ZERO HARBOR SECURITY

Atlanta metro, Georgia · contact@zeroharborsecurity.com

SAMPLE REPORT. THE CLIENT, SYSTEMS, PEOPLE AND FINDINGS BELOW ARE FICTIONAL, WRITTEN TO SHOW THE FORMAT OF A DELIVERED REPORT. THIS DOCUMENT DOES NOT DESCRIBE ANY REAL ENGAGEMENT.

PENETRATION TEST REPORT

Application and API penetration test

Fernhill Analytics, Inc. (fictional)

REPORT REFERENCE	ZH-SAMPLE-0001 · Version 1.1
TARGETS	app.fernhill.example · api.fernhill.example
TESTING WINDOW	3 to 7 August 2026
REPORT DELIVERED	14 August 2026 (10 business days from signed authorisation, 31 July 2026)
RETEST	21 August 2026
LEAD OPERATOR	Suhyun Smith, Founding Principal
CLASSIFICATION	Confidential. Prepared for the client and the recipients it designates.

CONTENTS

1 Executive summary

2 Scope, method and rating

3 Findings

4 Remediation status

5 Coverage record (excerpt)

6 Attestation letter

Document control

VERSION	DATE	CHANGE	AUTHOR
1.0	14 Aug 2026	Report delivered	S. Smith
1.1	21 Aug 2026	Retest results and remediation status added	S. Smith

How to read this report

Section 1 is written to be forwarded without editing. It is the page a prospect's security reviewer, an auditor or an executive usually reads, and it stands on its own. Sections 3 to 5 are for the engineers who fix and verify the findings. Section 6 is the one-page letter designed to be attached to a security questionnaire response.

Every finding carries a CVSS v3.1 base score and an engagement risk rating. They usually agree. Where they do not, the finding states why, in one sentence, so a reviewer can disagree with the adjustment rather than having to guess at it.

SECTION 1

Executive summary

Fernhill Analytics engaged Zero Harbor Security to test its multi-tenant analytics application and public API ahead of an enterprise customer's security review. Testing ran for five days, authenticated as three roles across two tenants, and focused on the classes an enterprise reviewer asks about first: whether one customer's data is isolated from another's, and whether a user can do more than their role allows.

Testing found **four issues**. The most serious allowed a user of one tenant to read another tenant's reports by changing an identifier in the request. That is the finding an enterprise reviewer would treat as a blocker, and it has been fixed and verified.

STATUS AFTER RETEST · 21 AUGUST 2026

Three of four findings are fixed and verified. The fourth, a Low-rated cookie attribute, is accepted with a stated rationale and scheduled for the next release. No Critical or High finding remains open.

Findings by risk

ID	FINDING	RISK	STATUS
ZH-01	Cross-tenant report access through a predictable identifier	◆ CRITICAL	Fixed
ZH-02	Role change enforced in the interface but not at the API	◆ HIGH	Fixed
ZH-03	Password reset token remains valid after use	◆ MEDIUM	Fixed
ZH-04	Session cookie missing SameSite attribute	◆ LOW	Accepted

What was not tested

The internal corporate network, cloud account configuration, mobile applications, physical security and social engineering were out of scope. Denial-of-service testing was excluded by agreement. A clean result in these areas should not be inferred from this report.

SECTION 2

Scope, method and rating

In scope

TARGET	DESCRIPTION	ACCESS
app.fernhill.example	Multi-tenant analytics web application	Unauthenticated; Viewer, Member and Admin in Tenant A; Member in Tenant B
api.fernhill.example	Public REST API, v2, including the reporting and membership endpoints	API keys issued per role above

Approach

Automated scanning was used for coverage of known vulnerability classes. The billed hours went into manual testing: access control across roles and tenants, business logic, authentication and session handling, and chaining lower-severity issues into higher-impact ones. Each finding in Section 3 was exploited to the point of demonstrating impact, then stopped.

References

OWASP Web Security Testing Guide v4.2 · OWASP API Security Top 10 (2023) · OWASP ASVS 4.0.3, Level 2 · CVSS v3.1 specification.

