M.O.P

MELBOURNE OPENDATA PLAYGROUND

# AWS/GCP Security Scheme for Chameleon MOP

**CHAMELEON DESIGN TEAM**

**Trimester 1, 2022**

# Document Details

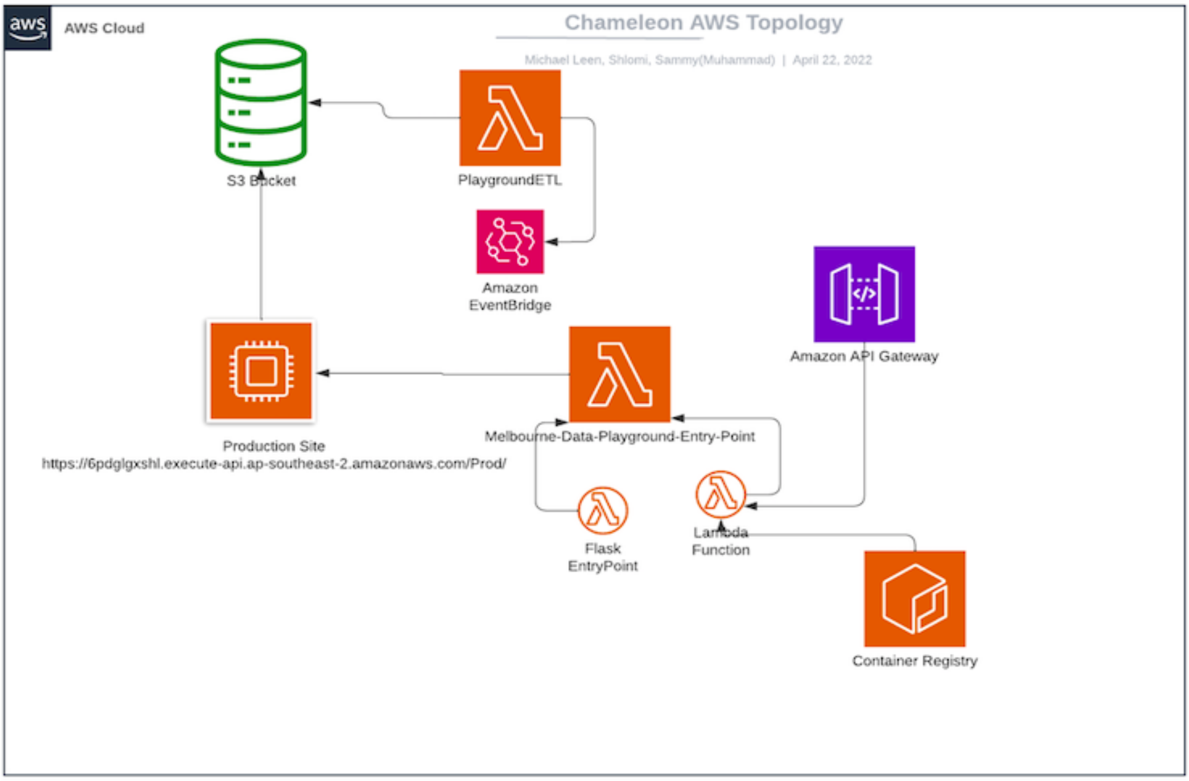
| Date | Authors | Version |
|---|---|---|
| 28/05/2022 | Bradie Robinson, Jacob Djaelani | 1.0 |
| | | |
| | | |
| | | |

# Table of Contents

# Amazon Web Services (AWS)

The AWS implementation is due to be replaced with GCP. However, we recommend the follow changes to ensure that AWS is secure before its deprecation.

## AWS Implementation



aws
AWS Cloud
Chameleon AWS Topology
Michael Leen, Shlomi, Sammy(Muhammad) | April 22, 2022
S3 Bucket
PlaygroundETL
Amazon EventBridge
Amazon API Gateway
Production Site
https://6pdglgxshl.execute-api.ap-southeast-2.amazonaws.com/Prod/
Melbourne-Data-Playground-Entry-Point
Flask EntryPoint
Lambda Function
Container Registry

## Ports

We recommend mandating all traffic to be via HTTPS (port 443). This ensures that all traffic is encrypted using a secure socket layer (SSL).
Additionally, using HTTP (port 80) instead of HTTPS has an impact on search engine rankings.

This can be implemented by:

1. Open EC2 console at https://console.aws.amazon.com/ec2/
2. Under ‘Load Balancing’, click ‘Load balancers’
3. Under ‘Protocol: port’ choose HTTP
4. Under ‘Default actions’ click ‘Add action’, then click ‘redirect to’ and enter port ‘443’
5. Under ‘Load balancer’ click ‘HTTP Listener’
6. Under ‘Rules’ click ‘View/edit rules’
7. Under ‘Edit Rule’, change the default to redirect HTTP requests to HTTPS
8. Under ‘Then’ delete the old default condition
9. Under ‘Redirect to’ enter port ‘443’
10. Save changes

## Multi Factor Authentication (MFA)

We recommend mandating multi factor authentication. Due to the practicality of purchasing MFA hardware we recommend: Virtual (software-based) MFA device. MFA ensures that if a username and password is leaked, then the hacker is still unable to access the AWS account.

