# Cloud Vulnerability Scanner Report

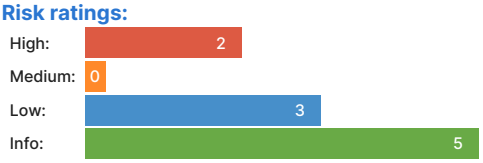
✔ **https://pentest-ground-bucket.s3.ca-central-1.amazonaws.com/**

## Summary

**Overall risk level:**

High

**Risk ratings:**




**Scan information:**

| | |
|---|---|
| Start time: | Mar 17, 2024 / 10:21:21 |
| Finish time: | Mar 17, 2024 / 10:21:43 |
| Scan duration: | 22 sec |
| Tests performed: | 10/10 |
| Scan status: | Finished |

## Findings

### Publicly writable AWS S3 buckets found

| Bucket Name | Region | URL | Owner | Other Users | No. of Files | Unauthenticated Permissions | Authenticated Permissions |
|---|---|---|---|---|---|---|---|
| pentest-ground-bucket | ca-central-1 | https://pentest-ground-bucket.s3.ca-central-1.amazonaws.com | - | - | 2 | s3:GetBucketAcl, s3:ListBucket | s3:GetBucketVersioning, s3:GetBucketCors, s3:GetBucketOwnershipControls, s3:PutBucketCors, s3:GetReplicationConfiguration, s3:PutObject, s3:PutEncryptionConfiguration, s3:GetBucketAcl, s3:GetBucketLogging, s3:GetEncryptionConfiguration, s3:ListBucket |

Details

**Vulnerability description:**
We have found one or more Amazon Simple Storage Service (S3) buckets hosted on Amazon Web Services (AWS) that are publicly writable. S3 is a scalable object storage service that allows users to store and retrieve large amounts of data securely.

**Risk description:**
While utilizing Amazon Simple Storage Service (S3) buckets provides numerous benefits, it is crucial to consider potential risks and vulnerabilities associated with this configuration. Identifying these risks allows for the implementation of appropriate security measures to protect the target's data and ensure its integrity.

**Recommendation:**
We recommend implementing robust security practices. This includes utilizing strong access controls, encryption, and monitoring, as well as regularly reviewing and auditing the S3 bucket configuration. As always, it is crucial to ensure that the target has authorized any security testing or assessments to be conducted on their infrastructure or data.

**References:**
https://aws.amazon.com/s3/
https://docs.aws.amazon.com/AmazonS3/latest/userguide/access-policy-language-overview.html

### Interesting writable files found on AWS S3 bucket

| Bucket Name | File | Unauthenticated Permissions | Authenticated Permissions |
|---|---|---|---|
| pentest-ground-bucket | wp-config | - | s3:PutObject, s3:GetObjectAcl, s3:GetObject |

| | | | |
|---|---|---|---|
| pentest-ground-bucket | .aws/credentials | - | s3:PutObject, s3:GetObjectAcl, s3:GetObject |

Details

**Vulnerability description:**

We have found that the target S3 bucket contains a collection of interesting files that are writable. These files present valuable and noteworthy information that may contribute to the investigation or provide insights into the activities, operations, or security posture of the target. It is important to handle these files with care, ensuring the preservation of their integrity and confidentiality. Following proper protocols and obtaining necessary permissions, the investigation team can analyze and leverage these files to gain a deeper understanding of the target's operations, uncover potential risks, or support legal proceedings if required.

**Risk description:**

While the discovery of interesting files on an Amazon Simple Storage Service (S3) bucket can provide valuable information, it is essential to consider the associated risks and implications. Identifying and accessing these files may pose certain risks that need to be carefully managed:

- Data Exposure: If the interesting files contain sensitive or confidential information, their presence in the S3 bucket increases the risk of unauthorized access or data exposure. Without proper access controls, these files could be accessible to unauthorized individuals or malicious actors, potentially leading to data breaches, intellectual property theft, or regulatory non-compliance.
- Legal and Compliance Issues: The interesting files may include sensitive data subject to legal or regulatory requirements, such as personally identifiable information (PII), financial records, or healthcare information. Mishandling or unauthorized access to such data can lead to legal consequences, regulatory penalties, and damage to the target's reputation.
- Intellectual Property Risks: If the interesting files include intellectual property, trade secrets, or proprietary information, their exposure could result in the theft of valuable assets. Competitors or malicious actors may exploit this information for their gain, undermining the target's competitive advantage and business interests.
- Reputational Damage: The exposure of sensitive or confidential information through the interesting files can significantly impact the target's reputation. Loss of customer trust, damage to brand image, and negative publicity may result from the unauthorized disclosure or misuse of sensitive data.
- Malware or Exploitation Risks: The interesting files could potentially contain malware or be used as a vector for cyber-attacks. Malicious actors may exploit vulnerabilities within the files or use them as part of social engineering tactics to gain unauthorized access to the target's systems or networks.
- Insider Threats: The discovery of interesting files may raise concerns about insider threats within the target organization. It is crucial to consider the possibility of intentional or unintentional insider actions that led to the presence of these files in the S3 bucket. Insider threats can include employees, contractors, or business partners with access to the target's systems and data.

**Recommendation:**

We recommend reviewing what files are exposed on the bucket. To mitigate these risks, several actions should be taken:

- Access Control and Encryption: Implement robust access controls and encryption mechanisms to protect the interesting files from unauthorized access or data leaks. This includes using AWS Identity and Access Management (IAM), bucket policies, and encryption at rest and in transit.
- Vulnerability Assessment: Conduct a thorough assessment of the security posture of the S3 bucket to identify and remediate any misconfigurations, vulnerabilities, or access control issues that could lead to data exposure or unauthorized access.
- Incident Response and Monitoring: Establish a comprehensive incident response plan to handle potential security incidents or data breaches. Implement continuous monitoring and logging practices to detect any suspicious activities related to the interesting files.
- Compliance and Data Protection: Ensure compliance with applicable laws, regulations, and industry standards concerning data protection and privacy. Review data handling practices, retention policies, and legal requirements to mitigate legal and regulatory risks.
- Employee Awareness and Training: Provide regular security awareness training to employees to educate them about the risks associated with sensitive data and the importance of adhering to security best practices. This can help mitigate insider threats and improve overall security hygiene.

By proactively addressing these risks and taking appropriate measures, the target can effectively manage the potential security implications of discovering interesting files within the S3 bucket and protect sensitive information from unauthorized access or misuse.

**References:**

https://docs.aws.amazon.com/AmazonS3/latest/userguide/UsingBucket.html

## AWS S3 Access Control Lists (ACLs) found

| Bucket Name | Permission | Grantee Type | Grantee |
|---|---|---|---|
| pentest-ground-bucket | READ | Group | http://acs.amazonaws.com/groups/global/AllUsers |
| pentest-ground-bucket | WRITE | Group | http://acs.amazonaws.com/groups/global/AuthenticatedUsers |
| pentest-ground-bucket | READ_ACP | Group | http://acs.amazonaws.com/groups/global/AllUsers |

Details

**Vulnerability description:**

We have found that the target utilizes Access Control Lists (ACLs) on Amazon Web Services (AWS). AWS ACLs are security mechanisms used to control access to AWS resources, including services, networks, or objects such as S3 buckets or EC2 instances. An AWS ACL acts as an additional layer of security, allowing the target to define granular permissions and restrict access to its resources based on specific rules and conditions.

**Risk description:**

While the use of Access Control Lists (ACLs) on Amazon Web Services (AWS) provides an additional layer of security, it is important to be aware of potential risks associated with their implementation. Identifying the presence of ACLs on AWS indicates the target's efforts to control access to its resources; however, certain risks should be considered:

- Misconfigured ACLs: Improperly configured ACLs can result in unintended access permissions or overly restrictive policies. Misconfiguration may inadvertently grant unauthorized access or block legitimate users from accessing resources, leading to service disruptions, data breaches, or operational inefficiencies.
- Incomplete or inconsistent policies: If ACLs are inconsistently applied or certain resources are not adequately protected, it can create security gaps. Incomplete policies may leave certain resources exposed, making them vulnerable to unauthorized access or exploitation.
- Complexity and management overhead: Managing ACLs across a complex infrastructure can be challenging. As the number of resources and access rules increases, ensuring consistency and enforcing proper access controls become more complex. This complexity can introduce administrative overhead and increase the risk of misconfigurations or errors.
- Lack of granularity: ACLs may lack the granularity needed to define highly specific permissions. In such cases, implementing fine-grained access controls might be difficult, potentially resulting in broader access privileges than necessary. This can increase the risk of data exposure or unauthorized actions.
- Difficulty in auditing and monitoring: Monitoring and auditing ACLs across a large-scale infrastructure can be challenging. Lack of visibility into ACL activities or limited centralized logging can hinder the ability to detect and investigate potential security incidents or policy violations.
- Overreliance on ACLs: Relying solely on ACLs for security without considering other security measures, such as encryption, authentication, or additional security services, can create a false sense of security. An attacker who successfully bypasses or compromises ACLs may still find other avenues to exploit vulnerabilities within the infrastructure.

