Most Villainous Hacks in History that Fall Under OWASP Top 10

In recent years, cybercriminals have shattered the defenses of some of the world's biggest names : AT&T's vendor breach compromised 9 million accounts, T-Mobile lost 37 million, JD Sports 10 million, MyDeal 2.2 million, Dropbox nearly 69 million, Flagstar Bank 1.5 million, and eBay an astonishing 145 million.

Terrifying? Yes. But these were just warm-ups.

The cyber underworld has delivered blows far more devastating attacks so ruthless, so technically insidious, they've become legends. These are not just data leaks. They are digital massacres. And among them, 39 stand out each a nightmare case study mapped directly to OWASP's Top 10 vulnerabilities.

These aren't just breaches. They are warnings.

1. Equifax Breach (2017)

- OWASP: A06 Vulnerable Components, A05 Misconfiguration
- What happened: Attackers exploited Apache Struts CVE-2017-5638 to run remote code on Equifax's systems.
- Equifax delayed patching the May-issued fix until mid-May; breach occurred in mid-May and persisted until late July.
- Nearly 148 million U.S. citizens had personal data :- SSNs, DOBs, addresses exfiltrated.
- Attackers used reconnaissance to map database schema, moved laterally, and stole immense data sets.
- Lack of patching, plaintext storage, expired certs, poor network segmentation, and weak monitoring compounded the breach.
- Lessons: Prioritize patch management, encrypt sensitive data, segment networks, and deploy real-time monitoring.

2. NotPetya/"Petya" Malware (2017)

- OWASP: A02 Cryptographic Failures, A05 Misconfiguration
- What happened: Disguised as ransomware, NotPetya attacked Ukrainian tax software updates, then spread globally.
- Victims included Maersk, Merck, WPP, Mondelez, and port systems, the damage exceeded $10 billion.

- The infection vector included default credentials, SMB exploits (eternal-blue), and compromised update channels.
- Organizations lacked secure backup practices: whole networks encrypted before detection.
- Lessons: Secure software supply chains, enforce strong credentials, isolate backups, and patch known SMB flaws.

3. SolarWinds Supply Chain Attack (2020)

- OWASP: A05 Misconfiguration, A09 Security Logging & Monitoring Failures
- What happened: Russian nation-state hackers inserted SUNBURST backdoor into Orion software update.
- Over 18,000 clients including U.S. government, Fortune 500 installed the malicious update.
- The attack went undetected for months due to deficient logging and not proactively analyzing update integrity.
- Lessons: Implement supply chain security, conduct code-signing validation, use anomaly-based monitoring.

4. Microsoft Exchange Server Hack (2021)

- OWASP: A10 Server-Side Request Forgery (SSRF), A01 Broken Access Control
- What happened: Four 0-day vulnerabilities (including CVE-2021-26855) enabled SSRF, remote code execution, and arbitrary file writes.
- Attackers installed web shells to harvest email and credentials across tens of thousands of networks.
- Many victims delayed applying Microsoft’s emergency patches.
- Lessons: Swiftly deploy patches, monitor for unknown web shells, restrict external access to Exchange OWA/ECP endpoints.

5. Capital One Breach (2019)

- OWASP: A05 Misconfiguration, A01 Broken Access Control
- What happened: Ex-AWS engineer used SSRF to access misconfigured S3 buckets and AWS metadata.
- Over 106 million individuals affected : SSNs, credit histories, balances, etc.
- Firewall and IAM misconfig allowed unauthorized roles to be assumed.
- Lessons: Enforce strong firewall rules, limit metadata access, and audit cloud IAM permissions.

6. Colonial Pipeline Ransomware (2021)

- OWASP: A02 Cryptographic Failures, A05 Misconfiguration
- What happened: DarkSide ransomware used compromised VPN credentials without MFA
- Entire operations halted; ransom of $4.4 M paid, partial recovery by U.S. DOJ.
- Password reuse from dark web leak negated security; no MFA enabled on VPN.
- Lessons: Enforce MFA, avoid password reuse, regularly rotate credentials, segment OT/IT systems.

7. Bangladesh Bank SWIFT Heist (2016)

- OWASP: A02 Cryptographic Failures, A05 Misconfiguration
- What happened: Hackers sent fraudulent SWIFT messages transferring $81 M to the Philippines and $20 M to Sri Lanka.
- Lack of whitelisting, monitoring, or app-layer authentication enabled unauthorized transfers.
- Most transactions flagged only due to a typo ("foundation" vs "fandation").
- Lessons: Monitor SWIFT endpoints, enforce strict transaction whitelisting, conduct anomaly detection.

8. Ukraine Power Grid Hack (2015)

- OWASP: A03 Injection (via spear-phishing), A09 Security Logging & Monitoring Failures
- What happened: Sandworm APT used spear phishing and BlackEnergy malware targeting SCADA systems, causing a 6-hour blackout for 230,000 users.
- Digital sabotage closed RTUs and UPS systems; call centers overwhelmed by DDoS.
- Lessons: Secure ICS systems, use network segregation, implement anti-DDoS for control centers.

9. Facebook–Cambridge Analytica Scandal (2018)

- OWASP: A01 Broken Access Control
- What happened: App developer gained access to millions of Facebook profiles via public friend-access API flaw.
- Cambridge Analytica harvested data used in political campaigns, users unaware.
- Violation of access control policies allowed excessive data exposure.
- Lessons: Strict API permission limits, conduct periodic audits of third-party apps, improve consent mechanisms.

10. Exactis Data Exposure (2018)

- OWASP: A03 Sensitive Data Exposure
- What happened: Marketing firm left ~340 million customer records (400 attributes) in publicly accessible cloud server.
- Data included personal demographics, contact info, no authentication on server.
- Lessons: Secure S3 buckets and cloud asset configuration, apply data masking, limit stored PII to necessity.

Team 2 -

Deeptansh Nagar, Keshav GoyaL