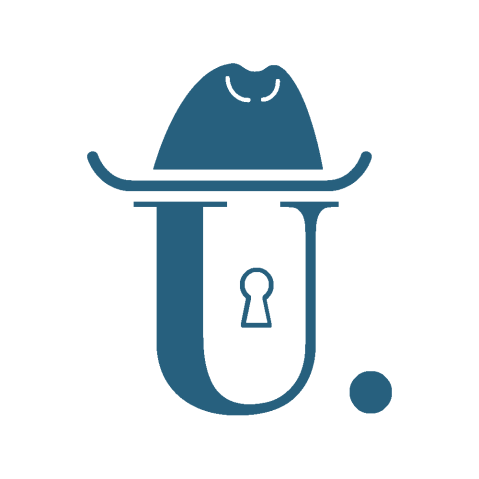
****

**LAB 02**

**Reconnaissance**

**TPAS**

**Leonardo Araújo Freitas | up202400832**

setembro, 2024

[Target 3](#_Toc661430009)

[1. Task 1 - Email Reconnaissance 3](#_Toc31020985)

[1.1. Email Service Provider (ESP) 3](#_Toc278514326)

[1.2. Configuration 4](#_Toc1507307804)

[2. Task 2 - Passive Subdomain Enumeration 5](#_Toc773585128)

[3. Task 3 - IP Tracking 6](#_Toc1316455315)

[4. Task 4 - Active http and https Services 7](#_Toc1553254757)

[5. Task 5 - URL Scanning 7](#_Toc1914462828)

[6. Task 6 - Special tasks 8](#_Toc301152161)

[6.1. Google Dorks 8](#_Toc148617954)

[6.2. Sensitive endpoints 10](#_Toc1522205733)

