

ATTACKING ORGANIZATIONS

FROM ZERO TO HERO

HUSSEIN DAHER

INTRODUCTION

- Hussein Daher
- CEO of **WebImmunity.com**
- over 10 years of cybersecurity experience
- business master's degree
- over 1000 vulnerabilities on bug bounty platforms
- H1-2010's Vigilante award
- Intigriti's 1337up competition #1
- Udemy course, "Bug Bounty - An Advanced Guide to Finding Good Bugs," - 1800 students

IMPORTANCE OF RECONNAISSANCE

- Reconnaissance is the first and one of the most critical steps in the bug bounty hunting process. It involves gathering as much information as possible about the target to identify potential weaknesses and entry points. Effective reconnaissance can significantly enhance the chances of finding valuable bugs.

IDENTIFYING POTENTIAL ATTACK SURFACES

- Attack surfaces are the various points in a system where an unauthorized user can try to enter data to or extract data from. Identifying these surfaces involves looking at the entire digital footprint of an organization, including web applications, network infrastructure, APIs, and more.

INTRO

- I've been able to take over FIS #1 spot in under 6 months with perseverance in recon combined with application hacking skills

The screenshot shows the FIS Hall of Fame page. At the top, there's a banner with the FIS logo and some text. Below the banner, the page header includes links for "Program details", "Announcements 60", "Hall of Fame" (which is underlined in orange), and "Your submissions 144". A "Submit report" button and a "Do you like this program?" poll are also present. The main content area is titled "Hall of Fame" and says "Thanks to the following researchers for reporting important security issues:". A table lists the top four researchers:

Rank	Researcher	Points
1	HusseiN98D	2620
2	ytcracker	1325
3	dmatrix	1315
4	brsn	1290

INTRO

- FIS is a large organization and their bug bounty program is about “everything they own” in scope. This gives us a huge attack surface to look at.

The screenshot shows the FIS Hall of Fame page. At the top, there's a banner with the FIS logo and some text. Below the banner, the page header includes links for "Program details", "Announcements 60", "Hall of Fame" (which is underlined in orange), and "Your submissions 144". A "Submit report" button and a "Do you like this program?" poll are also present. The main content area is titled "Hall of Fame" and lists researchers ranked by points. The table has columns for Rank, Researcher, and Points.

Rank	Researcher	Points
1	HusseiN98D	2620
2	ytcracker	1325
3	dmatrix	1315
4	brsn	1290

METHODOLOGIES

- Subdomain Enumeration
- VHOST Identification
- ASN Mapping
- Web Fuzzing
- Dorking
- Other tips and tricks

SUBDOMAIN ENUMERATION

- Identifying subdomains will give you a bigger attack surface
- Look for preprod/env subdomains
- Perform Recursive bruteforcing:
- FUZZ.host → dev.host → FUZZ.dev.host

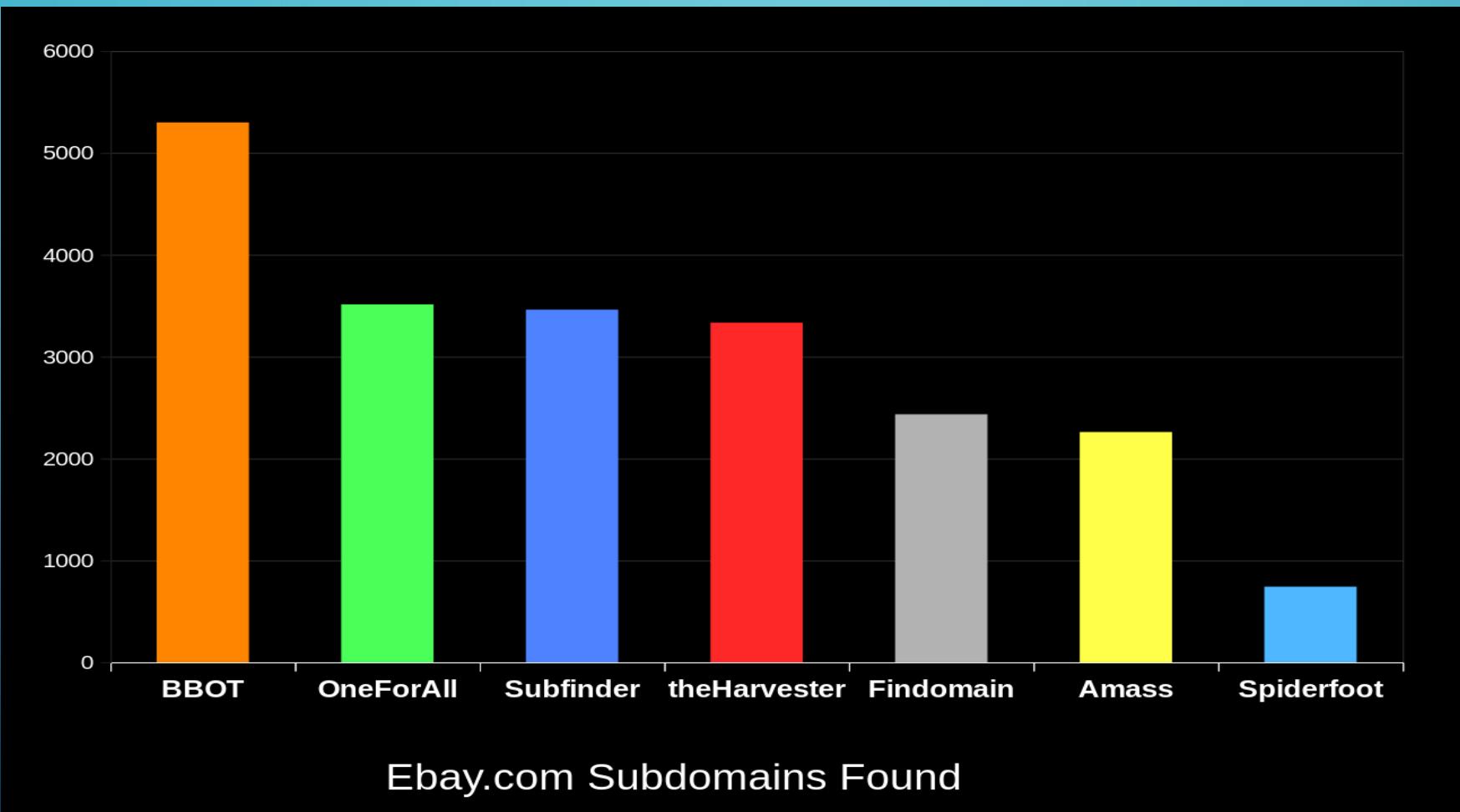
SUBDOMAIN ENUMERATION

- The good old scripts:
- `amass enum -passive -d example.com -o results.txt`
- `sublist3r -d example.com`
- Add to your toolset:
- <https://github.com/blacklanternsecurity/bbot>

☞ Comparison to Other Tools

BBOT consistently finds 20-50% more subdomains than other tools. The bigger the domain, the bigger the difference. To learn how this is possible, see [How It Works](#).

BBOT COMPARISON



VHOST IDENTIFICATION

- Less people deep into VHOSTS
- Identifying these will give you targets most people haven't seen yet
- Spot the differences

VHOST IDENTIFICATION

- What I love doing : BurpSuite Intruder

The screenshot shows the BurpSuite Intruder configuration interface. At the top, it says "Choose an attack type" with "Sniper" selected. Below that, under "Payload positions", it says "Configure the positions where payloads will be inserted, they can be added into the target as well as the base request." A red arrow points from the "Target" field (containing "https://[REDACTED]:31") to the "Host" line in the payload list. Another red arrow points from the "Host" line in the payload list up to the "Update Host header to match target" checkbox.

① Choose an attack type

Attack type: Sniper

② Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: https://[REDACTED]:31

Host: \$tests

Accept-Encoding: gzip, deflate, br

Accept: */*

Accept-Language: en-US;q=0.9,en;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.60 Safari/537.36

Connection: keep-alive

Cache-Control: max-age=0

Content-Length: 1

Add §

Clear §

Auto §

Refresh

Start attack

VHOST IDENTIFICATION

- Results

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
2	learn.r	301	179			472	
0		404	174			492	
1	educa	404	179			492	
3	ralice	404	174			492	
4	repo	404	179			492	
5	rgf.re	404	174			492	
6	rgfftp.	404	174			492	
7	rqade	404	179			492	
8	rti.reli	404	179			492	
9	sftp.re	404	178			492	
10	sftp2.	404	179			492	
11	stream	404	490			492	
12	support	404	496			492	
13	uat.re	404	495			492	
14	webe	404	495			492	
15	www	404	495			492	

Request	Response
Pretty	
Raw	
Hex	
1	GET / HTTP/1.1
2	Host: learn.███████████
3	Accept-Encoding: gzip, deflate, br
4	Accept: */*
5	Accept-Language: en-US;q=0.9,en;q=0.8
6	User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.60 Safari/537.36
7	Connection: keep-alive
8	Cache-Control: max-age=0
9	Content-Length: 1
10	TP:147 249 128 210



VHOST IDENTIFICATION

- More

The screenshot shows a NetworkMiner interface with two main panels: Request and Response.

