

THREAT SENTRY
SECURITY

PENETRATION TEST REPORT

THREAT SENTRY SECURITY

Penetration Test Report

External Network and Web Application Assessment

Item	Detail
Client	Meridian Health Partners (fictional)
Engagement	External penetration test
Test dates	3-14 March 2025
Report date	21 March 2025
Version	1.0 (Sample)
Prepared by	Threat Sentry Security

SAMPLE DOCUMENT. Meridian Health Partners is a fictional organization. All hosts, IP addresses, people, findings and scores are invented for demonstration and do not describe any real engagement, system or company.

CONFIDENTIAL - Client use only (sample)

1. Executive Summary

Threat Sentry Security (TSS) performed an external network and web application penetration test for Meridian Health Partners (MHP) between 3 and 14 March 2025. The objective was to determine whether an external attacker could gain access to patient scheduling data or internal systems.

Overall risk rating: HIGH. Testers chained a weak password policy on the patient portal with an insecure direct object reference (IDOR) to read other patients' appointment records, and obtained administrator access to the staff VPN gateway through an unpatched vulnerability. No denial-of-service testing or data exfiltration of real patient data was performed.

Severity	Count	Summary
Critical	1	Unauthenticated remote code execution on VPN gateway
High	2	IDOR exposing patient records; no account lockout / weak passwords
Medium	3	Missing security headers, outdated TLS config, verbose errors
Low	2	Banner disclosure, cookie flags
Info	1	Open ports reviewed

2. Scope and Rules of Engagement

Item	Detail
In scope	portal.meridianhealth.example (203.0.113.20), vpn.meridianhealth.example (203.0.113.10), 203.0.113.0/28
Out of scope	Third-party SaaS, social engineering, denial of service, physical access

Item	Detail
Approach	Black-box external, then authenticated test with a standard patient account
Testing window	Weekdays 20:00-06:00 local time; emergency contact: J. Rivera (MHP IT Director)
Authorization	Signed Rules of Engagement dated 24 Feb 2025

3. Methodology

Testing followed the PTES and OWASP Web Security Testing Guide, with risk scored using CVSS v3.1.

• **Reconnaissance:** DNS enumeration, certificate transparency, service fingerprinting

• **Vulnerability analysis:** Manual testing supported by scanners, with every result validated by hand

• **Exploitation:** Controlled proof-of-concept only; no persistence, no data modification

• **Post-exploitation:** Assess impact and lateral movement potential within agreed limits

• **Reporting:** Evidence, business impact and fix guidance for every finding

4. Findings Summary

ID	Finding	Severity	CVSS	Status
F-01	Unauthenticated RCE on VPN gateway (CVE-2024-XXXXX, fictional)	**Critical**	9.8	Open
F-02	IDOR on /api/appointments/{id}	**High**	8.1	Open
F-03	No account lockout; weak password policy	**High**	7.5	Open
F-04	TLS 1.0/1.1 enabled on portal	**Medium**	5.9	Open
F-05	Missing HSTS and CSP headers	**Medium**	5.3	Open
F-06	Verbose stack traces on error pages	**Medium**	5.3	Open
F-07	Server version banner disclosure	**Low**	3.7	Open
F-08	Session cookie missing SameSite	**Low**	3.1	Open

5. Detailed Findings

F-01: Unauthenticated Remote Code Execution on VPN Gateway (Critical, CVSS 9.8)

Affected: vpn.meridianhealth.example. **Description:** The gateway runs a firmware version vulnerable to command injection in the web management interface, allowing an unauthenticated attacker to run commands as root. **Evidence:** A benign command (`id`) returned `uid=0(root)`. **Impact:** Full compromise of the perimeter device, interception of staff traffic, and a foothold in the internal network. **Recommendation:** Upgrade to the vendor's fixed firmware immediately, restrict the management interface to an internal network, review logs for prior compromise, and rotate all credentials that traversed the device.

F-02: Insecure Direct Object Reference (High, CVSS 8.1)

Affected: portal.meridianhealth.example/api/appointments. **Description:** The API authorizes the session but not ownership of the requested record. Changing the numeric ID returned appointments belonging to other patients. **Evidence:** Request for ID 10482 with a test account returned a different patient's (fictional) record. **Impact:** Exposure of protected health information at scale. **Recommendation:** Enforce server-side ownership checks on every object request, use non-sequential identifiers, and add automated authorization tests.

F-03: No Account Lockout / Weak Password Policy (High, CVSS 7.5)

Description: 500 login attempts against a test account were accepted without throttling, and passwords of 6 characters were permitted. **Impact:** Credential stuffing and brute force are practical. **Recommendation:** Add rate limiting and progressive lockout, require 12+ character passwords checked against breach lists, and offer MFA.

F-04 to F-08: Medium and Low Findings

- **F-04:** Disable TLS 1.0/1.1; allow TLS 1.2+ with modern cipher suites.
- **F-05:** Add Strict-Transport-Security and a Content-Security-Policy.
- **F-06:** Return generic error pages; log details server-side only.
- **F-07:** Suppress version banners on web and SSH services.
- **F-08:** Set SameSite=Lax (or Strict) on session cookies.

6. Remediation Roadmap

Priority	Action	Owner	Target
1	Patch/replace VPN firmware; review logs (F-01)	Network team	48 hours
2	Fix IDOR and add authorization tests (F-02)	Dev team	14 days
3	Rate limiting, lockout, MFA (F-03)	Dev / IT	30 days
4	TLS, headers, error handling (F-04 to F-06)	IT / Dev	45 days
5	Banner and cookie hardening (F-07, F-08)	IT	60 days
6	Retest to confirm fixes	TSS	After step 3

7. Conclusion

MHP's external posture shows solid segmentation but is let down by one critical perimeter flaw and weak application authorization. Resolving F-01 and F-02 removes the most realistic attack paths. TSS recommends a retest once priorities 1 to 3 are complete.