Sri Lanka Institute of Information Technology

Specialized in Cyber Security

Year 2, Semester 2

IE2062 – Web Security

Bug Bounty – Report 10

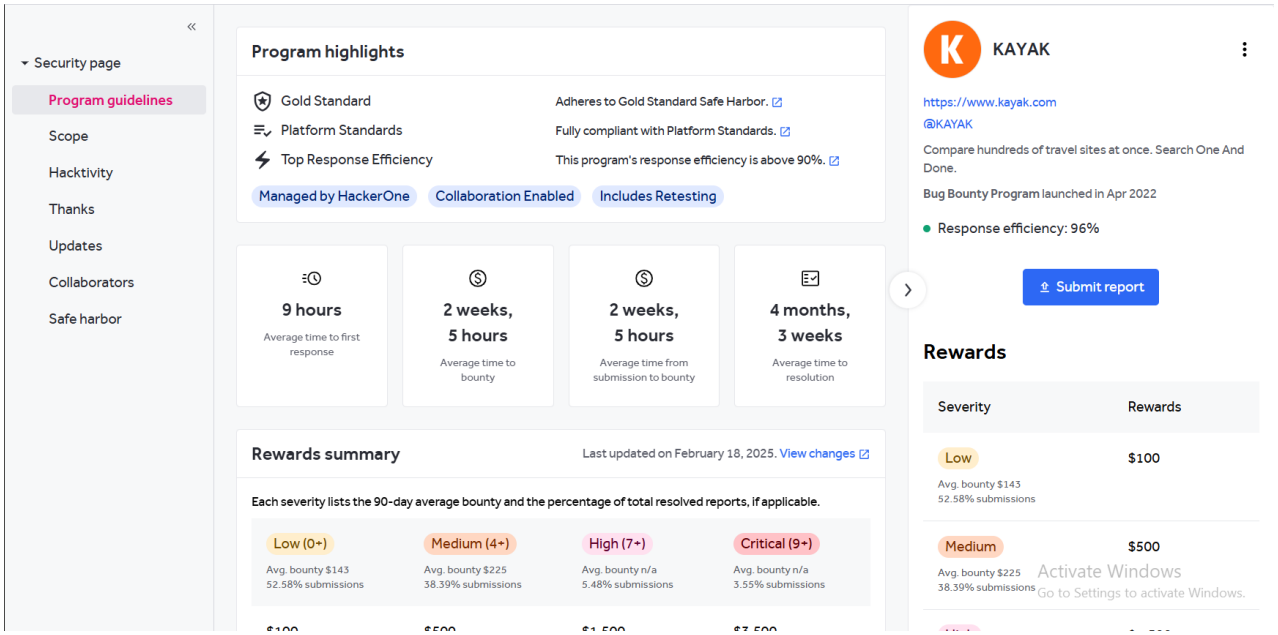
Student ID No.	Name
IT23136106	D.M.M. Pasindu Supushmika