Request Panel:

- Protocol: HTTP/1.1
- Method: GET /
- Host header: **45.79.100.45** (highlighted by a red arrow)
- User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.60 Safari/537.36
- Connection: keep-alive
- Content-Length: 1
- Ports: 80

Response Panel:

- Protocol: HTTP/1.1
- Status: 404 Not Found
- Reason: Not Found

Inspector Panel:

- Target: https://45.79.100.45:443
- Request attributes: 2
- Request query parameters: 0
- Request body parameters: 1
- Request cookies: 0
- Request headers: 9

Bottom Status Bar:

- Connection reset (highlighted by a red arrow)
- Search bar
- 0 highlights

Annotations:

- A red arrow points from the highlighted Host header in the Request panel to the Connection Reset status bar at the bottom.
- A red arrow points from the Target field in the Inspector panel to the Connection Reset status bar at the bottom.
- The text "same host header + target Connection Reset" is displayed in red near the bottom right.

VHOST IDENTIFICATION

- However, bruteforcing host header gives us more targets

103. Intruder attack of https://[REDACTED] 92

Results Positions Payloads Resource pool Settings

Intruder attack results filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
823	[REDACTED]	200	417			1412	
824	[REDACTED]	200	422			933	
815	[REDACTED]	503	519			380	
817	[REDACTED]	503	576			380	
816	[REDACTED]	503	603			380	
0	[REDACTED]	0	0				
1	[REDACTED]	0	0				
2	[REDACTED]	0	0				
3	[REDACTED]	0	0				
4	[REDACTED]	0	0				
5	[REDACTED]	0	0				
6	[REDACTED]	0	0				
7	[REDACTED]	0	0				
8	[REDACTED]	0	0				
9	[REDACTED]	0	0				
10	[REDACTED]	0	0				
11	[REDACTED]	0	0				
12	[REDACTED]	0	0				
13	[REDACTED]	0	0				
14	[REDACTED]	0	0				

Valid Response for valid host headers

Connection Reset on non-valid host headers

Request Response

Pretty Hex Render

```
1 HTTP/1.1 200 OK
2 Cache-Control: private
3 Server: [REDACTED]
4 Set-Cookie: [REDACTED]a65ea0f3-1d17-44a1-9dc0-e763072cea95; path=/; secure; HttpOnly
5 SessionExpiry: 1800
6 X-Powered-By: ASP.NET
7 Access-Control-Allow-Headers: Origin, Authorization, Content-Type, X-Requested-With
8 Access-Control-Allow-Methods: POST, GET, PUT, OPTIONS, DELETE, PATCH
9 Content-Security-Policy: default-src 'self' ; script-src 'self' https://cdn.cookie-law.org https://geolocation.onetrust.com https://cookies-data.onetrust.io https://consent-api.onetrust.com 'unsafe-eval' 'U'Unsafe-inline' data: blob: https:// object-src 'self' blob:img-src 'self' data: https://cdn.cookie-law.org https://geolocation.onetrust.com https://cookies-data.onetrust.io https://consent-api.onetrust.com; https:// connect-src 'self' https://cdn.cookie-law.org https://geolocation.onetrust.com https://cookies-data.onetrust.io https://consent-api.onetrust.com; frame-ancestors 'self' ; frame-src 'self' https://uni
10 Strict-Transport-Security: max-age=31536000; includeSubDomains;preload
11 X-Content-Type-Options: nosniff
12 X-XSS-Protection: 1; mode=block
13 Access-Control-Allow-Origin: https://[REDACTED]
14 X-Frame-Options: sameorigin
15 Date: Tue, 14 May 2024 19:33:16 GMT
16 Content-Length: 0
17
18
```

ASN MAPPING

- <https://bgp.he.net/search?search%5Bsearch%5D=Facebook.+Inc&commit=Search>

AS63293	ASN	Facebook, Inc.
AS54115	ASN	Facebook Inc
AS34825	ASN	FACEBOOK ISRAEL LTD
AS32934	ASN	Facebook, Inc.
AS149642	ASN	Facebook Singapore Pte Ltd.
74.119.76.0/22	Route	Facebook, Inc.
69.63.184.0/21	Route	Facebook, Inc.
69.63.176.0/21	Route	Facebook, Inc.
69.63.176.0/20	Route	Facebook, Inc.
69.171.250.0/24	Route	Facebook, Inc.
69.171.240.0/20	Route	Facebook, Inc.
69.171.224.0/20	Route	Facebook, Inc.
69.171.224.0/19	Route	Facebook, Inc.
66.220.152.0/21	Route	Facebook, Inc.
66.220.144.0/21	Route	Facebook, Inc.
66.220.144.0/20	Route	Facebook, Inc.
45.64.40.0/22	Route	Facebook Singapore Pte Ltd.
41.223.111.0/24	Route	for the above IPV4 we are using for google and facebook peering
41.189.185.0/24	Route	MTN Ghana Enterprise Internet Clients and facebook Cache
2c0f:ef78:f::/48	Route	Facebook South Africa (Pty) Ltd
2c0f:ef78:e::/48	Route	Facebook South Africa (Pty) Ltd
2c0f:ef78:d::/48	Route	Facebook South Africa (Pty) Ltd
2c0f:ef78:12::/48	Route	Facebook South Africa (Pty) Ltd
2c0f:ef78:11::/48	Route	Facebook South Africa (Pty) Ltd
2c0f:ef78:10::/48	Route	Facebook South Africa (Pty) Ltd
2620:10d:c09b::/48	Route	Facebook Inc
2620:10d:c09a::/48	Route	Facebook Inc
2620:10d:c099::/48	Route	Facebook Inc
2620:10d:c098::/48	Route	Facebook Inc

ASN MAPPING

- Copy all IP ranges

```
hussein98d@HusseiN98D:/tmp$ cat iplist | cut -f1  
129.134.156.0/24  
129.134.155.0/24  
129.134.154.0/24  
129.134.150.0/24  
129.134.149.0/24  
129.134.148.0/24  
129.134.147.0/24  
129.134.144.0/24  
129.134.143.0/24  
129.134.140.0/24  
129.134.139.0/24  
129.134.138.0/24  
129.134.136.0/24  
129.134.135.0/24  
129.134.134.0/24  
129.134.133.0/24  
129.134.132.0/24  
129.134.131.0/24  
129.134.130.0/24  
129.134.129.0/24
```

ASN MAPPING

- Send to prips

```
hussein98d@Hussein98D:/tmp$ for i in $(cat iplist | cut -f1); do pripps $i >> fb; done
hussein98d@Hussein98D:/tmp$ wc -l fb
5120 fb
hussein98d@Hussein98D:/tmp$ head -n 10 fb
129.134.156.0
129.134.156.1
129.134.156.2
129.134.156.3
129.134.156.4
129.134.156.5
129.134.156.6
129.134.156.7
129.134.156.8
129.134.156.9
hussein98d@Hussein98D:/tmp$
```

ASN MAPPING

- Gather all subdomains you can find for the org, even the ones not resolving

```
hussein98d@HusseiN98D:/tmp$ cat fbsubs | awk -F' '+'{print $2}' | sort -u
edgeray-fna-msgr-shv-01-fktw4.fbcdn.net
edgeray-fna-shv-01-fktw4.fbcdn.net
fna-fbcn-shv-01-fktw4.fbcn.net
fna-fbcn-video-shv-01-fktw4.fbcn.net
fna-fbcn-z-m-shv-01-fktw4.fbcn.net
fna-fbcn-z-p3-shv-01-fktw4.fbcn.net
fna-fbcn-z-p4-shv-01-fktw4.fbcn.net
fna-instagram-p42-shv-01-fktw4.fbcn.net
fna-instagram-p4-shv-01-fktw4.fbcn.net
fna-instagram-shv-01-fktw4.fbcn.net
fna-internal-services-shv-01-fktw4.fbsv.net
fna-whatsapp-shv-01-fktw4.fbcn.net
```

ASN MAPPING

- BruteForce : IPS:SUBDOMAINS

```
hussein98d@Hussein98D:/tmp$ for i in $(cat fbips);do ffuf -w fbsubs -u https://$i -H "Host: FUZZ" -of csv -o $i.csv ; done
_____
_____
_____
v2.1.0-dev
_____
:: Method      : GET
:: URL         : https://129.134.156.0
:: Wordlist    : FUZZ: /tmp/fbsubs
:: Header      : Host: FUZZ
:: Output file : 129.134.156.0.csv
:: File format : csv
:: Follow redirects : false
:: Calibration  : false
:: Timeout      : 10
:: Threads      : 40
:: Matcher      : Response status: 200-299,301,302,307,401,403,405,500
_____
:: Progress: [15/15] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00] :: Errors: 0 ::
```

WEB FUZZING

- Brute force using FFUF
- CRAWL using Katana
- Use archives such as waybackmachine
- Use URL shortners