# Target

#### The target domain for this assignment is oculus.com

## Task 1 - Email Reconnaissance

## 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.

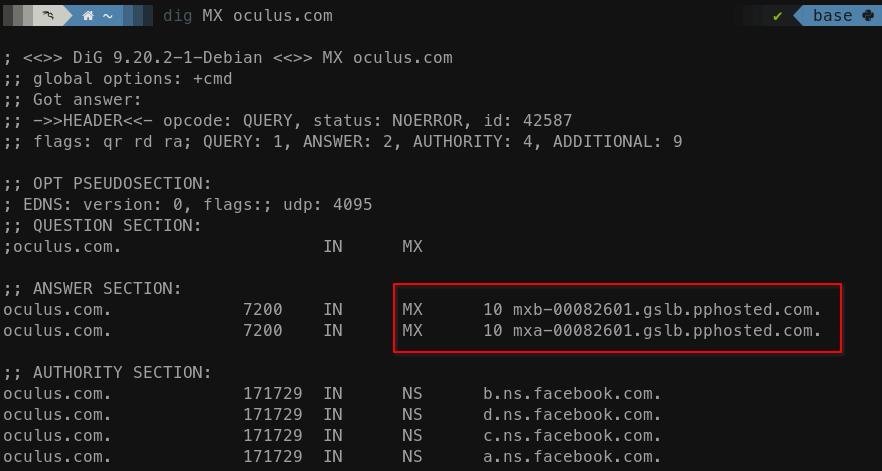


Figure 1: MX domains

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

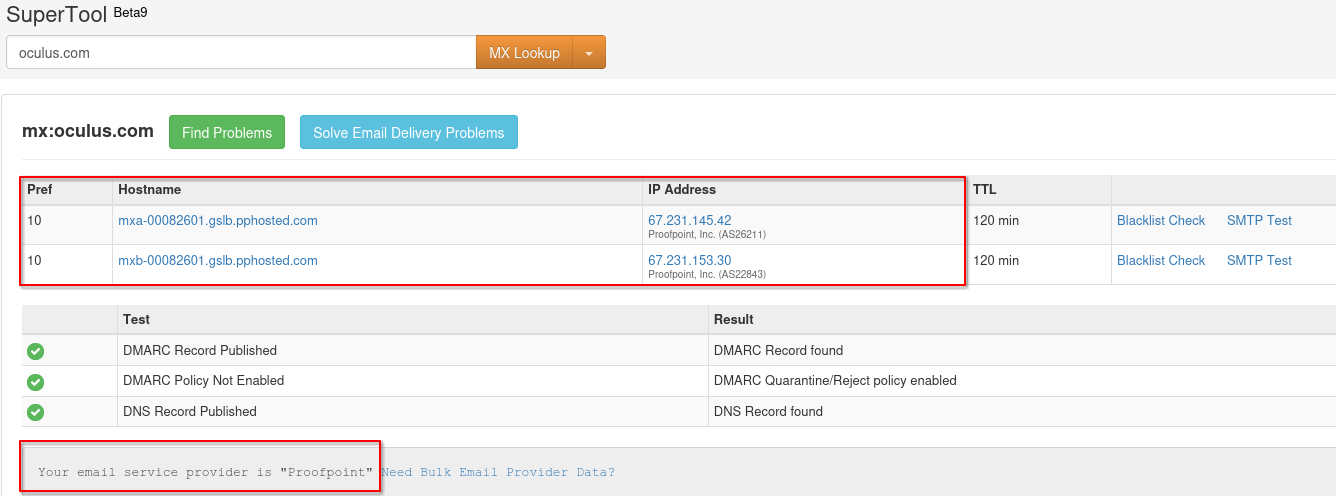
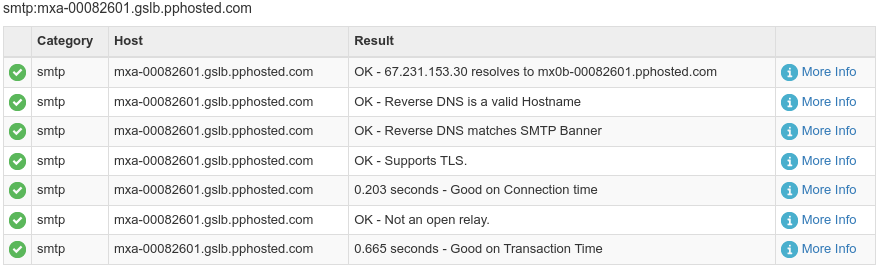
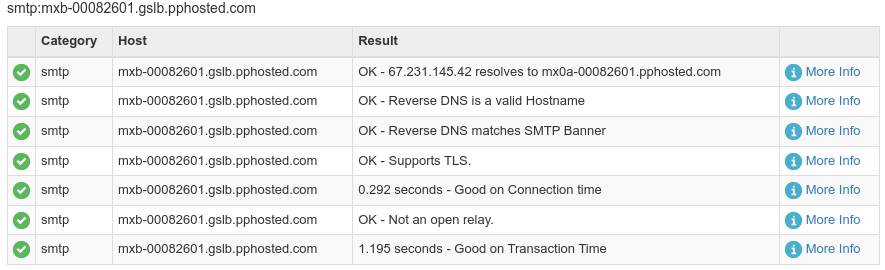


Figure 2: MX domains and ESP

## Configuration

Figure 3: Test on the first mail server Figure 4: Test on the second email server

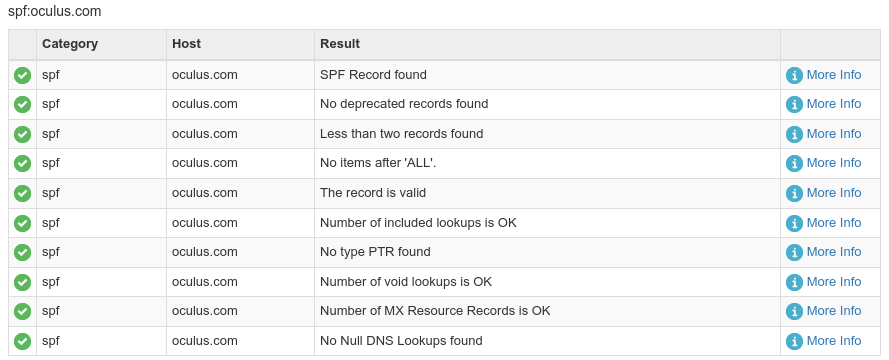
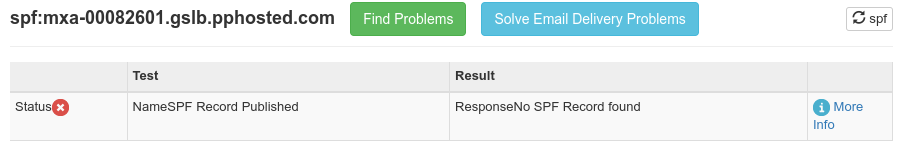
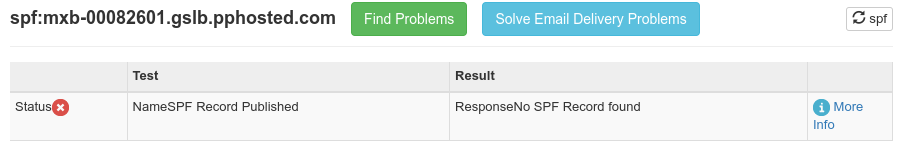


Figure 5 : SPF records information for oculus.com





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.

