

Sri Lanka Institute of Information Technology



Assignment report 02

IT22357762

Web Security -IE2062

**Web Security – IE2062**

B.Sc. (Hons) in Information

# Contents

1	Arkose Labs .....	3
1.1	Sub- domain list .....	4
1.2	Firewall detection .....	7
1.3	IP scanning .....	7
1.4	Port scanning .....	8
1.5	Nikto scanning .....	10
1.6	Burpsuite scanning .....	10
1.7	Netspaker scan .....	11
1.8	Vulnerabilities .....	11
1.8.1	Other vulnerabilities .....	12

# 1 Arkose Labs

Arkose labs is a software company which provide the security to the applications in order to stop bots prevent ATO and fake accounts.

The screenshot shows the Arkose Labs HackerOne page. At the top, there's a green header with the Arkose Labs logo and a 'Submit report' button. Below the header, the page is divided into sections. The first section, 'Arkose Labs', describes the company as 'Bankrupting the business model of fraud' and lists its backers: Microsoft, PayPal, SoftBank, and Wells Fargo. It also provides the website URL: <https://www.arkoselabs.com/>. The second section, 'Bug Bounty Program', states it was launched in Jan 2024 and is managed by HackerOne. It includes features like 'Includes retesting' and 'Collaboration enabled'. The third section, 'Rewards', shows a table of bounty amounts for different severity levels: Low, Medium, High, and Critical. The fourth section, 'Response Efficiency', shows the average time to first response, triage, and close, along with a 99% report success rate.

Low	Medium	High	Critical
\$200 - \$500	\$501 - \$1,000	\$1,001 - \$2,000	\$2,001 - \$4,000
\$50 - \$150	\$151 - \$400	\$401 - \$700	\$701 - \$1,000

We are offering two tiers of bounties as follows:

Core Applications	Low	Medium	High	Critical
	\$200 - \$500	\$501 - \$1,000	\$1,001 - \$2,000	\$2,001 - \$4,000

The screenshot shows the Arkose Labs website. The top navigation bar includes links for Solutions, Products, Resources, Company, and Customers. The main banner features the text 'Arkose Accelerate Virtual Event on April 4!' and a sub-headline: 'Because it takes a network to defeat a network. Sharing knowledge and know-how to create a formidable front against cyber attackers.' Below the banner, there are two buttons: 'Save Your Seat!' and 'Book Demo'. On the right side of the banner, there is a graphic of a globe with network connections.

## 1.1 Sub- domain list

Tool – amass

Command – amass enum -passive -d arkoselabs.com

```
(tharu@kali)~$ amass enum -passive -d arkoselabs.com
api-origin-oregon.arkoselabs.com
dashboard-staging.arkoselabs.com
match-api.arkoselabs.com
developer.arkoselabs.com
ec-api-production.us-east-2.arkoselabs.com
twitch-verify.arkoselabs.com
nojs-game3-prod-ap-southeast-1.arkoselabs.com
api-origin-nvirenia.arkoselabs.com
api-staging.arkoselabs.com
rsvp.arkoselabs.com
ap-northeast-1.internal.services.aws.arkoselabs.com
staging.arkoselabs.com
audio-us-west-2.arkoselabs.com
api-origin-devdog-sydney.arkoselabs.com
arkoselabs.com
www-staging.arkoselabs.com
match-verify.arkoselabs.com
st.arkoselabs.com
cloudfuze-api.arkoselabs.com
blizzard-api.arkoselabs.com
status.arkoselabs.com
production-blue.eu-west-1.services.aws.arkoselabs.com
boa-verify.arkoselabs.com
imvu-verify.arkoselabs.com
status-priv-1.arkoselabs.com
production-blue.us-east-1.services.aws.arkoselabs.com
tinder-verify.arkoselabs.com
ap-northeast-1.services.aws.arkoselabs.com
api-origin-utcat-sydney.arkoselabs.com
verify.arkoselabs.com
dashboard.arkoselabs.com
ec-api-production.ap-southeast-1.arkoselabs.com
auth-proxy.ap-southeast-2.aws.staging.arkoselabs.com
circle-verify.arkoselabs.com
client-demo.arkoselabs.com
us-west-2.services.aws.arkoselabs.com
api-origin-prod-singapore.arkoselabs.com
tableau-auth-proxy-prod.internal.aws.arkoselabs.com
audio-us-east-1.arkoselabs.com
roblox-verify.arkoselabs.com
image-prod-ap-southeast-1.arkoselabs.com
admin-development.arkoselabs.com
enterpriseenrollment.arkoselabs.com
www-prod-ohio.arkoselabs.com
prod-ohio.arkoselabs.com
linkedin-verify.arkoselabs.com
ps-labs.arkoselabs.com
microsoft-api.arkoselabs.com
client-demo-dev.arkoselabs.com
ec-api-production.us-west-2.arkoselabs.com
```

