



LAB 02

Reconnaissance

TPAS

Leonardo Araújo Freitas | up202400832

setembro, 2024

Target	3
1. Task 1 - Email Reconnaissance	3
1.1. Email Service Provider (ESP)	3
1.2. Configuration	4
2. Task 2 - Passive Subdomain Enumeration	5
3. Task 3 - IP Tracking	6
4. Task 4 - Active http and https Services	7
5. Task 5 - URL Scanning	7
6. Task 6 - Special tasks	8
6.1. Google Dorks	8
6.2. Sensitive endpoints	10

Target

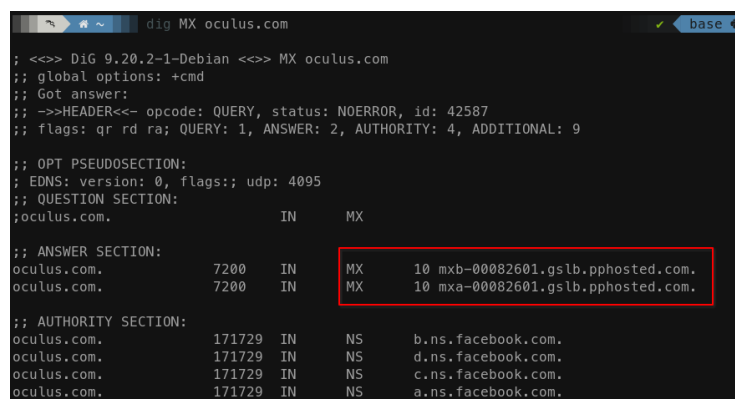
The target domain for this assignment is oculus.com

1. Task 1 - Email Reconnaissance

1.1. Email Service Provider (ESP)

Running *whois* command didn't give any information about the ESP.

Using *dig*: Gathered two answers which revealed MX domains associated with "Proofpoint" services.



```
dig MX oculus.com

; <<>> DiG 9.20.2-1-Debian <<>> MX oculus.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 42587
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 4, ADDITIONAL: 9

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4095
;; QUESTION SECTION:
;oculus.com.                IN      MX

;; ANSWER SECTION:
oculus.com.                7200    IN      MX      10 mxlb-00082601.gslb.pphosted.com.
oculus.com.                7200    IN      MX      10 mxa-00082601.gslb.pphosted.com.

;; AUTHORITY SECTION:
oculus.com.                171729  IN      NS      b.ns.facebook.com.
oculus.com.                171729  IN      NS      d.ns.facebook.com.
oculus.com.                171729  IN      NS      c.ns.facebook.com.
oculus.com.                171729  IN      NS      a.ns.facebook.com.
```

Figure 1: MX domains

Using MXToolBox: Found "Proofpoint" to be the ESP for the target.

SuperTool Beta9

oculus.com

MX Lookup

mx:oculus.com

Find Problems

Solve Email Delivery Problems

Pref	Hostname	IP Address	TTL		
10	mx-a-00082601.gslb.pphosted.com	67.231.145.42 Proofpoint, Inc. (AS28211)	120 min	Blacklist Check	SMTP Test
10	mx-b-00082601.gslb.pphosted.com	67.231.153.30 Proofpoint, Inc. (AS22843)	120 min	Blacklist Check	SMTP Test

Test	Result
DMARC Record Published	DMARC Record found
DMARC Policy Not Enabled	DMARC Quarantine/Reject policy enabled
DNS Record Published	DNS Record found

Your email service provider is "Proofpoint"

Need Bulk Email Provider Data?

Figure 2: MX domains and ESP

1.2. Configuration

smtp:mx-a-00082601.gslb.pphosted.com				
Category	Host	Result		
✓ smtp	mx-a-00082601.gslb.pphosted.com	OK - 67.231.153.30 resolves to mx-b-00082601.pphosted.com	More Info	
✓ smtp	mx-a-00082601.gslb.pphosted.com	OK - Reverse DNS is a valid Hostname	More Info	
✓ smtp	mx-a-00082601.gslb.pphosted.com	OK - Reverse DNS matches SMTP Banner	More Info	
✓ smtp	mx-a-00082601.gslb.pphosted.com	OK - Supports TLS.	More Info	
✓ smtp	mx-a-00082601.gslb.pphosted.com	0.203 seconds - Good on Connection time	More Info	
✓ smtp	mx-a-00082601.gslb.pphosted.com	OK - Not an open relay.	More Info	
✓ smtp	mx-a-00082601.gslb.pphosted.com	0.665 seconds - Good on Transaction Time	More Info	