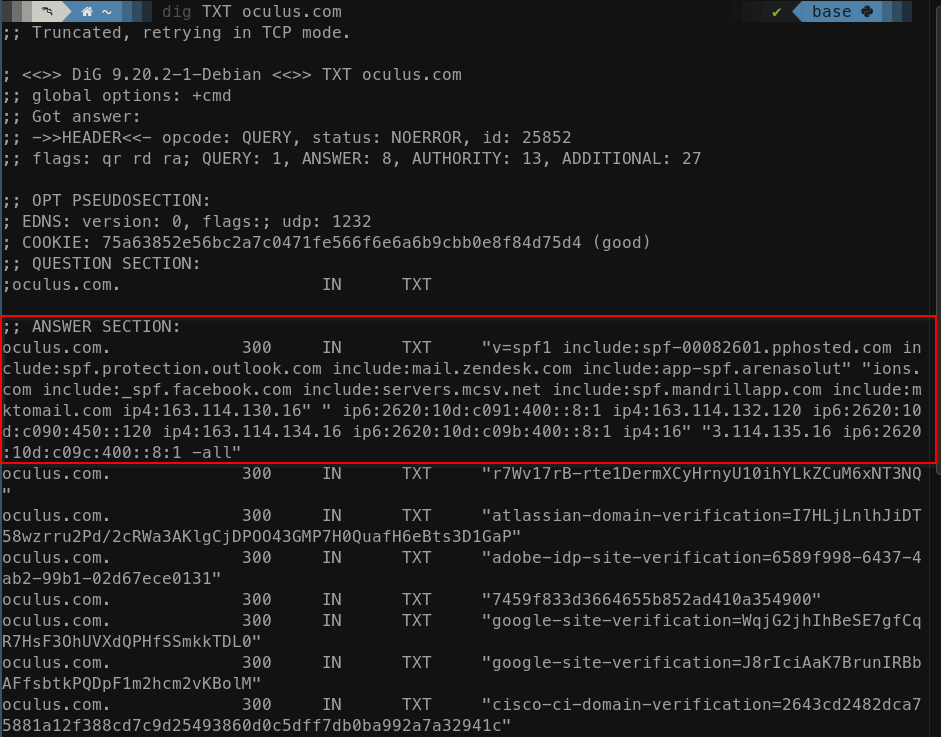


Figure 6: dig for type TXT

## Task 2 - Passive Subdomain Enumeration

Used subfinder and assetfinder as showed in the following figures:



Figure 7: subfinder tool



Figure 8: assetfinder tool

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

## Task 3 - IP Tracking

Subject chosen as subdomain: auth.oculus.com.