Sub domain list –

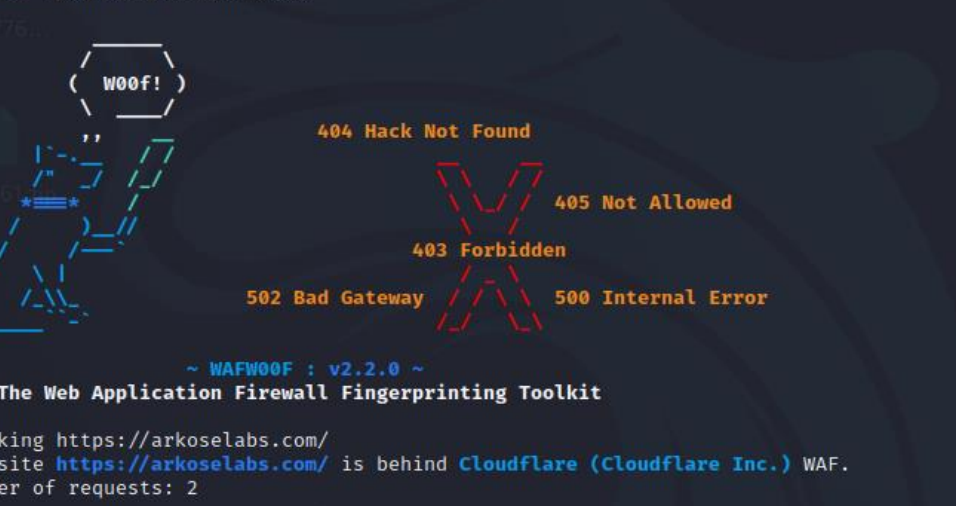
- api-origin-oregon.arkoselabs.com
- dashboard-staging.arkoselabs.com
- match-api.arkoselabs.com
- developer.arkoselabs.com
- ec-api-production.us-east-2.arkoselabs.com
- twitch-verify.arkoselabs.com
- nojs-game3-prod-ap-southeast-1.arkoselabs.com
- api-origin-nvirenia.arkoselabs.com
- api-staging.arkoselabs.com
- rsvp.arkoselabs.com
- ap-northeast-1.internal.services.aws.arkoselabs.com
- staging.arkoselabs.com
- audio-us-west-2.arkoselabs.com
- api-origin-devdog-sydney.arkoselabs.com
- arkoselabs.com
- www-staging.arkoselabs.com
- match-verify.arkoselabs.com
- st.arkoselabs.com
- cloudfuze-api.arkoselabs.com
- blizzard-api.arkoselabs.com
- status.arkoselabs.com
- production-blue.eu-west-1.services.aws.arkoselabs.com
- boa-verify.arkoselabs.com
- imvu-verify.arkoselabs.com
- status-priv-1.arkoselabs.com
- production-blue.us-east-1.services.aws.arkoselabs.com
- tinder-verify.arkoselabs.com
- ap-northeast-1.services.aws.arkoselabs.com
- api-origin-utcat-sydney.arkoselabs.com
- verify.arkoselabs.com
- dashboard.arkoselabs.com
- ec-api-production.ap-southeast-1.arkoselabs.com
- auth-proxy.ap-southeast-2.aws.staging.arkoselabs.com
- circle-verify.arkoselabs.com
- client-demo.arkoselabs.com
- us-west-2.services.aws.arkoselabs.com
- api-origin-prod-singapore.arkoselabs.com
- tableau-auth-proxy-prod.internal.aws.arkoselabs.com
- audio-us-east-1.arkoselabs.com

