hackerone

# HackerOne and AWS

## Hacker-Powered Security for Safer AWS Cloud Applications

# Introduction

With so many of your applications running on AWS, it's more important than ever to enhance your cloud security strategy by using ethical hacker expertise to find and remediate vulnerabilities before malicious actors can exploit them.

Your organization needs to expand digital value by taking advantage of cloud agility without creating risks leading to cybercrime. But events such as application migration, product rollouts, or past breach remediations can introduce new vulnerabilities that invite exploits. Adding the security expertise of hackers to assess vulnerabilities in your cloud applications helps ensure the outcome you expect from your cloud transformation.

HackerOne and AWS together accelerate the discovery of critical application vulnerabilities, streamline AWS security workflows, and strengthen your security teams to drive down organizational risk. By including a community of AWS Certified ethical hackers to find coding and deployment flaws, your teams can build and run their AWS applications with confidence, as shown in Figure 1 below.

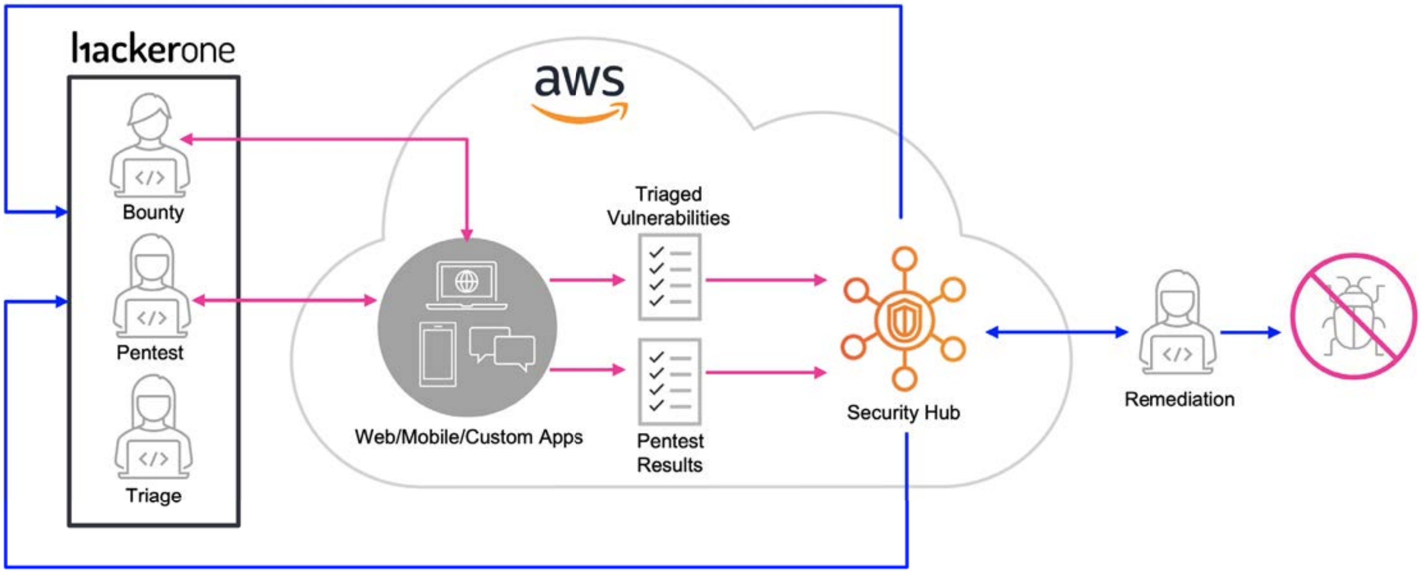
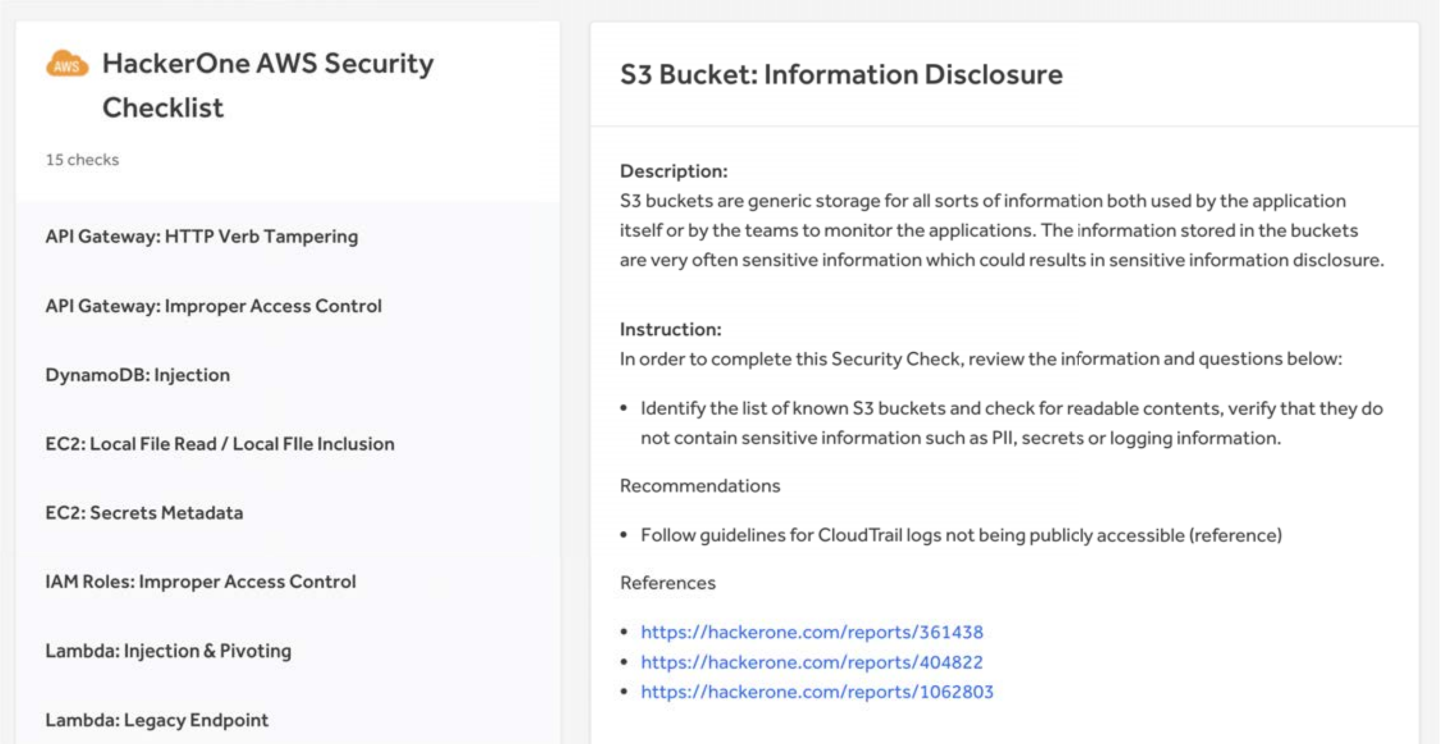