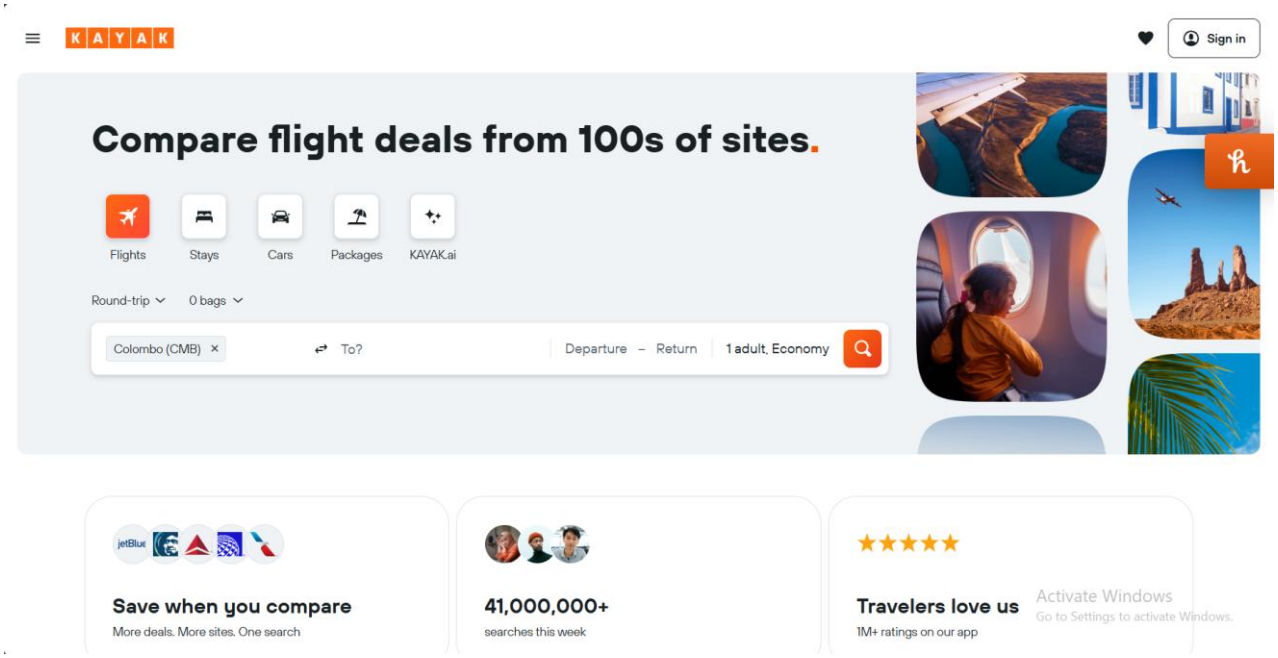
Table of Contents

1. Website Overview

KAYAK - [Search Flights, Hotels & Rental Cars]

HackerOne Link: [KAYAK | Bug Bounty Program Policy | HackerOne]





Step 01: Gather Information.

a. Sub-domain Discovery

i. Sublist3r: [sublist3r_kayak_results.txt]

Tool : Sublist3r
Code : python3 sublist3r.py -d kayak.com -o sublist3r_kayak_results.txt
Explanation:
python3 sublist3r.py - Run the script using python
-d kayak.com - Target domain
-o sublist3r_kayak_results.txt – Output file where the result is saved

```
# Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for kayak.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_kayak_results.txt
[-] Total Unique Subdomains Found: 275
www.kayak.com
1pass-scim-bridge.kayak.com
affiliate.kayak.com
buttermilk.affiliate.kayak.com
carrots.affiliate.kayak.com
peanuts.affiliate.kayak.com
affiliates.kayak.com
help.affiliates.kayak.com
signupapi.affiliates.kayak.com
agoda.kayak.com
agodaapp.kayak.com
ami.kayak.com
www.ar.kayak.com
at.kayak.com
www.at.kayak.com
urlaubsguru.at.kayak.com
au-rt-wp.kayak.com
backoffice.kayak.com
backpackers.kayak.com
```

www.kayak.com
1pass-scim-bridge.kayak.com
affiliate.kayak.com
buttermilk.affiliate.kayak.com
carrots.affiliate.kayak.com
peanuts.affiliate.kayak.com
affiliates.kayak.com
help.affiliates.kayak.com
signupapi.affiliates.kayak.com
agoda.kayak.com
agodaapp.kayak.com
ami.kayak.com
www.ar.kayak.com
at.kayak.com
www.at.kayak.com
urlaubsguru.at.kayak.com
au-rt-wp.kayak.com
backoffice.kayak.com
backpackers.kayak.com
www.be.kayak.com
booking.kayak.com
business.kayak.com
business-booking.kayak.com
c4.kayak.com
primer.c4.kayak.com
wp.primer.c4.kayak.com
c5.kayak.com
primer.c5.kayak.com
wp.primer.c5.kayak.com
c6.kayak.com
ca.kayak.com
www.ca.kayak.com
business.ca.kayak.com
ca-fr-rt-wp.kayak.com
ca-rt-wp.kayak.com
cashbackil.kayak.com
cc.kayak.com
cheapflights.kayak.com
cn.kayak.com
www.cn.kayak.com
comcast.kayak.com
commerce.kayak.com
www.cz.kayak.com
de.kayak.com
www.de.kayak.com
m.de.kayak.com
secure.de.kayak.com
www.secure.de.kayak.com
derekstravelsite.kayak.com
dk.kayak.com
www.dk.kayak.com
www.dk.kayak.com
ebates.kayak.com
email.kayak.com
es.kayak.com
www.es.kayak.com
es-rt-wp.kayak.com
espanol.kayak.com

