Sri Lanka Institute of Information Technology

Specialized in Cyber Security

Year 2, Semester 2

IE2062 – Web Security

Bug Bounty – Report 03

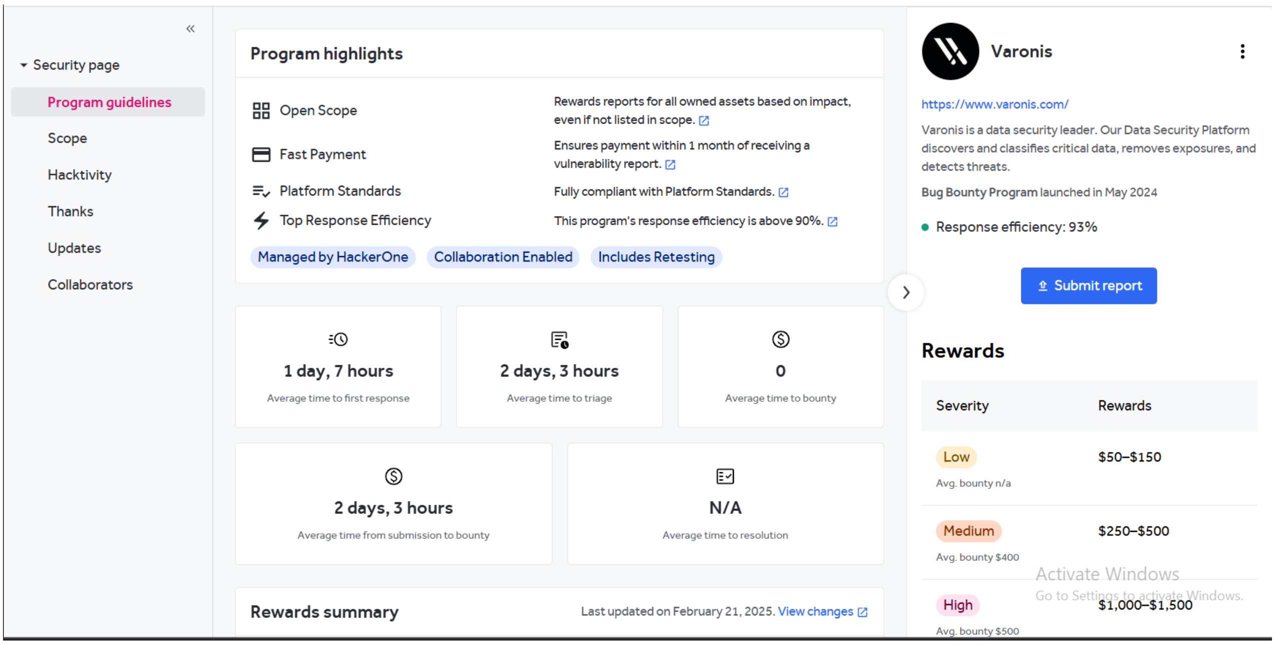
Student ID No.	Name
IT23136106	D.M.M. Pasindu Supushmika

Table of Contents

1. Website Overview

Varonis – Data Security Platform

HackerOne Link: Varonis | Bug Bounty Program Policy | HackerOne



Program highlights

Open Scope — Rewards reports for all owned assets based on impact, even if not listed in scope.

Fast Payment — Ensures payment within 1 month of receiving a vulnerability report.

Platform Standards — Fully compliant with Platform Standards.

Top Response Efficiency — This program's response efficiency is above 90%.

Managed by HackerOne · Collaboration Enabled · Includes Retesting

1 day, 7 hours — Average time to first response

2 days, 3 hours — Average time to triage

0 — Average time to bounty

2 days, 3 hours — Average time from submission to bounty

N/A — Average time to resolution

Rewards summary — Last updated on February 21, 2025. View changes

Varonis

https://www.varonis.com/

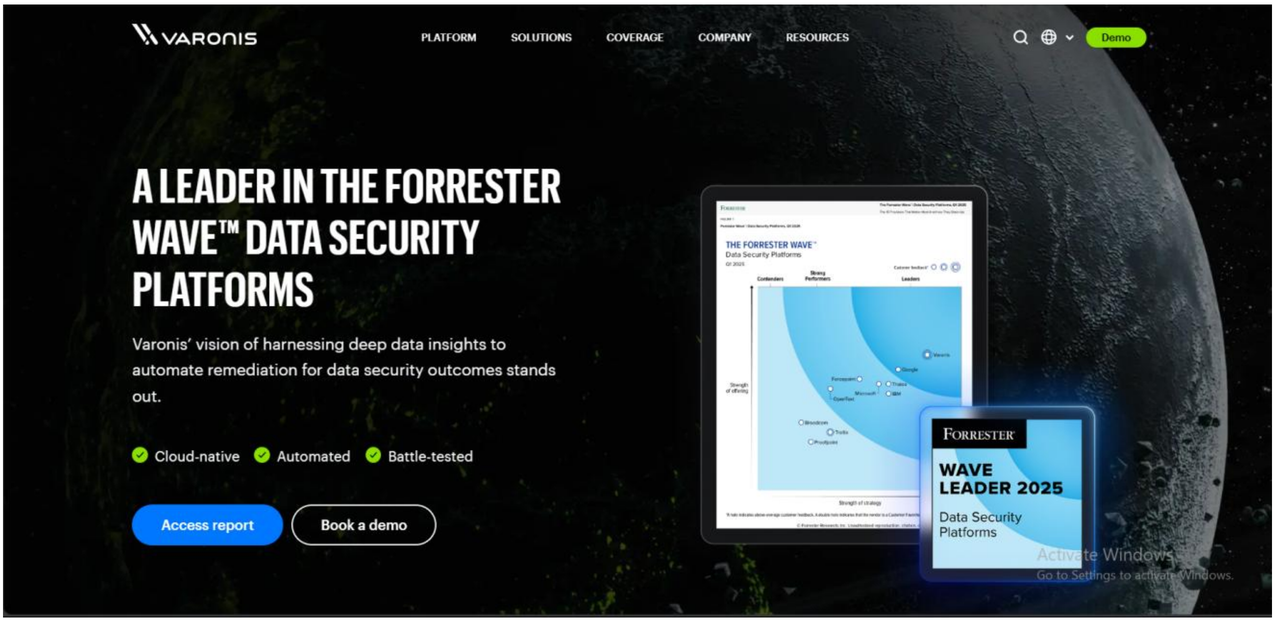
Varonis is a data security leader. Our Data Security Platform discovers and classifies critical data, removes exposures, and detects threats.

Bug Bounty Program launched in May 2024

● Response efficiency: 93%

Rewards

Severity	Rewards
Low Avg. bounty n/a	$50–$150
Medium Avg. bounty $400	$250–$500
High Avg. bounty $500	$1,000–$1,500



A LEADER IN THE FORRESTER WAVE™ DATA SECURITY PLATFORMS

Varonis' vision of harnessing deep data insights to automate remediation for data security outcomes stands out.

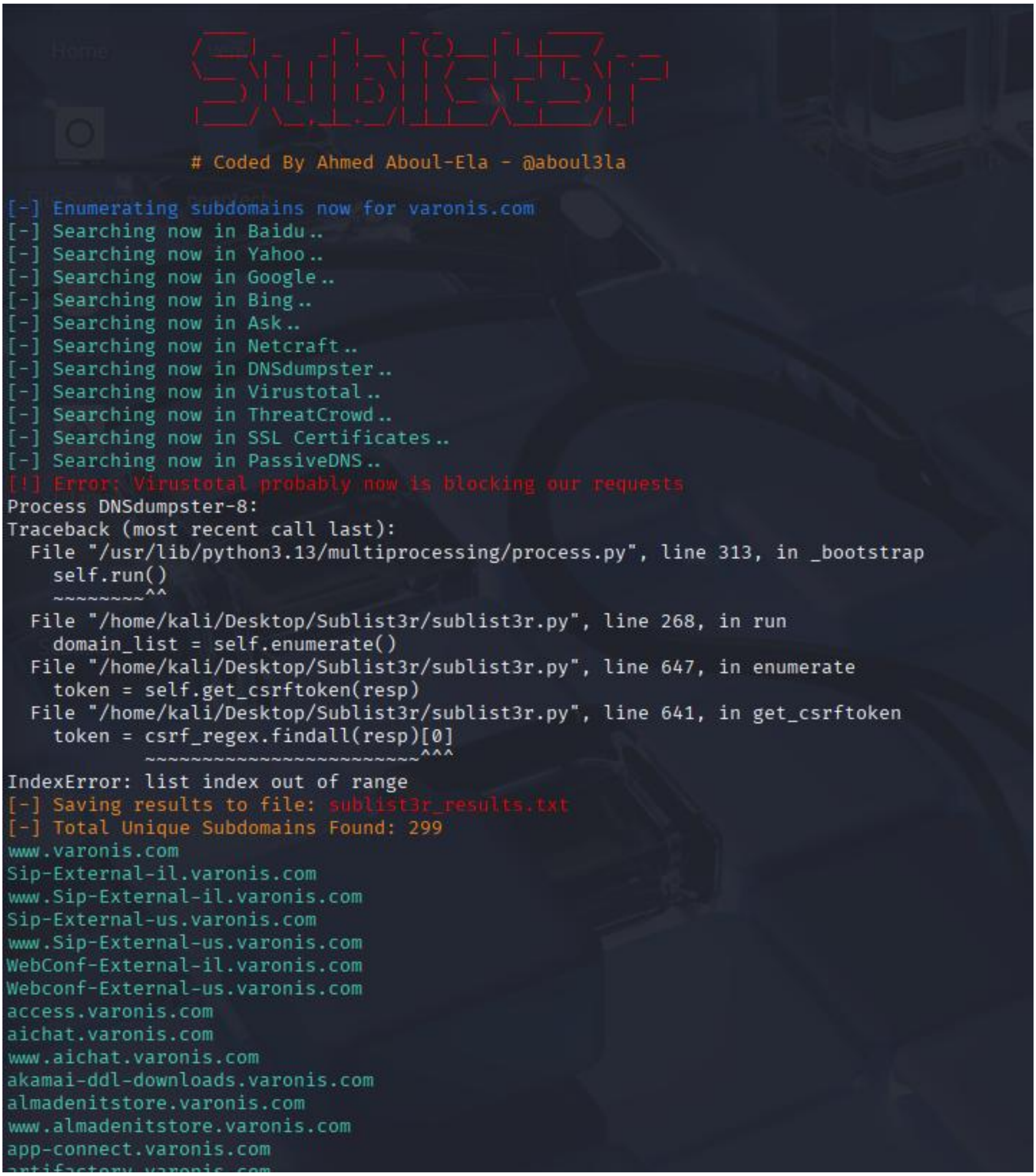
✓ Cloud-native ✓ Automated ✓ Battle-tested

