

EXTERNAL AND INTERNAL ASSESSMENT · HEAVY-INDUSTRY MANUFACTURER

From an internet-facing web app to full domain control

A heavy-industry manufacturer in the Gulf region

Anonymized with the client's written permission. The organization, systems, hostnames, addresses, accounts and other identifiers in the original report have been removed or generalized. Findings are described at a level that cannot be traced back to the client.

Client	A heavy-industry manufacturer (anonymized)
Engagement	External penetration test of internet-facing systems, continued into an internal Active Directory assessment
Approach	Grey-box, roughly two weeks, remote testing from a fixed source address
Tester	Ismail Regragui, Vallum Security · OSCP, OSEP, BSCP, OSWP · Synack Red Team
Standards	OWASP WSTG, OWASP API Security Top 10, NIST SP 800-115; severity by CVSS v3.1

What we were asked to do

Test the company's public-facing web applications and mail and remote-access services, then, using a standard low-privilege domain account, assess how far an attacker could move inside the corporate Active Directory environment.

Results at a glance



Findings at a glance

ID	FINDING	SEVERITY
1	Unauthenticated remote code execution via a long-forgotten web shell on a public application server	Critical

2	Full Active Directory domain compromise from a single standard user account	Critical
3	High-privilege service accounts exposed to offline password cracking (Kerberoasting)	High
4	Account enumeration and weak password-reset protection on a self-service portal	High
5	Account enumeration via a public login page	Medium
6	Weak brute-force protection on the webmail portal, bypassable by password spraying	Medium
7	Build-tooling output left publicly accessible, exposing internal application structure	Medium
8	File-upload validation enforced only at download time, not at upload	Medium
9	An outdated third-party UI component with public exploits (not exploitable here, due to compensating controls)	Low

Findings are renumbered and retitled for this case study. Hostnames, paths, account names and addresses from the original report have been removed.

Key attack chain: public web server to Domain Admin

The two critical findings combined into a single path from the open internet to complete control of the corporate domain.

1. **Foothold.** Content discovery on a public application server revealed a non-standard script left behind years earlier. It accepted commands without authentication, giving immediate code execution on the underlying Windows server.
2. **Credential harvest.** That access exposed application configuration files holding plaintext database and service credentials, and a set of internal corporate accounts could be enumerated from a separate self-service portal that leaked which accounts existed.
3. **Internal entry.** Using a standard low-privilege domain account, the internal environment was mapped. One application account held far broader rights than intended, including control over several high-value servers.
4. **Escalation.** Those excessive rights, combined with privileged administrator sessions left on ordinary servers and missing credential-protection hardening, allowed a standard delegation-abuse technique to escalate to Domain Admin.
5. **Impact.** From there, every domain-joined server, workstation and account was within reach, including systems holding sensitive commercial documents.

Removing the forgotten script and correcting one over-privileged account would each have broken the chain. Both fixes were low-effort relative to the risk.

What was working

- ✓ Endpoint protection blocked several escalation attempts and forced the use of quieter, hand-crafted techniques.

- ✓ TLS was correctly configured on the tested public services.
- ✓ Database access used parameterized queries; no SQL injection was found in the tested applications.

Remediation themes

- Remove unknown and legacy files from web roots, and treat the affected server as compromised: rebuild from clean sources and rotate every exposed credential.
- Reduce privileged group membership and delegation rights to the minimum, and keep administrator accounts off ordinary servers (tiered administration).
- Enforce credential-protection controls on servers and domain controllers, and move service accounts to managed accounts with automatic rotation.
- Add rate limiting, uniform error messages and multi-factor authentication to all internet-facing login and password-reset flows.

Outcome. All critical and high findings were retested after remediation and confirmed fixed, and the client received an updated report and an attestation letter for its auditors.