Security Assessment Report: Public S3 Bucket Exposure

Author: Ehmaan Shafqat

Fellow, Buildables Fellowship

Assessed Resource: flaws.cloud

Date: 20, Oct 2025

1. Executive Summary

A critical security misconfiguration was identified in the AWS S3 bucket flaws.cloud. The bucket was configured with public read access, allowing unauthenticated enumeration and download of all stored objects. This exposure included sensitive information revealing internal infrastructure details and a direct escalation path to additional systems.

2. Methodology

The assessment followed a structured approach to identify and validate the public exposure:

Phase 1: Discovery & Verification

```
┌──(eman㉿vbox)-[~]
└─$ nslookup 52.92.137.219
219.137.92.52.in-addr.arpa      name = s3-website-us-west-2.amazonaws.com.

Authoritative answers can be found from:
```

Confirmed S3 website hosting through reverse DNS resolution

Phase 2: Access Validation

```
┌──(eman㉿vbox)-[~]
└─$ aws s3 ls s3://flaws.cloud --no-sign-request
2017-03-14 08:00:38       2575 hint1.html
2017-03-03 09:05:17       1707 hint2.html
2017-03-03 09:05:11       1101 hint3.html
2024-02-22 07:32:41       2861 index.html
2018-07-10 21:47:16      15979 logo.png
2017-02-27 06:59:28         46 robots.txt
2017-02-27 06:59:30       1051 secret-dd02c7c.html
```

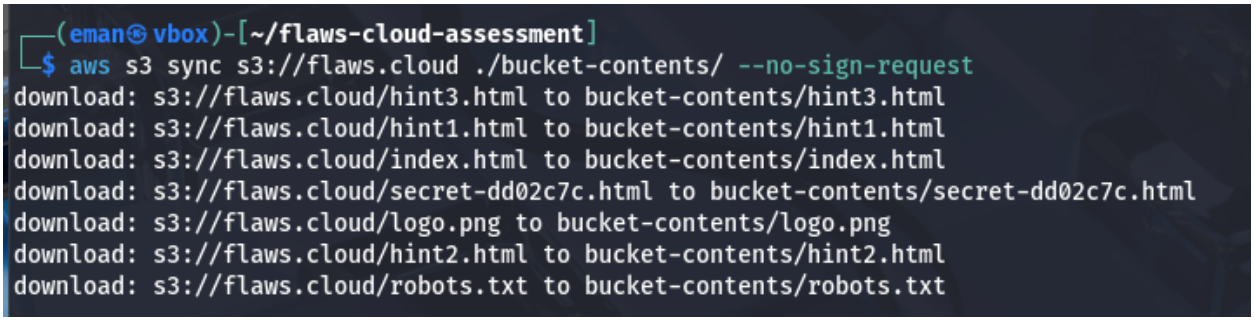
Verified unauthenticated list operations against the bucket

Phase 3: Permission Analysis

```
┌──(eman㉿vbox)-[~]
└─$ s3scanner -bucket flaws.cloud
INFO exists    | flaws.cloud | us-west-2 | AuthUsers: [] | AllUsers: [READ]
```

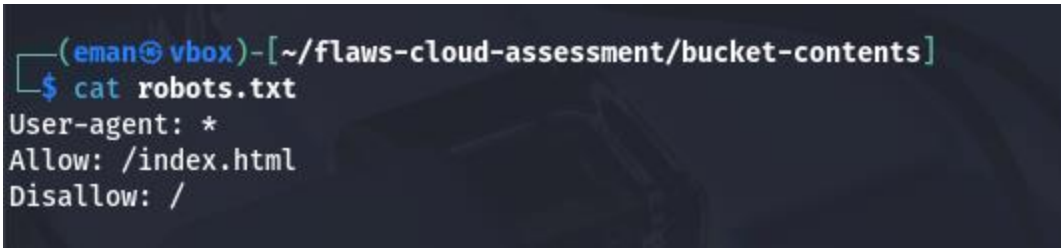
Confirmed public read permissions at bucket level

Phase 4: Data Extraction & Analysis



Downloaded complete bucket contents for analysis

Phase 5: Sensitive Data Review



Analyzed critical findings within exposed data

3. Findings

3.1 Public Access Misconfiguration

- Bucket flaws.cloud allowed public read access
- 7 objects (25 KB) fully accessible without authentication
- Permission confirmed via multiple assessment tools

3.2 Data Exposure Details

- Complete static website source code
- Internal hint files revealing infrastructure information
- robots.txt exposing directory structure
- secret-dd02c7c.html containing escalation path to level2-c8b217a33fcf1f839f6f1f73a00a9ae7.flaws.cloud

4. Risk Analysis

- **Data Confidentiality:** Complete loss - all bucket contents publicly accessible
- **Attack Surface Expansion**: Exposure provides direct path to additional internal systems
- **Compliance Impact:** Violates multiple security frameworks (CIS, NIST, PCI-DSS)

5. Recommendations

Immediate Actions (Within 24 hours):

- Disable public access on flaws.cloud S3 bucket
- Investigate the exposed level2 system for further compromise
- Review all S3 buckets in the environment for similar misconfigurations

Long-term Remediation:

- Implement S3 Block Public Access at the account level
- Deploy automated CSPM tooling for continuous monitoring
- Establish S3 security baselines in development pipelines