2. **Step 01:** Gather Information.

a. Sub-domain Discovery

i. Sublist3r: Sublist3r_Results.txt

Tool : Sublist3r
Code : python3 sublist3r.py -d varonis.com -o sublist3r_results.txt
Explanation:
python3 sublist3r.py - Run the script using python
-d varonis.com - Target domain
-o sublist3r_results.txt – Output file where the result is saved

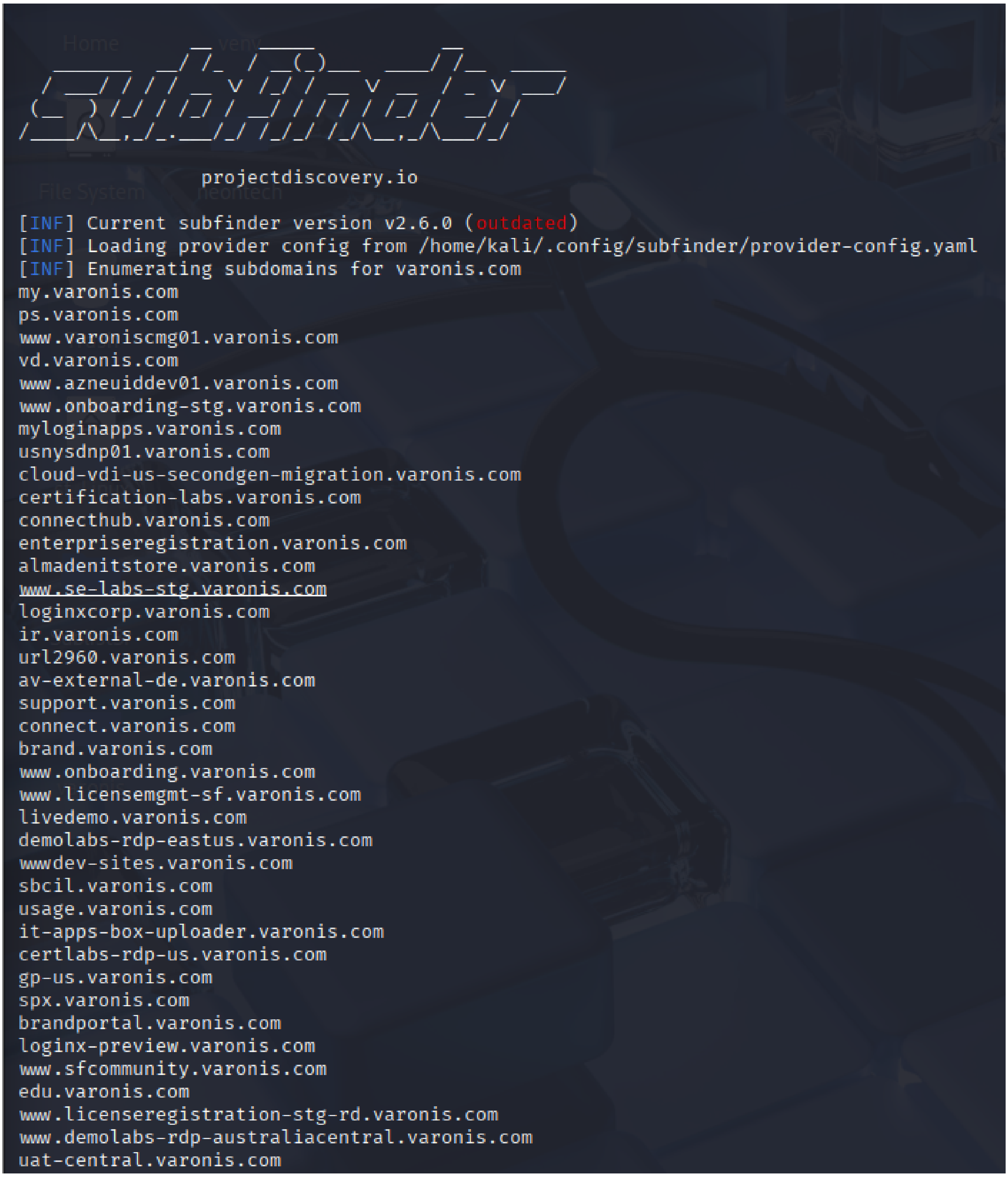


```
                 ____        _     _ _     _   _____
                / ___| _   _| |__ | (_)___| |_|___ / _ __
                \___ \| | | | '_ \| | / __| __| |_ \| '__|
                 ___) | |_| | |_) | | \__ \ |_ ___) | |
                |____/ \__,_|_.__/|_|_|___/\__|____/|_|

                # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for varonis.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Virustotal probably now is blocking our requests
Process DNSdumpster-8:
Traceback (most recent call last):
  File "/usr/lib/python3.13/multiprocessing/process.py", line 313, in _bootstrap
    self.run()
    ~~~~~~~~^^
  File "/home/kali/Desktop/Sublist3r/sublist3r.py", line 268, in run
    domain_list = self.enumerate()
  File "/home/kali/Desktop/Sublist3r/sublist3r.py", line 647, in enumerate
    token = self.get_csrftoken(resp)
  File "/home/kali/Desktop/Sublist3r/sublist3r.py", line 641, in get_csrftoken
    token = csrf_regex.findall(resp)[0]
            ~~~~~~~~~~~~~~~~~~~~~~~~^^^
IndexError: list index out of range
[-] Saving results to file: sublist3r_results.txt
[-] Total Unique Subdomains Found: 299
www.varonis.com
Sip-External-il.varonis.com
www.Sip-External-il.varonis.com
Sip-External-us.varonis.com
www.Sip-External-us.varonis.com
WebConf-External-il.varonis.com
Webconf-External-us.varonis.com
access.varonis.com
aichat.varonis.com
www.aichat.varonis.com
akamai-ddl-downloads.varonis.com
almadenitstore.varonis.com
www.almadenitstore.varonis.com
app-connect.varonis.com
artifactory.varonis.com
```

www.varonis.com
Sip-External-il.varonis.com
www.Sip-External-il.varonis.com
Sip-External-us.varonis.com
www.Sip-External-us.varonis.com
WebConf-External-il.varonis.com
Webconf-External-us.varonis.com
access.varonis.com
aichat.varonis.com
www.aichat.varonis.com
akamai-ddl-downloads.varonis.com
almadenitstore.varonis.com
www.almadenitstore.varonis.com
app-connect.varonis.com
artifactory.varonis.com
www.artifactory.varonis.com
artifactory02.varonis.com
ask.varonis.com
www.ask.varonis.com
ask2.varonis.com
attribution.varonis.com
authupload.varonis.com
www.authupload.varonis.com
av-external-de.varonis.com
av-external-il.varonis.com
av-external-us.varonis.com
azneuiddev01.varonis.com
www.azneuiddev01.varonis.com
blog.varonis.com
box-uploader-prod.varonis.com
www.box-uploader-prod.varonis.com
brand.varonis.com
brandportal.varonis.com
captiveportal-login.varonis.com
www.captiveportal-login.varonis.com
careers.varonis.com
www.careers.varonis.com
central.varonis.com
www.central.varonis.com
certification-labs.varonis.com
www.certification-labs.varonis.com
certlabs-rdp-eu.varonis.com
www.certlabs-rdp-eu.varonis.com
certlabs-rdp-us.varonis.com
www.certlabs-rdp-us.varonis.com
chat.varonis.com
www.chat.varonis.com
cloud-vdi-eu.varonis.com
www.cloud-vdi-eu.varonis.com
cloud-vdi-us.varonis.com
www.cloud-vdi-us.varonis.com
cloud-vdi-us-secondgen-migration.varonis.com
cloudatp-dashboard.varonis.com
cloudcrp.varonis.com
www.cloudcrp.varonis.com
connect.varonis.com
connecthub.varonis.com

ii. Subfindre: [Subfinder_Result.txt]