**Figure 1:** HackerOne and AWS Security Hub bi-directional exchange of vulnerability intelligence

# HackerOne Assessments: Application Pentest for AWS

HackerOne provides a portfolio of security assessments to meet the needs of our customers, ranging from web, mobile, network, and APIs. HackerOne Assessments: Application Pentest for AWS is explicitly tailored for AWS-deployed applications. It helps security, cloud, and applications teams identify risks caused by cloud transformations, deployment changes, and previous breaches. Our pentests are designed and executed based on a methodology checklist to assure scope is covered, as shown below in Figure 2. After the pentest, a report is generated valid for compliance attestation or to keep stakeholders apprised of the results.



HackerOne AWS Security Checklist

15 checks

- API Gateway: HTTP Verb Tampering
- API Gateway: Improper Access Control
- DynamoDB: Injection
- EC2: Local File Read / Local FIle Inclusion
- EC2: Secrets Metadata
- IAM Roles: Improper Access Control
- Lambda: Injection & Pivoting
- Lambda: Legacy Endpoint

S3 Bucket: Information Disclosure

**Description:**
S3 buckets are generic storage for all sorts of information both used by the application itself or by the teams to monitor the applications. The information stored in the buckets are very often sensitive information which could results in sensitive information disclosure.

**Instruction:**
In order to complete this Security Check, review the information and questions below:

- Identify the list of known S3 buckets and check for readable contents, verify that they do not contain sensitive information such as PII, secrets or logging information.