This can be implemented by:

1. Open SSO console: https://console.aws.amazon.com/singlesignon
2. Under ‘Settings’ click ‘Network and Security’
3. Under ‘Network and Security’ click ‘Configure’
4. Under ‘Configure multi-factor authentication’ click ‘Require them to register an MFA device at sign in’
5. Save changes

## Allowed Accounts

We recommend account holders should only include all current users of the system and any University administration staff. If an old senior requires access, this should only be granted temporarily for the duration required.

Accounts can be maintained via:

1. Open IAM console at https://console.aws.amazon.com/iam/
2. Under the 'Users' click 'Add User' OR ‘Delete User’

## Account Permissions

We recommend keeping the current permission implementation on the AWS account. This is for edit and read-only access.

For reference, adding a user to a permission group can be updated by:

1. Open IAM console at https://console.aws.amazon.com/iam/
2. Under ‘Users’ click ‘Groups’
3. Select the user to wish to modify their permissions
4. Under the ‘Permissions’ tab, click ‘Add permissions’
5. Add user to desired group

## Password Policy

We recommend following a strict password policy, outlined below.

Password policy can be maintained via:

1. Open IAM console at https://console.aws.amazon.com/iam/
2. Click ‘Account settings’
3. Under the 'Password policy' click 'Change password policy'

4. Make any required changes
5. Click ‘Save’

## Password Expiration

We recommend a mandated password expiry should be 5 months - slightly over the duration of a semester.

## Password Length

To ensure passwords are unable to be easily cracked, we recommend mandating an eight-character password length.

## Password Strength

We recommend mandating the following password requirements:

- One alphanumeric character: ! @ # $ % ^ & * ( ) _ + - = [ ] { } | '
- One number
- One uppercase
- One lowercase

## Password Reuse

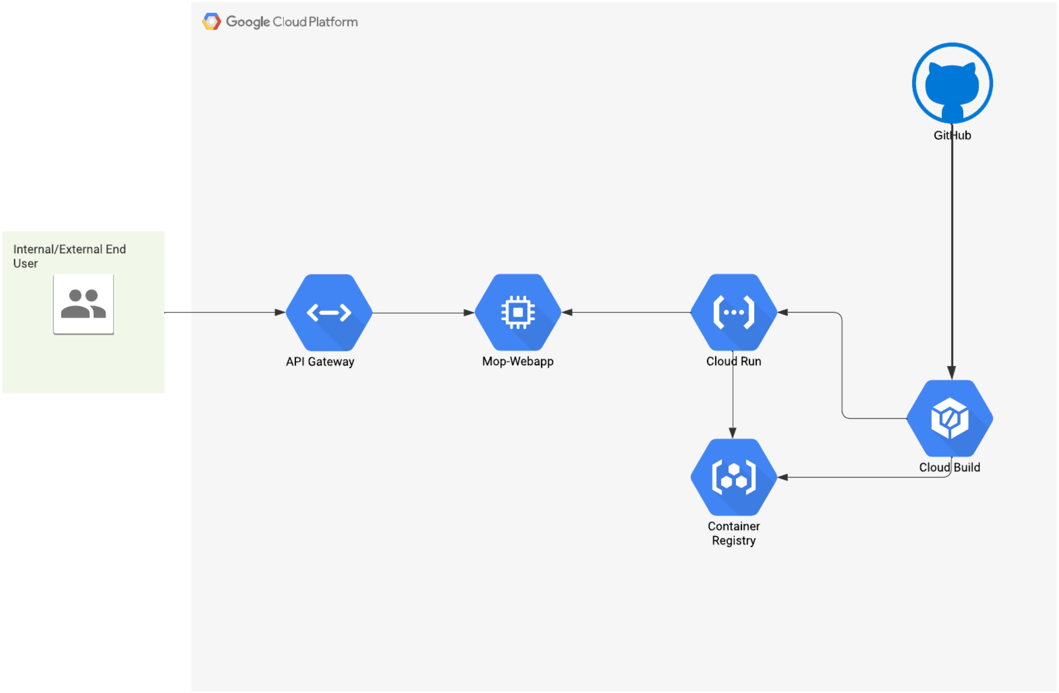
We recommend mandating a rule that users are unable to use any of their previous 10 passwords - covering the length of the student’s university degree.

# Google Cloud Platform (GCP)

## GCP Implementation

GCP MOP TOPOLOGY

Michael Leen | May 22, 2022



## Ports

We recommend mandating all traffic to be via HTTPS (port 443). This ensures that all traffic is encrypted using a secure socket layer (SSL).
Additionally, using HTTP (port 80) instead of HTTPS has an impact on search engine rankings.