Figure 3: Test on the first mail server

smtp:mx-b-00082601.gslb.pphosted.com				
Category	Host	Result		
✓ smtp	mx-b-00082601.gslb.pphosted.com	OK - 67.231.145.42 resolves to mx-a-00082601.pphosted.com	More Info	
✓ smtp	mx-b-00082601.gslb.pphosted.com	OK - Reverse DNS is a valid Hostname	More Info	
✓ smtp	mx-b-00082601.gslb.pphosted.com	OK - Reverse DNS matches SMTP Banner	More Info	
✓ smtp	mx-b-00082601.gslb.pphosted.com	OK - Supports TLS.	More Info	
✓ smtp	mx-b-00082601.gslb.pphosted.com	0.292 seconds - Good on Connection time	More Info	
✓ smtp	mx-b-00082601.gslb.pphosted.com	OK - Not an open relay.	More Info	
✓ smtp	mx-b-00082601.gslb.pphosted.com	1.195 seconds - Good on Transaction Time	More Info	

Figure 4: Test on the second email server

spf:oculus.com				
Category	Host	Result		
✓ spf	oculus.com	SPF Record found	More Info	
✓ spf	oculus.com	No deprecated records found	More Info	
✓ spf	oculus.com	Less than two records found	More Info	
✓ spf	oculus.com	No items after 'ALL'.	More Info	
✓ spf	oculus.com	The record is valid	More Info	
✓ spf	oculus.com	Number of included lookups is OK	More Info	
✓ spf	oculus.com	No type PTR found	More Info	
✓ spf	oculus.com	Number of void lookups is OK	More Info	
✓ spf	oculus.com	Number of MX Resource Records is OK	More Info	
✓ spf	oculus.com	No Null DNS Lookups found	More Info	

Figure 5 : SPF records information for oculus.com

spf:mx-a-00082601.gslb.pphosted.com Find Problems Solve Email Delivery Problems			spf
	Test	Result	
Status	NameSPF Record Published	ResponseNo SPF Record found	More Info

	Test	Result	
Status ✖	NameSPF Record Published	ResponseNo SPF Record found	More Info

The email provider appears to be well configured. The assessments ran confirmed no issues on SMTP and SPF. There have been no SPF records on each the MX hosts however if i looked for SPF on domain oculus.com I became capable of discover the existence of records. We can see that they also have a DMARC record published.

```

dig TXT oculus.com
;; Truncated, retrying in TCP mode.

; <<>> DiG 9.20.2-1-Debian <<>> TXT oculus.com
;; global options: +cmd
;; Got answer:
;; -->HEADER<-- opcode: QUERY, status: NOERROR, id: 25852
;; flags: qr rd ra; QUERY: 1, ANSWER: 8, AUTHORITY: 13, ADDITIONAL: 27

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 75a63852e56bc2a7c0471fe566f6e6a6b9cbb0e8f84d75d4 (good)
;; QUESTION SECTION:
;oculus.com.                IN      TXT

;; ANSWER SECTION:
oculus.com. 300 IN TXT "v=spf1 include:spf-00082601.pphosted.com include:spf.protection.outlook.com include:mail.zendesk.com include:app-spf.arenasolut" "ions.com include:spf.facebook.com include:servers.mcsv.net include:spf.mandrillapp.com include:mktomail.com ip4:163.114.130.16" " ip6:2620:10d:c091:400::8:1 ip4:163.114.132.120 ip6:2620:10d:c090:450::120 ip4:163.114.134.16 ip6:2620:10d:c09b:400::8:1 ip4:16" "3.114.135.16 ip6:2620:10d:c09c:400::8:1 -all"
oculus.com. 300 IN TXT "r7Wv17rB-rte1DermXCyHrnyU10ihYLkZCuM6xNT3NQ"
oculus.com. 300 IN TXT "atlassian-domain-verification=I7HLjLnLhJdIT58wzrru2Pd/2cRwa3AKlgCjDP0043GMP7H0QuafH6eBts3D1GaP"
oculus.com. 300 IN TXT "adobe-idp-site-verification=6589f998-6437-4ab2-99b1-02d67ece0131"
oculus.com. 300 IN TXT "7459f833d3664655b852ad410a354900"
oculus.com. 300 IN TXT "google-site-verification=WqjG2jhIhBeSE7gfCqR7HsF30hUVXdQPHfSSmkkTDL0"
oculus.com. 300 IN TXT "google-site-verification=J8rIciAaK7BrunIRBbAFfsbtkP0DpF1m2hcm2vKBoLM"
oculus.com. 300 IN TXT "cisco-ci-domain-verification=2643cd2482dca75881a12f388cd7c9d25493860dc5dff7db0ba992a7a32941c"