Tool **:** Subfinder
Code **:** subfinder -d varonis.com -o subfinder_result.txt
Explanation:
bfinder - run subfinder too
l -d varonis.com - Mention the target website
-o subfinder_result.txt – Mention the output file



```
               __    _____           __
   _______  __/ /_  / __(_)___  ____/ /__  _____
  / ___/ / / / __ \/ /_/ / __ \/ __  / _ \/ ___/
 (__  ) /_/ / /_/ / __/ / / / / /_/ /  __/ /
/____/\__,_/_.___/_/ /_/_/ /_/\__,_/\___/_/

                projectdiscovery.io

[INF] Current subfinder version v2.6.0 (outdated)
[INF] Loading provider config from /home/kali/.config/subfinder/provider-config.yaml
[INF] Enumerating subdomains for varonis.com
my.varonis.com
ps.varonis.com
www.varoniscmg01.varonis.com
vd.varonis.com
www.azneuiddev01.varonis.com
www.onboarding-stg.varonis.com
myloginapps.varonis.com
usnysdnp01.varonis.com
cloud-vdi-us-secondgen-migration.varonis.com
certification-labs.varonis.com
connecthub.varonis.com
enterpriseregistration.varonis.com
almadenitstore.varonis.com
www.se-labs-stg.varonis.com
loginxcorp.varonis.com
ir.varonis.com
url2960.varonis.com
av-external-de.varonis.com
support.varonis.com
connect.varonis.com
brand.varonis.com
www.onboarding.varonis.com
www.licensemgmt-sf.varonis.com
livedemo.varonis.com
demolabs-rdp-eastus.varonis.com
wwwdev-sites.varonis.com
sbcil.varonis.com
usage.varonis.com
it-apps-box-uploader.varonis.com
certlabs-rdp-us.varonis.com
gp-us.varonis.com
spx.varonis.com
brandportal.varonis.com
loginx-preview.varonis.com
www.sfcommunity.varonis.com
edu.varonis.com
www.licenseregistration-stg-rd.varonis.com
www.demolabs-rdp-australiacentral.varonis.com
uat-central.varonis.com
```

my.varonis.com
ps.varonis.com
www.varoniscmg01.varonis.com
vd.varonis.com
www.azneuiddev01.varonis.com

```
www.onboarding-stg.varonis.com
myloginapps.varonis.com
usnysdnp01.varonis.com
cloud-vdi-us-secondgen-migration.varonis.com
certification-labs.varonis.com
connecthub.varonis.com
enterpriseregistration.varonis.com
almadenitstore.varonis.com
www.se-labs-stg.varonis.com
loginxcorp.varonis.com
ir.varonis.com
url2960.varonis.com
av-external-de.varonis.com
support.varonis.com
connect.varonis.com
brand.varonis.com
www.onboarding.varonis.com
www.licensemgmt-sf.varonis.com
livedemo.varonis.com
demolabs-rdp-eastus.varonis.com
wwwdev-sites.varonis.com
sbcil.varonis.com
usage.varonis.com
it-apps-box-uploader.varonis.com
certlabs-rdp-us.varonis.com
gp-us.varonis.com
spx.varonis.com
brandportal.varonis.com
loginx-preview.varonis.com
www.sfcommunity.varonis.com
edu.varonis.com
www.licenseregistration-stg-rd.varonis.com
www.demolabs-rdp-australiacentral.varonis.com
uat-central.varonis.com
demo-labs.varonis.com
www.ps-labs.varonis.com
www.licensemgmt-stg-rd.varonis.com
www.cloud-vdi-us-secondgen-migration.varonis.com
help-uat.varonis.com
ilhrzdmzuag04.varonis.com
www.licensemgmt-stg-rd-salesforce.varonis.com
www.captiveportal-login.varonis.com
teamssbcus2.varonis.com
livedemostg.varonis.com
downloads.varonis.com
www.licenseregistration.varonis.com
www.my-varonisservicestg.varonis.com
```

b. Live Subdomain Discovery

Tool : httpx: Livesub_Results.txt

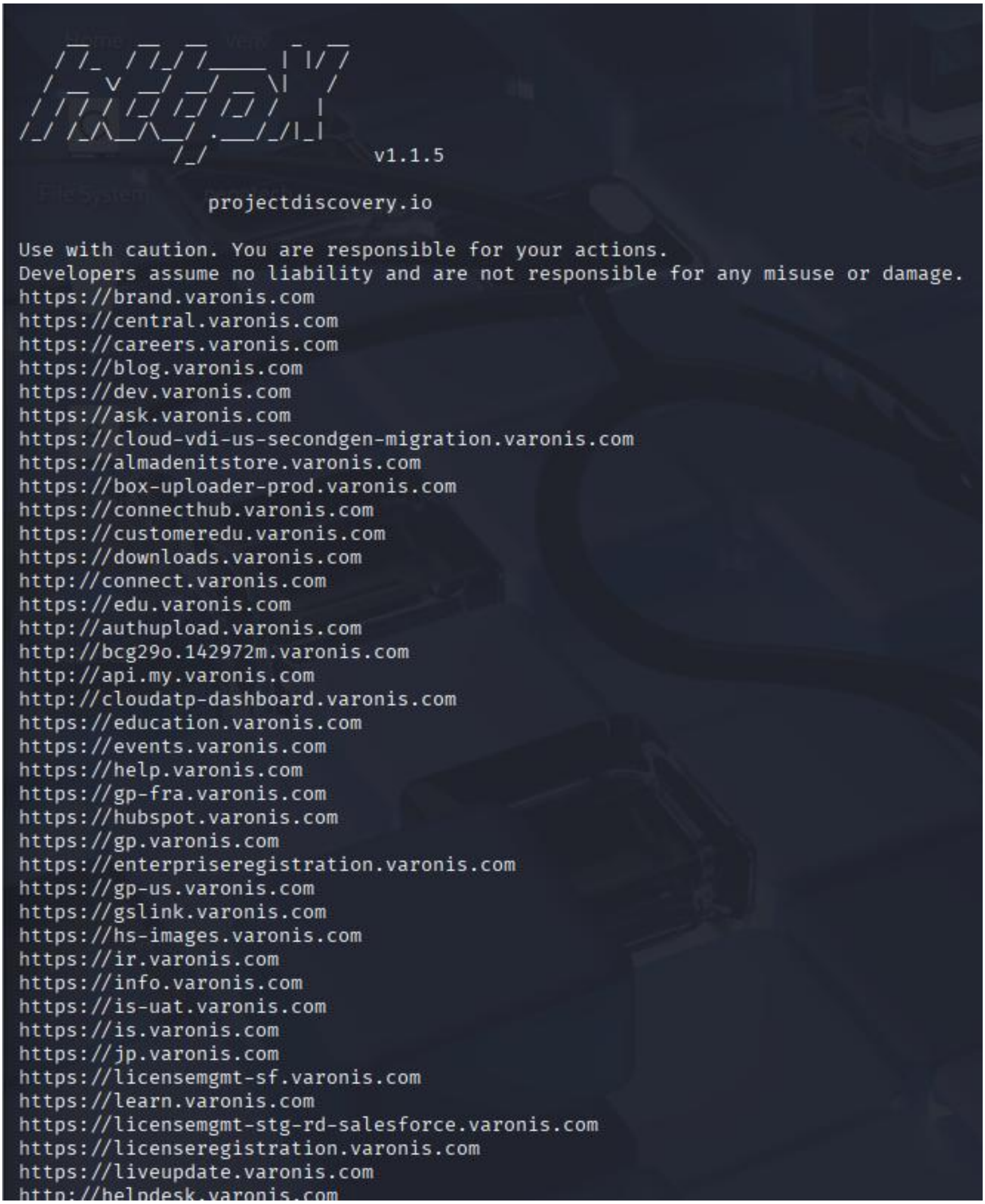
Code : httpx-toolkit -l subfinder_result.txt -o livesub_results.txt

