[PERDITION//SEC]

Penetration Test Report
Sample / Redacted

A fictional engagement summary, prepared in the same format we deliver to real clients. All clients, findings, and infrastructure references are illustrative only.

CLIENT
Acme Health (fictional)

ENGAGEMENT
External + Web Application Pentest

WINDOW
March 2 – March 13, 2026

CONSULTANT
David Sampson, CISSP, CISM

DOCUMENT VERSION
1.0 — sample

perditionsecurity.com · dsampson@perditionsecurity.com

// 00

Document Control

This document is a sample pentest report produced by Perdition Security Inc. The client, scope, findings, and infrastructure references are fictional and illustrative. The format, structure, and level of detail mirror what we deliver on real engagements.

CLASSIFICATION CONFIDENTIAL — Sample / Public Distribution OK
AUTHOR David Sampson, Perdition Security Inc.
REVIEWED BY —
ENGAGEMENT TYPE External Network + Web Application Pentest
METHODOLOGY PTES, OWASP WSTG v4.2, MITRE ATT&CK
RETEST INCLUDED Yes — 30 days post-delivery

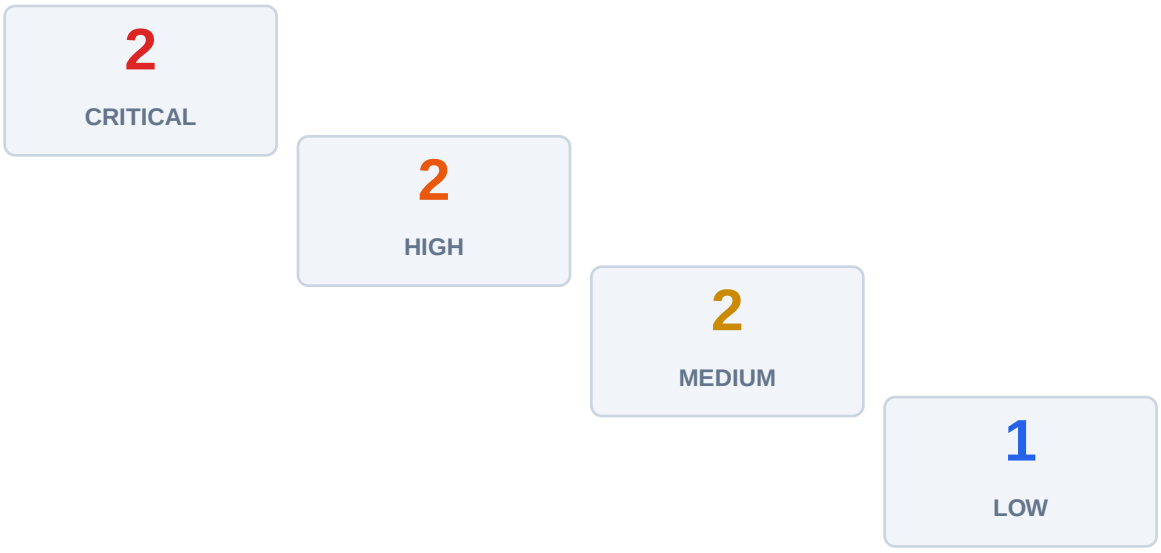
// 01

Executive Summary

Acme Health engaged Perdition Security to perform a two-week external attack-surface and web application penetration test of their patient portal (portal.acmehealth.example) and supporting AWS infrastructure. The engagement was conducted between March 2 and March 13, 2026.

We identified seven exploitable findings, including two of Critical severity. Both Critical findings were validated end-to-end in a controlled staging environment and reported to the client engineering team within four hours of discovery. All Critical and High findings were remediated before the engagement closed and re-verified during the final retest cycle.

Findings by Severity



Headline Risks

- Authentication bypass on the patient portal API allowing access to other patients' records (ACME-001).
- IAM privilege escalation path from the application service account to AWS administrative access via Lambda execution roles (ACME-002).
- Insecure direct object reference exposing appointment records across organizational boundaries (ACME-003).

// 02

Scope

The following assets were in scope for the engagement, as defined in the Statement of Work dated February 18, 2026.

In Scope

- portal.acmehealth.example (production patient portal)
- api.acmehealth.example (backend REST and GraphQL endpoints)
- AWS account 999999999999 (us-east-1, us-west-2)
- External attack surface for *.acmehealth.example

Out of Scope

- Mobile applications (iOS / Android) — separate engagement
- Third-party SaaS integrations (Salesforce, Okta, Twilio)
- Physical security and social engineering
- Denial-of-service testing of any kind

// 03

Methodology

Testing was conducted using the Penetration Testing Execution Standard (PTES) and the OWASP Web Security Testing Guide v4.2 as primary references. Findings are mapped to MITRE ATT&CK Enterprise where applicable. All testing was manual-led, with automated tools used only for reconnaissance and surface enumeration.

- Reconnaissance: passive enumeration of subdomains, exposed services, and TLS configurations.
- Discovery: authenticated and unauthenticated mapping of API surface and application functionality.
- Exploitation: manual validation of every reported finding with proof-of-concept where safe to do so.
- Lateral movement: post-exploitation pivoting limited to the agreed scope.
- Remediation support: daily synchronous communication with engineering during the retest window.