```

Figure 6: dig for type TXT

2. Task 2 - Passive Subdomain Enumeration

Used subfinder and assetfinder as showed in the following figures:

```

~/Doc/T/Lab2 subfinder -d oculus.com -o subfinder_output.txt

```

Figure 7: subfinder tool

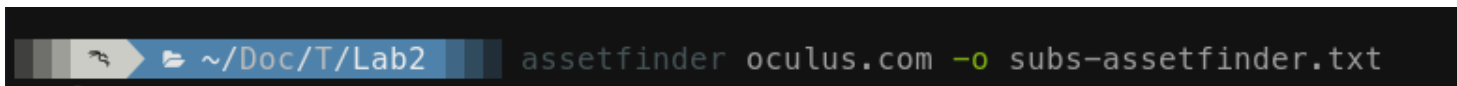


Figure 8: assetfinder tool

The file subs.txt with all the unique enumerated subdomains is included in the submitted zip.

3. Task 3 - IP Tracking

Subject chosen as subdomain: auth.ocius.com.

Executing the traceroute on the mentioned subdomain gets us the following figure:

```
Traceroute to auth.ocius.com (157.240.212.50), 30 hops max, 60 byte packets
 1  192.168.212.253 (192.168.212.253)  3.023 ms  3.545 ms  3.897 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  ae7.pr03.lisl.tfbnw.net (157.240.78.46)  73.987 ms  74.287 ms  73.688 ms
 9  po201.asw02.lisl.tfbnw.net (157.240.124.80)  73.622 ms  po201.asw01.lisl.tfbnw.net (157.240.124.78)  73.543 ms  73.472 ms
10  psw04.lisl.tfbnw.net (129.134.94.74)  73.404 ms  psw02.lisl.tfbnw.net (129.134.88.124)  73.344 ms  psw03.lisl.tfbnw.net (129.134.87.55)  73.266 ms
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

Figure 9: traceroute auth.ocius.com

Then we use the <https://www.ip-tracker.org> to track the location associated to with all the IPs from the trace.

The route resulting from the trace follows the order:

Private IP Address > Lisboa > US > Lisboa

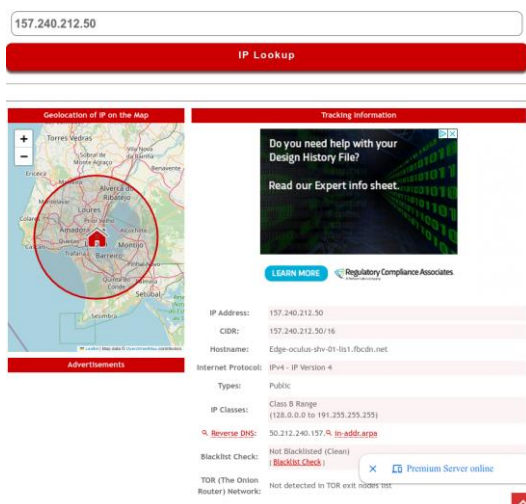


Figure 10

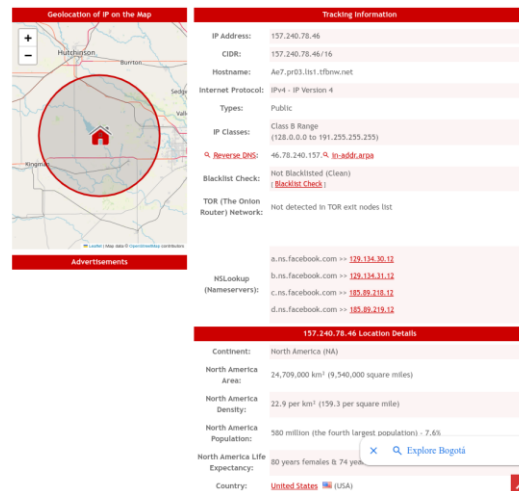


Figure 11

4. Task 4 - Active http and https Services

To remove subdomains that were outside of scope, it was used the command grep, and a new subs_edit.txt was generated.