This can be implemented by:

1. Under ‘Compute Engine’ click options under the target ‘Instance’
2. Under ‘Firewall’ deny all traffic apart from port 443

## Two Factor Authentication (2FA)

We recommend mandating two factor authentication via the Google Authenticator. 2FA ensures that if a username and password is leaked, then the hacker is still unable to access the GCP account.

1. 2FA firstly needs to be implemented by the domain administrator: https://support.google.com/a/answer/175197?hl=en&visit_id=637892509640510402-1611912816&rd=1

2. After enabled, open Cloud console: https://console.cloud.google.com/
3. Open ‘VM instances’
4. Under ‘Instance Details’ click ‘Edit’
5. Under ‘Custom metadata’ input:
    a. enable-oslogin to TRUE
    b. Set enable-oslogin-2fa to TRUE.
6. Click ‘Save’

# Allowed Accounts

Allowed accounts on GCP are created and managed by the University staff. Internal University policies should be strictly followed.

# Account Permissions

Account Permissions on GCP are created and managed by the University staff. Internal University policies should be strictly followed.

# Password Expiry

We recommend following a strict password policy - this can only be managed by university staff. The steps required are outlined below.

1. Open Google Admin console: https://admin.google.com/
2. Under ‘Security’ click ‘Password Management’
3. Make any required changes
4. Click ‘Save’

## Password Expiration

A mandated password expiry should be 5 months - slightly over the duration of a semester.

## Password Length

We recommend mandating an eight-character password length.

## Password Strength

We recommend mandating the following password requirements:

- One alphanumeric character: ! @ # $ % ^ & * ( ) _ + - = [ ] { } | '
- One number
- One uppercase
- One lowercase

## Password Reuse

A mandated rule that users are unable to use any of their previous 10 passwords - covering the length of the student’s university degree.

The following security measures below were considered regarding each component in the current topology plan of Chameleon's MOP implementation in GCP as stated above.
Each service suggested is considered from a variety of resources relating to security of GCP, most of which are provided officially by Google themselves.
Find a detailed Google Cloud Security Foundations Guide linked below:
https://services.google.com/fh/files/misc/google-cloud-security-foundations-guide.pdf

# Google Risk Protection Program

On March 2, 2021, Google had announced a program that would enable customers to utilise a tool in cooperation with Munich RE and Allianz that would scan our workload and provide proactive security recommendations. The program will provide reports, and an impact rating on the security posture to remediate issues in real time.

We recommend mandating this tool as this seems to be a reliable resource to utilise in receiving specialised insight on the current state of the Company's security posture.

In order to access the security diagnostic tool, an administrator needs to:

1. Select the organisation to onboard. (Risk Manager is only supported for Google Cloud Organisations)
    a. Click the project drop-down list at the top of the page.
    b. In the **Select from** dialog, click the organisation drop-down list, and select the organisation to onboard onto Risk Manager.
2. Set up Security Command Centre. This step is required for Risk Manager reports to be generated.
3. Ensure that the Security Health Analytics service is enabled in Security Command Center. This step is required for Risk Manager reports to be generated.
   To enable Security Health Analytics, refer to Setting up Security Command Center. Alternatively, go to the Security Command Center settings page and ensure that the Security Health Analytics service is set to Enabled by default.
4. Visit the Risk Manager in the Google Cloud console. These steps are detailed in Configuring Risk Manager.

# API Gateway

An API Gateway in itself can provide a good security measure, though we recommend mandating Authentication & Authorisation onto the gateway. This can be done by configuring a security definition that requires all incoming calls to provide a valid API key, as mentioned on Google Cloud Tech's video on the Google Cloud's API Gateway by adding this line into the yaml file:

```
security:
   - api_key: []
```

Traffic coming through the API Gateway can be monitored via the GCP Dashboard in the API Gateway service.

We recommend that this be monitored frequently in a timely manner, at least once a day, to detect any suspicious activity.

## Web app

We recommend taking advantage the web security scanner tool:
https://cloud.google.com/security-command-center/docs/concepts-web-security-scanner-overview
Google's in-built Web Security Scanner is another tool that can identify vulnerabilities in our App Engine, Google Kubernetes Engine (GKE), and Compute Engine web applications.
It will crawl through our application, following all links within the scope of our starting URLs, and attempts to exercise as many user inputs and event handlers as possible. Currently, Web Security Scanner only supports public URLs and IPs that aren't behind a firewall.

To access this security tool, it is located in the Security section of the GCP Dashboard, and the API needs to be enabled on first initiation.
A scan can be started from inside the Web Security Scanner, including the Name of the test, the starting URL, Authentication options, and also **scheduling scans**.
It is recommended to schedule scans on a **weekly** basis, and Risk level set to **low** to minimise potential of modifying data.