ii. Subfinder: subfinder_kayak_result.txt

Tool : Subfinder
Code : subfinder -d kayak.com -o subfinder_kayak_result.txt
Explanation:
subfinder - run subfinder too
l -d kayak.com - Mention the target website
-o subfinder_kayak_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 kayak.com
www.gr.kayak.com
kickads.kayak.com
27.trk.mg.kayak.com
c4.kayak.com
28.trk.mg.kayak.com
lb01.r4.kayak.com
focus.kayak.com
05test.som.kayak.com
kibana-geo-som.kayak.com
gr.kayak.com
mta04-86.mgs.kayak.com
27.trk.mgs.kayak.com
43.trk.mg.kayak.com
32.trk.mg.kayak.com
us-rt-wp.kayak.com
devimagecorona-pad1.kayak.com
mta04-63.mgs.kayak.com
www.ca.kayak.com
47.trk.mg.kayak.com
fw02.som.kayak.com
wp.primer.c4.kayak.com
lt.kayak.com
ami.staging.kayak.com
48.trk.mg.kayak.com
36.trk.mg.kayak.com
14.trk.mg.kayak.com
mundi-wp.kayak.com
fw-pci01.zrh.kayak.com
mta04-61.mgs.kayak.com
www.fi.kayak.com
15.trk.mg.kayak.com
vpnpci-primary.zrh.kayak.com
ca.kayak.com
vn.kayak.com
signupapi.staging.kayak.com
45.trk.mg.kayak.com
commerce.kayak.com
lb01-log.som.kayak.com
mta04-60.mgs.kayak.com
mta04-87.mgs.kayak.com
34.trk.mg.kayak.com
```

ww.gr.kayak.com
kickads.kayak.com
27.trk.mg.kayak.com
c4.kayak.com
28.trk.mg.kayak.com
lb01.r4.kayak.com
focus.kayak.com
05test.som.kayak.com
kibana-geo-som.kayak.com
gr.kayak.com
mta04-86.mgs.kayak.com
27.trk.mgs.kayak.com
43.trk.mg.kayak.com
32.trk.mg.kayak.com
us-rt-wp.kayak.com
devimagecorona-pad1.kayak.com
mta04-63.mgs.kayak.com
www.ca.kayak.com
47.trk.mg.kayak.com
fw02.som.kayak.com
wp.primer.c4.kayak.com
lt.kayak.com
ami.staging.kayak.com
48.trk.mg.kayak.com
36.trk.mg.kayak.com
14.trk.mg.kayak.com
mundi-wp.kayak.com
fw-pci01.zrh.kayak.com
mta04-61.mgs.kayak.com
www.fi.kayak.com
15.trk.mg.kayak.com
vpnpci-primary.zrh.kayak.com
ca.kayak.com
vn.kayak.com
signupapi.staging.kayak.com
45.trk.mg.kayak.com
commerce.kayak.com
lb01-log.som.kayak.com
mta04-60.mgs.kayak.com
mta04-87.mgs.kayak.com
34.trk.mg.kayak.com
au-rt-wp.kayak.com
jvmarena.zrh.kayak.com
fw02-primary.som.kayak.com
on.kayak.com
fi.kayak.com
optimise.kayak.com
business.kayak.com
opentable.kayak.com
primer.c4.kayak.com
11.trk.mg.kayak.com
backoffice.kayak.com
www.privatesale.kayak.com
14test.som.kayak.com
de.kayak.com
39.trk.mg.kayak.com
01test.som.kayak.com
help.affiliates.kayak.com

b. Live Subdomain Discovery

Tool : httpx: livesub_results.txt
Code : httpx-toolkit -l subfinder_kayak_result.txt -o livesub_results.txt
Explanation:
httpx-toolkit - run the httpx tool
-l subfinder_kayak_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://1.support.kayak.com
https://affiliate.kayak.com
https://auth.zrh.kayak.com
https://backoffice.kayak.com
https://au-rt-wp.kayak.com
https://at.kayak.com
https://ca-fr-rt-wp.kayak.com
https://ca-rt-wp.kayak.com
https://1pass-scim-bridge.kayak.com
https://c6.kayak.com
https://ami.staging.kayak.com
https://ami.kayak.com
https://cheapflights.kayak.com
https://cn.kayak.com
https://business-booking.kayak.com
https://commerce.kayak.com
https://de.kayak.com
https://comcast.kayak.com
https://derekstravelsite.kayak.com
https://devimagecorona-pad1.kayak.com
https://cc.kayak.com
https://ca.kayak.com
https://es.kayak.com
https://focus.kayak.com
https://ex.kayak.com
https://c5.x1.kayak.com
https://console.kayak.com
https://backpackers.kayak.com
https://espanol.kayak.com
https://business.kayak.com
https://expe.kayak.com
https://fi.kayak.com
https://carrots.affiliate.kayak.com
https://affiliates.kayak.com
https://business.ca.kayak.com
https://buttermilk.affiliate.kayak.com
https://fw-pci02.zrh.kayak.com
https://fw-pci01.zrh.kayak.com
https://dk.kayak.com
https://api.travel.kayak.com
https://agodaapp.kayak.com
https://c4.x1.kayak.com
```

