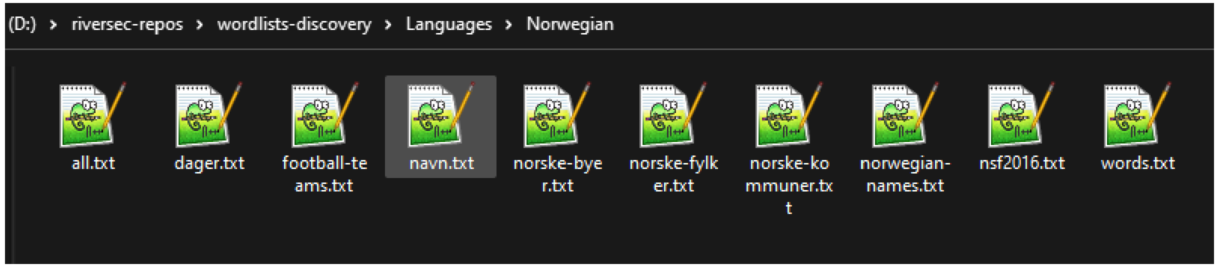
Link filter: □ Negative match □ Case sensitive Apply filter

Link exclusions: .css,.jpg,.jpeg,.png,.svg,.img,.gif,.mp4,.flv,.ogv,.webm,.webp,.mov,.mp3,.m4a,.m4p,.scss,.tif,.tiff,.ttf,.otf,.woff,.woff2,.bmp,.ico,.eot,.htc,.rtf,.swf,.image,w3.org,doubleclick.net,youtube.com



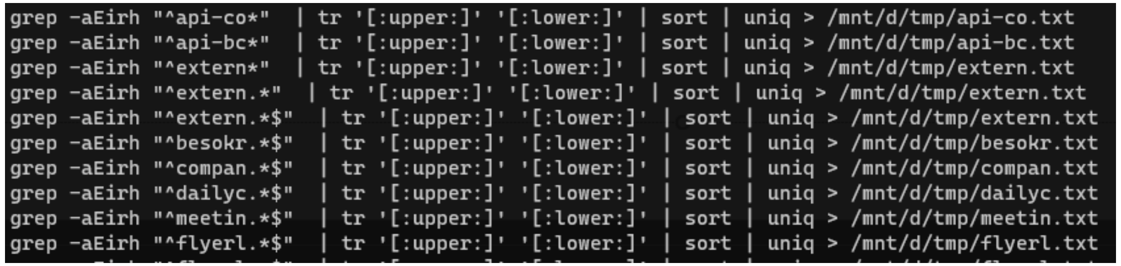
Data (D:) › riversec-repos › wordlists-discovery › Languages ›

Afrikaans, Croatian, Czech, Danish, Dutch, English, Finnish, French, German, Hungarian, Italian, Japanese, Latin, Norwegian, Palestine, Polish, Russian, Spanish, Swahili, Swedish, Turkish, Yiddish



(D:) › riversec-repos › wordlists-discovery › Languages › Norwegian

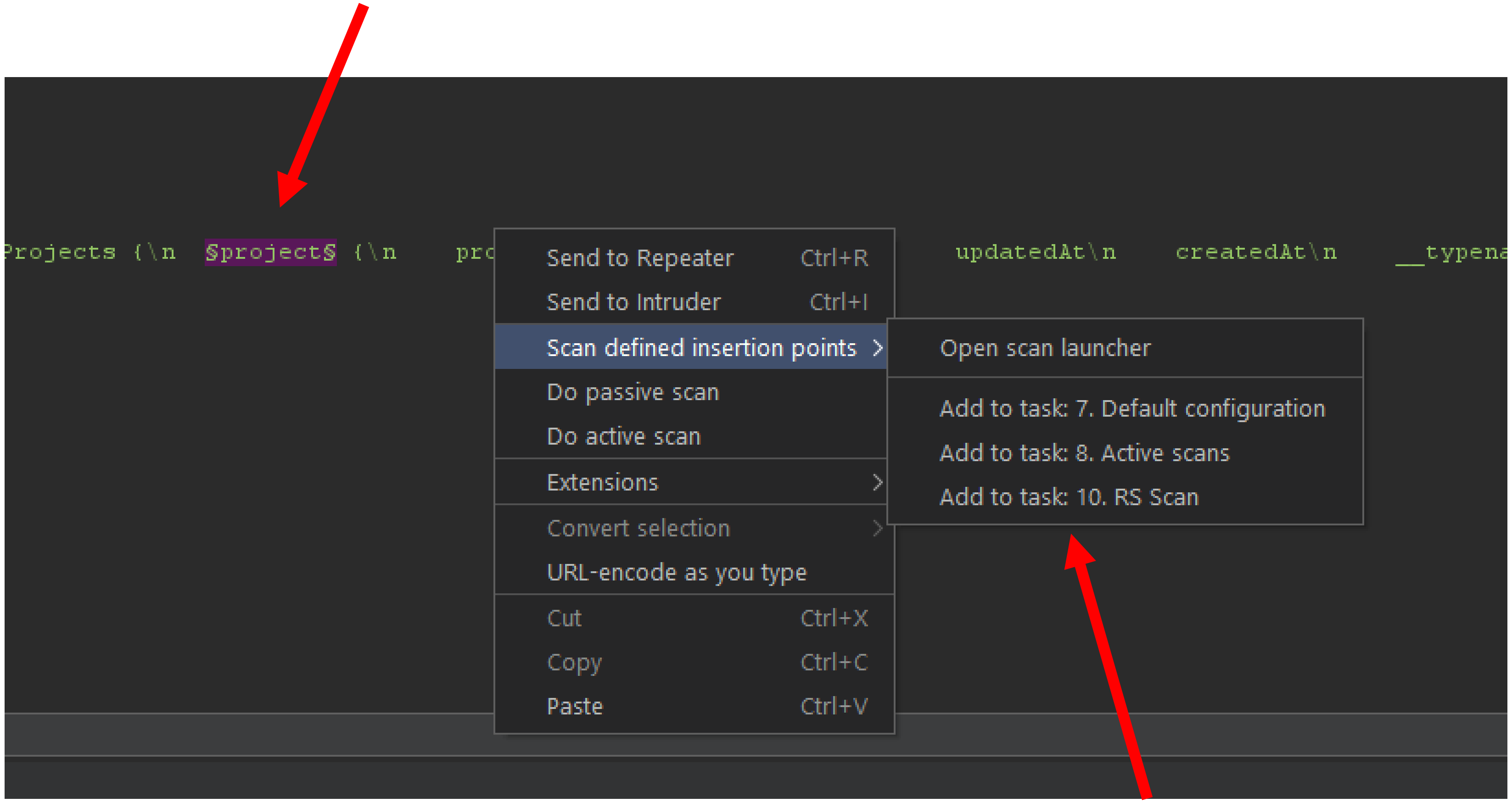
all.txt, dager.txt, football-teams.txt, navn.txt, norske-byer.txt, norske-fylker.txt, norske-kommuner.txt, norwegian-names.txt, nsf2016.txt, words.txt



```
grep -aEirh "^api-co*"  | tr '[:upper:]' '[:lower:]' | sort | uniq > /mnt/d/tmp/api-co.txt
grep -aEirh "^api-bc*"  | tr '[:upper:]' '[:lower:]' | sort | uniq > /mnt/d/tmp/api-bc.txt
grep -aEirh "^extern*"  | tr '[:upper:]' '[:lower:]' | sort | uniq > /mnt/d/tmp/extern.txt
grep -aEirh "^extern.*"  | tr '[:upper:]' '[:lower:]' | sort | uniq > /mnt/d/tmp/extern.txt
grep -aEirh "^extern.*$"  | tr '[:upper:]' '[:lower:]' | sort | uniq > /mnt/d/tmp/extern.txt
grep -aEirh "^besokr.*$"  | tr '[:upper:]' '[:lower:]' | sort | uniq > /mnt/d/tmp/besokr.txt
grep -aEirh "^compan.*$"  | tr '[:upper:]' '[:lower:]' | sort | uniq > /mnt/d/tmp/compan.txt
grep -aEirh "^dailyc.*$"  | tr '[:upper:]' '[:lower:]' | sort | uniq > /mnt/d/tmp/dailyc.txt
grep -aEirh "^meetin.*$"  | tr '[:upper:]' '[:lower:]' | sort | uniq > /mnt/d/tmp/meetin.txt
grep -aEirh "^flyerl.*$"  | tr '[:upper:]' '[:lower:]' | sort | uniq > /mnt/d/tmp/flyerl.txt
```