Rating method

RISK	CVSS V3.1 BASE	MEANING FOR THIS ENGAGEMENT
◆ CRITICAL	9.0 to 10.0	Exposes other customers' data or the whole platform. Fix before any enterprise review proceeds.
◆ HIGH	7.0 to 8.9	Account or privilege compromise within a tenant.
◆ MEDIUM	4.0 to 6.9	Exploitable, but requires conditions outside the attacker's control.
◆ LOW	0.1 to 3.9	Hardening. Material mainly when another finding provides the entry point.

The engagement risk rating starts from the CVSS base band. It moves only when the business context changes the real-world impact, and any adjustment is stated in the finding itself. Two findings in this report are adjusted: ZH-01 up, ZH-04 down.

Limitations

Testing is a point-in-time assessment of the systems as they were during the testing window. It does not establish that no other vulnerabilities exist, and changes deployed after 7 August 2026 are not covered except where retested on 21 August 2026.

SECTION 3

Findings

Cross-tenant report access through a predictable identifier

ZH-01

RISK	CVSS V3.1 BASE	STATUS
◆ CRITICAL	7.7	Fixed · verified 21 Aug

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N · CWE-639 · OWASP API1:2023 · WSTG-ATHZ-04

`GET /api/v2/reports/{id}`

Description

The reporting endpoint authorised requests by checking that the caller was authenticated, but not that the requested report belonged to the caller's tenant. Report identifiers are sequential integers, so any authenticated user could enumerate them.

Evidence

```
GET /api/v2/reports/48213 HTTP/1.1
Host: api.fernhill.example
Authorization: Bearer [Tenant B member key, redacted]

HTTP/1.1 200 OK
{"id":48213,"tenant_id":"t_a91f…","title":"Q3 churn by region", ...}
```

The key belongs to a Member of Tenant B. Report 48213 belongs to Tenant A. Requests for 40 sequential identifiers returned reports from 7 distinct tenants before testing stopped.

Business impact

Any customer, or anyone holding one customer's credentials, could read every other customer's reports. For a multi-tenant analytics product this is the failure an enterprise security reviewer tests for first.

Rating adjustment

Raised from High (7.7) to Critical. The base score reflects a single request. In context the exposure is every tenant's data, the identifiers are trivially enumerable, and no alert fired during enumeration.

Remediation

Enforce tenant ownership on every object lookup at the data-access layer rather than per endpoint, and replace sequential identifiers with non-guessable ones. Non-guessable identifiers reduce exposure but are not an authorisation control on their own. Add an alert on cross-tenant access attempts.

Role change enforced in the interface but not at the API

ZH-02

RISK	CVSS V3.1 BASE	STATUS
◆ HIGH	8.1	Fixed · verified 21 Aug

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N · CWE-602 · OWASP API5:2023 · WSTG-ATHZ-03

`PATCH /api/v2/members/{id}/role`

Description

The web interface hides the role selector from non-administrators. The API endpoint behind it does not check the caller's role, so the restriction existed only in the browser.

Evidence

```
PATCH /api/v2/members/u_7c20/role HTTP/1.1
Host: api.fernhill.example
Authorization: Bearer [Tenant A member key, redacted]
Content-Type: application/json

{"role":"admin"}

HTTP/1.1 200 OK
{"id":"u_7c20","role":"admin"}
```

u_7c20 is the Member account making the request. A subsequent request to the admin-only billing endpoint succeeded.

Business impact

Any member of a customer organisation could make themselves an administrator of it: read all of its data, change billing and invite or remove users.

Remediation

Authorise role changes on the server against the caller's current role. Review other endpoints whose only protection is a hidden control in the interface; this pattern rarely occurs once.

Password reset token remains valid after use

ZH-03

RISK	CVSS V3.1 BASE	STATUS
◆ MEDIUM	6.8	Fixed · verified 21 Aug

CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N · CWE-640 · WSTG-ATHN-09

`POST /auth/reset`

Description

A reset token could be used again after it had already set a new password, and it did not expire.

Business impact

Anyone who later obtained a used reset link, from a forwarded email, a shared mailbox or a proxy log, could take over the account long after the legitimate reset. The attacker has to obtain the link first, which is why this is Medium rather than High.

Remediation

Invalidate the token on first use, expire unused tokens within 30 minutes, and end existing sessions when the password changes.