Following are some techniques that may be considered, separately or in combination, to avoid unwanted outcomes:

1. **Run scans in a test environment.** Set up a test environment by creating a separate App Engine project and loading your application and data there. If you use the Google Cloud CLI, you can specify the target project as a command-line option when you upload your app.
2. **Use a test account.** Create a user account that doesn't have access to sensitive data or harmful operations, and use it when scanning your app. Many applications present a special workflow during a user's first-time login, like accepting terms and creating a profile. Because of the different workflow, a test account for an initial user can have different scan results than an established user account. It's best to scan with an account that is in the normal user state, after the first-time flow is complete.
3. **Block individual user interface elements** that you do not want activated by applying the CSS class inq-no-click. Event handlers that are attached to this element aren't activated during crawling and testing, regardless of whether they are inline JavaScript, or attached using addEventListener, or attached by setting the appropriate event handler property.
4. **Use backup data.** Consider making a backup of your data before scanning.
5. **Excluded URLs.** You can specify URL patterns that won't be crawled or tested. For information on syntax, see Excluding URLs.

Detailed results of every scan test can also be found in the Web Security Scanner, which shows each vulnerability (if any), and recommendations provided.

# Cloud Build

We recommend mandating thorough planning of the Identity and Access Management system.
Thorough planning with the company leads needs to be done before granting roles in Identity and Access Management (IAM) to other people on the project.
Access Control can be controlled within Cloud Build using the IAM by setting predefined IAM roles relating to the Cloud Build.
This ensures prevention of unwanted access, and we want to limit the possibility of human error by adopting the security principle of least privilege.
A list of available roles and permissions can be found here:
https://cloud.google.com/build/docs/iam-roles-permissions
A general recommendation would be to assign Cloud Build Editor (roles/cloudbuild.builds.editor) only to the lead of the WebDev team, and Cloud Build Viewer (roles/cloudbuild.builds.viewer) to other members of the team/company.
Roles can also be assigned to the Cloud Build Service account, which can be found in the Cloud Build Settings page, where the status of roles can be toggled for that account.

# GCP Premium Features

We recommend upgrading the GCP Security Command Centre licence to the Premium tier. This allows for inbuilt security features that further assist with the protection of the cyber security of the website.

## Container Registry

Container Threat Detection(Premium): https://cloud.google.com/security-command-center/docs/how-to-use-container-threat-detection
Container Threat Detection is another inbuilt security feature found in the Security Command Center only available under the Premium tier.
We recommend mandating this feature, as the tool can detect the most common container runtime attacks, and can provide alerts in Security Command Center (SCC) or optionally on Cloud Login.

To access this feature, you need to have an SCC admin, and SCC sources IAM role.
It is under Security Command Center > Sources > Container Threat Detection (toggle).
This will automatically enable the containerthreatdetection API during onboarding. This API should not be directly interacted with.
When the Container Threat Detection generates findings, you can find them in the SCC again.
Some of the types of findings that may surface include:

- Added Binary Executions
    - Triggers when a binary that was not part of the original container image was executed.
        - Possible sign of an attacker executing unwanted software. E.g. malware, crypto mining software
- Added Binary Loaded

    - Triggers when a library that was not part of the original container image was loaded.
        - Possible of an attacker executing arbitrary code
- Reverse shell
    - Triggers when a process started with stream redirection/s to a remote connected socket.
        - E.g. Part of a botnet

With these findings, we can find details of the threats in the SCC under Threats, which includes details such as environment variables, process arguments and Kurbenetes labels relating to the threat. The findings can be shared with the team and remediate by heading to the source.

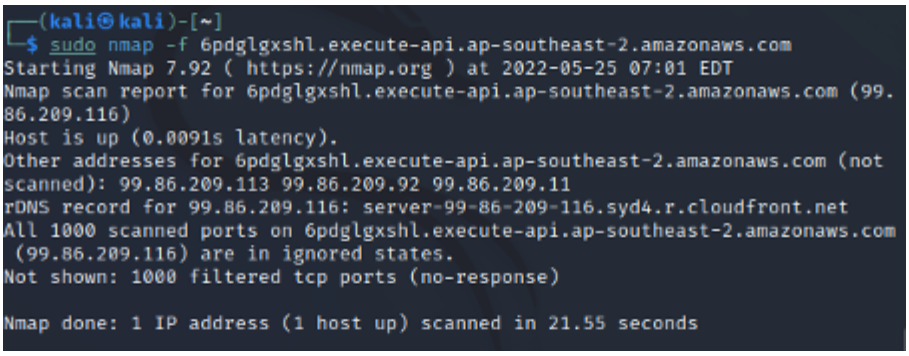
# Penetration Testing

Various penetration techniques were used to gain information on the current state of Chameleon’s Melbourne OpenData Playground website, as well as test for any vulnerabilities. These tests were conducted before the complete migration of AWS to GCP on the 30/05/2022.