WEB FUZZING

- Create custom wordlist for the application
- 1- gather all urls you can find of the target using katana, gau and others. Save all into one file and sort uniq

```
hussein98d@Hussein98D:/tmp$ gau example.com
https://mautic.example.com/
http://mautic.example.com/
http://www.example.com/5
http://policy-explanation.example.com
http://azwbqj95.example.com/
https://example.com/image/inspirational_quote.jpg
https://example.com/audio/inspirational_quote.mp3
http://example.com/..
http://www.example.com/source/caminho/para/script.php
https://geoserver.example.com/coredb
http://geoserver.example.com/
https://billing.example.com/discord.php&client_id=&client_secret=
https://billing.example.com/discord.php&client_id=1162861284455362570&client_secret
http://billing.example.com/
http://example.com/Main Page
http://www.example.com/some_img.jpg
https://scope.example.com/
http://scope.example.com/
http://scope2.example.com/
https://example.com/method/mymethod
http://example.com/method/mymethod
http://example.com/method/foo
https://example.com/method/foo
https://example.com/recordings/stream.mp4
https://link.example.com
```

WEB FUZZING

- Now, run LinkFinder on all of the URLs
- <https://github.com/GerbenJavado/LinkFinder>

```
hussein98d@Hussein98D:/tmp$ cat ex | rush -j10 "python3 /home/hussein98d/Desktop/Tools/LinkFinder/linkfinder.py -o cli -i {} | sort -u >> output"
[...]
[...]
```

WEB FUZZING

- Finally , sort uniq URLs + Endpoints found from LinkFinder and Crawling and create the wordlist

```
hussein98d@Hussein98D:/tmp$ cat ex.output | tr "/" "\n" | sort -u | more

%
*
*'
**'
*--><
*`'
.
..
...
...
:::<<
<
>
?
???
]
{{
|
~*
$
$$128technology.senecadata.com
$$abn.senecadata.com
$$bally.senecadata.com
$$products.senecadata.com
$$support.senecadata.com
```

WEB FUZZING

- FUZZ all subdomains/ips of the org with this wordlist
- Keep adding new paths/file names found

DORKING

- Be creative when using dorks
- Use multiple search engines (Google, Duck, Bing, etc)
- Create your own dorks

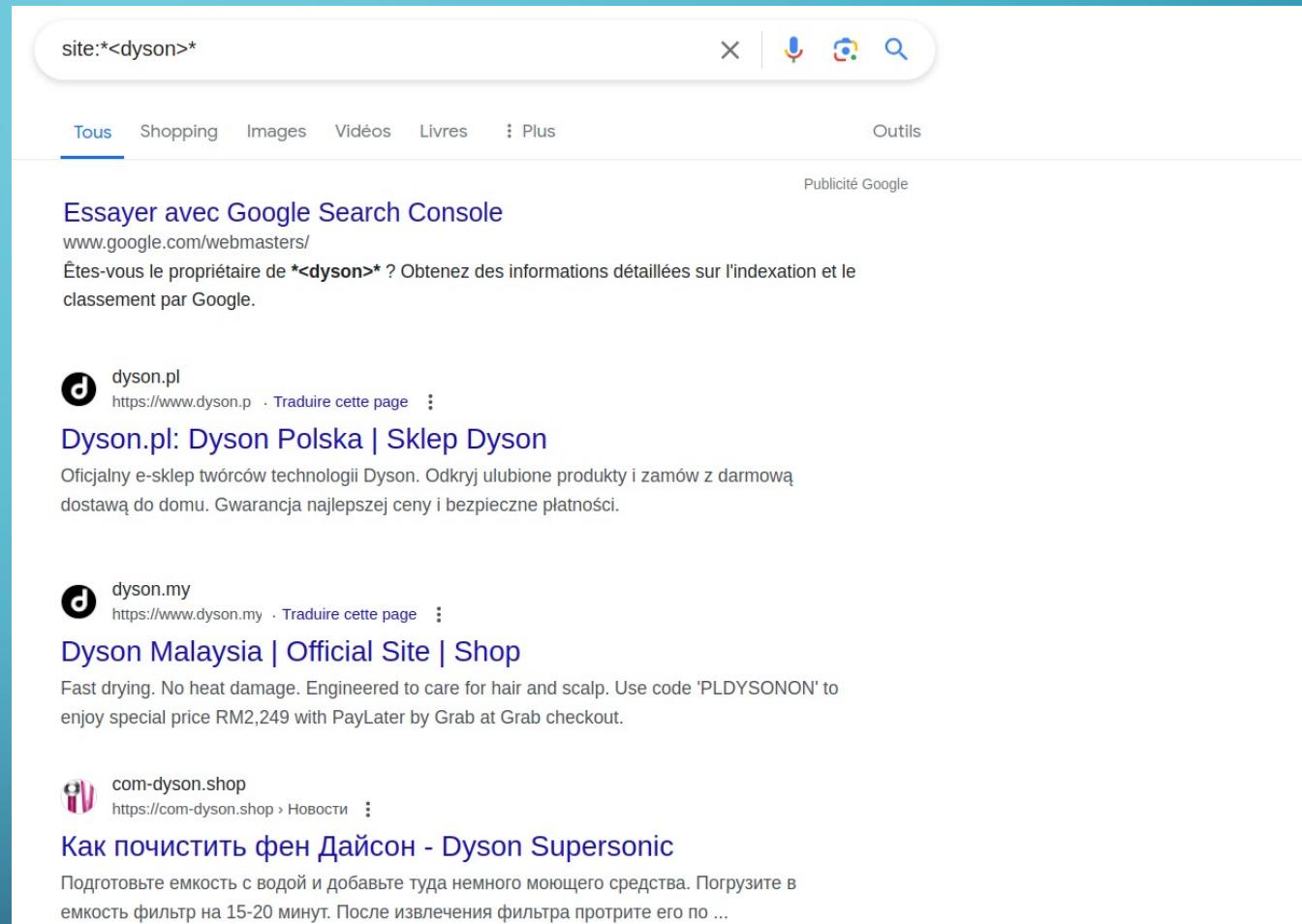
DORKING

- Powerful less known dorks

- site:*<example>*

site:: This operator restricts the search results to a specific site or domain.

<example>: The asterisks (*) are wildcards that match any character(s). In this case, the dork will match any domain or subdomain that contains the word "example".