- roblox-verify.arkoselabs.com
- image-prod-ap-southeast-1.arkoselabs.com
- admin-development.arkoselabs.com
- enterpriseenrollment.arkoselabs.com
- www.prod-ohio.arkoselabs.com
- prod-ohio.arkoselabs.com
- linkedin-verify.arkoselabs.com
- ps-labs.arkoselabs.com
- microsoft-api.arkoselabs.com
- client-demo-dev.arkoselabs.com
- ec-api-production.us-west-2.arkoselabs.com
- verify-api.arkoselabs.com
- github-verify.arkoselabs.com
- devdog-sydney.arkoselabs.com
- api-origin-singapore.arkoselabs.com
- www.arkoselabs.com
- dev.arkoselabs.com
- sso.arkoselabs.com
- devdog-ohio.arkoselabs.com
- preview-uatcat.arkoselabs.com
- rockstar-verify.arkoselabs.com
- nojs-game3-uatcat-us-east-1.arkoselabs.com
- autodiscover.arkoselabs.com
- microsoft-auth.arkoselabs.com
- ap-southeast-1.services.aws.arkoselabs.com
- roblox-api.arkoselabs.com
- us.auth0.arkoselabs.com
- ea-api.arkoselabs.com
- image-prod-us-east-1.arkoselabs.com
- hydrolix-eks.arkoselabs.com
- production-blue.us-east-2.internal.services.aws.arkoselabs.com
- nojs-game3-prod-us-east-1.arkoselabs.com
- ap-southeast-2.services.aws.arkoselabs.com
- prod-oregon.arkoselabs.com
- portal-prod.arkoselabs.com
- blizzard-verify.arkoselabs.com
- api-origin-devdog.arkoselabs.com
- customer-staging.arkoselabs.com
- boa-api.arkoselabs.com
- client.arkoselabs.com
- iframe.arkoselabs.com
- dataswan-test.arkoselabs.com
- minecraft-verify.arkoselabs.com
- portal.arkoselabs.com
- sso-dev.arkoselabs.com
- expedia-verify.arkoselabs.com
- hrt.arkoselabs.com
- api-origin-ireland.arkoselabs.com
- image-ap-northeast-1.arkoselabs.com
- image-devdog-ap-southeast-2.arkoselabs.com
- epic-games-verify.arkoselabs.com
- test-cases-ap-southeast-2.arkoselabs.com
- portal-dev.arkoselabs.com
- artist-prototype-ec.arkoselabs.com
- epic-games-api.arkoselabs.com
- api.arkoselabs.com
- twilio-api.arkoselabs.com
- api-origin-uatcat-nvrginia.arkoselabs.com
- production-blue.us-west-2.services.aws.arkoselabs.com
- image-ap-southeast-2.arkoselabs.com
- audio-eu-west-1.arkoselabs.com
- image-eu-west-1.arkoselabs.com
- prod-singapore.arkoselabs.com
- dropbox-api.arkoselabs.com
- twitch-api.arkoselabs.com
- twitter-verify.arkoselabs.com
- image-uatcat-ap-southeast-2.arkoselabs.com
- ecs.ap-southeast-2.aws.development.arkoselabs.com
- ea-verify.arkoselabs.com
- api-devdog.arkoselabs.com
- eu-west-1.internal.services.aws.arkoselabs.com
- twilio-verify.arkoselabs.com
- amazon-api.arkoselabs.com
- us-east-2.services.aws.arkoselabs.com
- image-ap-southeast-1.arkoselabs.com
- grafana.us-east-1.aws.development.arkoselabs.com
- production-blue.ap-southeast-2.services.aws.arkoselabs.com
- image-uatcat-us-east-1.arkoselabs.com
- minecraft-api.arkoselabs.com
- microsoft-verify.arkoselabs.com
- us-west-2.internal.services.aws.arkoselabs.com
- funcaptcha-eb-uatcat.arkoselabs.com
- hydrolix-eks-china.arkoselabs.com
- internal.aws.arkoselabs.com
- production-blue.eu-west-1.internal.services.aws.arkoselabs.com
- help.arkoselabs.com
- development.arkoselabs.com
- us-east-1.aws.production.arkoselabs.com
- rockstar-api.arkoselabs.com
- auth-proxy.us-east-1.aws.production.arkoselabs.com
- secure-ticket.arkoselabs.com