https://1.support.kayak.com
https://affiliate.kayak.com
https://auth.zrh.kayak.com
https://backoffice.kayak.com
https://au-rt-wp.kayak.com
https://at.kayak.com
https://ca-fr-rt-wp.kayak.com
https://ca-rt-wp.kayak.com
https://1pass-scim-bridge.kayak.com
https://c6.kayak.com
https://ami.staging.kayak.com
https://ami.kayak.com
https://cheapflights.kayak.com
https://cn.kayak.com
https://business-booking.kayak.com
https://commerce.kayak.com
https://de.kayak.com
https://comcast.kayak.com
https://derekstravelsite.kayak.com
https://devimagecorona-pad1.kayak.com
https://cc.kayak.com
https://ca.kayak.com
https://es.kayak.com
https://focus.kayak.com
https://ex.kayak.com
https://c5.x1.kayak.com
https://console.kayak.com
https://backpackers.kayak.com
https://espanol.kayak.com
https://business.kayak.com
https://expe.kayak.com
https://fi.kayak.com
https://carrots.affiliate.kayak.com
https://affiliates.kayak.com
https://business.ca.kayak.com
https://buttermilk.affiliate.kayak.com
https://fw-pci02.zrh.kayak.com
https://fw-pci01.zrh.kayak.com
https://dk.kayak.com
https://api.travel.kayak.com
https://agodaapp.kayak.com
https://c4.x1.kayak.com
https://fw01.zrh.kayak.com
https://fw02-primary.zrh.kayak.com
https://fw02.zrh.kayak.com
https://fw02-secondary.zrh.kayak.com
https://gr.kayak.com
https://click.notification.kayak.com
https://click.k4b.kayak.com
https://fw-vpn01.zrh.kayak.com
https://agoda.kayak.com
https://c4.kayak.com
https://c5.kayak.com
https://hotels.kayak.com
https://click.compare.kayak.com
https://il.kayak.com
https://jvmarena.zrh.kayak.com
https://it-rt-wp.kayak.com

c. IP Discovery

Tool: nslookup: nslookup_result.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: $sub" >> nslookup_result.txt
  nslookup "$sub" | awk '/^Name:|^Address:/' >> nslookup_result.txt
  echo "------------------------" >> nslookup_result.txt
done < livesub_results.txt
```

Explanation:

While read sub; do - start of the loop

Echo "Looking up: $sub">>nslookup_result.txt - print message "Looking up: subdomain" into the file "*nslookup_result*.txt"

nslookup "$sub" | awk '/^Name:|^Address:/' >> nslookup_result.txt - run the nslookup command

echo "_____" >> nslookup_result.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/kayak]
└─$ ./nslookup_script.sh

┌──(kali㉿kali)-[~/Desktop/kayak]
└─$ cat nslookup_result.txt
Looking up: https://1.support.kayak.com
Address:        192.168.43.93#53
------------------------
Looking up: https://affiliate.kayak.com
Address:        192.168.43.93#53
------------------------
Looking up: https://auth.zrh.kayak.com
Address:        192.168.43.93#53
------------------------
Looking up: https://backoffice.kayak.com
Address:        192.168.43.93#53
------------------------
Looking up: https://au-rt-wp.kayak.com
Address:        192.168.43.93#53
------------------------
Looking up: https://at.kayak.com
Address:        192.168.43.93#53
------------------------
Looking up: https://ca-fr-rt-wp.kayak.com
Address:        192.168.43.93#53
------------------------
Looking up: https://ca-rt-wp.kayak.com
Address:        192.168.43.93#53
------------------------
Looking up: https://1pass-scim-bridge.kayak.com
Address:        192.168.43.93#53
------------------------
Looking up: https://c6.kayak.com
Address:        192.168.43.93#53
------------------------
Looking up: https://ami.staging.kayak.com
Address:        192.168.43.93#53
------------------------
Looking up: https://ami.kayak.com
Address:        192.168.43.93#53
------------------------
Looking up: https://cheapflights.kayak.com
Address:        192.168.43.93#53
------------------------
Looking up: https://cn.kayak.com
Address:        192.168.43.93#53
------------------------
Looking up: https://business-booking.kayak.com
Address:        192.168.43.93#53
------------------------
Looking up: https://commerce.kayak.com
Address:        192.168.43.93#53
------------------------
```