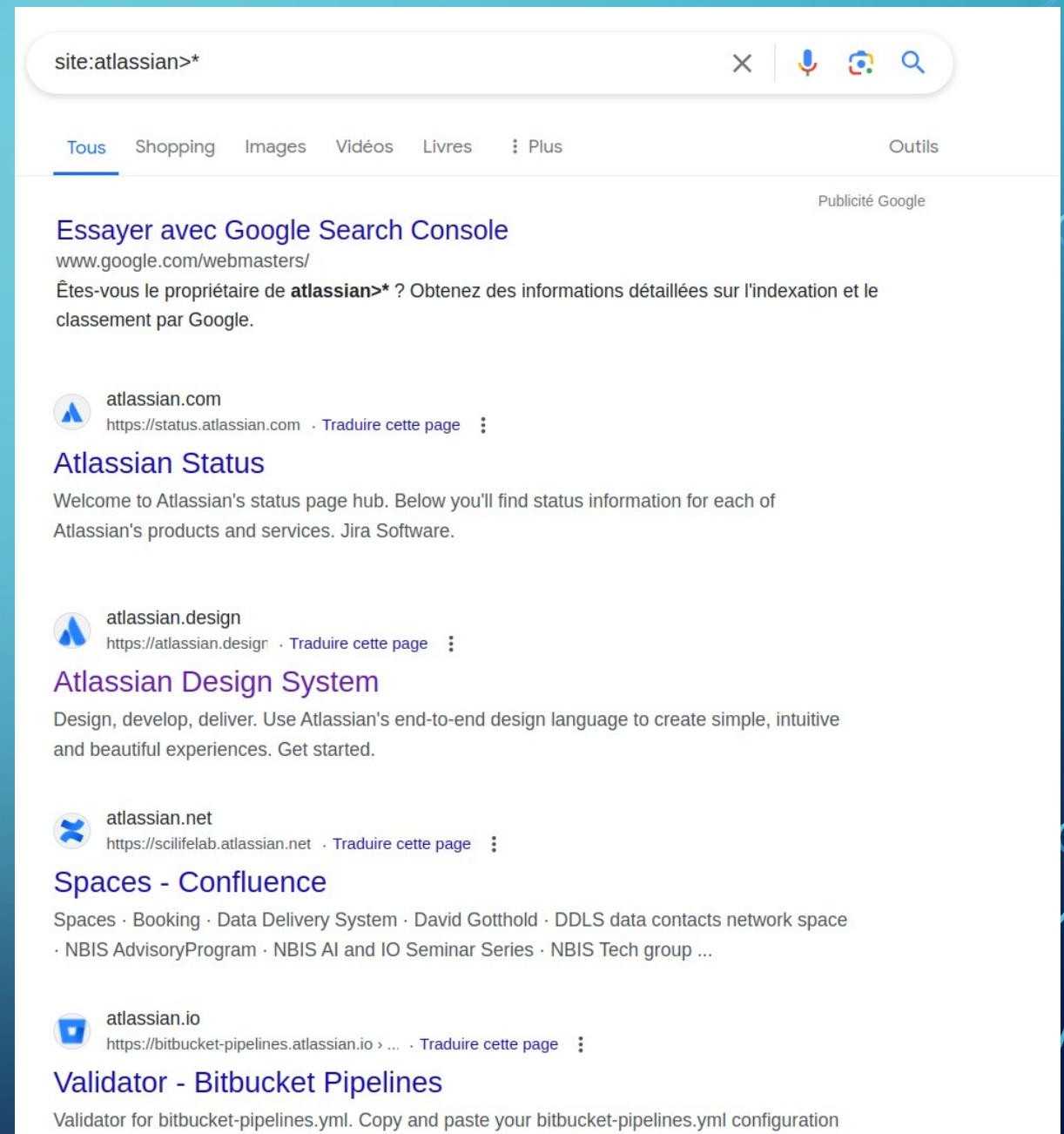


A screenshot of a Google search results page. The search bar at the top contains the query "site:*<dyson>*". Below the search bar, there are several navigation links: "Tous", "Shopping", "Images", "Vidéos", "Livres", "Plus", and "Outils". A "Publicité Google" link is also visible. The main content area displays three search results:

- dyson.pl**
https://www.dyson.p... · Traduire cette page ·
Dyson.pl: Dyson Polska | Sklep Dyson
Oficjalny e-sklep twórców technologii Dyson. Odkryj ulubione produkty i zamów z darmową dostawą do domu. Gwarancja najlepszej ceny i bezpieczne płatności.
- dyson.my**
https://www.dyson.my · Traduire cette page ·
Dyson Malaysia | Official Site | Shop
Fast drying. No heat damage. Engineered to care for hair and scalp. Use code 'PLDYSONON' to enjoy special price RM2,249 with PayLater by Grab at Grab checkout.
- com-dyson.shop**
https://com-dyson.shop > Новости ·
Как почистить фен Дайсон - Dyson Supersonic
Подготовьте емкость с водой и добавьте туда немного моющего средства. Погрузите в емкость фильтр на 15-20 минут. После извлечения фильтра протрите его по ...

DORKING

- Powerful less known dorks
- site:atlassian>*



A screenshot of a Google search results page. The search query is "site:atlassian>*". The results are filtered under the "Tous" tab. The first result is a snippet from the Google Search Console help center about the "atlassian>*" search operator. Below it are three links to Atlassian's own websites: "atlassian.com", "atlassian.design", and "atlassian.net". The last result is a link to a Bitbucket Pipelines configuration validator.

site:atlassian>*

Tous Shopping Images Vidéos Livres Plus Outils Publicité Google

Essayer avec Google Search Console
www.google.com/webmasters/
Êtes-vous le propriétaire de **atlassian>*** ? Obtenez des informations détaillées sur l'indexation et le classement par Google.

atlassian.com
<https://status.atlassian.com> · Traduire cette page

Atlassian Status
Welcome to Atlassian's status page hub. Below you'll find status information for each of Atlassian's products and services. Jira Software.

atlassian.design
<https://atlassian.design> · Traduire cette page

Atlassian Design System
Design, develop, deliver. Use Atlassian's end-to-end design language to create simple, intuitive and beautiful experiences. Get started.

atlassian.net
<https://scilifelab.atlassian.net> · Traduire cette page

Spaces - Confluence
Spaces · Booking · Data Delivery System · David Gotthold · DDLS data contacts network space · NBIS AdvisoryProgram · NBIS AI and IO Seminar Series · NBIS Tech group ...

atlassian.io
<https://bitbucket-pipelines.atlassian.io> · Traduire cette page

Validator - Bitbucket Pipelines
Validator for bitbucket-pipelines.yml. Copy and paste your bitbucket-pipelines.yml configuration

DORKING

- Powerful less known dorks
- site:`*<atlassian.*>*`

The screenshot shows a Google search results page with the query `site:*<atlassian.*>**` entered in the search bar. The results are filtered under the "Tous" tab. The first result is a link to the Atlassian website (`atlassian.co.jp`) with the title "アトラシアン". The second result is another link to the Atlassian website (`atlassian.co.jp`) with the title "製品". The third result is a blog post from tistory.com titled "Agile Project (Jira Software, Confluence, Portfolio for Jira)". The fourth result is another blog post from tistory.com titled "Jira Software Dashboard 활용 및 Gadget 추천 - Infraware". The results are displayed in Japanese.

site:`*<atlassian.*>*`

Tous Shopping Images Vidéos Livres Plus Outils Publicité Google

Essayer avec Google Search Console
www.google.com/webmasters/
Êtes-vous le propriétaire de `*<atlassian.*>*`? Obtenez des informations détaillées sur l'indexation et le classement par Google.

[atlassian.co.jp](http://www.atlassian.co.jp) http://www.atlassian.co.jp · Traduire cette page

アトラシアン
アトラシアンの Jira、Confluence、Trello などのコラボレーション ソフトウェアを使用すると、チームのコミュニケーションの促進、共同作業の管理・改善がしやすく ...

[atlassian.co.jp](https://www.atlassian.co.jp/software) https://www.atlassian.co.jp/software · Traduire cette page

製品
クラウド・アトラシアン製品で、インスタンスのセットアップやインフラ、セキュリティやメンテナンスを管理できます。 · アドオンを使うと、統合をカスタマイズできます。

[tistory.com](https://infrawaretech-atlassian.tistory.com) https://infrawaretech-atlassian.tistory.com > ... · Traduire cette page

Agile Project (Jira Software, Confluence, Portfolio for Jira)
22 août 2561 E. B. — Portfolio for Jira로 계획을 세우고 전체 그림을 확인할 수 있으며, 진행 상황을 추적하고 이해관계자와 간편하게 공유할 수 있습니다. - 일정 시각화 : ...

[tistory.com](https://infrawaretech-atlassian.tistory.com) https://infrawaretech-atlassian.tistory.com > ... · Traduire cette page

Jira Software Dashboard 활용 및 Gadget 추천 - Infraware
6 déc. 2561 E. B. — 1. 프로젝트의 실시간 정보를 확인 하는 보드(ex) 임원 및 프로젝트 관리자가 쉽게

DORKING

- Powerful less known dorks
- site:`*<*yahoo.*>*`

site:`*<*yahoo.*>*`

Tous Shopping Images Vidéos Livres Plus Outils Publicité Google

Essayer avec Google Search Console
www.google.com/webmasters/
Êtes-vous le propriétaire de `*<*yahoo.*>*`? Obtenez des informations détaillées sur l'indexation et le classement par Google.

yahoo.co.jp
<https://ads-promo.yahoo.co.jp> · Traduire cette page

【公式】Yahoo!広告でサイトへの集客アップ
Yahoo!広告とは、Yahoo! JAPANおよび提携パートナーサイトに広告配信ができるサービスです。Yahoo!広告には、「検索広告」と「ディスプレイ広告」の2種類があります。

yahoo.co.jp
<https://ymobile-store.yahoo.co.jp> · Traduire cette page

Yahoo!モバイル - ワイモバイルのSIMが合計最大26,000円相当 ...
【6/5まで】ワイモバイルのSIMにのりかえで合計最大26000円相当おトク（条件あり）。スマホのおトクな特典・キャンペーンも実施中！

yahoo.co.jp
<https://global-marketing.yahoo.co.jp> · Traduire cette page

Yahoo! JAPAN Marketing Solutions
Yahoo! JAPAN has various types of advertising. Offers a variety of custom solutions to build your brand, driving the response you want.

yahoo.co.jp
<https://store.shopping.yahoo.co.jp> · Traduire cette page

エレコムダイレクトショッピング - Yahoo!ショッピング

DORKING

- Powerful less known dorks

- site:yahoo.*

site:: This operator restricts the search results to a specific site or domain.

yahoo.: The asterisks (*) are wildcards that match any character(s).

In this case, the dork will match any subdomain and any top-level domain associated with Yahoo.