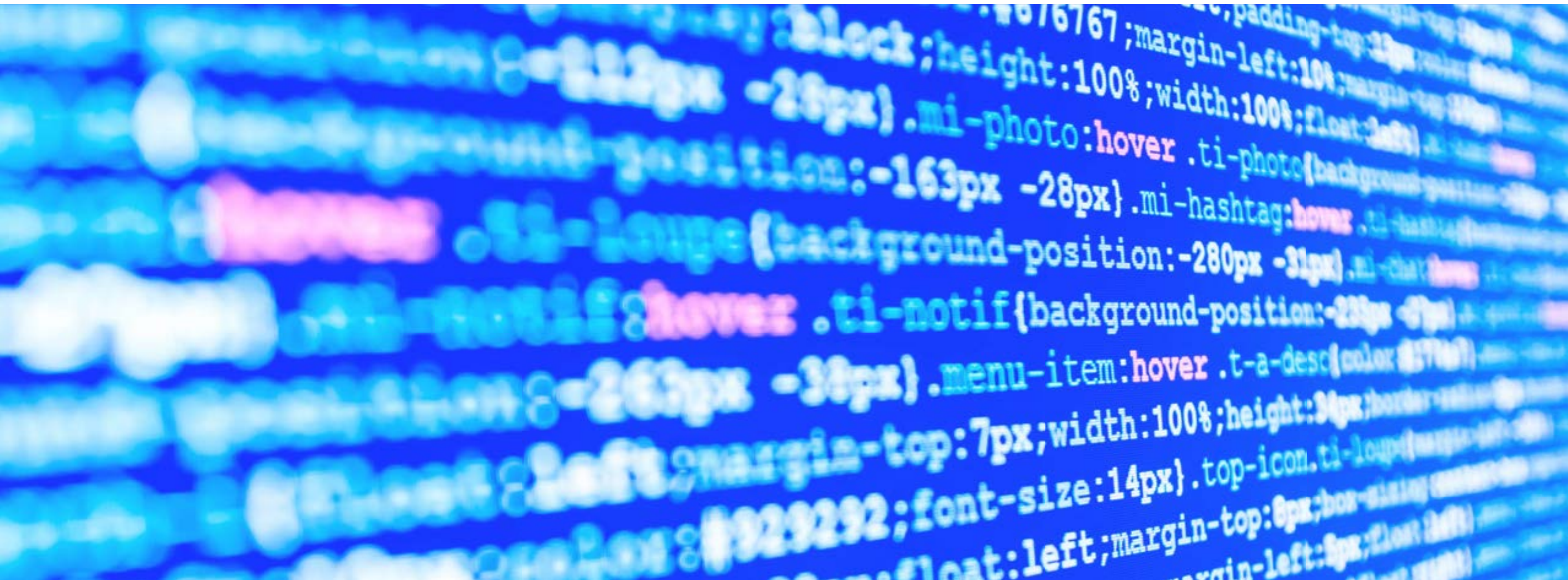
Recommendations

- Follow guidelines for CloudTrail logs not being publicly accessible (reference)

References

- https://hackerone.com/reports/361438
- https://hackerone.com/reports/404822
- https://hackerone.com/reports/1062803

**Figure 2:** HackerOne Assessments: Application Pentest for AWS methodology checklist



# Key Use Cases

**Compliance Assessment -** Respond to an upcoming audit that includes AWS-hosted applications with a pentest that follows an AWS-specific methodology and identifies vulnerabilities that can cause increased cloud risk.

**New Product Launch -** Reduce the time spent on vulnerability testing of AWS cloud applications ahead of significant initiatives such as new product introductions.

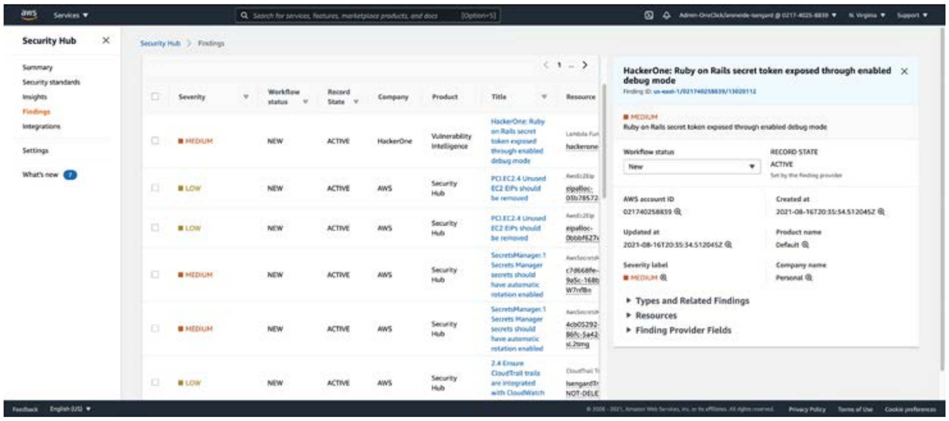
**Mergers & Acquisitions -** Find hidden security issues that are introduced into your cloud environments,  post-acquisition and assess the risk profile of newly acquired cloud applications.