IP list:

Looking up: https://1.support.kayak.com
Address: 192.168.43.93#53

Looking up: https://affiliate.kayak.com
Address: 192.168.43.93#53

Looking up: https://auth.zrh.kayak.com
Address: 192.168.43.93#53

Looking up: https://backoffice.kayak.com
Address: 192.168.43.93#53

Looking up: https://au-rt-wp.kayak.com
Address: 192.168.43.93#53

Looking up: https://at.kayak.com
Address: 192.168.43.93#53

Looking up: https://ca-fr-rt-wp.kayak.com
Address: 192.168.43.93#53

Looking up: https://ca-rt-wp.kayak.com
Address: 192.168.43.93#53

Looking up: https://1pass-scim-bridge.kayak.com
Address: 192.168.43.93#53

Looking up: https://c6.kayak.com
Address: 192.168.43.93#53

Looking up: https://ami.staging.kayak.com
Address: 192.168.43.93#53

Looking up: https://ami.kayak.com
Address: 192.168.43.93#53

Looking up: https://cheapflights.kayak.com
Address: 192.168.43.93#53

Looking up: https://cn.kayak.com
Address: 192.168.43.93#53

Looking up: https://business-booking.kayak.com
Address: 192.168.43.93#53

Looking up: https://commerce.kayak.com
Address: 192.168.43.93#53

Looking up: https://de.kayak.com
Address: 192.168.43.93#53
---

d. Open Ports

Tool: nmap: nmap_result.txt

Code: nmap -sV -A -v -O kayak.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
- *kayak.com* - target website
-oN nmap_results.txt - result in an output text file

```
┌──(kali㉿kali)-[~/Desktop/kayak]
└─$ nmap -sV -A -v -O kayak.com -oN nmap_result.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-27 22:22 +0530
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 22:22
Completed NSE at 22:22, 0.00s elapsed
Initiating NSE at 22:22
Completed NSE at 22:22, 0.00s elapsed
Initiating NSE at 22:22
Completed NSE at 22:22, 0.00s elapsed
Initiating Ping Scan at 22:22
Scanning kayak.com (151.101.1.29) [4 ports]
Completed Ping Scan at 22:22, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 22:22
Completed Parallel DNS resolution of 1 host. at 22:22, 0.08s elapsed
Initiating SYN Stealth Scan at 22:22
Scanning kayak.com (151.101.1.29) [1000 ports]
Discovered open port 554/tcp on 151.101.1.29
Discovered open port 443/tcp on 151.101.1.29
Discovered open port 21/tcp on 151.101.1.29
Discovered open port 1723/tcp on 151.101.1.29
Discovered open port 80/tcp on 151.101.1.29
Discovered open port 5060/tcp on 151.101.1.29
Completed SYN Stealth Scan at 22:22, 6.30s elapsed (1000 total ports)
Initiating Service scan at 22:22
Scanning 6 services on kayak.com (151.101.1.29)
Completed Service scan at 22:22, 5.01s elapsed (6 services on 1 host)
Initiating OS detection (try #1) against kayak.com (151.101.1.29)
Retrying OS detection (try #2) against kayak.com (151.101.1.29)
Initiating Traceroute at 22:23
Completed Traceroute at 22:23, 0.02s elapsed
Initiating Parallel DNS resolution of 2 hosts. at 22:23
Completed Parallel DNS resolution of 2 hosts. at 22:23, 13.01s elapsed
NSE: Script scanning 151.101.1.29.
Initiating NSE at 22:23
Completed NSE at 22:23, 22.79s elapsed
Initiating NSE at 22:23
Completed NSE at 22:25, 92.75s elapsed
Initiating NSE at 22:25
Completed NSE at 22:25, 0.01s elapsed
Nmap scan report for kayak.com (151.101.1.29)
Host is up (0.0078s latency).
Other addresses for kayak.com (not scanned): 151.101.129.29 151.101.193.29 151.101.65.29 2a04:4e42:400::285 2a04:4e
42:600::285 2a04:4e42::285 2a04:4e42:200::285
Not shown: 994 filtered tcp ports (no-response)
PORT     STATE SERVICE     VERSION
21/tcp   open  tcpwrapped
80/tcp   open  tcpwrapped
443/tcp  open  tcpwrapped
| ssl-cert: Subject: commonName=kayak.com
| Subject Alternative Name: DNS:kayak.com
| Issuer: commonName=R11/organizationName=Let's Encrypt/countryName=US
| Public Key type: rsa
```