- cdn.arkoselabs.com
- production-blue.ap-southeast-1.internal.services.aws.arkoselabs.com
- api-origin-uatcat.arkoselabs.com
- image-us-east-1.arkoselabs.com
- cloudfuze.arkoselabs.com
- ap-southeast-2.internal.services.aws.arkoselabs.com
- smart.arkoselabs.com
- funcaptcha-eb-prod2.arkoselabs.com
- go.arkoselabs.com
- production-blue.us-east-2.services.aws.arkoselabs.com
- image-us-west-2.arkoselabs.com
- image-prod-us-west-2.arkoselabs.com
- www.portal-prod.arkoselabs.com
- hotels-verify.arkoselabs.com
- api-prod.arkoselabs.com
- eu-west-1.services.aws.arkoselabs.com
- nojs-game3-prod-ap-northeast-1.arkoselabs.com
- jobs.arkoselabs.com
- www.cdn-origin-production-us-east-2.arkoselabs.com
- us-east-2.internal.services.aws.arkoselabs.com
- portal-staging.arkoselabs.com
- nojs-game3-prod-eu-west-1.arkoselabs.com
- iframe-auth.arkoselabs.com
- image-prod-eu-west-1.arkoselabs.com
- sonarqube.arkoselabs.com
- iframe-auth-staging.arkoselabs.com
- uatcat-ohio.arkoselabs.com
- customer-sessions.arkoselabs.com
- client-api.arkoselabs.com
- api-origin-prod-ireland.arkoselabs.com
- production.arkoselabs.com
- api-dev.arkoselabs.com
- expedia-api.arkoselabs.com
- nojs-game3-uatcat-ap-southeast-2.arkoselabs.com
- funcaptcha-eb-devdog.arkoselabs.com
- nojs-game3-devdog-ap-southeast-2.arkoselabs.com
- uatcat-sydney.arkoselabs.com
- api-origin-prod-nvirlnia.arkoselabs.com
- github-api.arkoselabs.com
- paypal-api.arkoselabs.com
- services.aws.arkoselabs.com
- insightvm.arkoselabs.com
- preview-devdog.arkoselabs.com
- ap-southeast-1.internal.services.aws.arkoselabs.com
- audio-ap-southeast-2.arkoselabs.com
- production-blue.us-west-2.internal.services.aws.arkoselabs.com
- tinder-api.arkoselabs.com
- audio-ap-southeast-1.arkoselabs.com
- circle-api.arkoselabs.com
- em.arkoselabs.com
- preview-api.arkoselabs.com
- nojs-game3-devdog-us-east-1.arkoselabs.com
- api-origin.arkoselabs.com
- hotels-api.arkoselabs.com
- dataswan.arkoselabs.com
- production-blue.ap-southeast-1.services.aws.arkoselabs.com
- production-blue.ap-northeast-1.services.aws.arkoselabs.com
- us-east-1.internal.services.aws.arkoselabs.com
- production-blue.ap-southeast-2.internal.services.aws.arkoselabs.com
- prod-nvirlnia.arkoselabs.com
- nojs-game3-prod-us-west-2.arkoselabs.com
- funcaptcha-eb-prod.arkoselabs.com
- prod-ireland.arkoselabs.com
- tableau.arkoselabs.com
- twitter-api.arkoselabs.com
- ec-api-production.us-east-1.arkoselabs.com
- sony-legacy-api.arkoselabs.com
- asurion-api.arkoselabs.com
- image-devdog-us-east-1.arkoselabs.com
- ec-api-production.eu-west-1.arkoselabs.com
- us-east-1.services.aws.arkoselabs.com
- dataswan-uat.arkoselabs.com
- ensemble.arkoselabs.com
- demo.arkoselabs.com
- test-cases.arkoselabs.com
- api-origin-prod-oregon.arkoselabs.com
- support.arkoselabs.com
- nojs-game3-ap-southeast-2.arkoselabs.com
- cdn-origin-production-us-east-2.arkoselabs.com
- dashboard-api.arkoselabs.com
- imvu-api.arkoselabs.com
- production-blue.us-east-1.internal.services.aws.arkoselabs.com
- enterpriseregistration.arkoselabs.com
- devdog-nvirlnia.arkoselabs.com
- arkosepremium.arkoselabs.com
- api-uatcat.arkoselabs.com
- client-demo-uat.arkoselabs.com
- linkedin-api.arkoselabs.com
- load-testing.arkoselabs.com
- admin.arkoselabs.com
- deployment-test.arkoselabs.com