Explanation:

httpx-toolkit - run the httpx tool

-*l subfinder_result.txt* – mention the file containing input

-*o livesub_results.txt* – mention the file which should write the output



```
    __    __  __       _  __
   / /_  / /_/ /_____ | |/ /
  / __ \/ __/ __/ __ \|   /
 / / / / /_/ /_/ /_/ /   |
/_/ /_/\__/\__/ .___/_/|_|
             /_/              v1.1.5

                projectdiscovery.io

Use with caution. You are responsible for your actions.
Developers assume no liability and are not responsible for any misuse or damage.
https://brand.varonis.com
https://central.varonis.com
https://careers.varonis.com
https://blog.varonis.com
https://dev.varonis.com
https://ask.varonis.com
https://cloud-vdi-us-secondgen-migration.varonis.com
https://almadenitstore.varonis.com
https://box-uploader-prod.varonis.com
https://connecthub.varonis.com
https://customeredu.varonis.com
https://downloads.varonis.com
http://connect.varonis.com
https://edu.varonis.com
http://authupload.varonis.com
http://bcg29o.142972m.varonis.com
http://api.my.varonis.com
http://cloudatp-dashboard.varonis.com
https://education.varonis.com
https://events.varonis.com
https://help.varonis.com
https://gp-fra.varonis.com
https://hubspot.varonis.com
https://gp.varonis.com
https://enterpriseregistration.varonis.com
https://gp-us.varonis.com
https://gslink.varonis.com
https://hs-images.varonis.com
https://ir.varonis.com
https://info.varonis.com
https://is-uat.varonis.com
https://is.varonis.com
https://jp.varonis.com
https://licensemgmt-sf.varonis.com
https://learn.varonis.com
https://licensemgmt-stg-rd-salesforce.varonis.com
https://licenseregistration.varonis.com
https://liveupdate.varonis.com
http://helpdesk.varonis.com
```

https://brand.varonis.com
https://central.varonis.com
https://careers.varonis.com
https://blog.varonis.com
https://dev.varonis.com
https://ask.varonis.com
https://cloud-vdi-us-secondgen-migration.varonis.com
https://almadenitstore.varonis.com
https://box-uploader-prod.varonis.com
https://connecthub.varonis.com
https://customeredu.varonis.com
https://downloads.varonis.com
http://connect.varonis.com
https://edu.varonis.com
http://authupload.varonis.com
http://bcg29o.142972m.varonis.com
http://api.my.varonis.com
http://cloudatp-dashboard.varonis.com
https://education.varonis.com
https://events.varonis.com
https://help.varonis.com
https://gp-fra.varonis.com
https://hubspot.varonis.com
https://gp.varonis.com
https://enterpriseregistration.varonis.com
https://gp-us.varonis.com
https://gslink.varonis.com
https://hs-images.varonis.com
https://ir.varonis.com
https://info.varonis.com
https://is-uat.varonis.com
https://is.varonis.com
https://jp.varonis.com
https://licensemgmt-sf.varonis.com
https://learn.varonis.com
https://licensemgmt-stg-rd-salesforce.varonis.com
https://licenseregistration.varonis.com
https://liveupdate.varonis.com
http://helpdesk.varonis.com
http://login.varonis.com
http://licensemgmt-stg-rd.varonis.com
http://liveupdatemanager.varonis.com
http://loginxcorp.varonis.com
http://myvaronis-sf-stg-rd.varonis.com
http://my.varonis.com
http://myvaronis-sf.varonis.com
http://loginx-preview.varonis.com
http://partnercommunity.varonis.com
http://loginx.varonis.com
http://partneredu.varonis.com
http://onboarding.varonis.com
http://onboarding-stg.varonis.com
http://login-preview.varonis.com
http://licensemgmt.varonis.com
http://myvaronis-api-stg-rd.varonis.com
http://partners.varonis.com
http://ps.varonis.com
http://pto.varonis.com

c. IP Discovery

Tool: nslookup: nslookup_Results.txt

Code: since we whole file with subdomains, to find IP addresses using “nslookup“ we need to make a loop until all the Ips of all the subdomains are found.

```
while read sub; do
 echo "Looking up: $sub" >> ips.txt
  nslookup "$sub" | awk '/^Name:|^Address:/' >> ips.txt
  echo "------------------------" >> ips.txt
done < livesub_results.txt
```

Explanation:

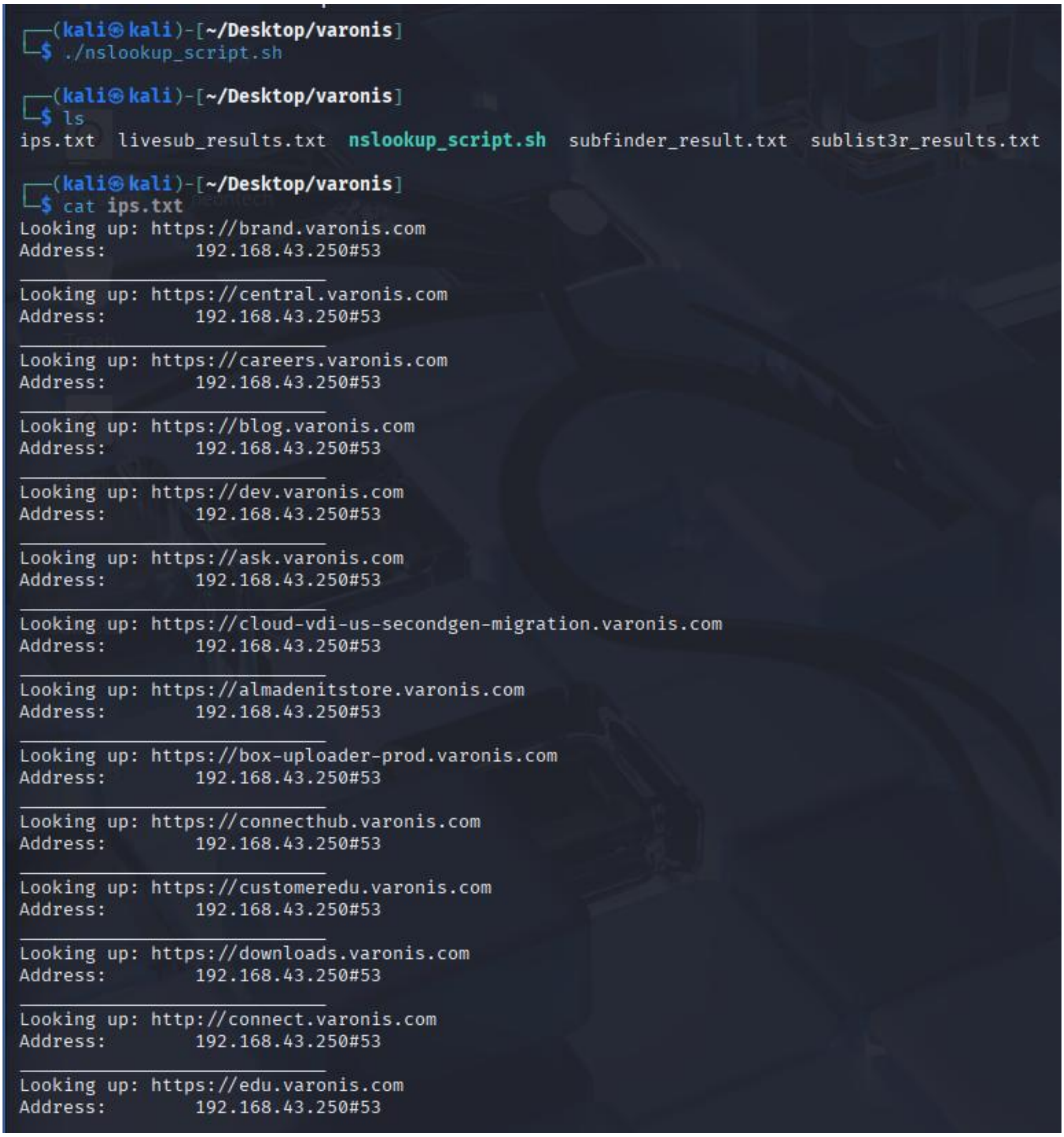
While read sub; do - start of the loop

Echo “Looking up: $sub”>>ips.txt - print message “Looking up: subdomain” into the file “ips.txt”

nslookup “$sub” | awk ‘/^Name:|^Address:/’ >> ips.txt - run the nslookup command

echo “__________________” >> ips.txt - separate one subdomain details from another

done < livesub_results.txt - End the loop and continue until the lines in the livesub_results.txt



```
┌──(kali㉿kali)-[~/Desktop/varonis]
└─$ ./nslookup_script.sh

┌──(kali㉿kali)-[~/Desktop/varonis]
└─$ ls
ips.txt  livesub_results.txt  nslookup_script.sh  subfinder_result.txt  sublist3r_results.txt

┌──(kali㉿kali)-[~/Desktop/varonis]
└─$ cat ips.txt
Looking up: https://brand.varonis.com
Address:        192.168.43.250#53
____________________________
Looking up: https://central.varonis.com
Address:        192.168.43.250#53
____________________________
Looking up: https://careers.varonis.com
Address:        192.168.43.250#53
____________________________
Looking up: https://blog.varonis.com
Address:        192.168.43.250#53
____________________________
Looking up: https://dev.varonis.com
Address:        192.168.43.250#53
____________________________
Looking up: https://ask.varonis.com
Address:        192.168.43.250#53
____________________________
Looking up: https://cloud-vdi-us-secondgen-migration.varonis.com
Address:        192.168.43.250#53
____________________________
Looking up: https://almadenitstore.varonis.com
Address:        192.168.43.250#53
____________________________
Looking up: https://box-uploader-prod.varonis.com
Address:        192.168.43.250#53
____________________________
Looking up: https://connecthub.varonis.com
Address:        192.168.43.250#53
____________________________
Looking up: https://customeredu.varonis.com
Address:        192.168.43.250#53
____________________________
Looking up: https://downloads.varonis.com
Address:        192.168.43.250#53
____________________________
Looking up: http://connect.varonis.com
Address:        192.168.43.250#53
____________________________
Looking up: https://edu.varonis.com
Address:        192.168.43.250#53
```