**Recommendation:**

We recommend implementing best practices for ACL management. This includes regularly reviewing and auditing ACL configurations, conducting thorough testing to ensure proper functionality and adherence to security policies, and utilizing tools or services that provide centralized monitoring and logging capabilities.

Additionally, it is important to adopt a defense-in-depth approach, combining ACLs with other security measures, such as Identity and Access Management (IAM), encryption, security groups, and network firewalls, to create a comprehensive security framework that addresses potential vulnerabilities and threats. Also, AWS recommends disabling ACLs and relying on other solutions, described above.

By proactively addressing these risks, the target can enhance the effectiveness of ACLs, reduce the likelihood of unauthorized access or data breaches, and maintain a secure and compliant AWS environment.

**References:**

https://docs.aws.amazon.com/AmazonS3/latest/userguide/acl-overview.html

## CORS enabled on AWS S3 buckets

| Bucket Name | Status | Configuration |
|---|---|---|
| pentest-ground-bucket | Enabled | {<br>"CORSRules": [<br>{<br>"AllowedHeaders": "["*"]",<br>"AllowedMethods": [<br>"PUT",<br>"POST",<br>"DELETE"<br>],<br>"AllowedOrigins": "["http://www.example1.com"]"<br>},<br>{<br>"AllowedHeaders": "["*"]",<br>"AllowedMethods": [<br>"PUT",<br>"POST",<br>"DELETE"<br>],<br>"AllowedOrigins": "["http://www.example2.com"]"<br>},<br>{<br>"AllowedMethods": [<br>"GET"<br>],<br>"AllowedOrigins": "["*"]"<br>}<br>]<br>} |

Details

**Vulnerability description:**

We have found one or more Amazon Simple Storage Service (S3) buckets hosted on Amazon Web Services (AWS) that have CORS enabled, along with their configuration.

**Risk description:**

Cross-origin resource sharing (CORS) in Amazon Web Services (AWS) S3 buckets is an essential mechanism that controls cross-origin requests made by web browsers to access resources hosted in different domains. When the CORS configuration is insecure or misconfigured, it can result in unauthorized access, data leakage, cross-site scripting (XSS) attacks, and compliance and security policy violations.

**Recommendation:**

We recommend reviewing the AWS S3 bucket CORS configuration to make sure it is properly configured, taking into account the following measures:
- Review and Restrict Allowed Origins: Carefully review and restrict the list of allowed origins (domains) in the CORS configuration. Limit it to only authorized domains that require access to S3 bucket resources.
- Specify Appropriate CORS Methods and Headers: Configure the CORS settings to allow only necessary HTTP methods (e.g., GET, POST) and appropriate headers required by your applications. Avoid overly permissive CORS configurations that may expose sensitive operations or information.
- Enable CORS Validation: Enable CORS validation on the server-side to enforce proper CORS usage. Reject requests that violate CORS policies to prevent unauthorized access attempts.
- Regularly Test CORS Configuration: Conduct regular testing and validation of the CORS configuration to ensure its effectiveness. Verify that the allowed origins, methods, and headers are correctly enforced and that there are no misconfigurations or loopholes.
- Implement Least Privilege Access Controls: Apply least privilege access controls to the S3 bucket resources, restricting access to only the necessary actions and authorized entities. This includes proper IAM policies, bucket policies, and access control lists (ACLs).
By addressing insecure CORS configurations in AWS S3 buckets and implementing the recommended mitigation measures, organizations can mitigate the risk of unauthorized access, data leakage, and potential XSS attacks. This enhances data security, protects sensitive information, and ensures compliance with security standards and regulations.

**References:**

https://docs.aws.amazon.com/AmazonS3/latest/userguide/ManageCorsUsing.html

## Logging disabled on AWS S3 buckets

| Bucket Name | Status | Configuration |
|---|---|---|
| pentest-ground-bucket | Disabled | - |

Details

**Vulnerability description:**

We have found one or more Amazon Simple Storage Service (S3) buckets hosted on Amazon Web Services (AWS) that have logging disabled.