## 1.2 Firewall detection

Command – wafw00f [https:// arkoselabs.com /](https://arkoselabs.com/)



```
(tharu@kali)-[~]
$ wafw00f https://arkoselabs.com/

[72235776]
( W00f! )
n2231361
~ WAFW00F : v2.2.0 ~
The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://arkoselabs.com/
[+] The site https://arkoselabs.com/ is behind Cloudflare (Cloudflare Inc.) WAF.
[~] Number of requests: 2

404 Hack Not Found
405 Not Allowed
403 Forbidden
502 Bad Gateway
500 Internal Error

(tharu@kali)-[~]
$
```

### 1.3 IP scanning

## Tool – nslookup

Command – nslookup arkoselabs.com

```
(tharu@kali)-[~]
$ nslookup arkoselabs.com
Server:      172.16.10.100
Address:     172.16.10.100#53

Non-authoritative answer:
Name:   arkoselabs.com
Address: 18.67.181.27
Name:   arkoselabs.com
Address: 18.67.181.100
Name:   arkoselabs.com
Address: 18.67.181.11
Name:   arkoselabs.com
Address: 18.67.181.120

(tharu@kali)-[~]
$
```

## 1.4 Port scanning

Tool - nmap

Command – nmap -sV -sC -Pn 18.67.181.27 -A

```
(tharu@kali)-[~]
$ nmap -sV -sC -Pn 18.67.181.27 -A
Starting Nmap 7.93 ( https://nmap.org ) at 2024-03-26 14:20 +0530
Stats: 0:02:06 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 50.00% done; ETC: 14:24 (0:01:12 remaining)
Nmap scan report for server-18-67-181-27.kul50.r.cloudfront.net (18.67.181.27)
Host is up (0.23s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Amazon CloudFront httpd
|_http-server-header: CloudFront
443/tcp    open  ssl/https    CloudFront
|_http-title: ERROR: The request could not be satisfied
|_http-server-header: CloudFront
8008/tcp   open  http
|_http-title: Did not follow redirect to https://server-18-67-181-27.kul50.r.cloudfront.net:8015/
|_fingerprint-strings:
|_FourOhFourRequest:
|_HTTP/1.1 302 Found
|_Location: https://:8015/nice%20ports%2C/Tri%6Eity.txt%2ebak
|_Connection: close
|_X-Frame-Options: SAMEORIGIN
|_X-XSS-Protection: 1; mode=block
|_X-Content-Type-Options: nosniff
|_Content-Security-Policy: frame-ancestors 'self'
GenericLines, HTTPOptions, RTSPRequest, SIPOptions:
|_HTTP/1.1 302 Found
|_Location: https://:8015
|_Connection: close
|_X-Frame-Options: SAMEORIGIN
|_X-XSS-Protection: 1; mode=block
|_X-Content-Type-Options: nosniff
|_Content-Security-Policy: frame-ancestors 'self'
GetRequest:
|_HTTP/1.1 302 Found
|_Location: https://:8015/
|_Connection: close
|_X-Frame-Options: SAMEORIGIN
|_X-XSS-Protection: 1; mode=block
|_X-Content-Type-Options: nosniff
|_Content-Security-Policy: frame-ancestors 'self'
8010/tcp   open  ssl/xmpp?
|_ssl-cert: Subject: commonName=18.67.181.27
|_Subject Alternative Name: DNS:18.67.181.27
|_Not valid before: 2022-04-27T15:17:46
|_Not valid after: 2024-07-30T15:17:46
|_fingerprint-strings:
```