IP list:

```
Looking up: https://brand.varonis.com
Address:        192.168.43.250#53
________________________________
Looking up: https://central.varonis.com
Address:        192.168.43.250#53
________________________________
Looking up: https://careers.varonis.com
Address:        192.168.43.250#53
________________________________
Looking up: https://blog.varonis.com
Address:        192.168.43.250#53
________________________________
Looking up: https://dev.varonis.com
Address:        192.168.43.250#53
________________________________
Looking up: https://ask.varonis.com
Address:        192.168.43.250#53
________________________________
Looking up: https://cloud-vdi-us-secondgen-migration.varonis.com
Address:        192.168.43.250#53
________________________________
Looking up: https://almadenitstore.varonis.com
Address:        192.168.43.250#53
________________________________
Looking up: https://box-uploader-prod.varonis.com
Address:        192.168.43.250#53
________________________________
Looking up: https://connecthub.varonis.com
Address:        192.168.43.250#53
________________________________
Looking up: https://customeredu.varonis.com
Address:        192.168.43.250#53
________________________________
Looking up: https://downloads.varonis.com
Address:        192.168.43.250#53
________________________________
Looking up: http://connect.varonis.com
Address:        192.168.43.250#53
________________________________
Looking up: https://edu.varonis.com
Address:        192.168.43.250#53
________________________________
Looking up: http://authupload.varonis.com
Address:        192.168.43.250#53
________________________________
Looking up: http://bcg29o.142972m.varonis.com
Address:        192.168.43.250#53
________________________________
Looking up: http://api.my.varonis.com
Address:        192.168.43.250#53
________________________________
```

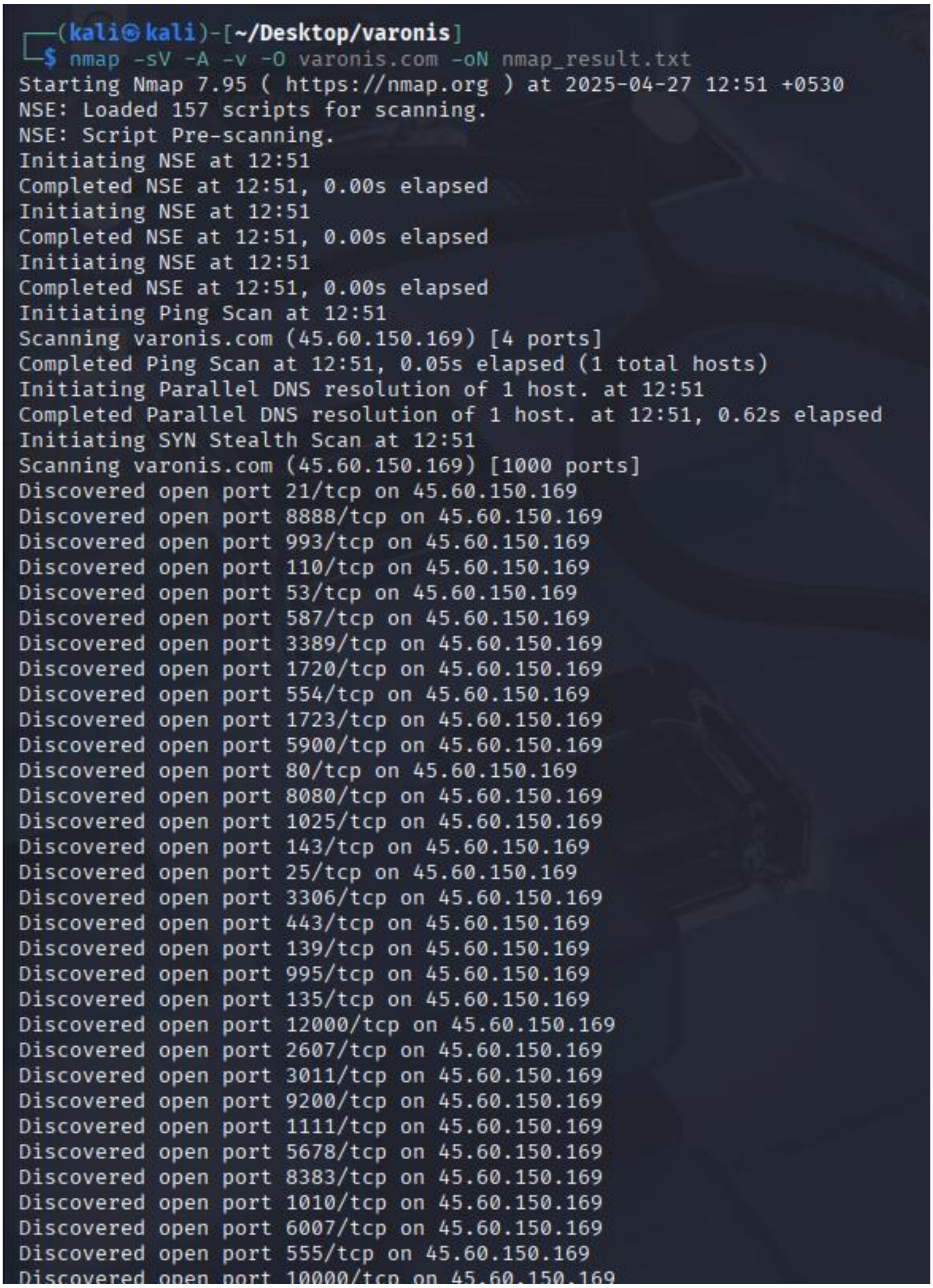
d. Open Ports

Tool: nmap: nmap_Result.txt

Code: nmap -sV -A -v -O varonis.com -oN nmap_results.txt

Explanation:

nmap - start the tool
-sV - Service and version detection
-A - OS detection, version detection, script scanning
-v - increase verbosity level
-O - Os detection
- *varonis.com* - target website
-oN nmap_results.txt - result in an output text file



```
┌──(kali㉿kali)-[~/Desktop/varonis]
└─$ nmap -sV -A -v -O varonis.com -oN nmap_result.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-27 12:51 +0530
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 12:51
Completed NSE at 12:51, 0.00s elapsed
Initiating NSE at 12:51
Completed NSE at 12:51, 0.00s elapsed
Initiating NSE at 12:51
Completed NSE at 12:51, 0.00s elapsed
Initiating Ping Scan at 12:51
Scanning varonis.com (45.60.150.169) [4 ports]
Completed Ping Scan at 12:51, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:51
Completed Parallel DNS resolution of 1 host. at 12:51, 0.62s elapsed
Initiating SYN Stealth Scan at 12:51
Scanning varonis.com (45.60.150.169) [1000 ports]
Discovered open port 21/tcp on 45.60.150.169
Discovered open port 8888/tcp on 45.60.150.169
Discovered open port 993/tcp on 45.60.150.169
Discovered open port 110/tcp on 45.60.150.169
Discovered open port 53/tcp on 45.60.150.169
Discovered open port 587/tcp on 45.60.150.169
Discovered open port 3389/tcp on 45.60.150.169
Discovered open port 1720/tcp on 45.60.150.169
Discovered open port 554/tcp on 45.60.150.169
Discovered open port 1723/tcp on 45.60.150.169
Discovered open port 5900/tcp on 45.60.150.169
Discovered open port 80/tcp on 45.60.150.169
Discovered open port 8080/tcp on 45.60.150.169
Discovered open port 1025/tcp on 45.60.150.169
Discovered open port 143/tcp on 45.60.150.169
Discovered open port 25/tcp on 45.60.150.169
Discovered open port 3306/tcp on 45.60.150.169
Discovered open port 443/tcp on 45.60.150.169
Discovered open port 139/tcp on 45.60.150.169
Discovered open port 995/tcp on 45.60.150.169
Discovered open port 135/tcp on 45.60.150.169
Discovered open port 12000/tcp on 45.60.150.169
Discovered open port 2607/tcp on 45.60.150.169
Discovered open port 3011/tcp on 45.60.150.169
Discovered open port 9200/tcp on 45.60.150.169
Discovered open port 1111/tcp on 45.60.150.169
Discovered open port 5678/tcp on 45.60.150.169
Discovered open port 8383/tcp on 45.60.150.169
Discovered open port 1010/tcp on 45.60.150.169
Discovered open port 6007/tcp on 45.60.150.169
Discovered open port 555/tcp on 45.60.150.169
Discovered open port 10000/tcp on 45.60.150.169
```