e. Used Technologies

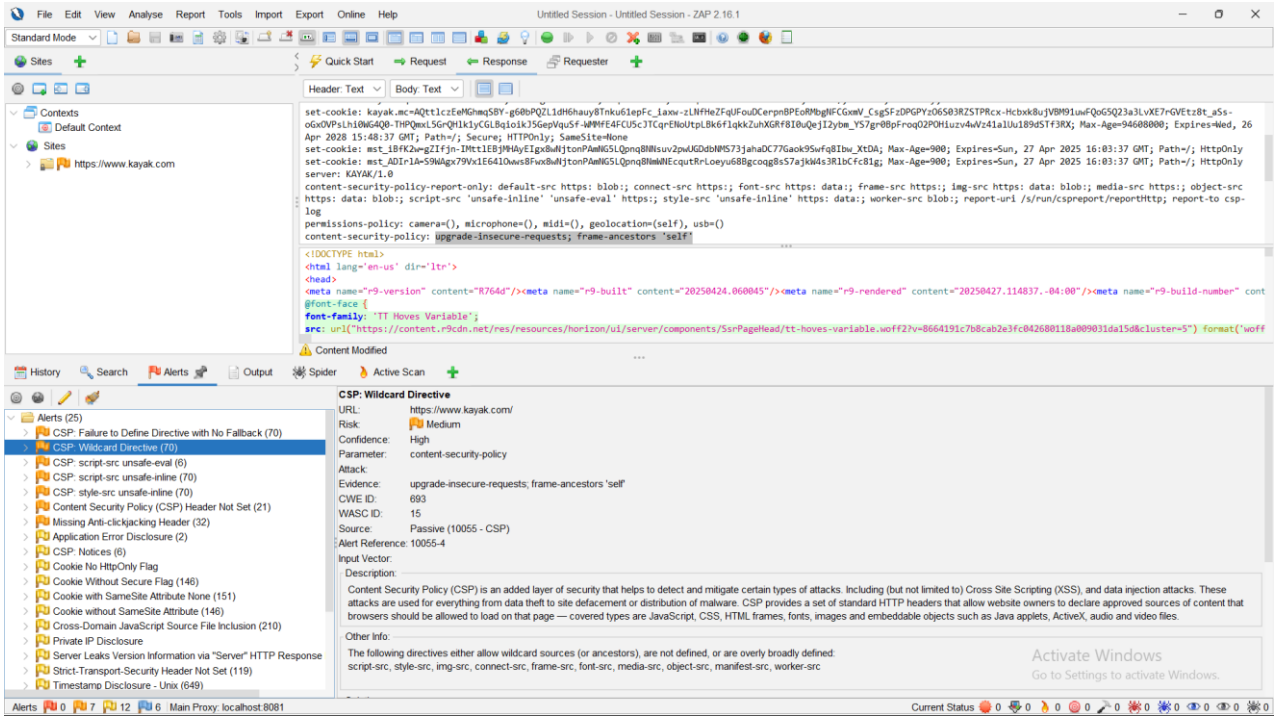
Tool: whatweb - [whatweb_kayak_result.txt]
Code: whatweb -v kayak.com > whatweb_result.txt
Explanation:
whatweb - start whatweb tool
-v - verbose
kayak.com - target website
> whatweb_result.txt - file with the output

```
┌──(kali㉿kali)-[~/Desktop/kayak]
└─$ whatweb -v kayak.com --o whatweb_kayak_result.txt
WhatWeb report for http://kayak.com
Status    : 301 Moved Permanently
Title     : 301 Moved Permanently
IP        : 151.101.129.29
Country   : UNITED STATES, US

Summary   : HTTPServer[Varnish], RedirectLocation[https://www.kayak.com/], UncommonHeaders[retry-after,x-served-by,
x-cache-hits], Varnish, Via-Proxy[1.1 varnish]

Detected Plugins:
[ HTTPServer ]
        HTTP server header string. This plugin also attempts to
        identify the operating system from the server header.

        String       : Varnish (from server string)

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

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

[ UncommonHeaders ]
        Uncommon HTTP server headers. The blacklist includes all
        the standard headers and many non standard but common ones.
        Interesting but fairly common headers should have their own
        plugins, eg. x-powered-by, server and x-aspnet-version.
        Info about headers can be found at www.http-stats.com

        String       : retry-after,x-served-by,x-cache-hits (from headers)

[ Varnish ]
        Varnish is an HTTP accelerator written in C designed for
        content-heavy dynamic web sites. In contrast to other HTTP
        accelerators, such as Squid, which began life as a
        client-side cache, or Apache, which is primarily an origin
        server, Varnish was designed from the ground up as an HTTP
        accelerator.

        Website      : http://www.varnish-cache.org/

[ Via-Proxy ]
        This plugin extracts the proxy server details from the Via
        param of the HTTP header.

        String       : 1.1 varnish

HTTP Headers:
        HTTP/1.1 301 Moved Permanently
        Connection: close
        Content-Length: 448
        Server: Varnish
        Retry-After: 0
```