Session cookie missing SameSite attribute

ZH-04

RISK	CVSS V3.1 BASE	STATUS
◆ LOW	4.2	Accepted · next release

CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N · CWE-1275 · WSTG-SESS-02

```
Set-Cookie: session
```

Description

The session cookie is set without a SameSite attribute.

Rating adjustment

Lowered from Medium (4.2) to Low. Current Chromium-based browsers treat a cookie without the attribute as Lax, and every state-changing request tested also required a per-request anti-CSRF token. It becomes material only if another finding provides an entry point.

Remediation

Set `SameSite=Lax` explicitly, alongside the existing Secure and HttpOnly attributes, so the protection does not depend on browser defaults.

SECTION 4

Remediation status

Retest performed 21 August 2026, within 30 days of report delivery, against the original scope. Each finding was re-verified with the original reproduction steps.

ID	RISK	STATUS	VERIFICATION OR RATIONALE
ZH-01	◆ CRITICAL	Fixed	Cross-tenant requests now return 404. Identifiers are non-sequential. Tenant ownership is enforced in the data-access layer and was re-tested across 12 endpoints, not only the original one.
ZH-02	◆ HIGH	Fixed	Role change by a Member now returns 403. Four other endpoints protected only in the interface were found by the client's own review and fixed in the same release.
ZH-03	◆ MEDIUM	Fixed	Reused token returns 400. Unused tokens expire after 30 minutes. Existing sessions end on password change.
ZH-04	◆ LOW	Risk accepted	Accepted by Fernhill's CTO on 20 August 2026 on the grounds stated in the finding. Scheduled for the next release. Not retested.

SECTION 5

Coverage record (excerpt)

What was checked and how, including the checks that found nothing. The full record for this engagement lists 118 checks; 14 are shown.

REFERENCE	CHECK	RESULT
WSTG-ATHZ-04	Insecure direct object references across tenants	Fail · ZH-01
WSTG-ATHZ-03	Privilege escalation between roles	Fail · ZH-02
WSTG-ATHN-09	Password change and reset functionality	Fail · ZH-03
WSTG-SESS-02	Cookie attributes	Fail · ZH-04
WSTG-ATHZ-02	Bypassing authorisation schema, unauthenticated	Pass
WSTG-ATHN-04	Bypassing authentication schema	Pass
WSTG-ATHN-03	Lockout and rate limiting on login	Pass
WSTG-SESS-05	Cross-site request forgery on state-changing requests	Pass
WSTG-INPV-01	Reflected cross-site scripting	Pass
WSTG-INPV-02	Stored cross-site scripting, report titles and comments	Pass
WSTG-INPV-05	SQL injection, API filter and sort parameters	Pass
WSTG-INPV-19	Server-side request forgery, report export webhook	Pass
WSTG-BUSL-05	Limits on repeated use of invitation and export functions	Pass
WSTG-CONF-07	HTTP Strict Transport Security	Pass

SECTION 6 · ATTESTATION LETTER

Letter of attestation

To whom it may concern,

Zero Harbor Security performed an application and API penetration test of Fernhill Analytics, Inc.'s multi-tenant analytics application (app.fernhill.example) and public REST API (api.fernhill.example) between 3 and 7 August 2026, under written authorisation signed on 31 July 2026.

Testing was performed manually, supported by automated tooling, with reference to the OWASP Web Security Testing Guide v4.2 and the OWASP API Security Top 10 (2023). It was conducted authenticated as three roles across two tenants and focused on tenant isolation, access control, authentication and session management, and business logic.

Testing identified one Critical, one High, one Medium and one Low finding. A retest on 21 August 2026 verified that the Critical, High and Medium findings had been remediated. The Low finding was formally accepted by the client with a stated rationale. **As of 21 August 2026, no Critical or High finding remains open.**

This letter describes a point-in-time assessment of the systems in scope during the testing window and the retest. It is not a certification and does not establish that no other vulnerabilities exist. The full report is available to recipients the client designates.

I performed and personally supervised the testing described above.

Suhyun Smith
Founding Principal, Zero Harbor Security
OSCP · CISSP · AWS Security – Specialty

This is a sample. It is not signed, it does not attest to any real engagement, and it must not be presented as evidence of testing. A real attestation letter carries a handwritten or verifiable digital signature and the operator's certification serial numbers.