**Risk description:**

The logging configuration in Amazon Web Services (AWS) S3 buckets is designed to provide detailed records of access and activity within an S3 bucket, enabling security teams to monitor and investigate potential security incidents. However, when this feature is not enabled, it hampers the ability to detect and respond to security breaches effectively, while also allowing unauthorized account access, data leakage, or malicious activity in an AWS infrastructure.

**Recommendation:**

We recommend ensuring that proper logging configurations are implemented for AWS S3 buckets, including the following measures:
- Enable S3 Bucket Logging: Activate the S3 bucket logging feature to record detailed access and activity logs. Configure the logs to be stored in a separate, secure S3 bucket, preferably in a different AWS account.
- Define Log File Permissions: Apply stringent access controls to the log files stored in the designated bucket. Restrict access to only authorized personnel, ensuring that the logs are adequately protected from unauthorized modification or deletion.
- Regular Log Monitoring: Establish a process to monitor the logs generated by S3 buckets regularly. Implement log analysis tools or services to detect anomalies, suspicious activities, or unauthorized access attempts.
- Implement Secure Backup: Create regular backups of the log files and store them in a secure location, separate from the primary S3 bucket. This ensures data availability in the event of an incident affecting the primary bucket.
- Conduct Audits and Assessments: Regularly review and audit the logging configurations of S3 buckets to identify any misconfigurations or deviations from best practices. Perform security assessments and penetration testing to identify vulnerabilities proactively.
By enabling logging in AWS S3 buckets and implementing the recommended measures, organizations can significantly enhance their security posture, maintain data integrity, and effectively respond to potential security incidents.

**References:**

https://docs.aws.amazon.com/AmazonS3/latest/userguide/s3-incident-response.html

## Target is hosted on Amazon Web Services (AWS)

| Target IP | IP Prefix | Region | Services |
|---|---|---|---|
| 52.95.190.66 | - | - | - |

Details

**Vulnerability description:**
We have found that the target is hosted on Amazon Web Services (AWS), one of the leading cloud computing platforms.

**Risk description:**
While hosting a target on Amazon Web Services (AWS) provides numerous benefits, it is essential to consider potential risks and vulnerabilities associated with this hosting environment. Identifying the risks helps ensure appropriate security measures are in place to protect the data and infrastructure.

**Recommendation:**
We recommend implementing robust security practices. This includes utilizing strong access controls, regularly auditing and monitoring AWS configurations, implementing encryption for sensitive data, employing multi-factor authentication, and staying up to date with AWS security best practices. Additionally, implementing backup and disaster recovery mechanisms can help minimize the impact of service disruptions or data breaches.

**References:**
https://aws.amazon.com/websites/

## Versioning enabled on AWS S3 buckets

| Bucket Name | Status | MFA Delete |
|---|---|---|
| pentest-ground-bucket | Enabled | Disabled |

Details

**Vulnerability description:**
We have found one or more Amazon Simple Storage Service (S3) buckets hosted on Amazon Web Services (AWS) that have versioning enabled.

**Risk description:**
Versioning in Amazon Web Services (AWS) S3 buckets is a critical feature that enables the preservation of previous versions of objects stored within the S3 bucket. It allows for easy recovery of accidentally deleted or overwritten objects and provides protection against malicious modifications. However, when versioning is incorrectly set up, it significantly affects data protection and recovery mechanisms.

**Recommendation:**
We recommend reviewing the AWS S3 bucket versioning configuration to make sure it is properly configured, taking into account the following measures:
- Implement Access Controls: Apply appropriate access controls to the versioning settings, limiting modifications to authorized personnel only. This ensures that versioning configurations remain secure and protected against unauthorized changes.
- Regularly Test Recovery Procedures: Validate the recovery procedures to ensure the ability to restore objects from previous versions. Regularly test the recovery process to verify its effectiveness and identify any potential issues or limitations.
- Educate Users and Administrators: Provide training and guidance to users and administrators regarding the importance of versioning and the proper handling of objects within S3 buckets. Raise awareness about the risks associated with disabling or misconfiguring versioning settings.
- Monitor and Review Versioning Configurations: Regularly monitor and review the versioning configurations of S3 buckets to identify any misconfigurations or deviations from best practices. Implement proactive monitoring and alerting mechanisms to detect changes in versioning settings.
By addressing insecure versioning configurations in AWS S3 buckets and implementing the recommended mitigation measures, organizations can significantly enhance their data integrity, recovery capabilities, and compliance with regulatory requirements.