3. Step 02: Scanning and vulnerability identification

a. Identify Potential Vulnerabilities

Tool : OWASP ZAP
Vulnerability : CSP: Wildcard Directive



CSP: Wildcard Directive:

URL: https://www.kayak.com/
Risk: Medium
Confidential: High
Parameter: content-security-policy
Attack:
Evidence: upgrade-insecure-requests; frame-ancestors 'self'
CWE ID: 693
WASC ID: 15
Source: Passive (10055 - CSP)
Input Vector:

- **Description**: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) Cross Site Scripting (XSS), and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

- **Other Info**: The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined:
  script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src

- **Solution**: Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.

- **Reference**:
  - https://www.w3.org/TR/CSP/
  - https://caniuse.com/#search=content+security+policy

- https://content-security-policy.com/
- https://github.com/HtmlUnit/htmlunit-csp
- https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources

- **Alert Tags**:
  - OWASP_2021_A05: https://owasp.org/Top10/A05_2021-Security_Misconfiguration/
  - CWE-693: https://cwe.mitre.org/data/definitions/693.html
  - OWASP_2017_A06: https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html

b. CSP: Wildcard Directive

CSP: Wildcard Directive refers to the use of the * (wildcard) character in a Content Security Policy (CSP), allowing content to be loaded from any origin. While CSP is designed to restrict and control the sources from which a website loads resources, using wildcards weakens its protection, making the application vulnerable to attacks like Cross-Site Scripting (XSS), data injection, and content hijacking.

Cause of Absence of Anti-CSRF Tokens in a website:

- Using * (wildcard) in directives like script-src, img-src, style-src, or connect-src
- Allowing all external domains without validating trusted sources
- Misunderstanding the security risks associated with wildcards in CSP
- Prioritizing ease of development over strict security enforcement
- Not updating CSP policies after adding third-party services (like CDNs, analytics)
- Auto-generating CSP policies without reviewing or customizing them properly

Propositions to Mitigation or Fix:

- Avoid Wildcards: Specify exact trusted domains in CSP directives instead of using *
- Use Strict CSP Directives: Limit allowed sources using specific protocols (https:) and domains
- Subresource Integrity (SRI): Use SRI for externally loaded scripts and styles to ensure their integrity
- Separate Critical Content: Load highly trusted scripts and styles from your own controlled domains
- Implement CSP Nonces or Hashes: Use nonces ('nonce-xyz') or hashes ('sha256-...') to allow specific inline scripts safely
- Regularly Review and Update CSP: Continuously monitor and adjust your CSP as your web app evolves
- Test CSP Policies: Use tools like CSP Evaluator or browser developer tools to verify the strictness and correctness of CSP settings