Scan with plugins and web app

Fuzzing

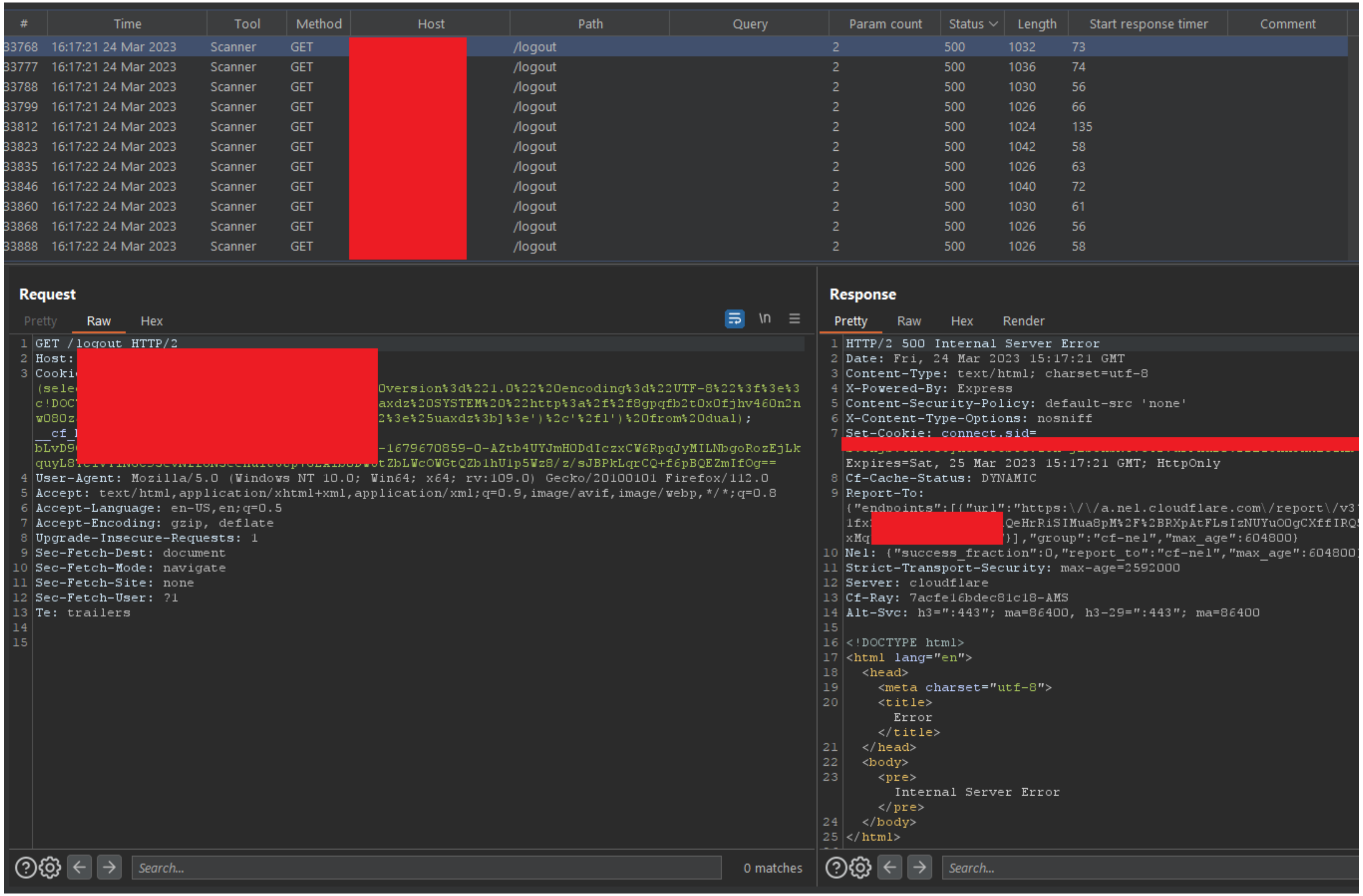


- Get a second opinion from your vulnerability scanner
- In this case, Burp Suite is tasked to scan the defined insert point §project§
- Does scanner find something?
  - Revisit methodology and ask yourself how you could improve it

Review Logger 500 errors

Fuzzing

- Review the request log
- Look for 500 Error Messages
- There could be potential for exploitation
- Once done, clear the log



#	Time	Tool	Method	Host	Path	Query	Param count	Status	Length	Start response timer	Comment
33768	16:17:21 24 Mar 2023	Scanner	GET	[redacted]	/logout		2	500	1032	73	
33777	16:17:21 24 Mar 2023	Scanner	GET	[redacted]	/logout		2	500	1036	74	
33788	16:17:21 24 Mar 2023	Scanner	GET	[redacted]	/logout		2	500	1030	56	
33799	16:17:21 24 Mar 2023	Scanner	GET	[redacted]	/logout		2	500	1026	66	
33812	16:17:21 24 Mar 2023	Scanner	GET	[redacted]	/logout		2	500	1024	135	
33823	16:17:22 24 Mar 2023	Scanner	GET	[redacted]	/logout		2	500	1042	58	
33835	16:17:22 24 Mar 2023	Scanner	GET	[redacted]	/logout		2	500	1026	63	
33846	16:17:22 24 Mar 2023	Scanner	GET	[redacted]	/logout		2	500	1040	72	
33860	16:17:22 24 Mar 2023	Scanner	GET	[redacted]	/logout		2	500	1030	61	
33868	16:17:22 24 Mar 2023	Scanner	GET	[redacted]	/logout		2	500	1026	56	
33888	16:17:22 24 Mar 2023	Scanner	GET	[redacted]	/logout		2	500	1026	58	

