PRAGYA

# AWS Cloud Security Assessment

Discover the pinnacle of security for your AWS cloud environment with our comprehensive AWS Cloud Security Assessment. Our expert team conducts a meticulous evaluation of your Amazon Web Services infrastructure to fortify your defenses against potential threats and vulnerabilities. Through in-depth analysis of identity and access management, network security, data encryption, and regulatory compliance, we uncover areas for enhancement and provide tailored solutions to safeguard your data, applications, and infrastructure. Elevate confidence in your cloud operations with our rigorous assessment, ensuring the confidentiality, integrity, and availability of your critical assets. Trust us to bolster your AWS security, enabling you to focus on driving innovation and growth with peace of mind

**Risk 1**
Misconfigured
Cloud buckets

**Risk 2**
Weak
passwords

**Risk 3**
Poor Access
Management

**Risk 4**
Missing MFA

## Typical scope of work

- Analyze code and configuration for sensitive information disclosure
- Privilege Escalation through Lambda IAM Roles and SDK's
- Analyze the API endpoints
- Checking type of Authentication implemented
- Basic HTTP authentication
- User Input validation checks
- Access token Cookies
- Check if all the endpoints are protected behind authentication to avoid broken Authentication process
- Test for API input fuzzing
- Test for unhandled http methods
- Analyze API request and response
- Test for the following vulnerabilities
- IAM privileges strength
- Data leakage
- Unauthorized access
- Injection vulnerabilities
- Parameter tampering
- Access permissions
- Insecure Direct Object reference tests

## Typical tools used

- CloudGoat
- Acunetix
- DirBuster
- FuzzAPI
- Commix

## Pre-requisites

- AWS permission for PEN Test
- Access to logs while testing for analysis

**Contact us today!**

✉ enquiries@pragyacyber.com