4. Step 03: Exploitation and Validation

Request:

```
GET https://www.kayak.com/ HTTP/1.1
host: www.kayak.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
```

Response:

```
set-cookie: kayak.mc=AQttlczEeMGhmqSBY-g60bPQZL1dH6hauy8Tnku61epFc_iaxw-zLNfHeZFqUFouDCerpnBPEoRMbgNFCGxmV_CsgSFzDPGPYzO6S03RZSTPRcx-Hcbxk8ujVBM91uwFQoG5Q23a3LvXE7rGVEtz8t_aSs-
oGxOVPsLhi0WG4Q0-THPQmxL5GrQHlk1yCGLBqioikJ5GepVquSf-WMMfE4FCU5cJTCqrENoUtpLBk6flqkkZuhXGRf8I0uQejI2ybm_YS7gr0BpFroqO2POHiuzv4wVz41alUu189dSTf3RX; Max-Age=94608000; Expires=Wed, 26
Apr 2028 15:48:37 GMT; Path=/; Secure; HTTPOnly; SameSite=None
set-cookie: mst_iBfK2w=gZIfjn-IMttlEBjMHAyEIgx8wNjtonPAmNG5LQpnq8NNsuv2pwUGDdbNMS73jahaDC77Gaok9Swfq8Ibw_XtDA; Max-Age=900; Expires=Sun, 27 Apr 2025 16:03:37 GMT; Path=/; HttpOnly
set-cookie: mst_ADIrlA=S9WAgx79Vx1E64lOwws8Fwx8wNjtonPAmNG5LQpnq8NmWNEcqutRrLoeyu68Bgcoqg8sS7ajkW4s3RlbCfc81g; Max-Age=900; Expires=Sun, 27 Apr 2025 16:03:37 GMT; Path=/; HttpOnly
server: KAYAK/1.0
content-security-policy-report-only: default-src https: blob:; connect-src https:; font-src https: data:; frame-src https:; img-src https: data: blob:; media-src https:; object-src
https: data: blob:; script-src 'unsafe-inline' 'unsafe-eval' https:; style-src 'unsafe-inline' https: data:; worker-src blob:; report-uri /s/run/cspreport/reportHttp; report-to csp-
log
permissions-policy: camera=(), microphone=(), midi=(), geolocation=(self), usb=()
content-security-policy: upgrade-insecure-requests; frame-ancestors 'self'
x-sn-waf-code:
x-xss-protection: 1; mode=block
content-language: en-US
content-type: text/html;charset=UTF-8
x-content-type-options: nosniff
referrer-policy: origin-when-cross-origin
report-to: { "group": "csp-log", "max_age": 43200, "endpoints": [ { "url": "https://www.kayak.com/s/run/cspreport/reportHttp" } ] }
Accept-Ranges: bytes
```

```
<!DOCTYPE html>
<html lang='en-us' dir='ltr'>
<head>
<meta name="r9-version" content="R764d"/><meta name="r9-built" content="20250424.060045"/><meta name="r9-rendered" content="20250427.114837.-04:00"/><meta name="r9-build-number" cont
@font-face {
font-family: 'TT Hoves Variable';
src: url("https://content.r9cdn.net/res/resources/horizon/ui/server/components/SsrPageHead/tt-hoves-variable.woff2?v=8664191c7b8cab2e3fc042680118a009031da15d&cluster=5") format('woff
url("https://content.r9cdn.net/res/resources/horizon/ui/server/components/SsrPageHead/tt-hoves-variable.woff2?v=8664191c7b8cab2e3fc042680118a009031da15d&cluster=5") format('woff2-var
font-display: swap;
font-weight: 50 900;
font-style: normal;
}
</style><meta name="viewport" content="width=device-width, initial-scale=1, minimum-scale=1"/><meta name="format-detection" content="telephone=no"/><link rel="icon" href="/favicon.ic
var safari13PlusRegex = /Macintosh;.*?Version\/(1[3-9]|[2-9][0-9][0-9]+)(\.[0-9]+)* Safari/;
if (
```

5. Step 04: Mitigation / Fix

Immediate Mitigation Actions:
1. Define Strict CSP Directives

Long Term Prevention:
1. Automate CSP Generation using tools like *Report-URI* or *CSP Evaluator*.
2. Integrate CSP checks into CI/CD