Request

```
GET /logout HTTP/2
Host: [redacted]
Cooki
(sele                              Oversion%3d%221.0%22%20encoding%3d%22UTF-8%22%3f%3e%3
c!DOC                              axdz%20SYSTEM%20%22http%3a%2f%2f8gpqfb2t0x0fjhv460n2n
w08Oz                              2%3e%25uaxdz%3b]%3e')%2c'%2fl')%20from%20dual);
__cf_l
bLvD9                              -1679670859-0-AZtb4UYJmHODdIczxCW6RpqJyMILNbgoRozEjLk
quyL8                              tZbLWcOWGtQZb1hU1p5Wz8/z/sJBPkLqrCQ+f6pBQEZmIfOg==
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/112.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
```

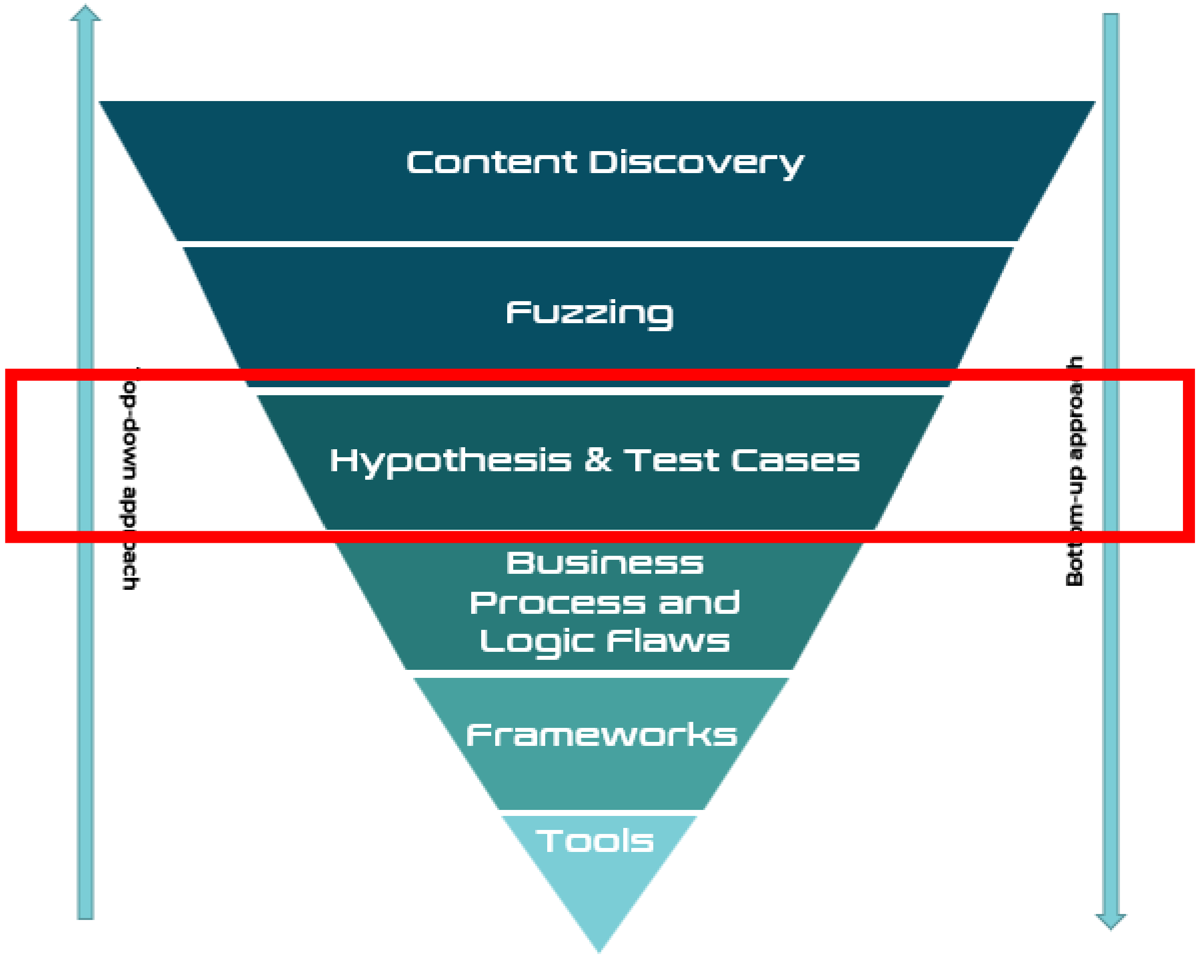
Response

```
HTTP/2 500 Internal Server Error
Date: Fri, 24 Mar 2023 15:17:21 GMT
Content-Type: text/html; charset=utf-8
X-Powered-By: Express
Content-Security-Policy: default-src 'none'
X-Content-Type-Options: nosniff
Set-Cookie: connect.sid=
[redacted]
Expires=Sat, 25 Mar 2023 15:17:21 GMT; HttpOnly
Cf-Cache-Status: DYNAMIC
Report-To:
{"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3
1fx[redacted]QeHrRiSIMua8pM%2F%2BRXpAtFLsIzNUYuO0gCXffIRQ
xMq                  }],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800
Strict-Transport-Security: max-age=2592000
Server: cloudflare
Cf-Ray: 7acfe16bdec81c18-AMS
Alt-Svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <title>
      Error
    </title>
  </head>
  <body>
    <pre>
      Internal Server Error
    </pre>
  </body>
</html>
```

Hypothesis and test cases

Be creative and utilize your team.

Test and conclude hypothesizes

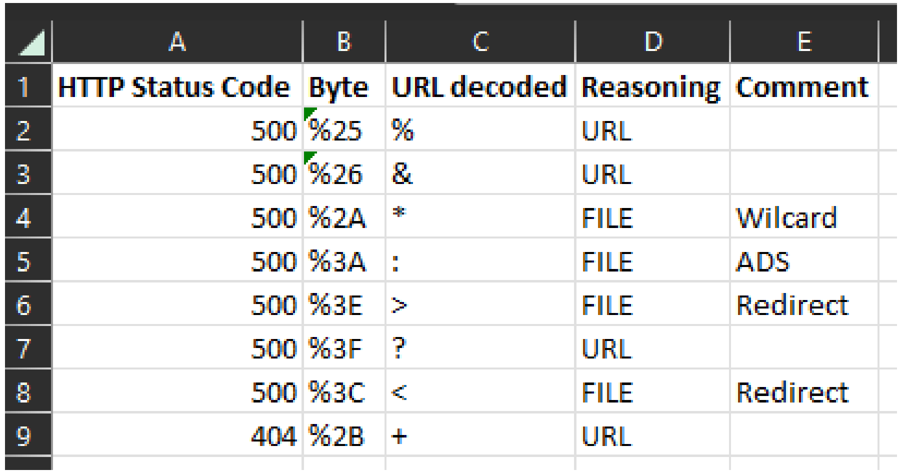


Utilize the Team

- Pen Testing is a team effort, not an individual effort.
- Utilize a team to maximize the penetration test efforts.
- Ensure you can work together on tackling breaking the application
- If you can’t properly explain and create valid hypothesis
  - Ask your team
  - Work together (knowledge transfer)
- Source your rabbit holes to team members