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

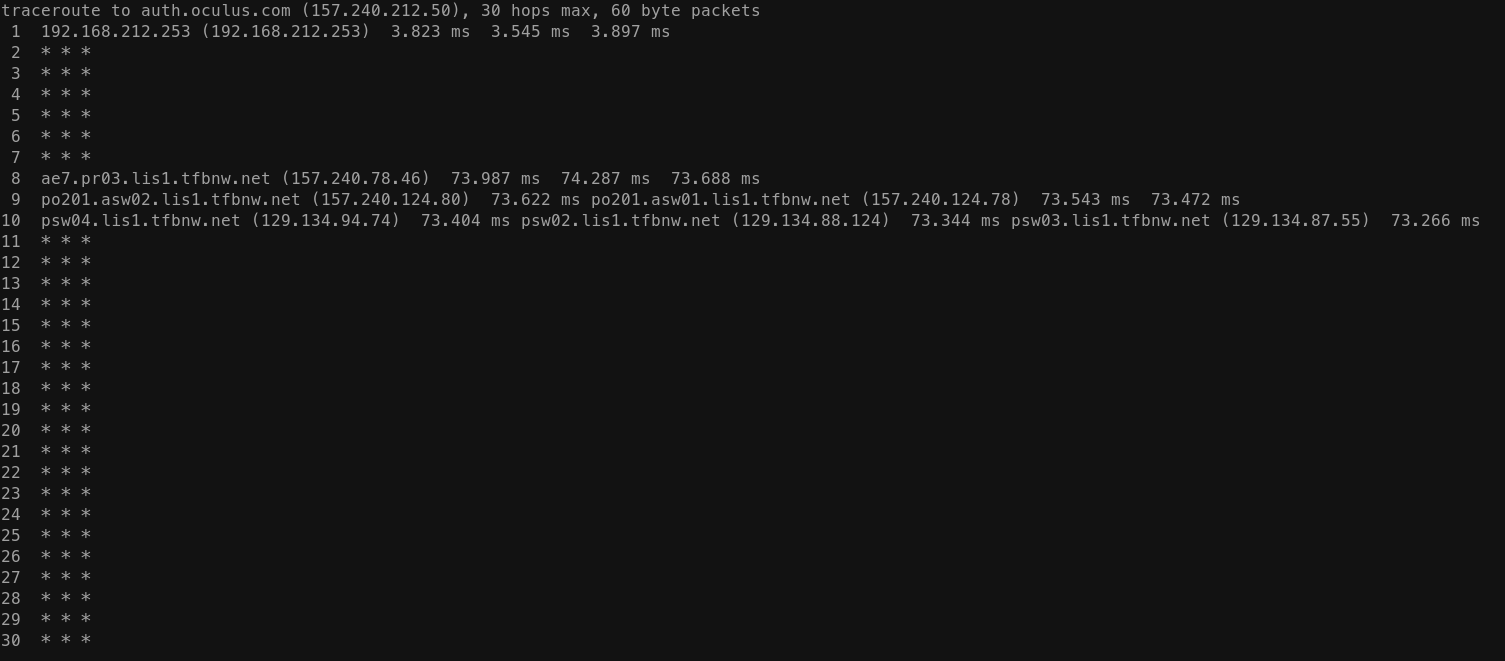


Figure 9: traceroute auth.oculus.com