**Cloud Migration Testing -** Track and protect against cloud application flaws as part of your cloud migration.

# HackerOne Integration with AWS Security Hub

With workflow automation, this integration reduces the manual processes of comparing and taking action on vulnerability findings between HackerOne and AWS Security Hub, as seen in Figure 3 below. Use the integration to:

- **Aggregate and prioritize vulnerabilities from HackerOne in Security Hub:** Sync all HackerOne vulnerability findings and use AWS Security Hub as the single console to manage and prioritize those findings.
- **Forward findings from Security Hub and other partners to HackerOne:** Compare findings aggregated from AWS Partner Network (APN) in AWS Security Hub with those from HackerOne to eliminate duplicates, understand status, and plan security actions.



| □ | Severity | Workflow status | Record State | Company | Product | Title | Resource |
|---|---|---|---|---|---|---|---|
| □ | ■ MEDIUM | NEW | ACTIVE | HackerOne | Vulnerability Intelligence | HackerOne: Ruby on Rails secret token exposed through enabled debug mode | Lambda Fun<br>hackerone- |
| □ | ■ LOW | NEW | ACTIVE | AWS | Security Hub | PCI.EC2.4 Unused EC2 EIPs should be removed | AwsEc2Eip<br>eipalloc-03b78572 |
| □ | ■ LOW | NEW | ACTIVE | AWS | Security Hub | PCI.EC2.4 Unused EC2 EIPs should be removed | AwsEc2Eip<br>eipalloc-0bbbf627e |
| □ | ■ MEDIUM | NEW | ACTIVE | AWS | Security Hub | SecretsManager.1 Secrets Manager secrets should have automatic rotation enabled | AwsSecretsM<br>c7d668fe-9a5c-168b W7nfBn |
| □ | ■ MEDIUM | NEW | ACTIVE | AWS | Security Hub | SecretsManager.1 Secrets Manager secrets should have automatic rotation enabled | AwsSecretsM<br>4cb05292-86fc-5a42 sL2tmg |
| □ | ■ LOW | NEW | ACTIVE | AWS | Security Hub | 2.4 Ensure CloudTrail trails are integrated with CloudWatch | CloudTrail Tr<br>hengardTr NOT-DELE |

**HackerOne: Ruby on Rails secret token exposed through enabled debug mode** ×

Finding ID: us-east-1/021740258839/13020112

■ MEDIUM

Ruby on Rails secret token exposed through enabled debug mode

Workflow status: New ▾

RECORD STATE: ACTIVE

Set by the finding provider

AWS account ID: 021740258839

Created at: 2021-08-16T20:35:54.512045Z

Updated at: 2021-08-16T20:35:34.512045Z

Product name: Default

Severity label: ■ MEDIUM

Company name: Personal

▸ Types and Related Findings

▸ Resources

▸ Finding Provider Fields

**Figure 3:** HackerOne vulnerability findings  in AWS Security Hub

## Supported Compliance Frameworks

**SOC 2 Type II -** SOC 2 compliance is the industry standard for technology service organizations. Customers will typically run annual pentests to maintain certification.

**ISO 27001 -** ISO 27001 helps organizations build out an Information Security Management System. Customers will generally get certified every three years.