Hypothesis

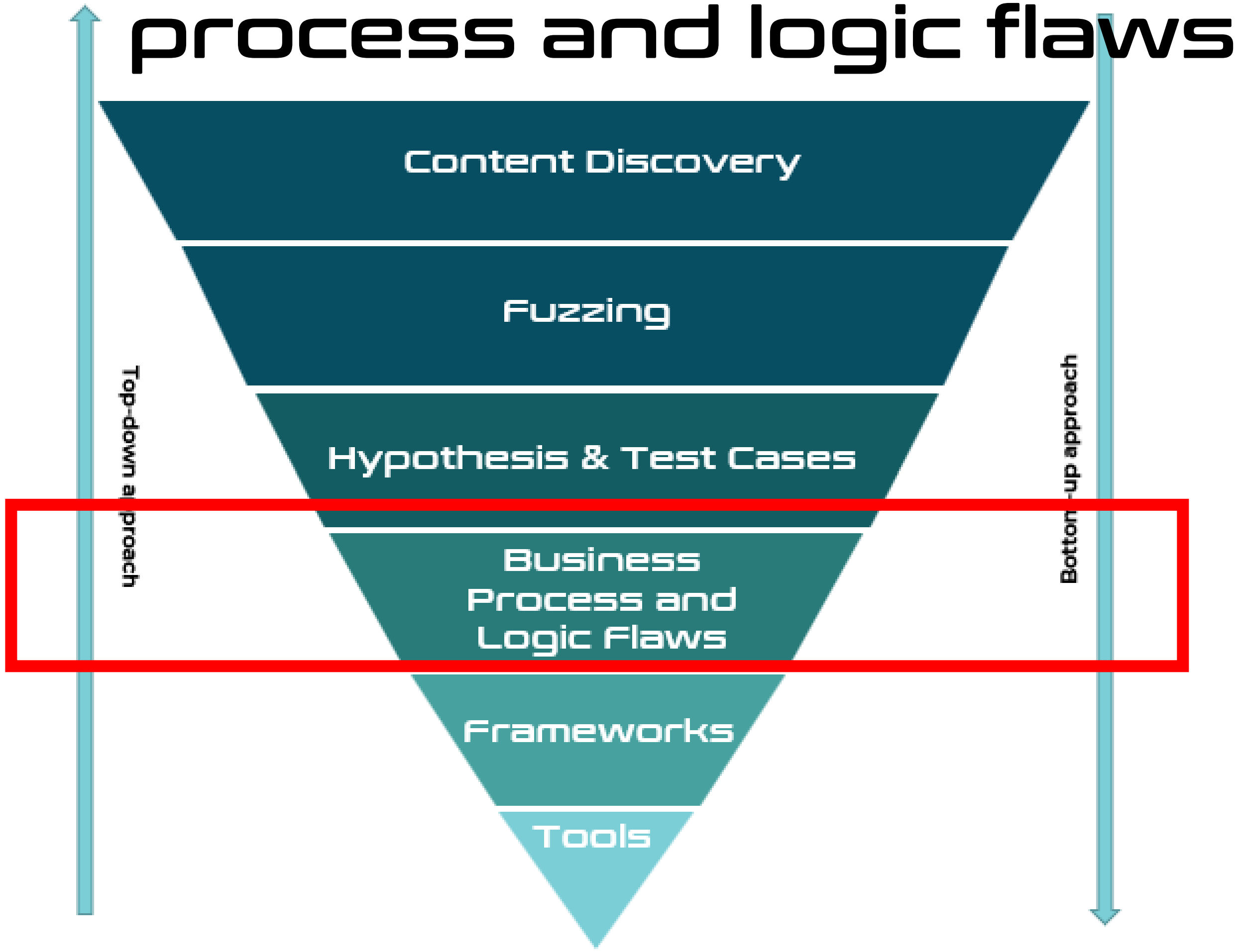
I am seeing that : > < and * are influencing file reads of the file server. I want to explore Local File Inclusion, SSRF and similar kinds of vulnerabilities



	A	B	C	D	E
1	HTTP Status Code	Byte	URL decoded	Reasoning	Comment
2	500	%25	%	URL	
3	500	%26	&	URL	
4	500	%2A	*	FILE	Wilcard
5	500	%3A	:	FILE	ADS
6	500	%3E	>	FILE	Redirect
7	500	%3F	?	URL	
8	500	%3C	<	FILE	Redirect
9	404	%2B	+	URL	