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

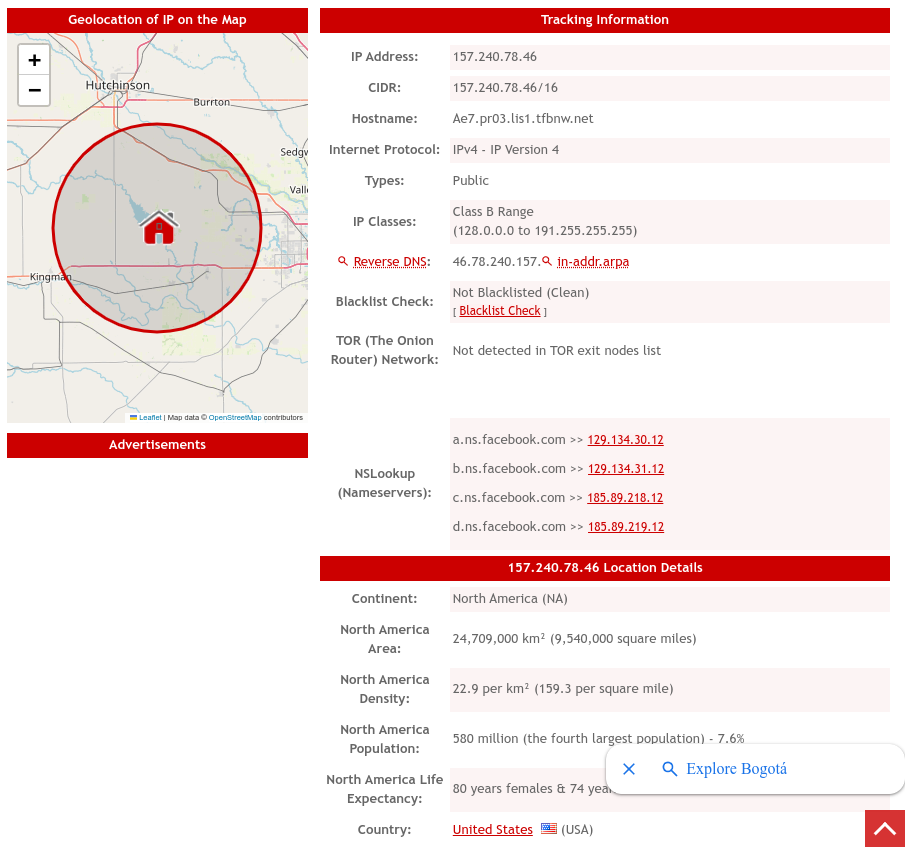
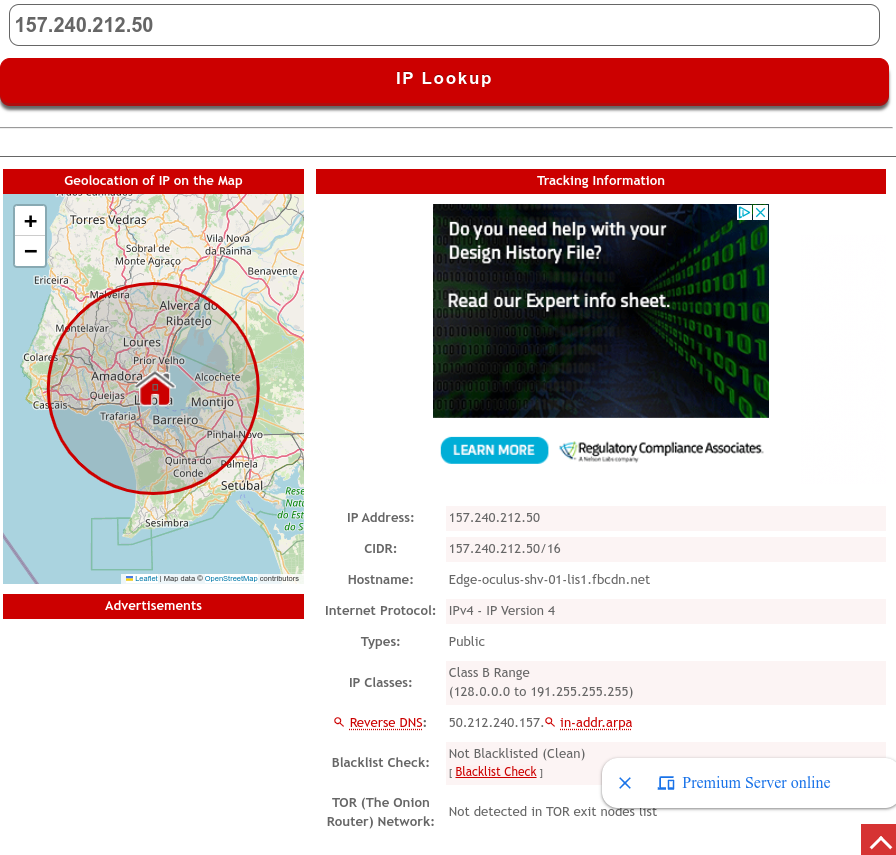