## 1.5 Nikto scanning

Tool – Nikto

Command - `sudo nikto -h arkoselabs.com`

```
(tharu@kali): ~  
$ sudo nikto -h arkoselabs.com  
[sudo] password for tharu:  
- Nikto v2.5.0  
  
+ Multiple IPs found: 18.67.181.100, 18.67.181.120, 18.67.181.27, 18.67.181.11  
+ Target IP: 18.67.181.100  
+ Target Hostname: arkoselabs.com  
+ Target Port: 80  
+ Start Time: 2024-03-26 14:31:37 (GMT+5)  
  
+ Server: CloudFront  
+ /: Retrieved via header: 1.1 5bdc6e79c2722cbcd20de22c26610822.cloudfront.net (CloudFront).  
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options  
+ /: An alt-svc header was found which is advertising HTTP/3. The endpoint is: ':443'. Nikto cannot test HTTP/3 over QUIC. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/alt-svc  
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/  
+ Root page / redirects to: https://arkoselabs.com/  
+ No CGI Directories found (use '-C all' to force check all possible dirs)  
  
+ 7962 requests: 0 error(s) and 4 item(s) reported on remote host  
+ End Time: 2024-03-26 14:45:01 (GMT+5) (804 seconds)  
  
+ 1 host(s) tested
```

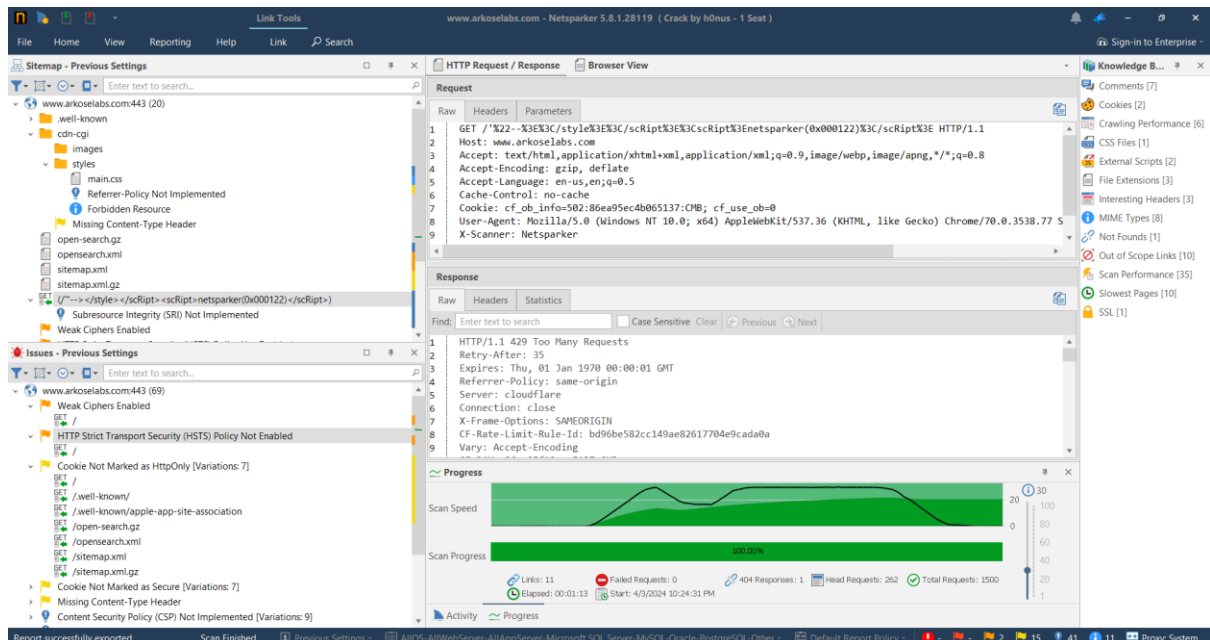
## 1.6 Burpsuite scanning

The screenshot displays the Burp Suite Professional interface. The top menu bar includes options like Dashboard, Target, Proxy, Intruder, Repeater, Collaborator, Sequencer, Decoder, Comparer, Logger, Organizer, Extensions, and Learn. The main workspace is divided into several panels:

- Site map:** Shows a tree view of the scanned website structure, including URLs like `https://js-agent.newrelic.com`, `https://js-zi-scripts.com`, and `https://arkoselabs.com`.
- Contents:** A table listing the scanned content. The table has columns for Host, Method, URL, Params, Status Code, Length, MIME type, and Title. The first row shows a GET request to `https://www.arkoselabs.com/` with a status code of 200 and a MIME type of HTML.
- Issues:** A list of security issues found during the scan. The first issue is "Session token in URL" with a severity of Medium and a confidence of Firm. The second issue is "HTML does not specify charset" with a severity of Low and a confidence of Firm.
- Request/Response:** A detailed view of the selected request and response, showing the raw data and the decoded content.

The bottom status bar indicates the memory usage: 292.9MB.

## 1.7 Netsparker scan



## 1.8 Vulnerabilities

**Vulnerability Title:** Session ID Exposure in URLs

**Vulnerability Description:** As session id is transmitted as a part of URL it's making the vulnerability to intercept, session hijacking and unauthorized access.

**Affected Components:** Web application's authentication and session management components are being affected.

**Impact Assessment:** Impact of vulnerability includes,

- Unauthorized access to user accounts and sensitive information.
- Session hijacking – control legitimate user's session
- Information leakage – logged session id in server logs and transmitted over insecure channels.

**Steps to Reproduce:**

1. Access the application using a web browser.
2. Log into the application using valid credentials.
3. Observe the URL which contains the session id in the query when using the path /v1/beacon/img.gif

**Proof of concept:**

```
Advisory Request Response Path to issue
Pretty Raw Hex
1 GET /v1/beacon/img.gif?token=538ccccb4b8f5f5832717a1344b59cfd&visitor=null&visitor=
9cdd5c27-b55a-452d-8c39-585811f3862a&session=47a308f3-1cb8-442c-879c-209af4b4e966&event=a_pageLoad&qf=
%7B%22pageLoadTime%22%3A%22Wed%2C%2003%20Apr%202024%2010%3A22%3A54%20GMT%22%7D&isIframe=false&mf=
%7B%22description%22%3A%22Stop%20account%20takeover%2C%20man-in-the-middle%20attacks%2C%20credential%20s
g%2C%20new%20account%20fraud%2C%20SMS%20to11%20fraud%20and%20more%20E2%80%93%20with%20protection%20that
ls%20out%20in%20hours.%22%2C%22keywords%22%3A%22%22%2C%22title%22%3A%22Stop%20Bots.%20Prevent%20ATOs%20%
3B%20Fake%20Accounts%20%7C%20Arkose%20Labs%22%7D&cb=&r=&thirdParty=%7B%7D&v2=1&pageURL=
https%3A%2F%2Fwww.arkoselabs.com%2F&pageViewId=64c6db86-9b72-44bd-885e-e823e06ef259&webTagId=
ae003ad5-0c22-4718-ba7d-e1432c9e169c&v=1.1.15 HTTP/1.1
2 Host: b.6s.co
3 Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
4 Sec-Ch-Ua-Mobile: ?0
```

**Proposed Mitigation or Fix:** Should use alternative method of transmitting session tokens such as HTTP cookies or using POST method to form submission.

1. HTTP Strict Transport Security (HSTS) Policy Not Enabled.
2. Weak Ciphers Enabled.
3. Cookie Not Marked as HttpOnly.
4. Cookie Not Marked as Secure.
5. Missing Content-Type Header.
6. Content Security Policy (CSP) Not Implemented.
7. Expect-CT Not Enabled.
8. Missing X-XSS-Protection Header.

9. Referrer-Policy Not Implemented.
10. SameSite Cookie Not Implemented.
11. Forbidden Resource.