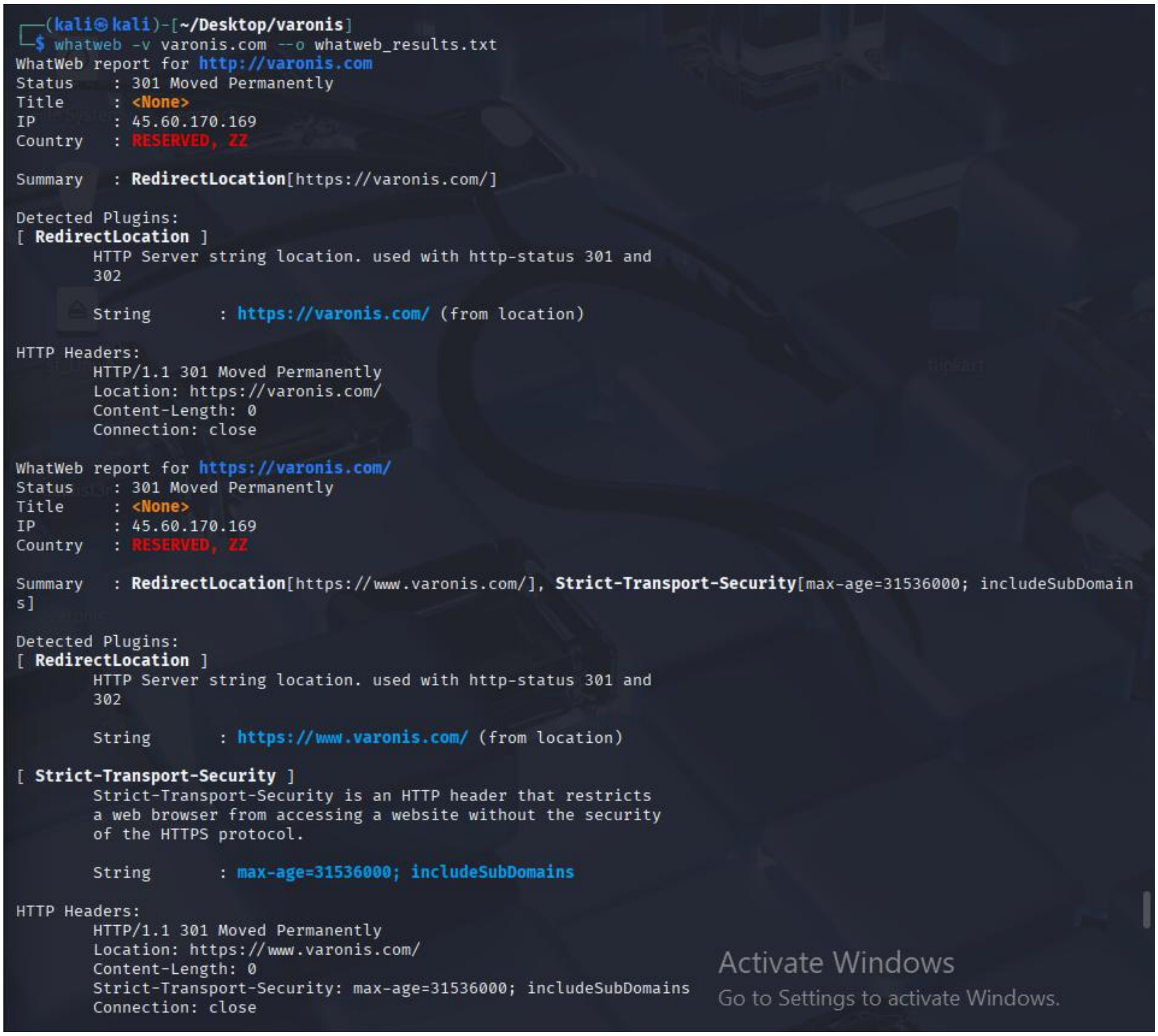
e. Used Technologies

Tool: whatweb - whatweb_Result.txt

Code: whatweb -v varonis.com > whatweb_result.txt

Explanation:

whatweb - start whatweb tool
-v - verbose
varonis.com - target website
> whatweb_result.txt - file with the output



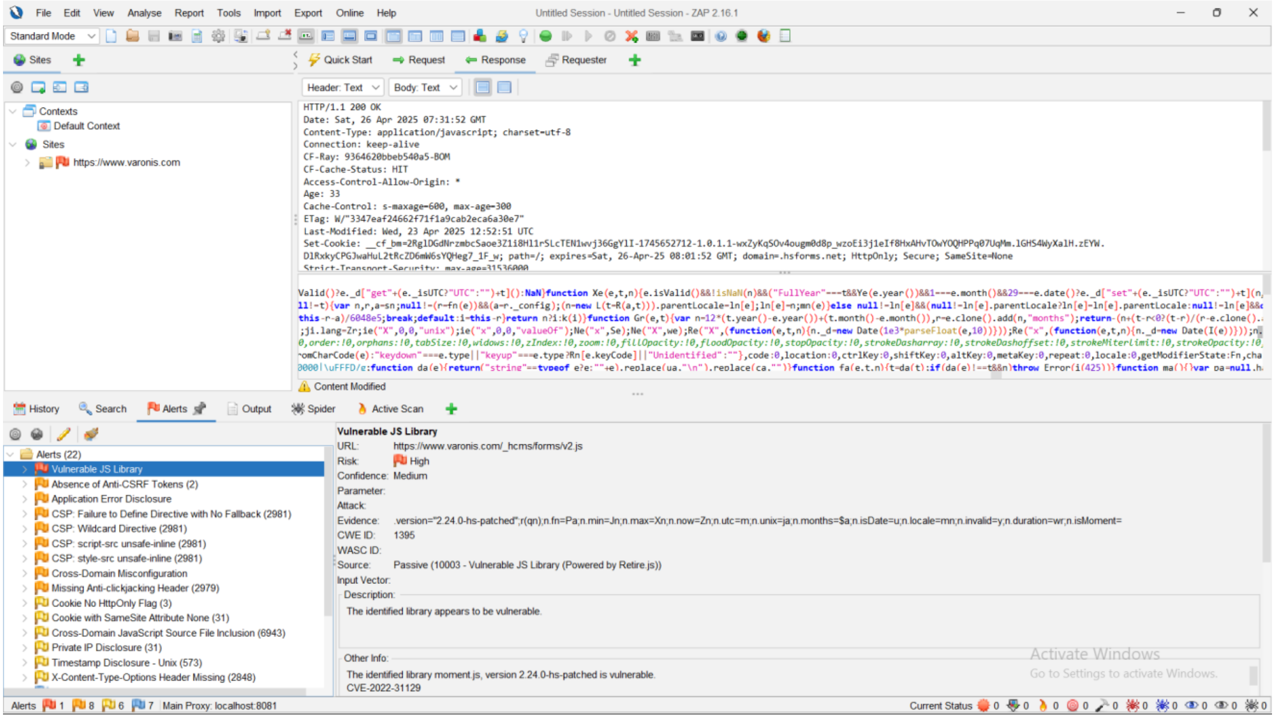
```
┌──(kali㉿kali)-[~/Desktop/varonis]
└─$ whatweb -v varonis.com --o whatweb_results.txt
WhatWeb report for http://varonis.com
Status    : 301 Moved Permanently
Title     : <None>
IP        : 45.60.170.169
Country   : RESERVED, ZZ

Summary   : RedirectLocation[https://varonis.com/]

Detected Plugins:
[ RedirectLocation ]
        HTTP Server string location. used with http-status 301 and
        302

        String       : https://varonis.com/ (from location)

HTTP Headers:
        HTTP/1.1 301 Moved Permanently
        Location: https://varonis.com/
        Content-Length: 0
        Connection: close

WhatWeb report for https://varonis.com/
Status    : 301 Moved Permanently
Title     : <None>
IP        : 45.60.170.169
Country   : RESERVED, ZZ

Summary   : RedirectLocation[https://www.varonis.com/], Strict-Transport-Security[max-age=31536000; includeSubDomain
s]

Detected Plugins:
[ RedirectLocation ]
        HTTP Server string location. used with http-status 301 and
        302

        String       : https://www.varonis.com/ (from location)

[ Strict-Transport-Security ]
        Strict-Transport-Security is an HTTP header that restricts
        a web browser from accessing a website without the security
        of the HTTPS protocol.

        String       : max-age=31536000; includeSubDomains

HTTP Headers:
        HTTP/1.1 301 Moved Permanently
        Location: https://www.varonis.com/
        Content-Length: 0
        Strict-Transport-Security: max-age=31536000; includeSubDomains
        Connection: close
```