## NMAP

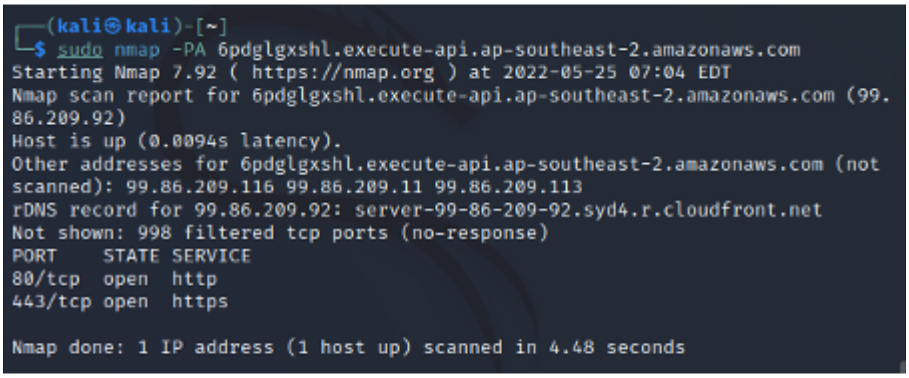
Nmap allows for the discovery of services as well as hosts on a computer network. This is achieved by sending packets and analysing responses.

1. Sending an IMCP request. As expected, the host responds:



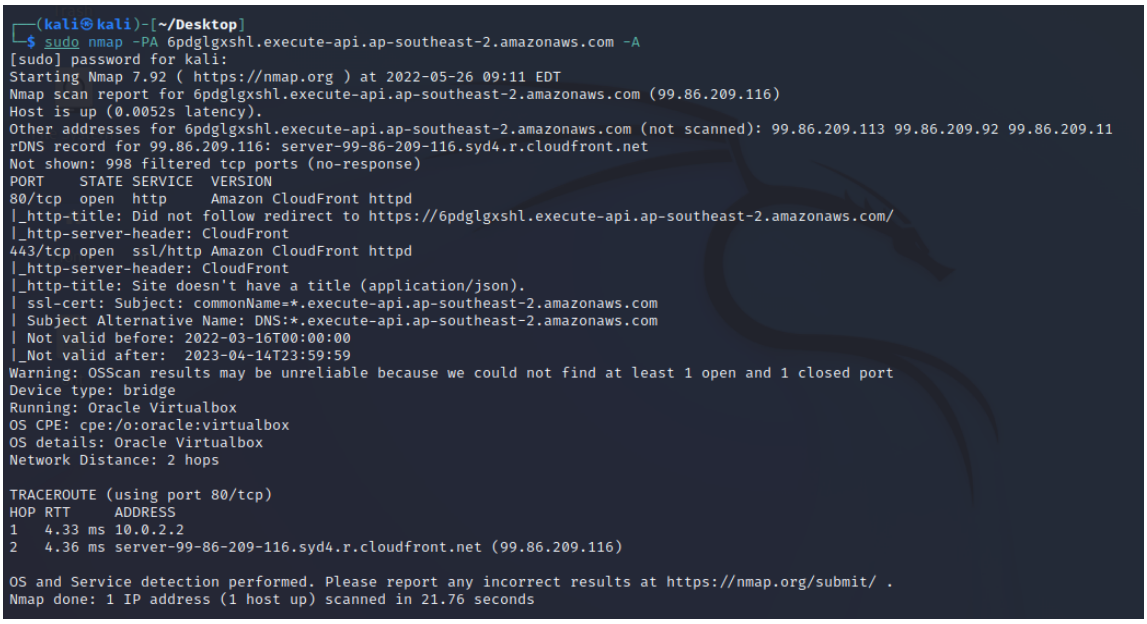
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -f 6pdglgxshl.execute-api.ap-southeast-2.amazonaws.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-25 07:01 EDT
Nmap scan report for 6pdglgxshl.execute-api.ap-southeast-2.amazonaws.com (99.
86.209.116)
Host is up (0.0091s latency).
Other addresses for 6pdglgxshl.execute-api.ap-southeast-2.amazonaws.com (not
scanned): 99.86.209.113 99.86.209.92 99.86.209.11
rDNS record for 99.86.209.116: server-99-86-209-116.syd4.r.cloudfront.net
All 1000 scanned ports on 6pdglgxshl.execute-api.ap-southeast-2.amazonaws.com
 (99.86.209.116) are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 21.55 seconds
```

2. Sending TCP ACK, the host responds with open ports, 80 and 443:



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -PA 6pdglgxshl.execute-api.ap-southeast-2.amazonaws.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-25 07:04 EDT
Nmap scan report for 6pdglgxshl.execute-api.ap-southeast-2.amazonaws.com (99.
86.209.92)
Host is up (0.0094s latency).
Other addresses for 6pdglgxshl.execute-api.ap-southeast-2.amazonaws.com (not
scanned): 99.86.209.116 99.86.209.11 99.86.209.113
rDNS record for 99.86.209.92: server-99-86-209-92.syd4.r.cloudfront.net
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 4.48 seconds
```