Figure 10 Figure 11

## 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.

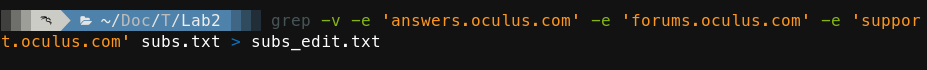


Figure 12

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

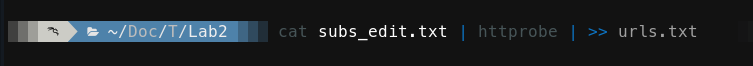


Figure 13

1. 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>

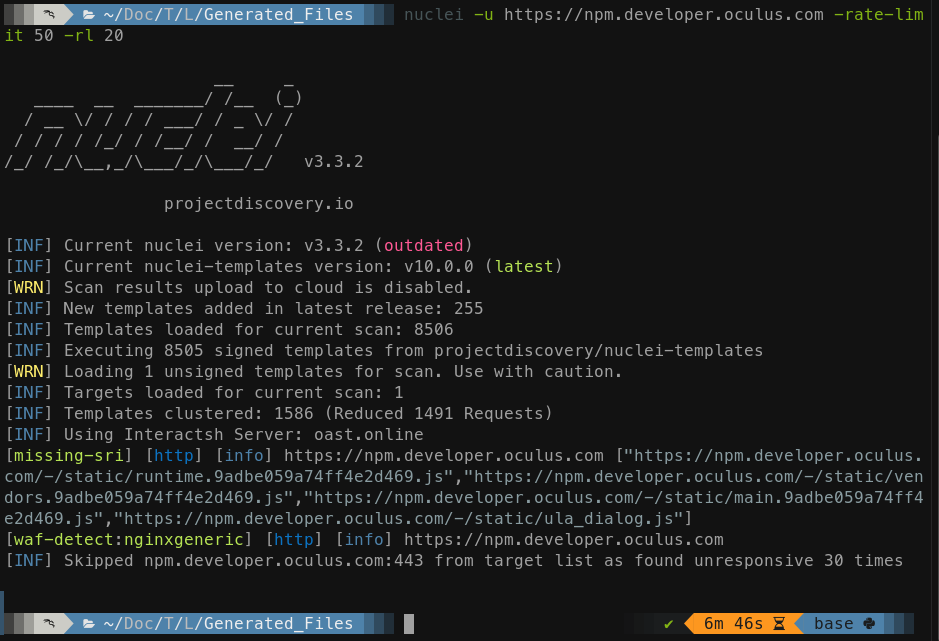


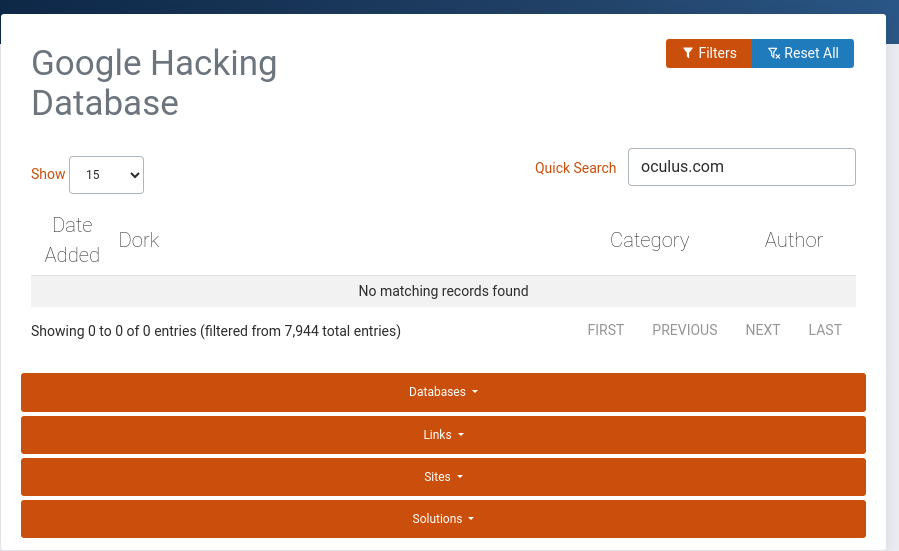
Figure 14

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

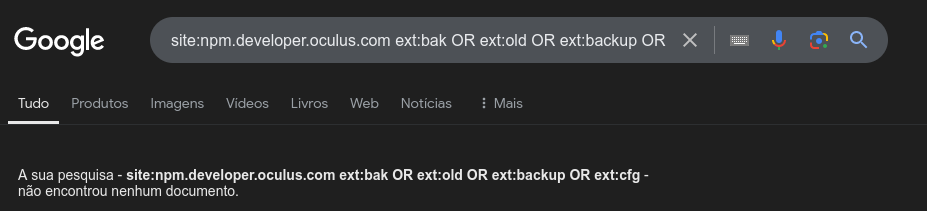
## Task 6 - Special tasks

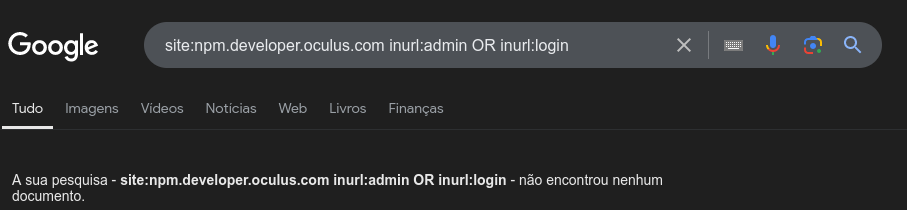
### Google Dorks

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.





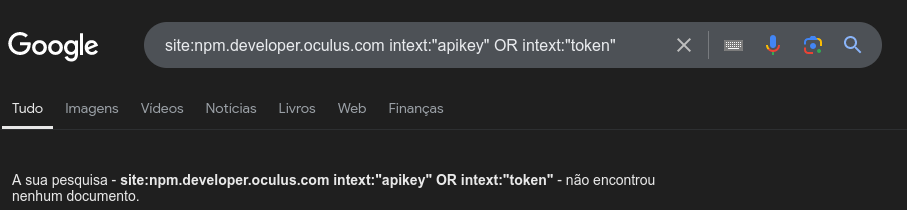


Figure 15

### Sensitive endpoints

Unfortunatly, 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.