3. Step 02: Scanning and vulnerability identification

a. Identify Potential Vulnerabilities

Tool : OWASP ZAP

Vulnerability : Vulnerable JS Library


File Edit View Analyse Report Tools Import Export Online Help
Untitled Session - Untitled Session - ZAP 2.16.1
Standard Mode
Sites
Quick Start
Request
Response
Requester
Header: Text
Body: Text
Contexts
Default Context
Sites
https://www.varonis.com
Content Modified
History
Search
Alerts
Output
Spider
Active Scan
Alerts 1 8 6 7 Main Proxy: localhost:8081
Current Status 0 0 0 0 0 0 0 0 0 0
Activate Windows
Go to Settings to activate Windows.

```
HTTP/1.1 200 OK
Date: Sat, 26 Apr 2025 07:31:52 GMT
Content-Type: application/javascript; charset=utf-8
Connection: keep-alive
CF-Ray: 9364620bbeb540a5-BOM
CF-Cache-Status: HIT
Access-Control-Allow-Origin: *
Age: 33
Cache-Control: s-maxage=600, max-age=300
ETag: W/"3347eaf24662f71f1a9cab2eca6a30e7"
Last-Modified: Wed, 23 Apr 2025 12:52:51 UTC
Set-Cookie: __cf_bm=2Rg1DGdNrzmbcSaoe3Z1i8H11rSLcTEN1wvj36GgY1I-1745652712-1.0.1.1-wxZyKqSOv4ougm0d8p_wzoEi3j1eIf8HxAHvTOwYOQHPPq07UqMm.1GHS4WyXa1H.zEYW.
D1RxkyCPGJwaHuL2tRcZD6mW6sYQHeg7_1F_w; path=/; expires=Sat, 26-Apr-25 08:01:52 GMT; domain=.hsforms.net; HttpOnly; Secure; SameSite=None
Strict-Transport-Security: max-age=31536000
```

```
Valid()?e._d["get"+(e._isUTC?"UTC":"")+t]():NaN}function Xe(e,t,n){e.isValid()&&!isNaN(n)&&("FullYear"===t&&Ye(e.year())&&1===e.month()&&29===e.date()?e._d["set"+(e._isUTC?"UTC":"")+t](n,
ll!=t){var n,r,a=sn;null!=(r=fn(e))&&(a=r._config);(n=new L(t=R(a,t))).parentLocale=ln[e];ln[e]=n;mn(e)}else null!=ln[e]&&(null!=ln[e].parentLocale?ln[e]=ln[e].parentLocale:null!=ln[e]&&
this-r-a)/6048e5;break;default:i=this-r}return n?i:k(i)}function Gr(e,t){var n=12*(t.year()-e.year())+(t.month()-e.month()),r=e.clone().add(n,"months");return-(n+(t-r<0?(t-r)/(r-e.clone().
;ji.lang=Zr;ie("X",0,0,"unix");ie("x",0,0,"valueOf");Ne("x",Se);Ne("X",we);Re("X",(function(e,t,n){n._d=new Date(1e3*parseFloat(e,10))}));Re("x",(function(e,t,n){n._d=new Date(I(e))}));n.
0,order:!0,orphans:!0,tabSize:!0,widows:!0,zIndex:!0,zoom:!0,fillOpacity:!0,floodOpacity:!0,stopOpacity:!0,strokeDasharray:!0,strokeDashoffset:!0,strokeMiterlimit:!0,strokeOpacity:!0,
omCharCode(e):"keydown"===e.type||"keyup"===e.type?Rn[e.keyCode]||"Unidentified":""},code:0,location:0,ctrlKey:0,shiftKey:0,altKey:0,metaKey:0,repeat:0,locale:0,getModifierState:Fn,cha
0000|\uFFFD/g:function da(e){return("string"==typeof e?e:""+e).replace(ua,"\n").replace(ca,"")}function fa(e,t,n){t=da(t);if(da(e)!==t&&n)throw Error(i(425))}function ma(){}var pa=null.h
```

Alerts (22)
- Vulnerable JS Library
- Absence of Anti-CSRF Tokens (2)
- Application Error Disclosure
- CSP: Failure to Define Directive with No Fallback (2981)
- CSP: Wildcard Directive (2981)
- CSP: script-src unsafe-inline (2981)
- CSP: style-src unsafe-inline (2981)
- Cross-Domain Misconfiguration
- Missing Anti-clickjacking Header (2979)
- Cookie No HttpOnly Flag (3)
- Cookie with SameSite Attribute None (31)
- Cross-Domain JavaScript Source File Inclusion (6943)
- Private IP Disclosure (31)
- Timestamp Disclosure - Unix (573)
- X-Content-Type-Options Header Missing (2848)

Vulnerable JS Library
URL: https://www.varonis.com/_hcms/forms/v2.js
Risk: High
Confidence: Medium
Parameter:
Attack:
Evidence: .version="2.24.0-hs-patched";r(qn);n.fn=Pa;n.min=Jn;n.max=Xn;n.now=Zn;n.utc=m;n.unix=ja;n.months=$a;n.isDate=u;n.locale=mn;n.invalid=y;n.duration=wr;n.isMoment=
CWE ID: 1395
WASC ID:
Source: Passive (10003 - Vulnerable JS Library (Powered by Retire.js))
Input Vector:
Description:
The identified library appears to be vulnerable.
Other Info:
The identified library moment.js, version 2.24.0-hs-patched is vulnerable.
CVE-2022-31129

Vulnerable JS Library:

URL: https://www.varonis.com/_hcms/forms/v2.js
Risk: High
Confidential: Medium
Parameter:
Attack:
Evidence: .version="2.24.0-hs-patched";r(qn);n.fn=Pa;n.min=Jn;n.max=Xn;n.now=Zn;n.utc=m;n.unix=ja;n.months=$a;n.isDate=u;n.locale=mn;n.invalid=y;n.duration=wr;n.isMoment=
CWE ID: 1395
WASC ID:
Source: Passive (10003 - Vulnerable JS Library (Powered by Retire.js))
Input Vector:

- Description: The identified library appears to be vulnerable..
- Other Info:
  - The identified library moment.js, version 2.24.0-hs-patched is vulnerable.
  - CVE-2022-31129
  - CVE-2022-24785
  - https://github.com/moment/moment/security/advisories/GHSA-wc69-rhjr-hc9g
  - https://security.snyk.io/vuln/SNYK-JS-MOMENT-2944238
  - https://github.com/moment/moment/security/advisories/GHSA-8hfj-j24r-96c4
- Solution: Upgrade to the latest version of the affected library.
- Reference: https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/
- Alert Tags:
  - OWASP_2017_A09: https://owasp.org/www-project-top-ten/2017/A9_2017-Using_Components_with_Known_Vulnerabilities.html
  - CVE-2022-31129: https://nvd.nist.gov/vuln/detail/CVE-2022-31129
  - OWASP_2021_A06: https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/
  - CWE-1395: https://cwe.mitre.org/data/definitions/1395.html
  - CVE-2022-24785: https://nvd.nist.gov/vuln/detail/CVE-2022-24785

b. Vulnerable JS Library

Vulnerable JavaScript (JS) libraries refer to the use of outdated or insecure JavaScript components in websites or web applications. These libraries might have known security flaws that attackers can exploit, such as Cross-Site Scripting (XSS), Cross-Origin Resource Sharing (CORS) misconfigurations, or Remote Code Execution (RCE). If not updated or properly secured, vulnerable JS libraries can be an easy entry point for attackers to compromise the application and its users.

Cause of Vulnerable JS Library in website:

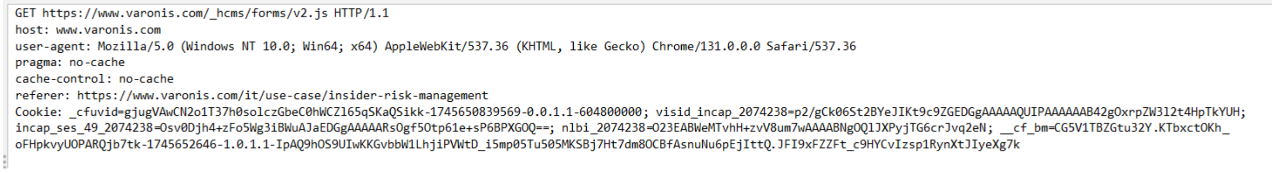
- Using outdated versions of third-party libraries with known security flaws
- Failing to monitor and update dependencies regularly
- Including unnecessary or unused libraries that increase the attack surface
- Downloading libraries from untrusted or compromised sources
- Lack of vulnerability scanning tools in the development pipeline
- Not validating or restricting third-party scripts' behavior on the site

Propositions to Mitigation or Fix:

- Use Dependency Management Tools: Use tools like npm, yarn, or package managers that can alert you to vulnerabilities
- Regular Updates: Frequently update JavaScript libraries and monitor for security advisories
- Sub resource Integrity (SRI): Use SRI to ensure that external libraries have not been tampered with
- Content Security Policy (CSP): Implement a strict CSP to limit the risk if a library gets compromised
- Remove Unused Libraries: Audit and eliminate unnecessary or outdated libraries from your project
- Use Trusted Sources Only: Always load JS libraries from reputable and verified CDNs
- Automated Vulnerability Scanning: Integrate tools like Snyk, retire.js, or npm audit into your CI/CD pipeline to detect vulnerabilities early