Business Process and Logic Flaws

With extensive knowledge of the target, explore process and logic flaws



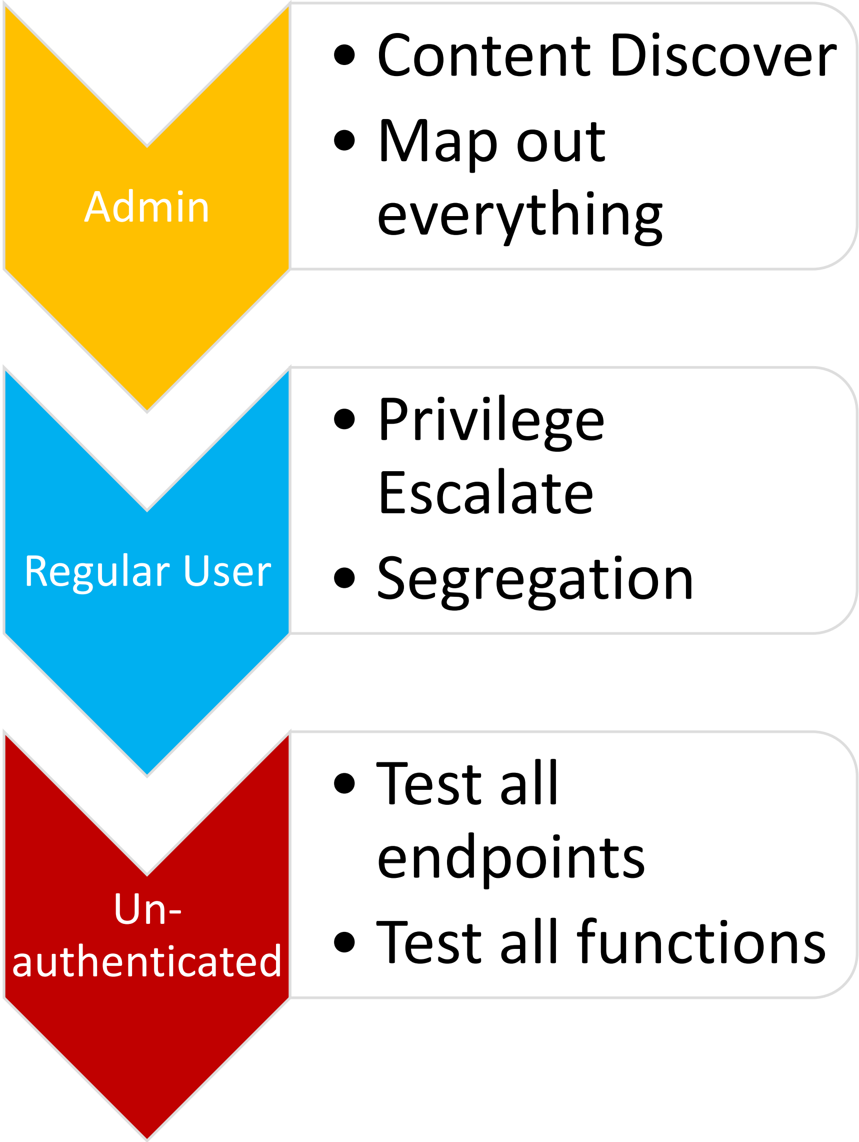
Take a Step Back

- Finding bugs and vulnerabilities often require you to think outside the box
- Work with team members – Explain the system to them
- Try produce hypothesis and test cases based on a short presentation by the primary tester
- Each system have different flows, attack vectors and challenges; brain storm a little bit and you drastically increase the odds of success.

Authentication Example

Business Process and Logic Flaws

- Technically a part of discovery / scoping / planning
  - Pentesting is not a one-size fits all
  - Work with the customer to find THEIR needs
- Applications typically have different privileges levels:
  - Super Admin
  - Customer admin
  - User
  - Unauthenticated
- Regardless of the scope you have worked through with your customer, ask for super admin
  - Map out everything as super admin, you don't have to pentest it, but build overview of functionality
- Make sure customer admin, user and unauthenticated is secure, and provides segregation



- Content Discover
- Map out everything

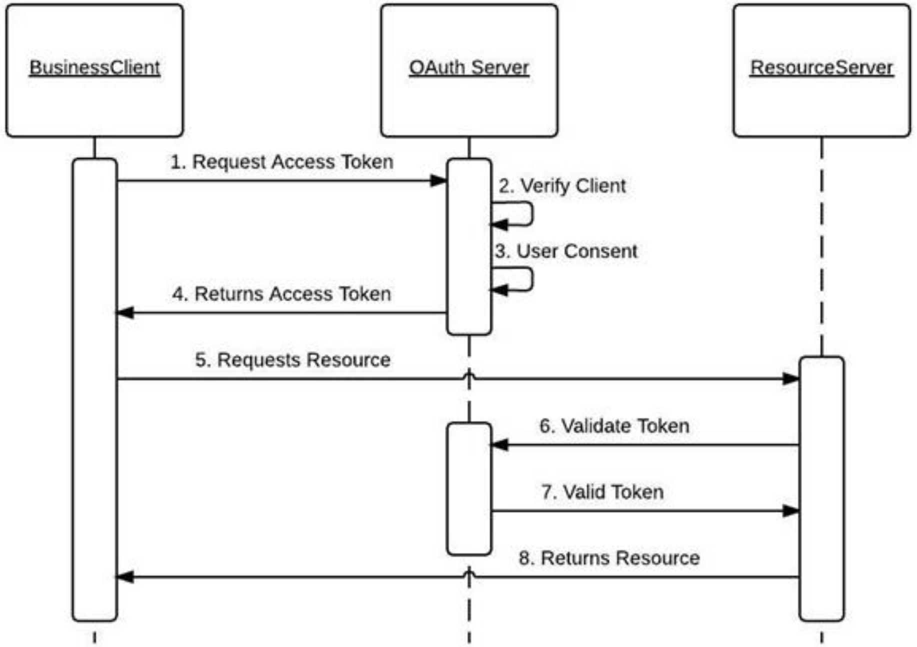
- Privilege Escalate
- Segregation

- Test all endpoints
- Test all functions

Map Out Application Flows

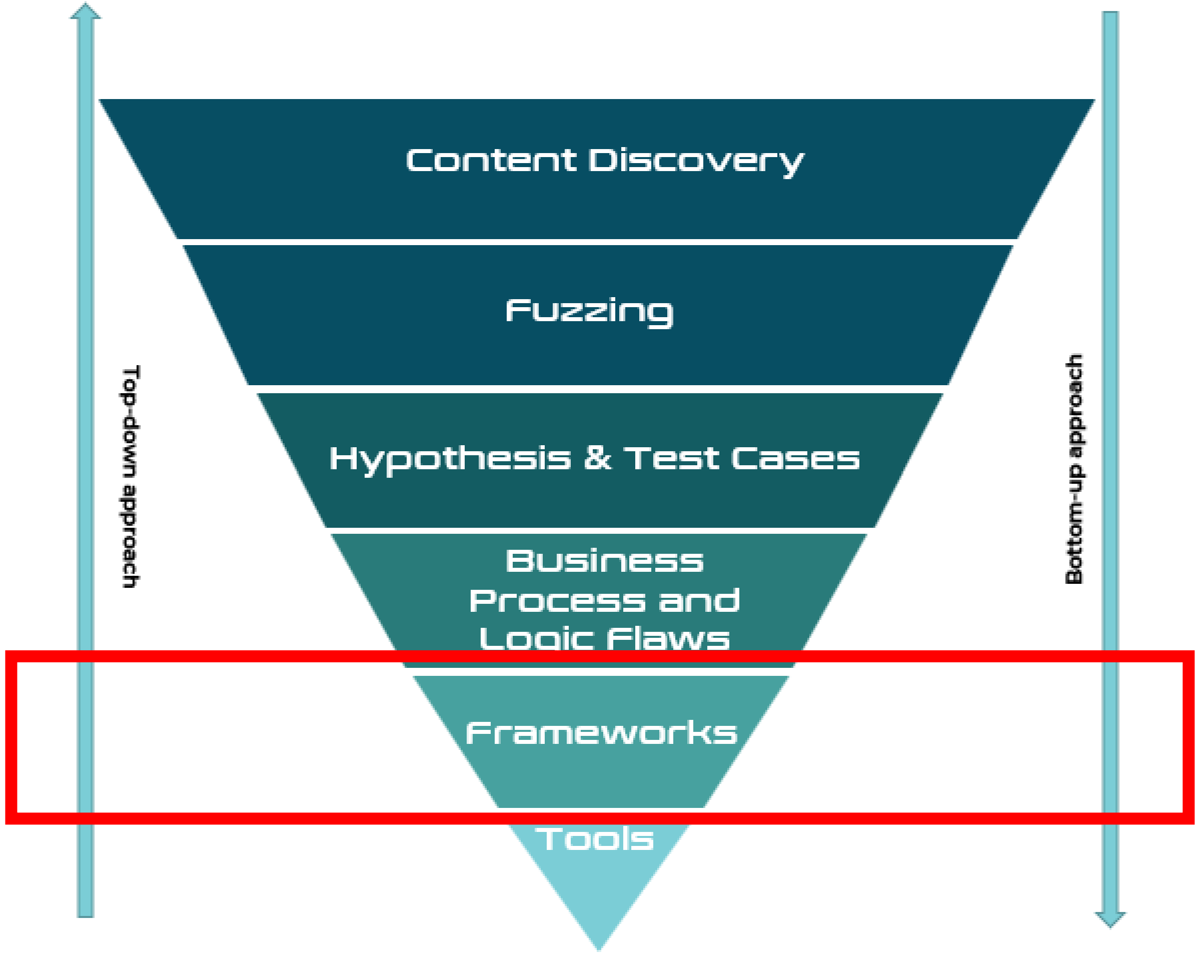
Business Process and Logic Flaws

- Mapping out the flow of behavior
- Draw.io / Diagrams.net is easy quick win
- Helps look at things from a bird eye perspective
- Map out requests and response
- Example flows:
  - Purchasing
  - Authentication
  - Impersonation / privilege escalation
  - Password reset flow
  - …



Frameworks

Compliance and pentest support. Utilize frameworks.