3. Sending OS version request, host confirms AWS:



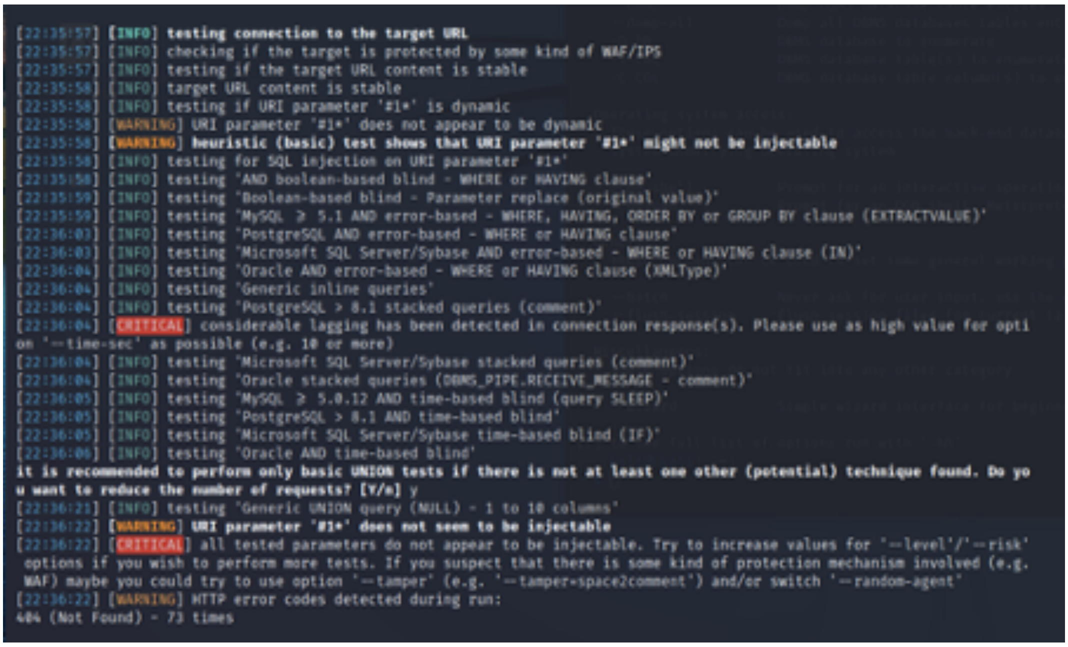
```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nmap -PA 6pdglgxshl.execute-api.ap-southeast-2.amazonaws.com -A
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-26 09:11 EDT
Nmap scan report for 6pdglgxshl.execute-api.ap-southeast-2.amazonaws.com (99.86.209.116)
Host is up (0.0052s latency).
Other addresses for 6pdglgxshl.execute-api.ap-southeast-2.amazonaws.com (not scanned): 99.86.209.113 99.86.209.92 99.86.209.11
rDNS record for 99.86.209.116: server-99-86-209-116.syd4.r.cloudfront.net
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
80/tcp  open  http     Amazon CloudFront httpd
|_http-title: Did not follow redirect to https://6pdglgxshl.execute-api.ap-southeast-2.amazonaws.com/
|_http-server-header: CloudFront
443/tcp open  ssl/http Amazon CloudFront httpd
|_http-server-header: CloudFront
|_http-title: Site doesn't have a title (application/json).
| ssl-cert: Subject: commonName=*.execute-api.ap-southeast-2.amazonaws.com
| Subject Alternative Name: DNS:*.execute-api.ap-southeast-2.amazonaws.com
| Not valid before: 2022-03-16T00:00:00
|_Not valid after:  2023-04-14T23:59:59
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge
Running: Oracle Virtualbox
OS CPE: cpe:/o:oracle:virtualbox
OS details: Oracle Virtualbox
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   4.33 ms 10.0.2.2
2   4.36 ms server-99-86-209-116.syd4.r.cloudfront.net (99.86.209.116)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.76 seconds
```

No valuable information was able to be gained through Nmap. Although post 80 should be disabled, there is no immediate threat to the safety of the website.

# SQLMAP

SQLMAP allows for penetration tests on database servers. This service allows a user to exploit any SQL injection flaws.