**References:**
https://docs.aws.amazon.com/AmazonS3/latest/userguide/Versioning.html

## Replication enabled for AWS S3 buckets

| Bucket Name | Status | Configuration |
|---|---|---|

| | | |
|---|---|---|
| pentest-ground-bucket | Enabled | {<br>"Role": "arn:aws:iam::161398989590:role/IAMDummyRoleForSecurityTesting",<br>"Rules": [<br>{<br>"ID": ""Rule1"",<br>"Priority": 0,<br>"Filter": "{}",<br>"Status": "Enabled",<br>"Destination": {<br>"Bucket": "arn:aws:s3:::pentest-ground-bucket2"<br>},<br>"DeleteMarkerReplication": {<br>"Status": "Disabled"<br>}<br>},<br>{<br>"ID": ""Rule2"",<br>"Priority": 1,<br>"Filter": "{"Prefix": "config"}",<br>"Status": "Disabled",<br>"Destination": {<br>"Bucket": "arn:aws:s3:::pentest-ground-bucket2"<br>},<br>"DeleteMarkerReplication": {<br>"Status": "Disabled"<br>}<br>}<br>]<br>} |

Details

**Vulnerability description:**

We have found one or more Amazon Simple Storage Service (S3) buckets hosted on Amazon Web Services (AWS) that have replication enabled, along with their configuration.

**Risk description:**

Replication in Amazon Web Services (AWS) S3 buckets is a crucial feature that enables the automatic copying of objects from a source bucket to a destination bucket in a different AWS region or account. However, misconfigurations in the replication settings may lead to incomplete or improper replication of objects between source and destination buckets, jeopardizing data availability and resiliency and causing unauthorized access to replicated data in the destination bucket.

**Recommendation:**

We recommend reviewing the AWS S3 bucket replication configuration to make sure it is properly configured, taking into account the following measures:
- Review Replication Settings: Perform a comprehensive review of the replication settings for S3 buckets. Ensure that the source and destination buckets are correctly specified, and replication rules accurately define the desired behavior.
- Enable Encryption: Enable encryption for replicated objects to ensure the confidentiality and integrity of data during the replication process. Utilize AWS S3 encryption options, such as SSE-S3 or SSE-KMS, to protect replicated data.
- Implement Access Controls: Apply strict access controls and permissions to the replication configuration, limiting modifications to authorized personnel only. Regularly review and update access policies to prevent unauthorized changes or access to replicated data.
- Test Replication Process: Regularly test the replication process to validate its effectiveness and identify any potential issues or delays. Conduct regular checks to ensure the replication is functioning as intended and that data integrity is maintained.
- Monitor and Alert: Implement monitoring and alerting mechanisms to detect any failures or anomalies in the replication process. Configure notifications to promptly address any replication issues or failures.
By addressing misconfigured replication configurations in AWS S3 buckets and implementing the recommended mitigation measures, organizations can enhance data consistency, integrity, and disaster recovery capabilities, minimizing the risk of data loss and unauthorized access.

**References:**

https://docs.aws.amazon.com/AmazonS3/latest/userguide/replication.html

## Encryption enabled on AWS S3 buckets

| Bucket Name | Status | Configuration |
|---|---|---|

| | | |
|---|---|---|
| pentest-ground-bucket | Enabled | {<br>"Rules": [<br>{<br>"ApplyServerSideEncryptionByDefault": {<br>"SSEAlgorithm": "AES256"<br>},<br>"BucketKeyEnabled": true<br>}<br>]<br>} |

Details

**Vulnerability description:**

We have found one or more Amazon Simple Storage Service (S3) buckets hosted on Amazon Web Services (AWS) that have encryption enabled, along with their configuration.

**Risk description:**

Encryption in Amazon Web Services (AWS) S3 buckets is a fundamental security measure that safeguards data stored in S3 buckets by converting it into an unreadable format unless decrypted with the appropriate keys. However, when encryption is inadequately configured, it can result in unauthorized data access, data exposure, non-compliance with data protection regulations, and increased data tampering risks.