**FISMA -** FISMA follows NIST 800-53, which we support. Pentesting is an annual requirement.

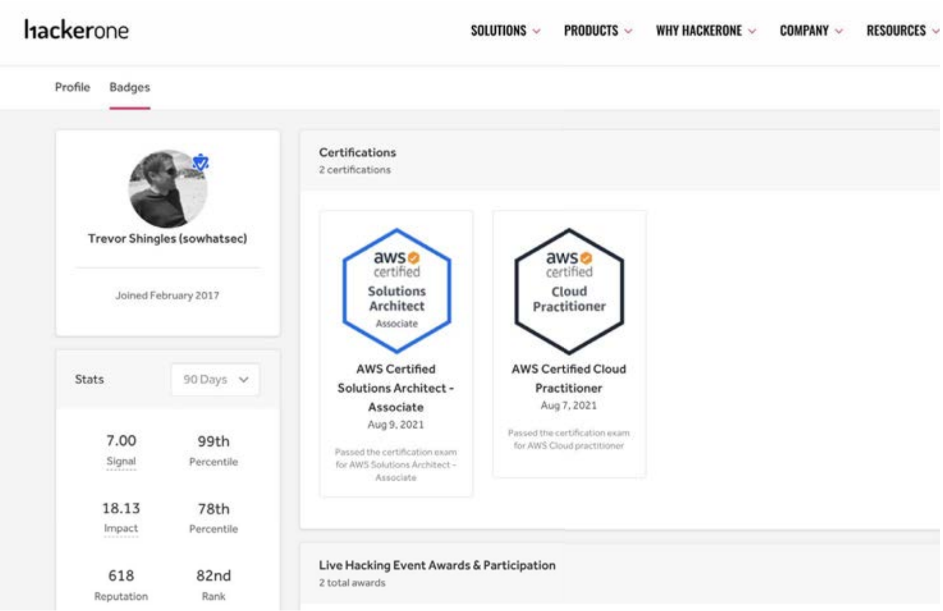
**GDPR -** GDPR is a data privacy framework that suggests "a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing." A pentest could meet this requirement, but there is no specified methodology or reporting output.

**HITRUST -** The HITRUST assessment methodology specifically requires assessors to gather and examine documentation. Customers would know which areas to include for the HITRUST certification, and therefore, for the pentest. The scope requirements should be agreed upon with the customer and the external assessor.

# Community of AWS Certified Security Experts

HackerOne's global community of AWS Certified ethical hackers ensures that vulnerability hunters know the intricacies of AWS application security analysis to deliver fast, accurate vulnerability assessments.

- AWS Certified hackers specialized in finding security gaps in AWS applications, as seen in Figure 4 below
- Pentester teams that have validated the security of the most security-mature customers
- Part of the largest and most diverse global hacker community


hackerone
SOLUTIONS
PRODUCTS
WHY HACKERONE
COMPANY
RESOURCES
Profile
Badges
aws certified Solutions Architect Associate
aws certified Cloud Practitioner
90 Days

Trevor Shingles (sowhatsec)

Joined February 2017

Stats

| | |
|---|---|
| 7.00<br>Signal | 99th<br>Percentile |
| 18.13<br>Impact | 78th<br>Percentile |
| 618<br>Reputation | 82nd<br>Rank |

Certifications
2 certifications

AWS Certified Solutions Architect - Associate
Aug 9, 2021
Passed the certification exam for AWS Solutions Architect - Associate

AWS Certified Cloud Practitioner
Aug 7, 2021
Passed the certification exam for AWS Cloud practitioner

Live Hacking Event Awards & Participation
2 total awards

**Figure 4:** Hacker profile in the HackerOne platform with earned AWS Certification badges

# Using HackerOne and AWS Together for Better Cloud Security

Your cloud transformation can deliver considerable advantages to your business, and the protection of your digital applications can improve your overall cloud security. HackerOne brings you highly skilled expert hackers to find application weaknesses, and we help build trust for some of the biggest brands.

HackerOne helps keep the Amazon retail experience safe. Amazon has an active Vulnerability Research Program managed by HackerOne and driven by the Amazon Information Security team. The program scope includes retail marketplaces and mobile apps internationally.  Additionally, HackerOne is a Select Technology Partner and HackerOne products available in the AWS Marketplace. To learn more, visit our HackerOne and AWS page.

hackerone

# HackerOne has vetted hackers for hundreds of organizations including:

GM
Lufthansa
European Commission

Spotify
TSRC
Tencent Security Response Center
PayPal
UBER
HYATT

HACK THE ARMY
Google
New Relic
Nintendo
Adobe

HBO
Dropbox
yahoo!
priceline

shopify
slack
yelp
verizon media
TOYOTA

## With over 2,000 customer programs, more companies trust HackerOne than any other vendor

Contact Us

www.hackerone.com / sales@hackerone.com