The screenshot shows a search results page from Google. The search bar at the top contains the query "site:yahoo.*". Below the search bar, there are tabs for "Tous", "Shopping", "Images", "Vidéos", "Livres", and "Plus", with "Tous" being the selected tab. To the right of the tabs is a "Outils" (Tools) button. A blue banner at the top of the results page reads: "Conseil : Limiter cette recherche aux résultats en français. Pour en savoir plus sur le filtrage par langue, cliquez ici." (Tip: Limit this search to French results. For more information on language filtering, click here.) On the right side of the page, there is a "Publicité Google" (Google Ad) for "Essayer avec Google Search Console" (Try with Google Search Console), which links to www.google.com/webmasters/. The ad text says: "Êtes-vous le propriétaire de *yahoo.* ? Obtenez des informations détaillées sur l'indexation et le classement par Google." (Are you the owner of *yahoo.*? Get detailed information on indexing and ranking by Google.) The search results list three entries:

- Yahoo**
yahoo.com
<https://login.yahoo.com> · Traduire cette page ·
Best in class Yahoo Mail, breaking local, national and global news, finance, sports, music, movies... You get more out of the web, you get more out of life.
- Yahoo France | Actualités, mail et recherche**
yahoo.com
<https://fr.yahoo.com> ·
Boîte de réception · Actualités · Santé · Sport · Finance · People · Life · Fact Check · Vidéos · Shopping · Auto · Horoscope · Plus.
- Yahoo | Mail, Weather, Search, Politics, News, Finance, Sport ...**
yahoo.com
<https://nz.yahoo.com> · Traduire cette page ·
Latest news coverage, email, free stock quotes, live scores and videos are just the beginning. Discover more every day at Yahoo!

BING

- Remember the IP list we got from ASN?
- Use bing to find valid hosts on the server
- Dork: “ip:127.0.0.1”

BING

microsoft Bing Deep search

SEARCH COPILOT AMASHUSHO VIDEWO AMAKARITA AMAKURU MORE TOOLS

About 3 results

valutec.net
<https://uat-vt-fullsteam.valutec.net> ▾

VTMerchantPortal

Web Multi-factor authentication is available for users to increase login security to your gift card reporting. This service requires an additional registration to include your mobile phone ...

REBA IBIRENZE

Valutec Customer Application Center
Vt Merchant Portal
Login
Create User - VTMerchantPortal
VT Merchant Portal - Valutec Card Solutions

Ni byo baguhitiyemo bashingiye ku bikunzwe cyane • Ibitekerezo

valutec.net
portalslink.com
vt.merchante-solutions....
vtmerchantportal.com
valutec.net

valutec.net
<https://uat-vt-shift4.valutec.net>

VTMerchantPortal - Valutec Card Solutions

Web Sign in to your account. Please enter your login information ... Congratulations!

REBA IBIRENZE

Log In – Valutech Inc.
Valutec Merchant Portal

Ni byo baguhitiyemo bashingiye ku bikunzwe cyane • Ibitekerezo

valutechinc.com
portalslink.com

valutec.net
<https://valuteccardsolutions-uat.valutec.net/Content/docs...> · PDF file

GOLF INDUSTRY GIFT CARD HELPFUL TIPS

Web GOLF INDUSTRY GIFT CARD HELPFUL TIPS There are many ways that you can use your loyalty and gift card program for your golf course, clubhouse, and pro-shop.

BING

- Sometimes the DNS name will not resolve . In this case, send IP + Domain name returned by Bing

The screenshot shows a browser developer tools interface with the Network tab selected. The request section shows a GET request to `https://156.55.138.226`. The response section shows the server's response headers, including a Content-Security-Policy header. The inspector panel on the right shows the target URL as `https://156.55.138.226`.

Request

```
1 GET / HTTP/1.1
2 Host: uat-vt-shift4.valutec.net
3 Accept-Encoding: gzip, deflate, br
4 Accept: */*
5 Accept-Language: en-US;q=0.9,el;q=0.8
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
    Chrome/124.0.6367.60 Safari/537.6
7 Connection: close
8 Cache-Control: max-age=0
9
10
```

Response

```
1 HTTP/1.1 200 OK
2 Date: Fri, 24 May 2024 03:39:49 GMT
3 Server: server
4 Cache-Control: Private, no-cache, no-store, must-revalidate, pre-check=0, post-check=0, max-age=0,
    s-maxage=0, no-transform
5 Pragma: no-cache
6 Content-Type: text/html; charset=utf-8
7 Expires: -1
8 Vary: Accept-Encoding
9 Content-Security-Policy: default-src 'self' ; script-src 'self' *.google-analytics.com *.googleapis.com
    *.googlecode.com *.jquery.com:* ;connect-src 'self'; img-src 'self'; style-src 'self' ;frame-ancestors
    'self' *.valutec.net;
10 X-Frame-Options: SAMEORIGIN
11 Strict-Transport-Security: max-age=31536000; includeSubDomains
12 X-Content-Type-Options: nosniff
13 X-XSS-Protection: 1; mode=block
14 Content-Length: 14552
15 Content-Security-Policy: default-src 'self' ; script-src 'self' 'unsafe-inline' 'unsafe-eval' ; style-src
    'self' 'unsafe-inline' 'unsafe-eval'; img-src 'self' data;
16 Connection: close
17
18
19
20 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
    "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
21 <html xmlns="http://www.w3.org/1999/xhtml">
22     <head id="Head1">
        <title>
            VMMerchantPortal
    </head>
23     <body>
        <div>
            <h1>VMMerchantPortal</h1>
            <p>Welcome to the VMMerchantPortal!</p>
            <p>Please log in to access your account information.</p>
        </div>
    </body>
</html>
```

Inspector

Target: `https://156.55.138.226`

- Request attributes
- Request query parameters
- Request body parameters
- Request cookies
- Request headers
- Response headers

BING

- Use inbody:example
instreamset:(title url):example

The screenshot shows the Microsoft Bing search interface. The search bar contains the query "domain:fisglobal.com inbody:login". Below the search bar, it says "About 4,230 results". The first result is for "FISLink - FIS Secure File and Message Transfer". It includes a "Sign in" button, a "register here" link, and a "CLIENTS/CUSTOMERS: Reset you..." link. The page also lists various URLs under "REBA IBIRENZE" and "fisglobal.com". The second result is for "Investran - FIS". The third result is for "Ibindi abantu babaza". At the bottom, there are three cards: "What is FIS code connect?", "Is FIS a member of the Fortune 500?", and "What c".

Microsoft Bing

domain:fisglobal.com inbody:login

SEARCH COPILOT AMASHUSHO VIDEWO AMAKARITA AMAKURU MORE TOOLS Deep search

About 4,230 results

fisglobal.com https://fislink.fisglobal.com

FISLink - FIS Secure File and Message Transfer

Web CLIENT/CUSTOMER LOGIN: Login on the left with the email address and password you provided during registration. CLIENT/CUSTOMER SUPPORT: Do you need assistance ...

Sign in register here

CLIENTS/CUSTOMERS: Reset you...

REBA IBIRENZE

[Login | FIS](#)

[Login to FIS Client Portal](#)

[FISLink - FIS Secure File and Message Transfer](#)

[FISLink – Employee Login Instructions](#)

[FIS Client Self-Service Portal Help](#)

fisglobal.com

my.fisglobal.com

fislink.fisglobal.com

fislink.fisglobal.com

clientssp.fnfis.com

Ni byo baguhitiyemo bashingiye ku bikunzwe cyane • Ibitekerezo

fisglobal.com

https://login.fisglobal.com/idp/investran

Investran - FIS

Web This is a FIS Application environment, which may be accessed and used only for official business by authorized personnel. Unauthorized access or use of this environment is ...

Ibindi abantu babaza

What is FIS code connect?

Code Connect: FIS Code Connect is an **API Marketplace** or **API Gateway**, which provides one-stop access to all

Is FIS a member of the Fortune 500?

Headquartered in Jacksonville, Florida, **FIS** is a member of the Fortune 500®

What c

FIS is a **financial** solution

TIPS AND TRICKS

- Gather all URLs of target using all techniques discussed
- Sent to Intruder and mass-test
- Example: GET http://localhost:22 HTTP/2

TIPS AND TRICKS

- Gather all URLs of target using all techniques discussed
- Sent to Intruder and mass-test
- Example: GET http://localhost:22 HTTP/2

② Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: `https://$example.com$` subdomain wordlist

```
1 GET http://localhost:22 HTTP/1.1
2 Host: example.com
3 Accept-Encoding: gzip, deflate, br
4 Accept: /*
5 Accept-Language: en-US;q=0.9,en;q=0.8
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.60 Safari/537.36
7 Connection: close
8 Cache-Control: max-age=0
9
10
```

SSRF Payload

TIPS AND TRICKS

The screenshot shows a network traffic capture interface with two main sections: Request and Response.