**Recommendation:**

We recommend reviewing the AWS S3 bucket encryption configuration to make sure it is properly configured, taking into account the following measures:
- Use Strong Encryption Algorithms: Select encryption algorithms that offer robust security, such as AES-256, for encrypting data within S3 buckets. Avoid weaker or deprecated encryption algorithms that may be susceptible to known vulnerabilities.
- Implement Client-Side Encryption: Consider implementing client-side encryption, where data is encrypted before being uploaded to S3 buckets. This provides an additional layer of protection, as the data remains encrypted throughout the entire transfer process.
- Manage Encryption Keys Securely: Properly manage and protect encryption keys used for server-side or client-side encryption. Utilize AWS Key Management Service (KMS) to centrally manage and secure encryption keys, and enforce strong access controls for key management.
- Regularly Monitor and Audit Encryption Settings: Conduct regular audits and reviews of the encryption settings in S3 buckets to identify any misconfigurations or deviations from best practices. Monitor encryption status and ensure that all objects are appropriately encrypted.
By addressing inadequate encryption configurations in AWS S3 buckets and implementing the recommended mitigation measures, organizations can enhance data security, protect sensitive information, and maintain compliance with data protection regulations.

**References:**

https://docs.aws.amazon.com/AmazonS3/latest/userguide/UsingEncryption.html

## Ownership Control enabled on AWS S3 buckets

| Bucket Name | Status | Configuration |
|---|---|---|
| pentest-ground-bucket | Enabled | {<br>"Rules": [<br>{<br>"ObjectOwnership": "BucketOwnerPreferred"<br>}<br>]<br>} |

Details

**Vulnerability description:**

We have found one or more Amazon Simple Storage Service (S3) buckets hosted on Amazon Web Services (AWS) that have ownership control enabled, along with their configuration.

**Risk description:**

Ownership Control in Amazon Web Services (AWS) S3 buckets is a crucial feature that governs the ownership and access rights of objects within an S3 bucket. When ownership control is misconfigured, it can result in unauthorized data access, data loss or deletion, privacy violations, such as the exposure of personally identifiable information (PII), confidential documents, or proprietary information, and compliance and regulatory issues.

**Recommendation:**

We recommend reviewing the AWS S3 bucket ownership control configuration to make sure it is properly configured, taking into account the following measures:
- Review and Restrict Access Policies: Regularly review and update access policies to ensure that only authorized accounts or users have ownership and access rights to S3 bucket objects. Implement the principle of least privilege to restrict access to only the necessary actions and individuals.
- Monitor Ownership Changes: Implement monitoring mechanisms to track ownership changes and modifications within S3 buckets. Regularly review ownership control logs or event notifications to detect any unauthorized ownership changes or suspicious

activities.
- Regular Audits and Assessments: Conduct periodic audits and assessments of ownership control configurations in S3 buckets. Identify any misconfigurations, deviations from best practices, or vulnerabilities. Perform security assessments and penetration testing to proactively identify and address ownership control vulnerabilities.
- User Education and Awareness: Provide training and education to users and administrators regarding the importance of ownership control and the proper handling of S3 bucket objects. Raise awareness about the risks associated with misconfigurations and the potential impact on data security and privacy.
By addressing insecure ownership control configurations in AWS S3 buckets and implementing the recommended mitigation measures, organizations can enhance data security, prevent unauthorized access or modifications, and maintain compliance with data protection regulations.

**References:**

https://docs.aws.amazon.com/AmazonS3/latest/userguide/about-object-ownership.html

## Scan coverage information

### List of tests performed (10/10)

- ✔ Trying to detect the cloud provider...
- ✔ Searching for AWS S3 buckets...
- ✔ Searching for AWS S3 ACLs...
- ✔ Searching for interesting files in AWS S3 buckets...
- ✔ Searching for AWS S3 buckets versioning configuration...
- ✔ Searching for AWS S3 buckets replication configuration...
- ✔ Searching for AWS S3 buckets encryption configuration...
- ✔ Searching for AWS S3 buckets CORS configuration...
- ✔ Searching for AWS S3 buckets ownership control configuration...
- ✔ Searching for AWS S3 buckets logging configuration...

### Scan parameters

| | |
|---|---|
| Target: | https://pentest-ground-bucket.s3.ca-central-1.amazonaws.com/ |
| Detect cloud provider: | True |
| Detect cloud vulnerabilities: | True |