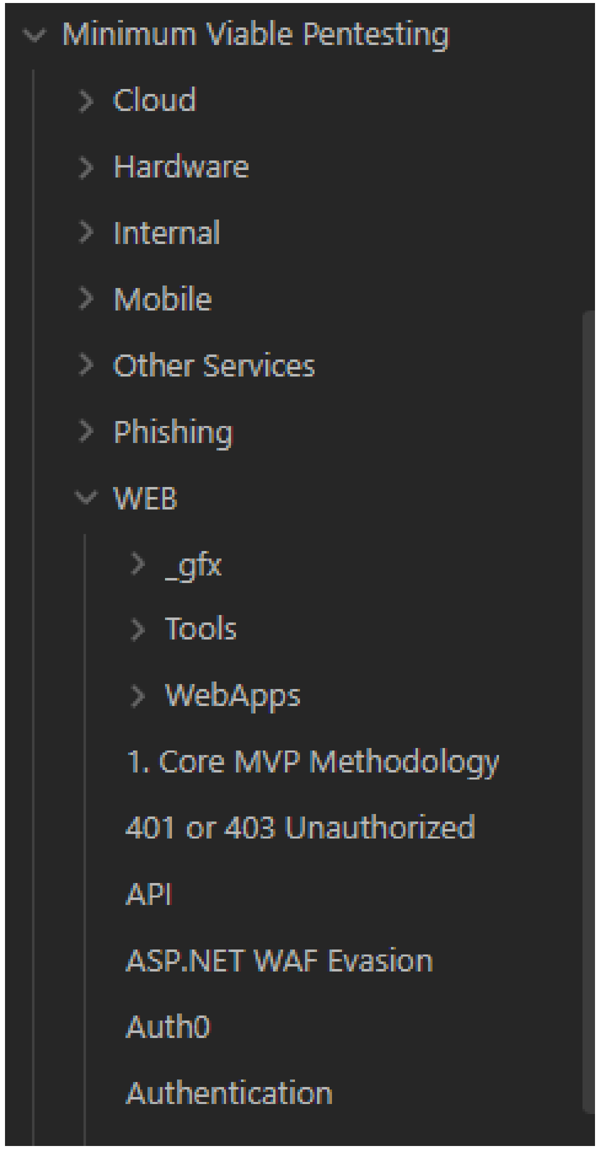


Minimum Viable Penetration Testing

Define an **absolute minimum** of activity to perform on a certain system or piece of technology or application.

- Allow experience from previous tests to be reused
- A way to support pentesters. Don’t start from scratch.
  - Your own refined Google / Hacktricks.xyz / etc.
- Not training on concepts, but simple bullets of what needs to be done
- Make pentester accountable to:
  - Check the things which needs to be checked
  - Ask team for help when there are interesting anomalies
- There are application and technology specific MVP’s

Frameworks

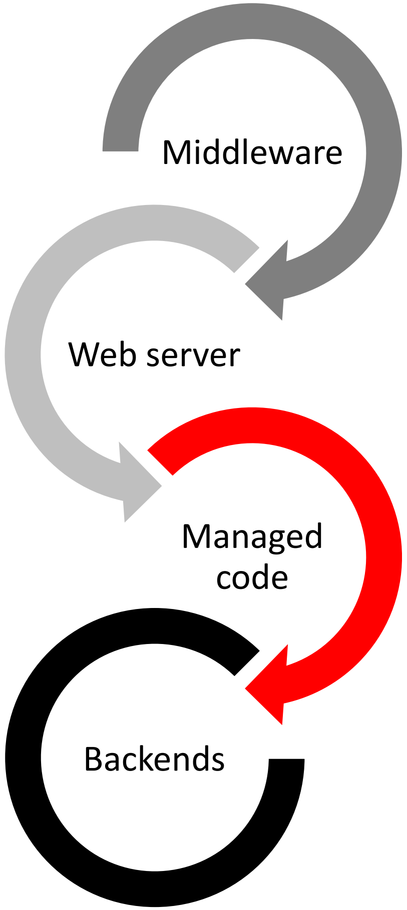


- Minimum Viable Pentesting
  - Cloud
  - Hardware
  - Internal
  - Mobile
  - Other Services
  - Phishing
  - WEB
    - _gfx
    - Tools
    - WebApps
    - 1. Core MVP Methodology
    - 401 or 403 Unauthorized
    - API
    - ASP.NET WAF Evasion
    - Auth0
    - Authentication

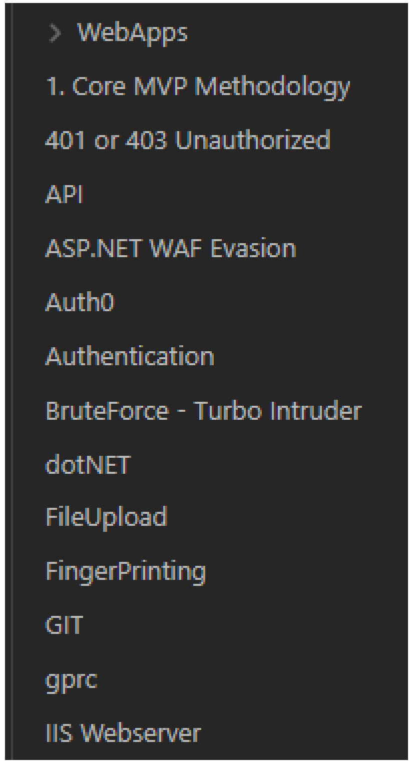
Tech and Application Specific MVP

Frameworks

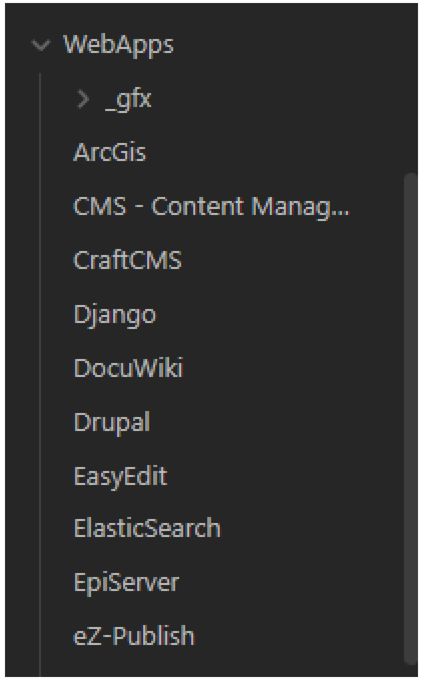
Attack The Stack



Tech & App Specific MVP



› WebApps
1. Core MVP Methodology
401 or 403 Unauthorized
API
ASP.NET WAF Evasion
Auth0
Authentication
BruteForce - Turbo Intruder
dotNET
FileUpload
FingerPrinting
GIT
gprc
IIS Webserver