Request:

- Buttons: Send, Cancel, < >.
- Section title: Request.
- Sub-sections: Pretty, Raw, Hex.
- Text area:

```
1 GET http://localhost:22 HTTP/1.1
2 Host: mka-...
3 Connection: ...
4
5
```

Response:

- Section title: Response.
- Sub-sections: Pretty, Raw, Hex, Render.
- Text area:

```
1 HTTP/1.1 200 OK
2 Date: Mon, 06 Feb 2023 14:53:45 GMT
3 Server: Apache
4 Connection: close
5 Content-Length: 38
6
7 SSH-2.0-OpenSSH_7.4Protocol mismatch.
8
```

CASE STUDY

- When I started to hack on FIS program, I found tons of domain names they own by using reverse whois:
<https://www.whoxy.com/company/41024>

Fidelity National Information Services

[Reverse Whois](#) » COMPANY [Fidelity National Information Services] { 190,312 domain names }

NUM	DOMAIN NAME	REGISTRAR	CREATED	UPDATED	EXPIRY
1	fnx.com	MarkMonitor Inc.	8 Jun 1994	6 May 2024	7 Jun 2025
2	cdonexus.com	MarkMonitor Inc.	6 Jun 2005	24 May 2024	6 Jun 2026
3	cardholderadoption.com	MarkMonitor Inc.	31 May 2016	29 Apr 2024	31 May 2025
4	privacyu.com	MarkMonitor Inc.	31 May 2000	29 Apr 2024	31 May 2025
5	platformsecurities.com	MarkMonitor Inc.	19 Jun 2013	18 May 2024	19 Jun 2025
6	cuvance.net	MarkMonitor Inc.	14 Jun 2016	13 May 2024	14 Jun 2025
7	cuvance.com	MarkMonitor Inc.	14 Jun 2016	13 May 2024	14 Jun 2025
8	cuvance.org	MarkMonitor Inc.	14 Jun 2016	18 May 2024	14 Jun 2025
9	webticketsystem.com	MarkMonitor Inc.	11 Jun 2002	10 May 2024	11 Jun 2025
10	webticketsystem.net	MarkMonitor Inc.	11 Jun 2002	10 May 2024	11 Jun 2025
11	xfgate.com	MarkMonitor Inc.	9 Jun 2009	8 May 2024	9 Jun 2025
12	nomadcards.com	MarkMonitor Inc.	15 Jun 2007	14 May 2024	15 Jun 2025
13	aptrisk.com	MarkMonitor Inc.	9 Apr 2002	10 Apr 2024	9 Apr 2025

CASE STUDY

- It would be impossible for me to dork all these domains manually
- Decided to take the hard way and code a tool to bypass search engines captchas, rate limits , and others

CASE STUDY

- It would be impossible for me to dork all these domains manually
- Decided to take the hard way and code a tool to bypass search engines captchas, rate limits , and others

CASE STUDY

- After spending a couple days coding my tool, I finally came up with a tool to dork on Google, Bing, Yahoo, DuckDuckgo and Baidu in no time

```
root@localhost:/tmp# bash dork.sh
Usage: dork.sh <dork> [--engines engine1 engine2 ...]

Arguments:
  <dork>                  The dork query to search for.
  --engines engine1 engine2 (Optional) Specify the search engines to use (default: aol baidu google duck bing).
                           Available engines: aol, baidu, google, duck, bing.

Example:
  dork.sh "inurl:admin" --engines google bing
root@localhost:/tmp# rm dork.sh ; nano dork.sh
root@localhost:/tmp# bash dork.sh
Usage: dork.sh <dork> [--engines engine1 engine2 ...]

Arguments:
  <dork>                  The dork query to search for.
  --engines engine1 engine2 (Optional) Specify the search engines to use (default: aol baidu google duck bing).
                           Available engines: aol, baidu, google, duck, bing.

Example:
  dork.sh "inurl:admin" --engines google bing
coded by @hussein98d
root@localhost:/tmp#
```

CASE STUDY

- My tool would take as input the dork and the engines to search on

```
root@localhost:/tmp# bash dork.sh "site:fisglobal.com 'login'" --engines google bing > fisout
root@localhost:/tmp# cat fisout | httplinks | wc -l
391
root@localhost:/tmp# cat fisout | head -n 20
295
95
1445
595
1095
1495
1845
895
1795
40
80
1195
40
30
545
30
745
120
190
60
root@localhost:/tmp# cat fisout | httplinks| head -n 20
http://empower2.fisglobal.com/rs/092-EMI-875/images/MultiPay
https://acbs-docs-public-pnc.fisglobal.com/
https://acttst.fisglobal.com/
https://acttst.fisglobal.com/idpInitGlobalLogout.html
https://advisorgroup-sms.fisglobal.com/BackEnd/WebObjects/BackEnd.woa/wa/
https://advisorgroup-sms.fisglobal.com/Client/WebObjects/Client.woa/wa/
https://agla-sms.fisglobal.com/
https://aisecure-lr.fisglobal.com/
https://amer-pts-dr.fisglobal.com/
https://app.fcm.fisglobal.com/
https://aps2-sftp.imcs.fisglobal.com/EFTClient/Account/LostUsername.htm
https://aps-sftp.imcs.fisglobal.com/
https://ap-uat3.fisglobal.com/
https://bankofchinadrcitrix.fisglobal.com/
https://brinksvision1.fisglobal.com/VArchiveWebClient/Login.aspx
https://bts-hedgesuite-uat.fisglobal.com/
https://careers.fisglobal.com/us/en
https://careers.fisglobal.com/us/en/c/call-center-jobs?from=10
https://careers.fisglobal.com/us/en/c/finance-accounting-jobs
https://careers.fisglobal.com/us/en/c/sales-jobs?from=10
root@localhost:/tmp#
```

CASE STUDY

- Now, we have a dork tool working and a huge list of domains. What next? Dork with all sites!

```
root@localhost:/tmp/fis# head -n 10 list
infinity.com
olaccess.com
perfplusk12.com
sungarddx.com
automatedfinancial.com
securitiesinterlink7.com
automatedfinancial.com
benefitwebaccess.com
benefitwebaccess.net
infinity.com
root@localhost:/tmp/fis# for i in $(cat list); do bash dork.sh "site:$i 'login'" >> all
```

CASE STUDY

- After a couple permutations on dork and on all sites - example: site:example ‘login’ , site:example ‘upload’ etc I was left with around 100,000 unique links

```
root@localhost:/tmp/fis# cat out* | sort -u | httplinks | wc -l  
99266  
root@localhost:/tmp/fis# █
```

CASE STUDY

- And just like this, we have a ton to look into

```
root@localhost:/tmp/fis# cat outall | grep -i login | head -n 30
http://demo-coe.automatedfinancial.com/login.html
http://ebtedge.com/cardholderlogin/
http://ebtedge.com/ezLogin.htm
http://ebtedge.com/login
http://ezcardinfo.com/login
http://infinity.com/login
http://login.billsupport.com/
http://retirementlogin.com/
http://retirementlogin.net/
http://retirementlogin.net/efc/help/ENG/contents.htm
http://retirementlogin.net/retirementllc/help/ENG/contents.htm
https://abacusbank.coreshare.insidefsi.com/Login.aspx
https://achievacu.coreshare.insidefsi.com/Login.aspx
https://achievacu.coreshare.insidefsi.com/Login_Auth.aspx
https://adamscommunity.coreshare.insidefsi.com/login.aspx
https://admin.regulatoryu.com/cgi/login.cgi
https://akron-oh.perfplusk12.com/login_process.asp
https://alpinsecurities.fisglobal.com/investor/login/oauth2/authorization/idp-wst
https://alpinsecurities.fisglobal.com/investor/ws/loginredirect
https://americanmetrobank.coreshare.insidefsi.com/Login.aspx
https://ameritas.infinity.com/login.aspx
https://ameritas.infinity.com/loginerror.aspx
https://ameritas.omniasp.com/loginerror.aspx
https://ameritas-temp.omniasp.com/login.aspx
https://anywhere-connections.fisglobal.com/login
https://anywhere-connections.fisglobal.com/login/authenticate
https://aon.infinity.com/login.aspx
https://app.biznowcard.com/login
https://app.fcm.fisglobal.com/account/login
https://app.nextgencontrol.com/Core/Authentication/Login
```

CASE STUDY

- All the discovered URLs can be again crawled using Katana to discover more and more endpoints/paths, and then again sent to LinkFinder, and then again back to katana, and then again LinkFinder .
- It's a rinse and repeat process.
- Do not forget directory fuzzing on all sub-paths. For example `hxxps://alpinesecurities.fisglobal.com/investor/login/oauth2/authorization/FUZZ`

CASE STUDY

- During Mass-Dorking on my target, found a link similar to this:
- <https://host/Documentation/Branch/archive.zip>
- Upon downloading the archive, I found some credentials in a file