// 04

Findings

CRITICAL ACME-001

Authentication bypass on patient record API

CVSS 9.1 — AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N
AFFECTED GET /api/v1/patients/{id}/records
MITRE T1190 — Exploit Public-Facing Application

Description

The patient record retrieval endpoint validates authentication via a JWT bearer token, but does not verify that the patient_id in the URL path corresponds to the authenticated user. Any authenticated patient session can read records belonging to any other patient by substituting the patient_id in the request URL.

Reproduction

1. Log into the patient portal as a test patient (ID: 100001).
2. Capture the bearer token from the session.
3. Issue: GET /api/v1/patients/100002/records with the captured token.
4. The API returns the records of patient 100002 with HTTP 200.

Impact

Full unauthorized read access to all patient records in the production system. Constitutes a HIPAA-reportable disclosure under §164.402 if exploited against real patient data. Estimated blast radius: ~530,000 patient records.

Recommendation

Add an authorization middleware that compares the patient_id parameter against the patient_id claim in the JWT for every endpoint that accepts a patient_id path parameter. Default-deny on mismatch. Add an integration test that explicitly verifies cross-patient access is rejected.

Status

REMEDIATION Fixed in commit 4f1a2b3 (March 7, 2026)
RETESTED Verified closed during retest cycle on March 13, 2026

CRITICAL **ACME-002**

IAM escalation via Lambda execution role

CVSS 9.0 — AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
AFFECTED AWS account 999999999999 — IAM
MITRE T1078.004 — Valid Accounts: Cloud Accounts

Description

The application service principal (svc-portal-app) holds the lambda:UpdateFunctionCode permission on the patient-record-export Lambda function. The Lambda's execution role is assigned the AdministratorAccess managed policy. A compromise of the service principal therefore allows arbitrary code execution as an AWS administrator via the Lambda code-replacement primitive.

Recommendation

Replace the AdministratorAccess policy on the Lambda execution role with a least-privilege policy scoped to the resources the function actually needs. Audit all Lambda execution roles in the account for similar over-privilege. Enable AWS IAM Access Analyzer on the account.

Status

REMEDIATION Execution role re-scoped to least privilege; verified March 11, 2026

HIGH ACME-003

IDOR exposing appointment records across organizations

CVSS 8.2 — AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N
AFFECTED GET /api/v1/appointments/{id}

Description

The appointment retrieval endpoint authorizes on the basis of a valid session but does not verify that the appointment belongs to an organization the authenticated user is a member of. Any authenticated provider can read any appointment in the system by guessing or enumerating IDs.

Status

REMEDIATION Tenant-aware authorization middleware added; verified March 12, 2026

HIGH ACME-004

Stored XSS in clinician notes field

CVSS 7.6 — AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:L/A:N
AFFECTED POST /api/v1/encounters/{id}/notes

Description

The clinician notes field on the encounter detail page does not sanitize HTML on input or escape on output. A malicious script payload entered into the notes field is rendered to other clinicians who view the same encounter, providing session theft and lateral movement potential within the provider organization.

Status

REMEDIATION Output encoding added via DOMPurify; verified March 12, 2026

MEDIUM ACME-005

Missing rate limiting on authentication endpoint

CVSS 5.3 — AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

Description

The /auth/login endpoint does not implement per-IP or per-account rate limiting, enabling credential stuffing and password-spraying attacks at scale. We confirmed >2000 attempts/minute were accepted from a single source IP without any throttling or alerting.

Status

REMEDIATION Cloudflare rate-limiting rule deployed; verified March 12, 2026

MEDIUM ACME-006

Verbose error messages disclose stack traces

CVSS 5.0 — AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Description

The API returns full Python stack traces in 500 response bodies in production, including module paths,

line numbers, and a partial environment dump. This significantly accelerates further exploitation by revealing internal structure and dependency versions.

Status

REMEDIATION Production error handler updated; verified March 13, 2026

LOW ACME-007

TLS configuration allows TLS 1.0 / 1.1

CVSS 3.7 — AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

Description

The patient portal load balancer accepts TLS 1.0 and TLS 1.1 connections in addition to TLS 1.2 and 1.3. While not directly exploitable in our test, this fails PCI DSS 4.0 and HIPAA technical safeguards expectations and should be disabled.

Status

REMEDIATION ALB TLS policy updated to TLSv1.2_2021; verified March 13, 2026

// 05

Remediation Status

All seven findings have been remediated and re-verified during the retest cycle that concluded on March 13, 2026. The engagement closes with no open Critical, High, Medium, or Low findings.

Recommended Next Steps

- Quarterly external attack-surface assessments to catch regression early.
- Annual full-scope pentest covering mobile and the partner API surface.
- Continuous IAM permission graph monitoring (e.g., Cloudsplaining or equivalent).
- Threat-model the next major release before code freeze, not after.

// 06

About Perdition Security

Perdition Security Inc. is a boutique cybersecurity consultancy led by David Sampson — CISSP, CISM, and ten years of hands-on offensive and defensive experience across crypto, healthcare, telecom, retail, and financial services. We take on a small number of engagements at a time so the practitioner who scopes the work is the practitioner who does it. No subcontractors. No offshore handoffs.

Perdition Security Inc.
Ontario, Canada
dsampson@perditionsecurity.com
https://perditionsecurity.com