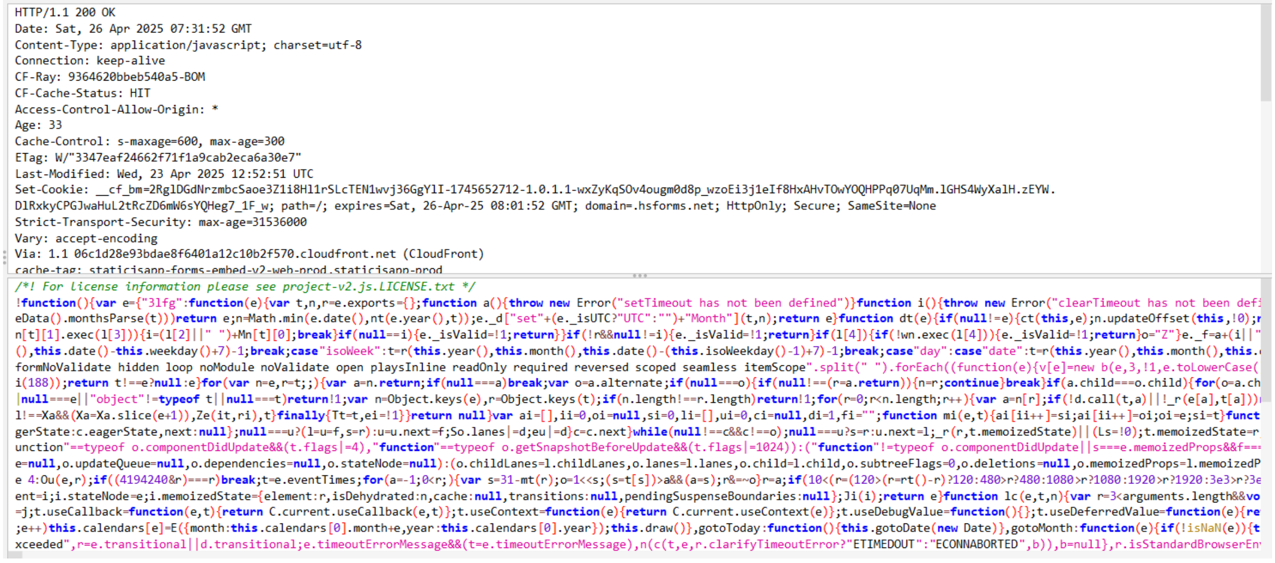
4. Step 03: Exploitation and Validation

Request:



```
GET https://www.varonis.com/_hcms/forms/v2.js HTTP/1.1
host: www.varonis.com
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36
pragma: no-cache
cache-control: no-cache
referer: https://www.varonis.com/it/use-case/insider-risk-management
Cookie: _cfuvid=gjugVAwCN2o1T37h0solczGbeC0hWCZl65qSKaQSikk-1745650839569-0.0.1.1-604800000; visid_incap_2074238=p2/gCk06St2BYeJIKt9c9ZGEDGgAAAAAQUIPAAAAAAB42gOxrpZW3l2t4HpTkYUH;
incap_ses_49_2074238=Osv0Djh4+zFo5Wg3iBWuAJaEDGgAAAAARsOgf5Otp61e+sP6BPXGOQ==; nlbi_2074238=O23EABWeMTvhH+zvV8um7wAAAABNgOQlJXPyjTG6crJvq2eN; __cf_bm=CG5V1TBZGtu32Y.KTbxctOKh_
oFHpkvyUOPARQjb7tk-1745652646-1.0.1.1-IpAQ9hOS9UIwKKGvbbW1LhjiPVWtD_i5mp05Tu505MKSBj7Ht7dm8OCBfAsnuNu6pEjIttQ.JFI9xFZZFt_c9HYCvIzsp1RynXtJIyeXg7k
```

Response:



```
HTTP/1.1 200 OK
Date: Sat, 26 Apr 2025 07:31:52 GMT
Content-Type: application/javascript; charset=utf-8
Connection: keep-alive
CF-Ray: 9364620bbeb540a5-BOM
CF-Cache-Status: HIT
Access-Control-Allow-Origin: *
Age: 33
Cache-Control: s-maxage=600, max-age=300
ETag: W/"3347eaf24662f71f1a9cab2eca6a30e7"
Last-Modified: Wed, 23 Apr 2025 12:52:51 UTC
Set-Cookie: __cf_bm=2RglDGdNrzmbcSaoe3Z1i8Hl1rSLcTEN1wvj36GgYlI-1745652712-1.0.1.1-wxZyKqSOv4ougm0d8p_wzoEi3j1eIf8HxAHvTOwYOQHPPq07UqMm.lGHS4WyXalH.zEYW.
DlRxkyCPGJwaHuL2tRcZD6mW6sYQHeg7_1F_w; path=/; expires=Sat, 26-Apr-25 08:01:52 GMT; domain=.hsforms.net; HttpOnly; Secure; SameSite=None
Strict-Transport-Security: max-age=31536000
Vary: accept-encoding
Via: 1.1 06c1d28e93bdae8f6401a12c10b2f570.cloudfront.net (CloudFront)
cache-tag: staticjsapp-forms-embed-v2-web-prod.staticjsapp-prod
```

```
/*! For license information please see project-v2.js.LICENSE.txt */
!function(){var e={"31fg":function(e){var t,n,r=e.exports={};function a(){throw new Error("setTimeout has not been defined")}function i(){throw new Error("clearTimeout has not been defi
eData().monthsParse(t)))return e;n=Math.min(e.date(),nt(e.year(),t));e._d["set"+(e._isUTC?"UTC":"")+"Month"](t,n);return e}function dt(e){if(null!=e){ct(this,e);n.updateOffset(this,!0);r
n[t][1].exec(l[3])){i=(l[2]||" ")+Mn[t][0];break}if(null==i){e._isValid=!1;return}}if(!r&&null!=i){e._isValid=!1;return}if(l[4]){if(!wn.exec(l[4])){e._isValid=!1;return}o="Z"}e._f=a+(i||"
(),this.date()-this.weekday()+7)-1;break;case"isoWeek":t=r(this.year(),this.month(),this.date()-(this.isoWeekday()-1)+7)-1;break;case"day":case"date":t=r(this.year(),this.month(),this.
formNoValidate hidden loop noModule noValidate open playsInline readOnly required reversed scoped seamless itemScope".split(" ").forEach((function(e){v[e]=new b(e,3,!1,e.toLowerCase(
i(188));return t!==e?null:e}for(var n=e,r=t;;){var a=n.return;if(null===a)break;var o=a.alternate;if(null===o){if(null!==(r=a.return)){n=r;continue}break}if(a.child===o.child){for(o=a.ch
|null===e||"object"!=typeof t||null===t)return!1;var n=Object.keys(e),r=Object.keys(t);if(n.length!==r.length)return!1;for(r=0;r<n.length;r++){var a=n[r];if(!d.call(t,a)||!_r(e[a],t[a]))
l!==Xa&&(Xa=Xa.slice(e+1)),Ze(it,ri),t}finally{Tt=t,ei=!1}}return null}var ai=[],ii=0,oi=null,si=0,li=[],ui=0,ci=null,di=1,fi="";function mi(e,t){ai[ii++]=si;ai[ii++]=oi;oi=e;si=t}funct
gerState:c.eagerState,next:null};null===u?(l=u=f,s=r):u=u.next=f;So.lanes|=d;eu|=d}c=c.next}while(null!==c&&c!==o);null===u?s=r:u.next=l;_r(r,t.memoizedState)||(Ls=!0);t.memoizedState=r
unction"==typeof o.componentDidUpdate&&(t.flags|=4),"function"==typeof o.getSnapshotBeforeUpdate&&(t.flags|=1024)):("function"!=typeof o.componentDidUpdate||s===e.memoizedProps&&f===
e=null,o.updateQueue=null,o.dependencies=null,o.stateNode=null):(o.childLanes=l.childLanes,o.lanes=l.lanes,o.child=l.child,o.subtreeFlags=0,o.deletions=null,o.memoizedProps=l.memoizedP
e 4:Ou(e,r);if((4194240&r)===r)break;t=e.eventTimes;for(a=-1;0<r;){var s=31-mt(r);o=1<<s;(s=t[s])>a&&(a=s);r&=~o}r=a;if(10<(r=(120>(r=rt()-r)?120:480>r?480:1080>r?1080:1920>r?1920:3e3>r?3e
ent=i;i.stateNode=e;i.memoizedState={element:r,isDehydrated:n,cache:null,transitions:null,pendingSuspenseBoundaries:null};Ji(i);return e}function lc(e,t,n){var r=3<arguments.length&&vo
=j;t.useCallback=function(e,t){return C.current.useCallback(e,t)};t.useContext=function(e){return C.current.useContext(e)};t.useDebugValue=function(){};t.useDeferredValue=function(e){re
;e++)this.calendars[e]=E({month:this.calendars[0].month+e,year:this.calendars[0].year});this.draw()},gotoToday:function(){this.gotoDate(new Date)},gotoMonth:function(e){if(!isNaN(e)){t
xceeded",r=e.transitional||d.transitional;e.timeoutErrorMessage&&(t=e.timeoutErrorMessage),n(c(t,e,r.clarifyTimeoutError?"ETIMEDOUT":"ECONNABORTED",b)),b=null},r.isStandardBrowserEn
```

5. **Step 04:** Mitigation / Fix

Immediate Mitigation Actions:

1. Remove or Replace “moment.js” file
2. If the file (moment.js) is required, upgrade it with the latest patch.

Long Term Prevention:

1. Automate dependency checks in CI/CD pipelines (automated processes that enable teams to **continuously integrate** and **continuously deliver/deploy** software changes).
2. Monitor new vulnerabilities.