ZABALA GAILETAK, S.A.

HACKING ETIKOA

Penetration Testing Txostena 2026

IT Azpiegituran Gray-Box Pentest Emaitzak

Dokumentu Kodea:	HACK-ZG-001
Bertsioa:	1.0
Data:	2026-02-19
Ikasturtea:	2026
Sailkapena:	Heziketa — Barne Erabilera
Egilea:	Zabala Gailetak Zibersegurtasun Taldea

1. Txostenaren Laburpen Exekutiboa

Penetration test hau Zabala Gailetak-en IT azpiegituraren segurtasun-egoera ebaluatzeko egin da, erakunde berak emandako idatzizko baimenarekin (Rules of Engagement). Helburu nagusia IT-OT azpiegituran ahultasunak aurkitzea da, haiek ustiatu aurretik.

Parametroa	Xehetasuna
Test Mota	Grisa (Gray Box) — sarbide partzialarekin
Esparrua	Web aplikazioa, VPN, WiFi korporatiboa, sare perimetroa
Metodologia	PTES + OWASP Testing Guide v4.2 + NIST SP 800-115
Iraupena	2026-01-20 / 2026-02-05 (2 aste)
Taldearen nagusia	Mikel Etxebarria (OSCP, CISSP)
Ahultzeen kopurua	Kritikoak: 2 | Altuak: 5 | Ertainak: 8 | Baxuak: 12

2. Metodologia eta Fase Nagusiak

Fasea	Ekintzak	Iraupena
1. Errekonozimendu	OSINT, DNS enumeration, Shodan, LinkedIn	2 egun
2. Eskaneatzea	Nmap, Nessus, Nikto, gobuster	2 egun
3. Ustiatzea	Metasploit, Burp Suite, SQLmap, Hydra	5 egun
4. Post-exploitation	Pribilegioaren igoera, lateral movement	2 egun
5. Txostena	Aurkikuntzak, ebaluazioa, gomendioak	3 egun

3. Aurkikuntza Nagusiak

3.1 Ahultasun Kritikoak

■ KRITIKOA: CVE-2025-1234 — SQL Injection web aplikazioan. Erabiltzaile taulara baimenik gabe sartu daiteke.

CVE / ID	Deskribapena	CVSS	Egoera
CVE-2025-1234	SQL Injection — /api/employees/search	9.8	■ Konpondu
CVE-2025-5678	Authenticated RCE — zahartu liburutegi	9.0	■ Konpondu
PEN-007	Broken Access Control — admin panel	8.1	■ Konpontzen
PEN-012	Insecure Direct Object Reference (IDOR)	7.5	■ Konpontzen
PEN-018	Default credentials — WiFi AP admin	7.2	■ Planifikatua

4. OWASP Top 10 Azterketa — Zabala Gailetak

OWASP Kategoria	Egoera	Kontrola
A01 — Broken Access Control	■■ AURKITU	RBAC indartu, IDOR konpondu
A02 — Cryptographic Failures	■ Ongi	TLS 1.3, AES-256
A03 — Injection (SQLi, XSS, SSTI)	■■ AURKITU	Parameterized queries ezarri
A04 — Insecure Design	■ Ongi	Threat Modeling eginda
A05 — Security Misconfiguration	■■ Partziala	Debug itzali, headers gehitu
A06 — Vulnerable Components	■■ AURKITU	Snyk SCA — 3 lib zahartu
A07 — Auth & Session Failures	■ Ongi	JWT + TOTP MFA
A08 — Data Integrity Failures	■ Ongi	SRI + npm audit
A09 — Logging & Monitoring Failures	■ Ongi	SIEM + Wazuh
A10 — SSRF	■ Ongi	URL filtraketa ezarrita

5. Esplotazio Adibideak

5.1 SQL Injection — Aurkikuntza eta Konponketa

```
# Jatorrizko kode ahula (PHP) $query = "SELECT * FROM employees WHERE id = " .
$_GET['id']; # Explotazioa (sqlmap) sqlmap -u
'https://hr.zabala-gailetak.eus/api/employees/search?id=1' --dbs # Konpondutako kodea —
Prepared Statements $stmt = $pdo->prepare('SELECT * FROM employees WHERE id = ?');
$stmt->execute([$_GET['id']]);
```

6. Gomendioak eta Ekintza Plana

Ahultasun kritikoak eta altuak konpontzeko prioritate-zerrenda:

- **Berehala (<7 egun):** SQL Injection patch-a —prepared statements erabili.
- **Berehala (<7 egun):** RCE ahultasuna duen liburutegia eguneratu.
- **Epe laburra (<30 egun):** Access control berrikusi eta IDOR konpondu.
- **Epe laburra (<30 egun):** WiFi AP-en pasahitz lehenetsiak aldatu.
- **Epe ertaina (<90 egun):** SCA tresna CI/CD-n integratu dependentzia zahartuak auto-detektatzeko.
- **Etengabe:** Urteroko penetration testing kanpoko auditoreekin.