```
~/Doc/T/Lab2 grep -v -e 'answers.oculus.com' -e 'forums.oculus.com' -e 'support.oculus.com' subs.txt > subs_edit.txt
```

Figure 12

Then httpprobe was used, saving all the URLs in the file urls.txt.

```
~/Doc/T/Lab2 cat subs_edit.txt | httpprobe | >> urls.txt
```

Figure 13

5. Task 5 - URL Scanning

Many of the URLs found were deprecated links or simply redirects. I ran the nuclei for the target:

<https://npm.developer.oculus.com>

```
~/Doc/T/L/Generated_Files nuclei -u https://npm.developer.oculus.com -rate-lim
it 50 -rl 20

v3.3.2
projectdiscovery.io

[INF] Current nuclei version: v3.3.2 (outdated)
[INF] Current nuclei-templates version: v10.0.0 (latest)
[WRN] Scan results upload to cloud is disabled.
[INF] New templates added in latest release: 255
[INF] Templates loaded for current scan: 8506
[INF] Executing 8505 signed templates from projectdiscovery/nuclei-templates
[WRN] Loading 1 unsigned templates for scan. Use with caution.
[INF] Targets loaded for current scan: 1
[INF] Templates clustered: 1586 (Reduced 1491 Requests)
[INF] Using Interactsh Server: oast.online
[missing-sri] [http] [info] https://npm.developer.oculus.com ["https://npm.developer.oculus.