CASE STUDY

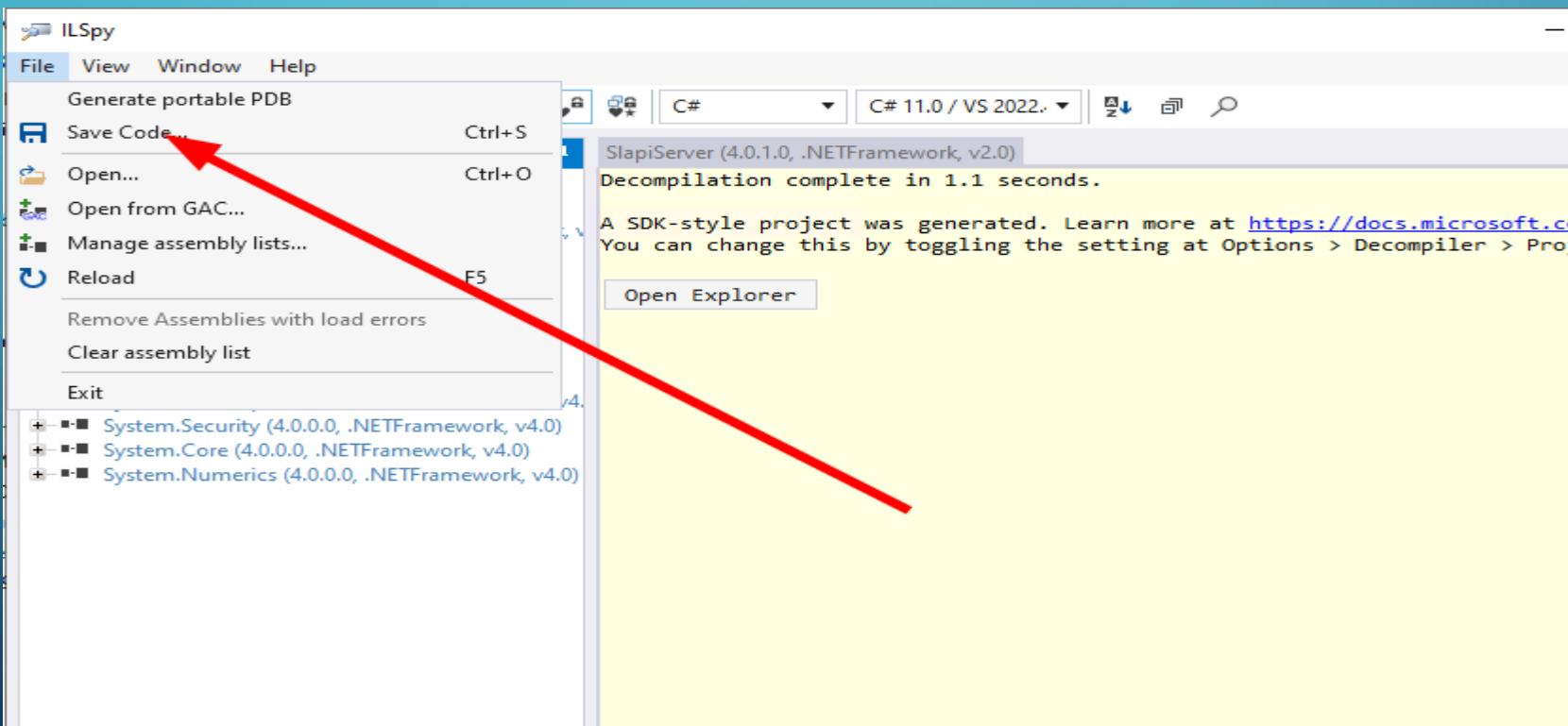
- **Credentials:**

CASE STUDY

- Great, we have credentials – what next? What endpoint to hit with these credentials?
- Archive contained a .exe installer
- After installing the software on my VPS, I was left with a couple DLLs files

CASE STUDY

- Decompile using <https://github.com/icsharpcode/ILSpy> or Similar



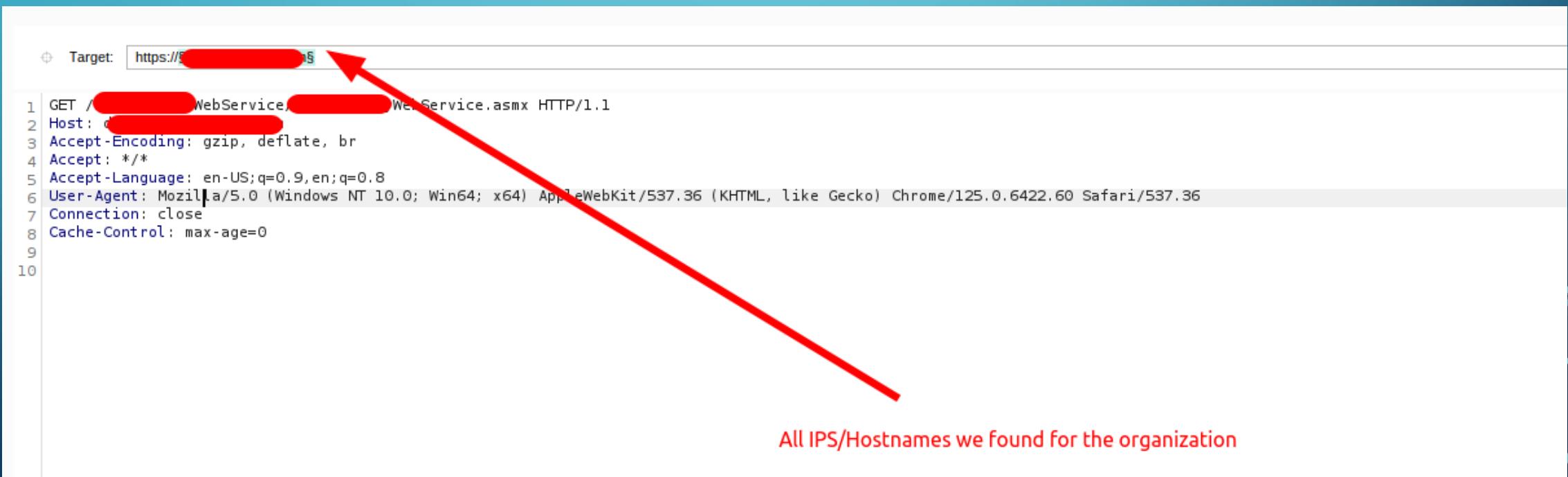
CASE STUDY

- Decompiled code showed some localhost URLs

```
decompiled/pda/Infragistics2.Win.UltraWinToolbars.v10.2/Infragistics.Win.UltraWinToolbars.Images.CheckMarkOptionWindowsVista.png: binary file matches
grep: decompiled/pda/Infragistics2.Win.UltraWinToolbars.v10.2/Infragistics.Win.UltraWinToolbars.Images.CheckMarkWindowsVista.png: binary file matches
grep: decompiled/pda/Infragistics2.Win.UltraWinGrid.v10.2/Infragistics.Win.UltraWinGrid.Images.UltraGridRowEditTemplateLauncher.png: binary file matches
grep: decompiled/pda/Infragistics2.Win.UltraWinGrid.v10.2/Infragistics.Win.UltraWinGrid.Images.ColorizableDropIndicatorDownArrow.png: binary file matches
grep: decompiled/pda/Infragistics2.Win.UltraWinGrid.v10.2/Infragistics.Win.UltraWinGrid.Images.DefaultDropIndicatorDownArrow.png: binary file matches
grep: decompiled/pda/Microsoft.ReportViewer.WebForms/Microsoft.Reporting.WebForms.rsclientprint-x64.cab: binary file matches
grep: decompiled/pda/Microsoft.ReportViewer.WebForms/Microsoft.Reporting.WebForms.rsclientprint-ia64.cab: binary file matches
grep: decompiled/pda/Microsoft.ReportViewer.WebForms/Microsoft.Reporting.WebForms.rsclientprint-x86.cab: binary file matches
grep: decompiled/pda/Infragistics2.Win.UltraWinDock.v10.2/Infragistics.Win.UltraWinDock.Graphics.DockingIndicator_Center_Bottom_Normal_VS2008_Vista.png: binary file matches
grep: decompiled/pda/Infragistics2.Win.UltraWinDock.v10.2/Infragistics.Win.UltraWinDock.Graphics.DockingIndicator_Center_Active_VS2008_Vista.png: binary file matches
grep: decompiled/pda/Infragistics2.Win.UltraWinDock.v10.2/Infragistics.Win.UltraWinDock.Graphics.DockingIndicator_Center_Top_Normal_VS2008_Vista.png: binary file matches
grep: decompiled/pda/Infragistics2.Win.UltraWinDock.v10.2/Infragistics.Win.UltraWinDock.Graphics.DockingIndicator_Center_Bottom_Active_VS2008_Vista.png: binary file matches
grep: decompiled/pda/Infragistics2.Win.UltraWinDock.v10.2/Infragistics.Win.UltraWinDock.Graphics.DockingIndicator_Arrow_VS2008_Vista.png: binary file matches
grep: decompiled/pda/Infragistics2.Win.UltraWinDock.v10.2/Infragistics.Win.UltraWinDock.Graphics.DockingIndicator_Center_Normal_VS2008_Vista.png: binary file matches
grep: decompiled/pda/Infragistics2.Win.UltraWinDock.v10.2/Infragistics.Win.UltraWinDock.Graphics.NavigatorDialog_VS2008_HeaderImage.png: binary file matches
grep: decompiled/pda/Infragistics2.Win.UltraWinDock.v10.2/Infragistics.Win.UltraWinDock.Graphics.DockingIndicator_Horizontal_Active_VS2008_Vista.png: binary file matches
grep: decompiled/pda/Infragistics2.Win.UltraWinDock.v10.2/Infragistics.Win.UltraWinDock.Graphics.DockingIndicator_Vertical_Normal_VS2008_Vista.png: binary file matches
grep: decompiled/pda/Infragistics2.Win.UltraWinDock.v10.2/Infragistics.Win.UltraWinDock.Graphics.DockingIndicator_Center_Top_Active_VS2008_Vista.png: binary file matches
grep: decompiled/pda/Infragistics2.Win.UltraWinDock.v10.2/Infragistics.Win.UltraWinDock.Graphics.DockingIndicator_Vertical_Active_VS2008_Vista.png: binary file matches
grep: decompiled/pda/Infragistics2.Win.UltraWinDock.v10.2/Infragistics.Win.UltraWinDock.Graphics.DockingIndicator_Horizontal_Normal_VS2008_Vista.png: binary file matches
decompiled/pda/A[REDACTED]es/Settings.cs:19: [DefaultSettingValue("http://localhost:2164/Branch[REDACTED]WebService.asmx")]
```

