FORENOVA

EXTERNAL ATTACK SURFACE MANAGEMENT (EASM) REPORT

Example Real Estate GmbH

Conducted Date: April 4, 2025

Project Background

ForeNova's security team was commissioned by Example Real Estate Gmbh to perform a comprehensive External Attack Surface Management (EASM) assessment on April 4, 2025. The scope included:

- Internet exposure analysis
- External attack surface discovery

Client Name: XX Real Estate GmbH
Domains Monitored: *(Redacted for confidentiality; see Appendix)*
IP Segments: 111.***.***.65/28, 8.***.***.225, 124.***.***.96/27, 124.***.***.237/30

Executive Summary

A total of 48 subdomain assets, 353 webpages, and 47 digital assets were identified. Critical vulnerabilities such as Remote Code Execution (RCE) and SQL Injection were present, posing a high risk to the organization.

Key issues include:

- Sensitive document exposure
- Impersonation websites
- Backend login portals exposed publicly
- SQL injection in admin interfaces
- Insecure configurations on public IPs

Internet Exposure Overview

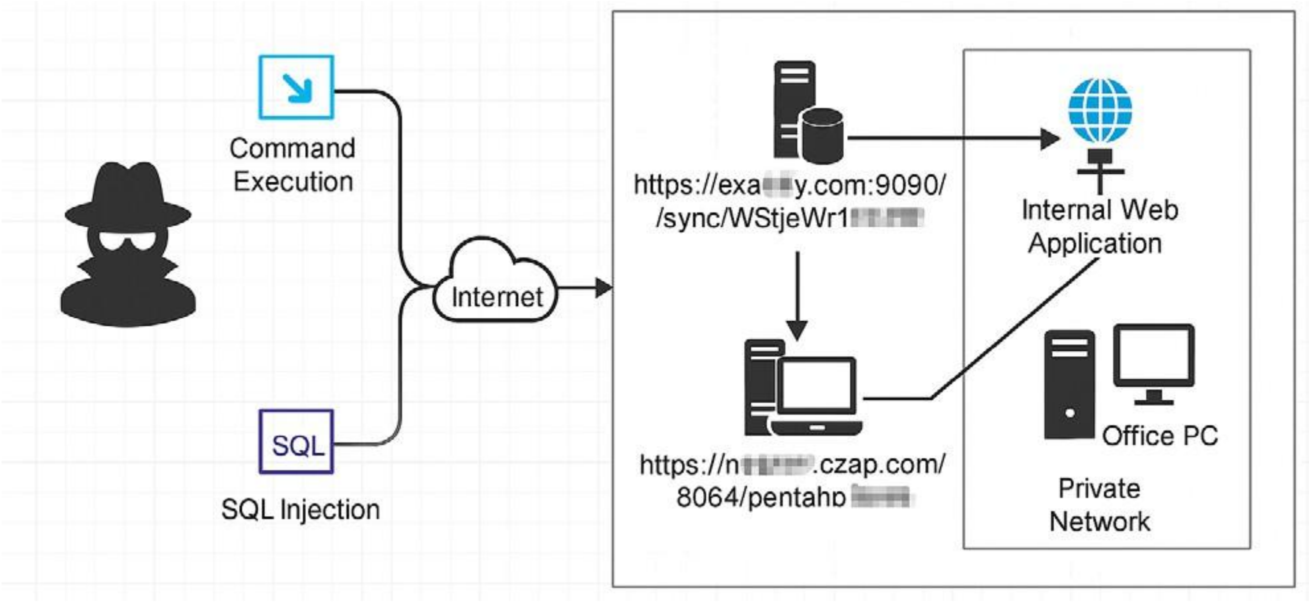
Asset Type	Count
Root Domain Names	2
Subdomain Assets	48
IP Addresses	54
Open Ports	633
Web Services	353
Non-Web Assets	280
Cloud Assets	22
SSL Certificates	13

External Risks Summary

Risk Type	High	Medium	Low
Vulnerabilities	11	18	1
Weak Passwords	0	0	0
Essential Components	37	-	-
Port/Service Exposures	8	-	-