1. The host was tested for SQL flaws:



```
[22:35:57] [INFO] testing connection to the target URL
[22:35:57] [INFO] checking if the target is protected by some kind of WAF/IPS
[22:35:57] [INFO] testing if the target URL content is stable
[22:35:58] [INFO] target URL content is stable
[22:35:58] [INFO] testing if URI parameter '#1*' is dynamic
[22:35:58] [WARNING] URI parameter '#1*' does not appear to be dynamic
[22:35:58] [WARNING] heuristic (basic) test shows that URI parameter '#1*' might not be injectable
[22:35:58] [INFO] testing for SQL injection on URI parameter '#1*'
[22:35:58] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[22:35:59] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[22:35:59] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[22:36:03] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[22:36:03] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[22:36:04] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[22:36:04] [INFO] testing 'Generic inline queries'
[22:36:04] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[22:36:04] [CRITICAL] considerable lagging has been detected in connection response(s). Please use as high value for opti
on '--time-sec' as possible (e.g. 10 or more)
[22:36:04] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[22:36:04] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[22:36:05] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[22:36:05] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[22:36:05] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[22:36:06] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do yo
u want to reduce the number of requests? [Y/n] y
[22:36:21] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[22:36:22] [WARNING] URI parameter '#1*' does not seem to be injectable
[22:36:22] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk'
 options if you wish to perform more tests. If you suspect that there is some kind of protection mechanism involved (e.g.
 WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment') and/or switch '--random-agent'
[22:36:22] [WARNING] HTTP error codes detected during run:
404 (Not Found) - 73 times
```

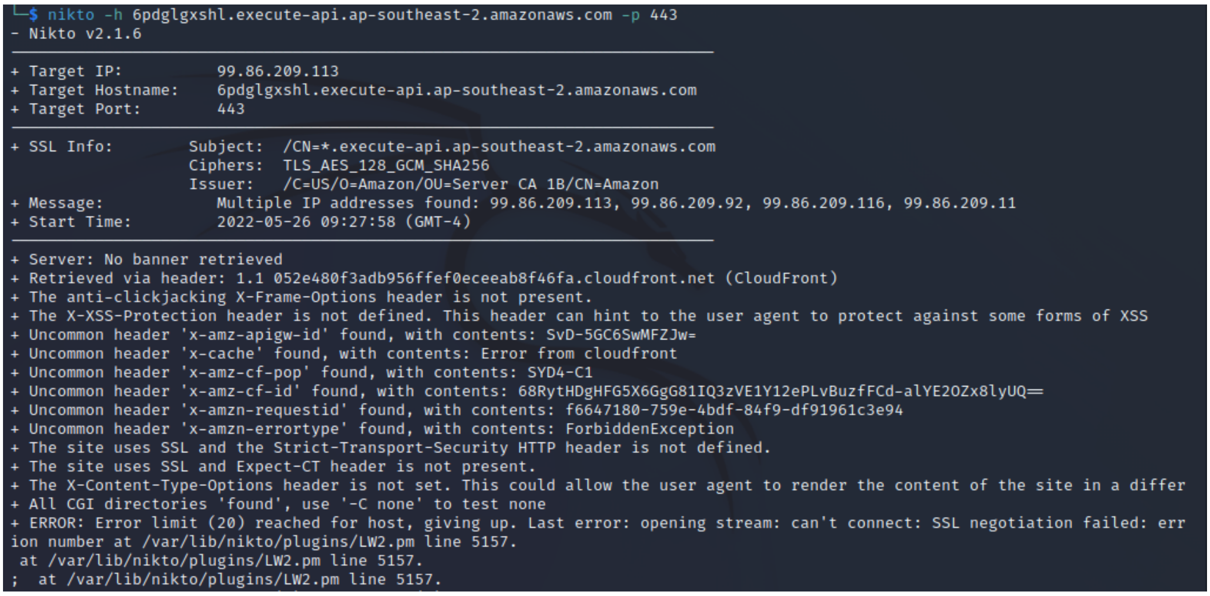
Firstly, this is checking if SQL is running on the server. As expected, there is no SQL on the server - hence no SQL flaws.

# Nikito

Nikito allows for vulnerability scanning for:

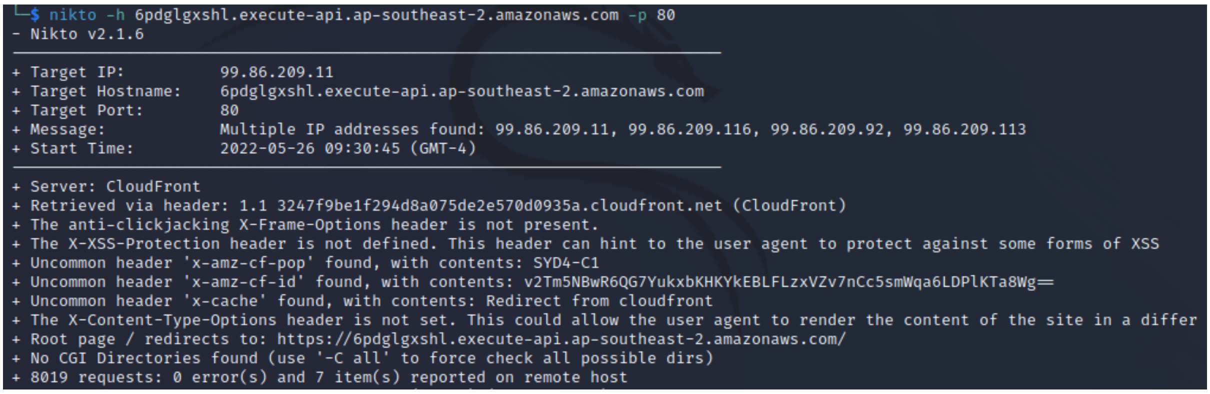
- Web servers - Scanning for over 6.7k files/programs
- Outdated versions - Checking over 1250 versions
- Configuration specific problems - Checking over 270 problems