CASE STUDY

- It's now time to find the endpoint on one of the web servers of the org – we used burp intruder

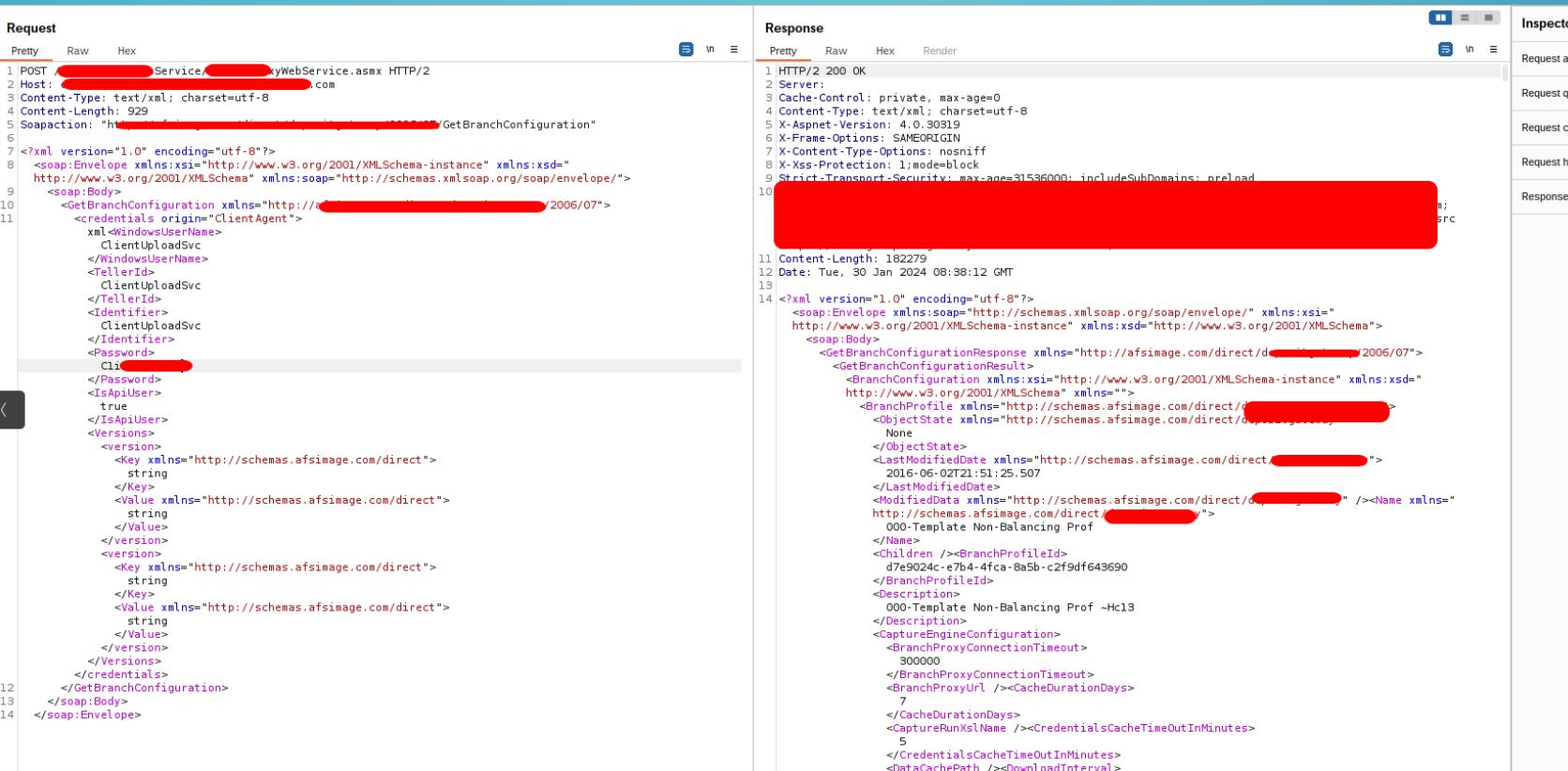


```
Target: https://[REDACTED].org:443
1 GET /[REDACTED] WebService/[REDACTED] Web.Service.asmx HTTP/1.1
2 Host: [REDACTED]
3 Accept-Encoding: gzip, deflate, br
4 Accept: */*
5 Accept-Language: en-US;q=0.9,en;q=0.8
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.60 Safari/537.36
7 Connection: close
8 Cache-Control: max-age=0
9
10
```

All IPs/Hostnames we found for the organization

CASE STUDY

- Found a subdomain with the path we are looking for! Time to send the correct credentials and XML data



The screenshot shows a web proxy interface with three main sections: Request, Response, and Inspector.

Request:

```
1 POST [REDACTED]Service.asmx HTTP/2
2 Host: [REDACTED].com
3 Content-Type: text/xml; charset=utf-8
4 Content-Length: 929
5 Soapaction: "http://[REDACTED]/GetBranchConfiguration"
6
7<?xml version="1.0" encoding="utf-8"?>
8<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
9  <soap:Body>
10   <GetBranchConfiguration xmlns="http://[REDACTED]/2006/07">
11     <credentials origin="ClientAgent">
12       <WindowsUserName>
13         ClientUploadSvc
14       </WindowsUserName>
15     <TellerId>
16       ClientUploadSvc
17     </TellerId>
18     <Identifier>
19       ClientUploadSvc
20     </Identifier>
21     <Password>
22       Cli[REDACTED]
23     </Password>
24     <IsApiUser>
25       true
26     </IsApiUser>
27     <Versions>
28       <version>
29         <Key xmlns="http://schemas.afsimage.com/direct">
30           string
31         </Key>
32         <Value xmlns="http://schemas.afsimage.com/direct">
33           string
34         </Value>
35       </version>
36       <version>
37         <Key xmlns="http://schemas.afsimage.com/direct">
38           string
39         </Key>
40         <Value xmlns="http://schemas.afsimage.com/direct">
41           string
42         </Value>
43       </version>
44     </Versions>
45   </credentials>
46 </GetBranchConfiguration>
47 <soap:Body>
48 </soap:Envelope>
```

Response:

```
1 HTTP/2 200 OK
2 Server:
3 Cache-Control: private, max-age=0
4 Content-Type: text/xml; charset=utf-8
5 X-Aspnet-Version: 4.0.30319
6 X-Frame-Options: SAMEORIGIN
7 X-Content-Type-Options: nosniff
8 X-Xss-Protection: 1;mode=block
9 Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
10
11 Content-Length: 182279
12 Date: Tue, 30 Jan 2024 08:38:12 GMT
13
14<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
<soap:Body>
<GetBranchConfigurationResponse xmlns="http://afsimage.com/direct/[REDACTED]/2006/07">
<GetBranchConfigurationResult>
<BranchConfiguration xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns="http://schemas.afsimage.com/direct/[REDACTED]">
<BranchProfile xmlns="http://schemas.afsimage.com/direct/[REDACTED]">
<ObjectState>
<LastModifiedDate xmlns="http://schemas.afsimage.com/direct/[REDACTED]">2016-06-02T21:51:25.507</LastModifiedDate>
<ModifiedData xmlns="http://schemas.afsimage.com/direct/[REDACTED]" /><Name xmlns="http://schemas.afsimage.com/direct/[REDACTED]">000-Template Non-Balancing Prof</Name>
<Children /><BranchProfileId>d7e9024c-e7b4-4fc4-8a5b-c2f9df643690</BranchProfileId>
<Description>000-Template Non-Balancing Prof ~Hc13</Description>
<CaptureEngineConfiguration>
<BranchProxyConnectionTimeout>300000</BranchProxyConnectionTimeout>
<BranchProxyConnectionTimeout>300000</BranchProxyConnectionTimeout>
<CacheDurationDays>7</CacheDurationDays>
<CacheRunXslName>/><CredentialsCacheTimeOutInMinutes>5</CredentialsCacheTimeOutInMinutes>
<DataCachePath /><DownloadInterval>
```

Inspector:

This section contains several dropdown menus and buttons for inspecting the request and response, such as Request attributes, Request query, Request cookie, Request header, and Response header.

TAKEAWAYS

- Don't be afraid to try new things
- Nothing is sure, nothing is unsure. Try what you have in mind and hope for the best.
- Spend a lot of time gathering intel about the org
- Hack when you feel like hacking

THANKS!