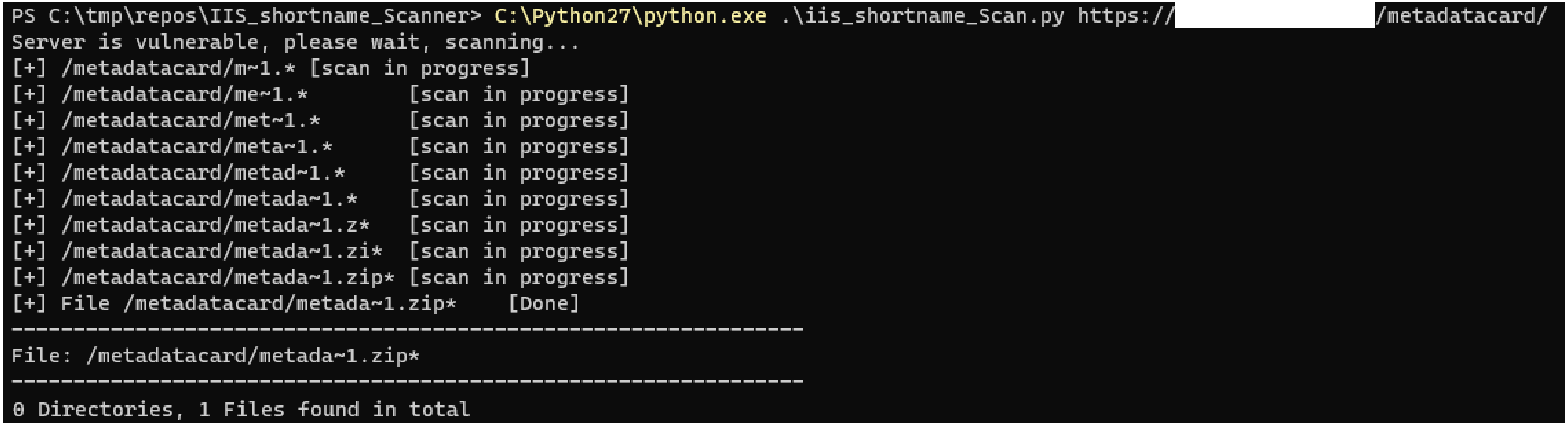
⌄ WebApps
› _gfx
ArcGis
CMS - Content Manag...
CraftCMS
Django
DocuWiki
Drupal
EasyEdit
ElasticSearch
EpiServer
eZ-Publish

Testing Frameworks

- ASVS – Application Security Verification Standard
- WSTG – Web Security Testing Guide
- …

IIS Short Name Scanning

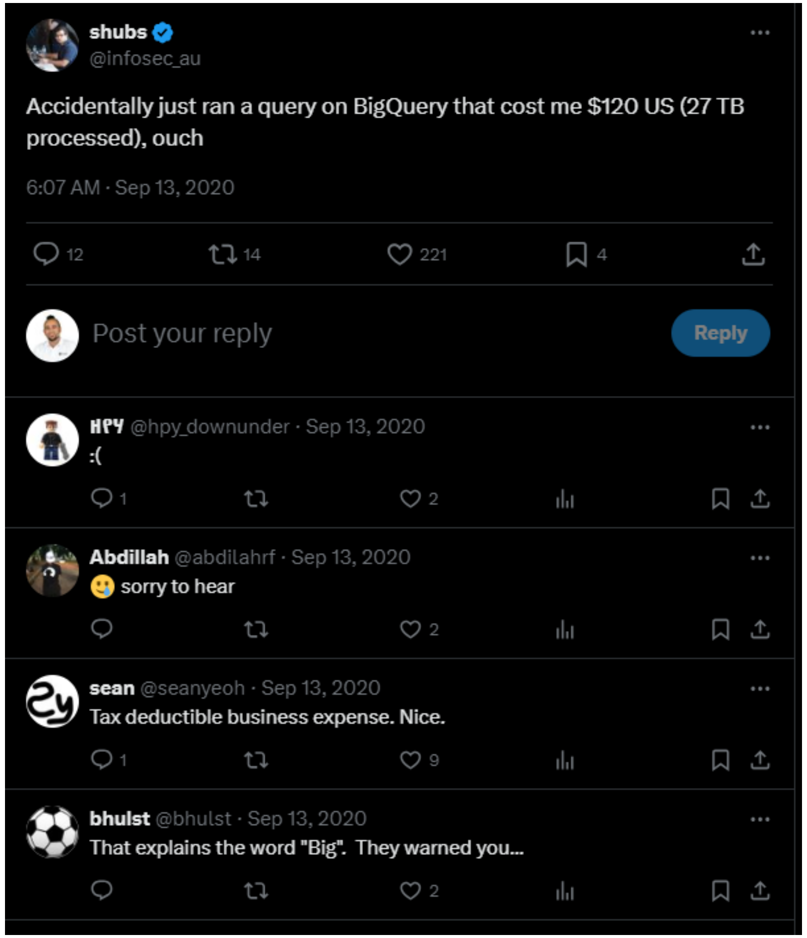
Frameworks



```
PS C:\tmp\repos\IIS_shortname_Scanner> C:\Python27\python.exe .\iis_shortname_Scan.py https://[redacted]/metadatacard/
Server is vulnerable, please wait, scanning...
[+] /metadatacard/m~1.* [scan in progress]
[+] /metadatacard/me~1.*        [scan in progress]
[+] /metadatacard/met~1.*       [scan in progress]
[+] /metadatacard/meta~1.*      [scan in progress]
[+] /metadatacard/metad~1.*     [scan in progress]
[+] /metadatacard/metada~1.*    [scan in progress]
[+] /metadatacard/metada~1.z*   [scan in progress]
[+] /metadatacard/metada~1.zi*  [scan in progress]
[+] /metadatacard/metada~1.zip* [scan in progress]
[+] File /metadatacard/metada~1.zip*    [Done]
----------------------------------------------------------------
File: /metadatacard/metada~1.zip*
----------------------------------------------------------------
0 Directories, 1 Files found in total
```

Ideas to Help Find Content

- Build and test with wordlist
  grep -aEirh ‘^metada.*' * | sort | uniq
- Intruder: metada§POSITION§.zip
  - Settings: bruteforce 1-3 a-z 0-9
- Dork it:
  - inurl: metada
  - Site: target.com
- Google BigQuery
- Wayback Machine



shubs
@infosec_au

Accidentally just ran a query on BigQuery that cost me $120 US (27 TB processed), ouch

6:07 AM · Sep 13, 2020

HPY @hpy_downunder · Sep 13, 2020
:(

Abdillah @abdilahrf · Sep 13, 2020
🥲 sorry to hear

sean @seanyeoh · Sep 13, 2020
Tax deductible business expense. Nice.

bhulst @bhulst · Sep 13, 2020
That explains the word "Big". They warned you...