com/-/static/runtime.9adbe059a74ff4e2d469.js","https://npm.developer.oculus.com/-/static/ven
dors.9adbe059a74ff4e2d469.js","https://npm.developer.oculus.com/-/static/main.9adbe059a74ff4
e2d469.js","https://npm.developer.oculus.com/-/static/ula_dialog.js"]
[waf-detect:nginxgeneric] [http] [info] https://npm.developer.oculus.com
[INF] Skipped npm.developer.oculus.com:443 from target list as found unresponsive 30 times
```

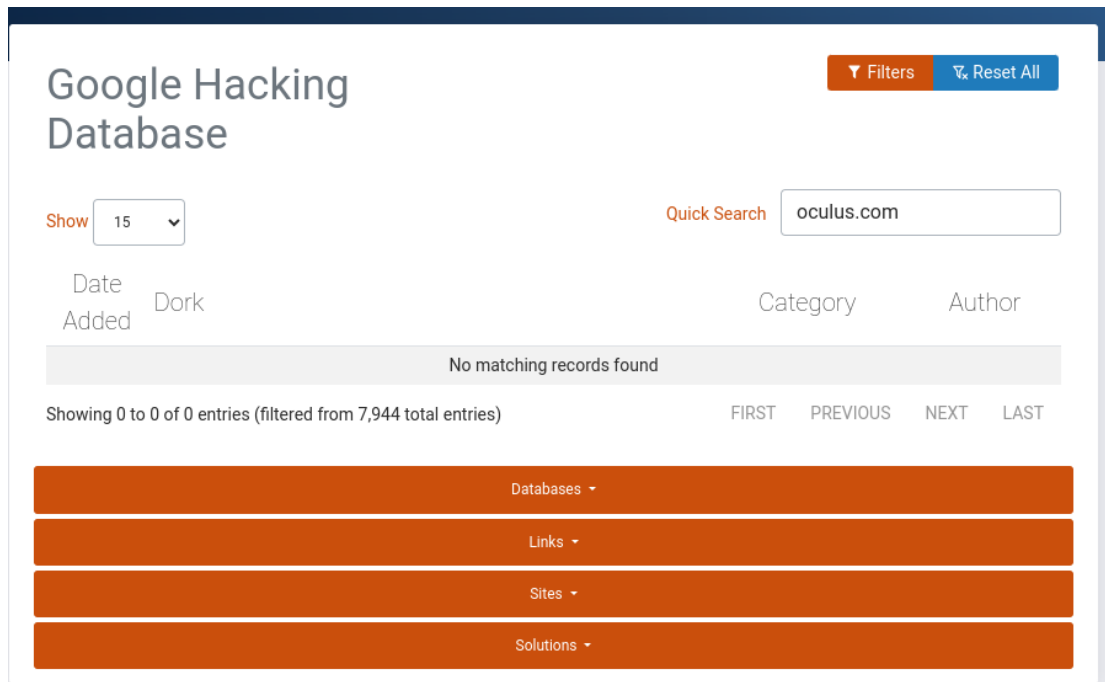
Figure 14

Nuclei detected several JavaScript files on the target missing Subresource Integrity (SRI) checks and a generic Nginx Web Application Firewall (WAF) was detected.

6. Task 6 - Special tasks

6.1. Google Dorks

By searching oculus.com on the Google Hacking Database, there was no dork published.



I tried running some google dorks that would make sense for the url but I didn't get any results.

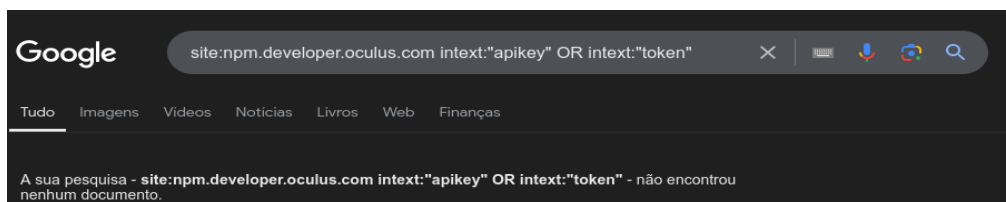
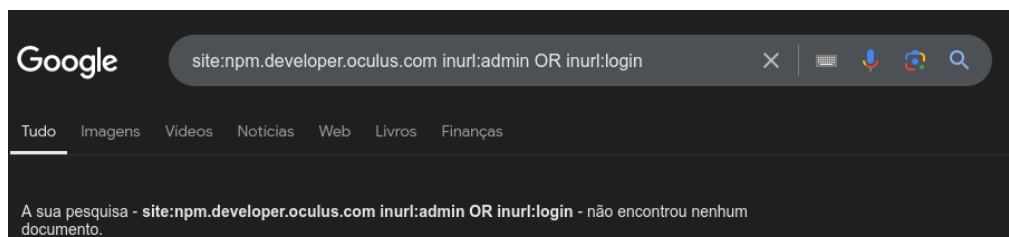
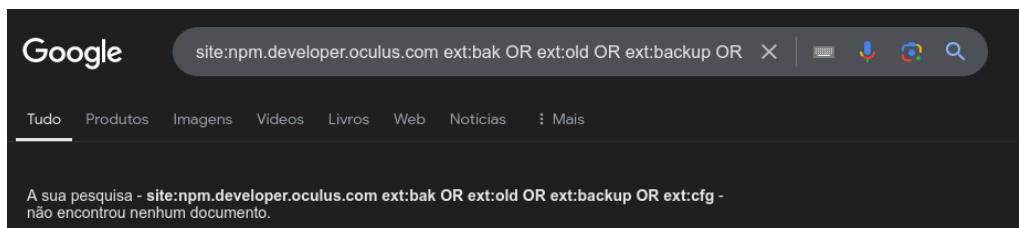


Figure 15

6.2. Sensitive endpoints

Unfortunately, the findings of task 5 don't seem to be relevant enough or sensitive enough to explore deeper. The dorks didn't produce any relevant or sensitive information either.