1. Testing via port 443. The anti-clickjacking X-Frame-Options header is not present, and the X-XSS-Protection header is not defined:



```
└─$ nikto -h 6pdglgxshl.execute-api.ap-southeast-2.amazonaws.com -p 443
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          99.86.209.113
+ Target Hostname:    6pdglgxshl.execute-api.ap-southeast-2.amazonaws.com
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /CN=*.execute-api.ap-southeast-2.amazonaws.com
                   Ciphers:  TLS_AES_128_GCM_SHA256
                   Issuer:   /C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
+ Message:            Multiple IP addresses found: 99.86.209.113, 99.86.209.92, 99.86.209.116, 99.86.209.11
+ Start Time:         2022-05-26 09:27:58 (GMT-4)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ Retrieved via header: 1.1 052e480f3adb956ffef0eceeab8f46fa.cloudfront.net (CloudFront)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'x-amz-apigw-id' found, with contents: SvD-5GC6SwMFZJw=
+ Uncommon header 'x-cache' found, with contents: Error from cloudfront
+ Uncommon header 'x-amz-cf-pop' found, with contents: SYD4-C1
+ Uncommon header 'x-amz-cf-id' found, with contents: 68RytHDgHFG5X6GgG81IQ3zVE1Y12ePLvBuzfFCd-alYE2OZx8lyUQ==
+ Uncommon header 'x-amzn-requestid' found, with contents: f6647180-759e-4bdf-84f9-df91961c3e94
+ Uncommon header 'x-amzn-errortype' found, with contents: ForbiddenException
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ The site uses SSL and Expect-CT header is not present.
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a differ
+ All CGI directories 'found', use '-C none' to test none
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect: SSL negotiation failed: err
ion number at /var/lib/nikto/plugins/LW2.pm line 5157.
 at /var/lib/nikto/plugins/LW2.pm line 5157.
;  at /var/lib/nikto/plugins/LW2.pm line 5157.
```

2. Testing via post 80. Identical threats:



```
└─$ nikto -h 6pdglgxshl.execute-api.ap-southeast-2.amazonaws.com -p 80
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          99.86.209.11
+ Target Hostname:    6pdglgxshl.execute-api.ap-southeast-2.amazonaws.com
+ Target Port:        80
+ Message:            Multiple IP addresses found: 99.86.209.11, 99.86.209.116, 99.86.209.92, 99.86.209.113
+ Start Time:         2022-05-26 09:30:45 (GMT-4)
---------------------------------------------------------------------------
+ Server: CloudFront
+ Retrieved via header: 1.1 3247f9be1f294d8a075de2e570d0935a.cloudfront.net (CloudFront)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'x-amz-cf-pop' found, with contents: SYD4-C1
+ Uncommon header 'x-amz-cf-id' found, with contents: v2Tm5NBwR6QG7YukxbKHKYkEBLFLzxVZv7nCc5smWqa6LDPlKTa8Wg==
+ Uncommon header 'x-cache' found, with contents: Redirect from cloudfront
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a differ
+ Root page / redirects to: https://6pdglgxshl.execute-api.ap-southeast-2.amazonaws.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 8019 requests: 0 error(s) and 7 item(s) reported on remote host
```

Firstly, as the anti-clickjacking X-Frame-Options header is not present, resulting in the website potentially being at risk of a clickjacking attack. Secondly, the X-XSS-Protection header is not defined, meaning the website could be at risk of a Cross-Site Scripting (XSS) attack.

# Penetration Testing Summary

From our findings in our penetration testing, our recommendations are:

- Force only access via HTTPS (port 443). GCP and AWS methods mentioned in document.
- For an AWS Implementation: Add security headers to the response headers. Steps required: https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/example-function-add-security-headers.html
  Detailed GitHub implementation: https://github.com/aws-samples/amazon-cloudfront-functions/tree/main/add-security-headers
- For GCP implementation: The current threat is due to the AWS implementation; however, if this occurs via GCP, this can be solved by: https://cloud.google.com/security-command-center/docs/how-to-remediate-web-security-scanner-findings