## Sri Lanka Institute of Information Technology



Assignment report 02 IT22357762 Web Security -IE2062

Web Security – IE2062

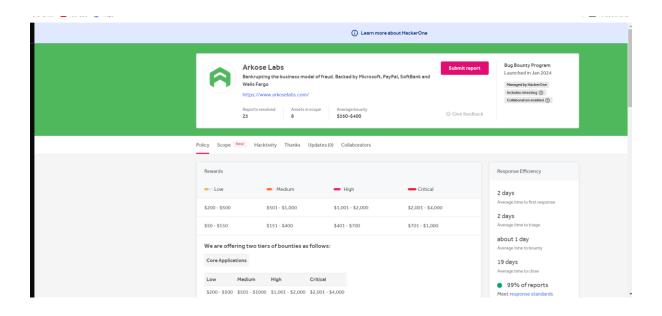
B.Sc. (Hons) in Information

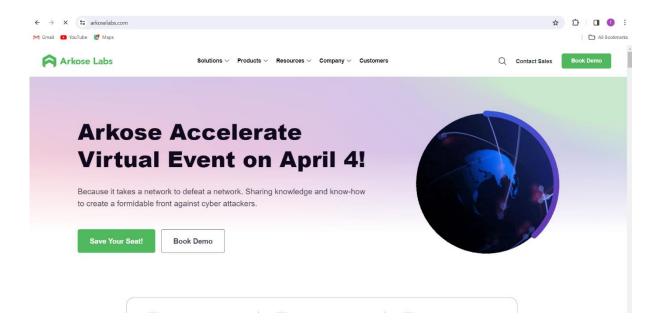
# **Contents**

1	Arko	se 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	Vulnerabilities	11
	1.7.1	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.





#### 1.1 **Sub-domain list**

#### Tool – amass

#### Command - amass enum -passive -d arkoselabs.com

```
aru® kali)-[~]
ass enum -passive -d arkoselabs.com
igin-oregon.arkoselabs.com
ard-staging.arkoselabs.com
api.arkoselabs.com
per.arkoselabs.com
-production.us-east-2.arkoselabs.com
-verify.arkoselabs.com
agi-prod-ap-outheast-1.arkoselabs.com
igin-nvirginia.arkoselabs.com
aging.arkoselabs.com
rkoselabs.com
rkoselabs.com
sus-set-2.arkoselabs.com
koselabs.com
isin-arkoselabs.com
isin-arkoselabs.com
isin-arkoselabs.com
isin-devidg-sydney.arkoselabs.com
isin-devidg-sydney.arkoselabs.com
isin-devidg-sydney.arkoselabs.com
isin-devidg-sydney.arkoselabs.com
isin-devidg-sydney.arkoselabs.com
isin-devidg-sydney.arkoselabs.com
isin-devidg-sydney.arkoselabs.com
-staging_arkoselabs.com
arkoselabs.com
durue-api.arkoselabs.com
api.arkoselabs.com
api.arkose
```

#### 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-game 3-prod-ap-southeast-1. arkosel abs. com
- api-origin-nvirginia.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-dev dog-sydney. arkosel abs. 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-uat cat-sydney. arkosel abs.com
- verify.arkoselabs.com
- dashboard.arkoselabs.com
- $ec\hbox{-}api\hbox{-}production.ap\hbox{-}southeast\hbox{-}1.arkoselabs.com$
- $auth\mbox{-}proxy.ap\mbox{-}southeast\mbox{-}2.aws.staging.arkoselabs.com} \\ circle\mbox{-}verify.arkoselabs.com}$
- client-demo.arkoselabs.com
- $us\hbox{-}west\hbox{-}2.services.aws.arkoselabs.com$
- 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-ap-northeast-1.arkosetabs.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-nvirginia.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.comtwitter-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

- production-blue. ap-southeast-1. in ternal. services. aws. arkosel abs. com
- api-origin-uatcat.arkoselabs.com
- image-us-east-1.arkoselabs.com
- cloudfuze.arkoselabs.com
- ap-southeast-2. in ternal. services. aws. arkosel abs. 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
- iobs.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
- $nojs\hbox{-} game \hbox{3--devdog-ap-southeast-2.} arkos elabs.com$
- uatcat-sydney.arkoselabs.com
- api-origin-prod-nvirginia.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. arkosel abs. com
- production-blue.ap-northeast-1.services.aws.arkoselabs.com

us-east-1.internal.services.aws.arkoselabs.com

- production-blue. ap-southeast-2. in ternal. services. aws. arkosel abs. com
- prod-nvirginia.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
- $cdn\hbox{-}origin\hbox{-}production\hbox{-}us\hbox{-}east\hbox{-}2.arkoselabs.com$
- dashboard-api.arkoselabs.com
- imvu-api.arkoselabs.com
- $\stackrel{\cdot}{\text{production-blue.us-east-1.internal.services.aws.arkoselabs.com}}$
- enterpriseregistration.arkoselabs.com
- devdog-nvirginia.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 /

### 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: 18.67.181.11

Name: arkoselabs.com
Address: 18.67.181.120
```

#### 1.4 Port scanning

Tool - nmap

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





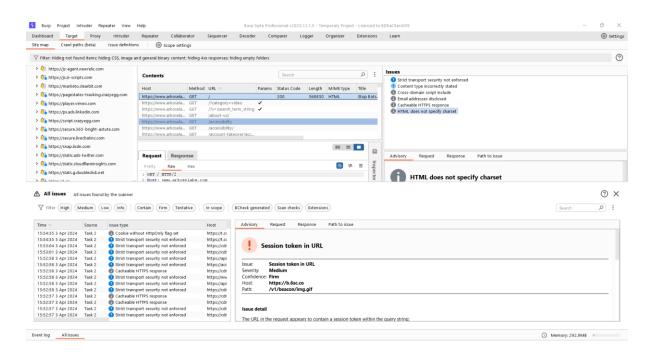


#### 1.5 Nikto scanning

#### Tool - Nikto

Command - sudo nikto -h arkoselabs.com

#### 1.6 Burpsuite scanning



#### 1.7 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,

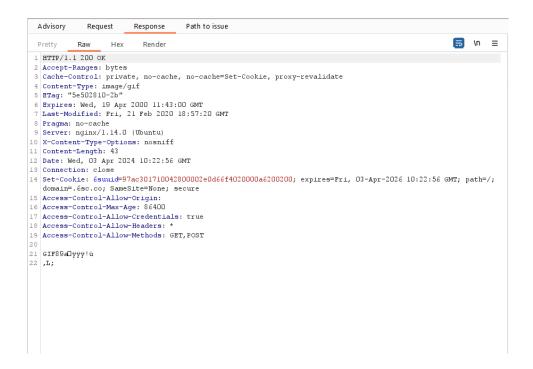
- Unauthorized access to user accounts and sensitive information.
- Session hijacking control legitimate user's session
- Information leakage logged session id in server logs and transmitted over insecure channels.

#### **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:**





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

#### 1.7.1 Other vulnerabilities

- 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.