WAR IS PEACE
BIG BROTHER IS WATCHING YOU
IS
BIG BROTHER
I will not be owned
RIVER SECURITY
Offensive SOC
Continuous Attack Surface Management
Always-On Penetration Testing
By your SANS instructor
SANS
Chris Dale
Empower Your Defenses
Proactive & Continuous Penetration Testing
Seize Control, Gain Visibility, Become Compliant
SANS
I hacked the Dutch government
and all I got was this lousy t-shirt
FREEDOM ONLINE
HAK5
HACK NAKED
Security Weekly
dev.to
GOT OWASP?
FREEDOM ONLINE
HACK NAKED
FIGHT DYSTOPIA

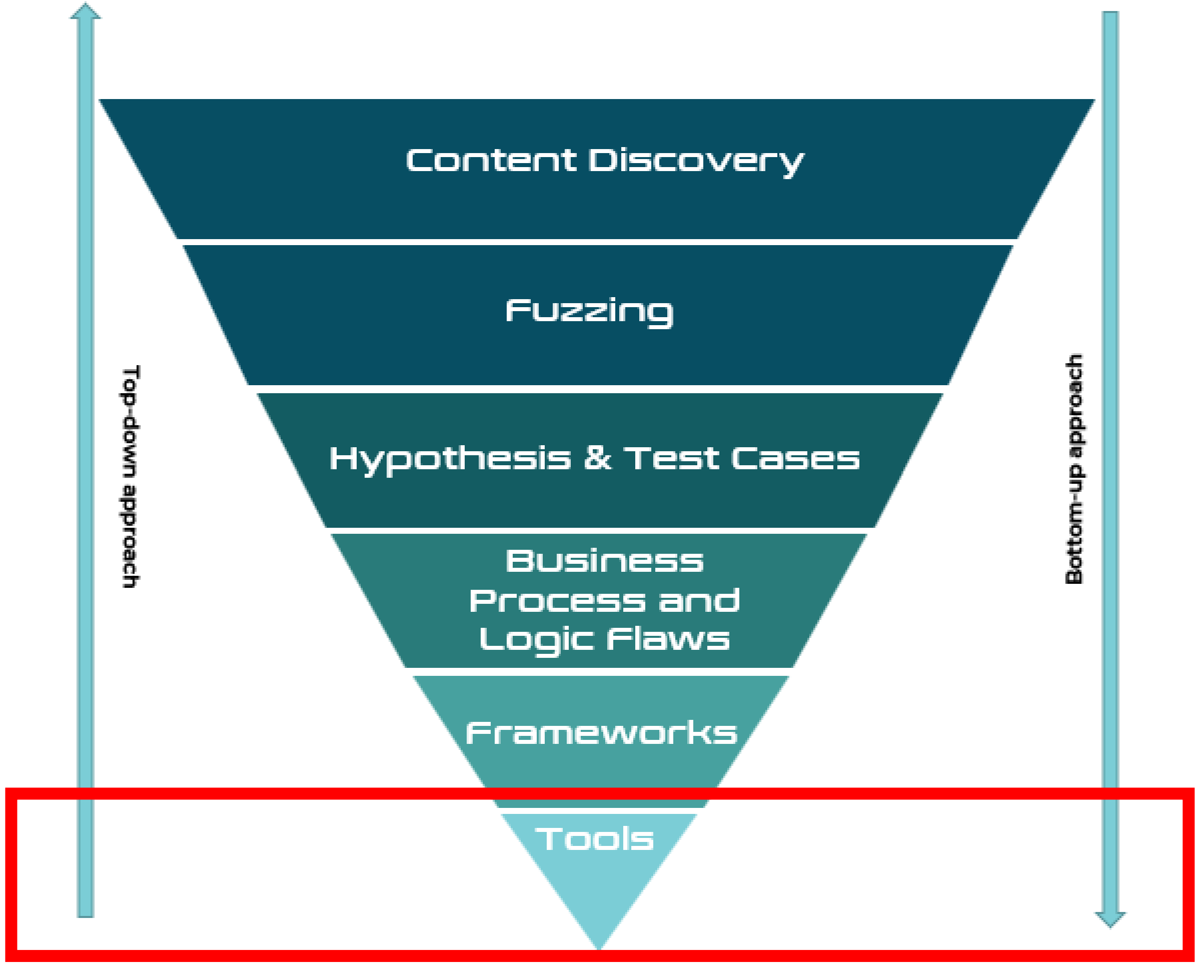
When You Don't Have MVP

Frameworks

- Create one
  - It is **minimum** viable
  - A starting point is better than nothing
- Dedicate days before the engagement to:
  - Build
  - Set-up
  - Configure
  - Break & Hack
  - Create CTF challenges ;)
- Create foundations for future hypothesis

Tools

Vulnerability scanners, application and technology specific tools



Tools are plentiful

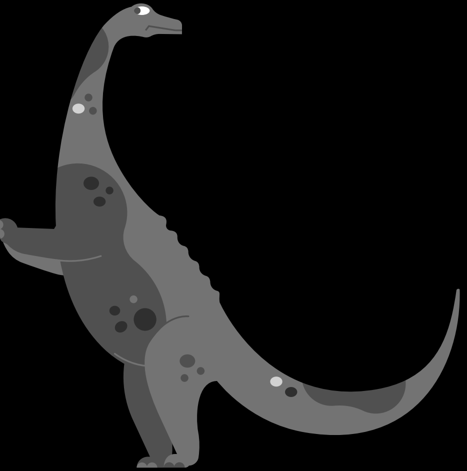
Go find them, review them, or build them yourself. Tools are useful for assisting and automating, but always remember to **seek to understand, not just to solve**. Don’t run the tools without understanding how they work; understand what they’re trying to achieve and identify tool failure.

Continuity

Finally, the most important point

How do we make an actual long term impact with security testing?

With Traditional Penetration Testing – Are we playing the same game as attackers?



Continuity

- To effectively prevent threat actors from exploiting new vulnerabilities, continuity is imperative
- Trigger penetration testing when changes happen
- Example:
  - Status code changes: 401 Unauthorized to 200 OK
  - Swagger.json with new definitions
  - Crawling results with new dynamic scripts
  - CTI with new hacking techniques

RIVER SECURITY

https://into.bio/chrisdale & https://into.bio/rivsec

⮤ Download slides here!

Twitter – https://twitter.com/ChrisADale

LinkedIn – https://www.linkedin.com/in/chrisad/

Fighting Cyber Crime – https://riversecurity.eu