Attack Vectors

Attack Route Map


Command Execution
SQL
SQL Injection
Internet
https://exa[redacted]y.com:9090/ /sync/WStjeWr1[redacted]
https://n[redacted].czap.com/ 8064/pentahb[redacted]
Internal Web Application
Office PC
Private Network

Attack Details

Attackers may exploit vulnerabilities like SQL injection or command execution in public-facing systems to:

- Gain unauthorized access
- Escalate privileges
- Move laterally within internal networks

Lateral Movement Methods

- Credential harvesting from compromised servers
- Exploiting known vulnerabilities (e.g., MS17-010)
- Brute-force attacks on internal login systems

Domain Names

Example domains (full list redacted):

- xfw.m***y.com
- tjs***m.m***y.com
- sjz***nchant.m***y.com
- mail.m***y.com
- vpn.m***y.com

IP Addresses

Sample Range:

- 111.***.***.65 – 111.***.***.77

High-Risk Exposed Assets

Host	Port	Service
sjbi.my.com	3389	RDP
111.*..130	6379	Redis
111.*..152	5985	WinRM
8.*..225	3389	RDP

Open Ports and Services

Host	Port	URL	Technology Stack
www.m***y.com	1187	http://www.m***y.com:1187	PHP, jQuery, nginx, Tongda OA
mail.m***y.com	80	http://mail.m***y.com	Apache httpd
124.*..109	8088	http://124.***.**.109:8088	Panmicro e-Bridge, nginx

Detailed Vulnerability Example

SQL Injection (Critical)

URL

https://sj***portal.m***y.com:9070/system/adminUsers/getAdminUsersList.do?state=1

Risk: Allows attackers to inject malicious SQL queries to bypass authentication or access sensitive data.

Proof-of-Concept Snippet

```
POST /system/adminUsers/getAdminUsersList.do?state=1 HTTP/1.1
Injection in: sortName=(case when 1=1 then name else id end)
```

Recommendations

- Enforce strict input validation
- Implement parameterized queries
- Harden database access privileges
- Deploy WAFs with SQLi detection

High-Level Recommendations

Fix Critical Vulnerabilities

Patch systems affected by SQL Injection and Remote Code Execution (RCE).

- Sanitize all user input (use whitelisting and input validation).
- Use parameterized SQL queries in all applications.
- Patch vulnerable systems and update frameworks.
- Deploy a Web Application Firewall (WAF) with SQLi/RCE protection.

Restrict Public Access to Sensitive Services

Lock down services like RDP, WinRM, Redis, and admin portals.

- Use firewall rules to limit access to specific IPs.
- Enforce VPN access for remote management.
- Disable unused services or move them behind authentication gateways.

Remove or Secure Exposed Documents

Identify and remove documents exposed online.

- Use tools like Google Dorking or DLP scanners to find exposed documents.
- Review public folders or misconfigured cloud buckets.
- Set proper file permissions and encrypt sensitive files.

Enable Multi-Factor Authentication (MFA)

Add MFA to all external-facing portals and user accounts.

- Use app-based MFA (like Google Authenticator or Microsoft Authenticator).
- Enforce MFA for email, VPN, admin dashboards, and cloud accounts.
- Educate users about phishing-resistant MFA.

Deploy a Web Application Firewall (WAF)

Use a WAF to protect web applications from common attacks.

- Choose a WAF (e.g., Cloudflare, AWS WAF, or Imperva).
- Set rules to block malicious traffic.
- Monitor logs and alerts to track blocked threats.

Monitor and Clean Up Exposed Assets

Continuously discover and secure exposed domains, subdomains, and services.

- Use EASM tools (e.g., Shodan, Censys, or Attack Surface Management platforms).
- Audit DNS records and IP ranges monthly.
- Remove or disable stale subdomains and assets.

Harden Public-Facing Services

Secure services like webmail, VPNs, and portals.

- Disable default accounts or change default passwords.
- Turn off directory listings and unnecessary features.
- Use secure protocols (HTTPS, SFTP, etc.)