MUSHRAF MUSTAFA

Security Researcher | Offensive Security & Secure Software Engineering

CONTACT

NORSBORG, Stockholm, Sweden
+46 72 7735 623
hello@mushraf.com
mushraf.com
github.com/mushrafmustafa
in/mushrafmustafa

SUMMARY

Security researcher, author of CVE-2017-9551, alongside 60+ acknowledged disclosures to IBM, Oracle, Spotify and the Dutch National Cyber Security Centre. Seven years across bank SOC operations, enterprise vulnerability management and independent consulting.
Today I design, build and secure commerce platforms ERP, web shops, B2B portals and deepening low-level capability in binary analysis and reverse engineering.

SECURITY RESEARCH & DISCLOSURE

CVE-2017-9551 | Stored Cross-Site Scripting, Mahara ePortfolio Platform

CWE-79 - CVSS 3.0 base score 6.1 (NVD) - vendor-rated High - published 25 Sep 2017

Identified an unauthenticated stored XSS in Mahara's self-registration flow: a payload injected into the applicant's name field persisted to the usr_registration table and was then delivered by email to both the applicant and the site administrator, executing in an administrator context on approval (CVSS scope change, AV:N / AC:L / PR:N). Affected every release before 15.04.14, 16.04.8, 16.10.5 and 17.04.3, on a platform deployed by universities and public institutions worldwide. Remediated in a vendor security release.

nvd.nist.gov/vuln/detail/CVE-2017-9551

Oracle | On-Line Presence Security Contributor. Publicly credited in Oracle's Critical Patch Update advisories, October 2017 (3 reports) and July 2018, for vulnerabilities reported in Oracle's external-facing systems.

Coordinated disclosure | 60+ organisations. Acknowledged by IBM , Intel , Dell , Sony , Spotify , Pinterest , GitHub , Docker , Bitdefender , Sophos , Symantec , ESET , OLX , SoundCloud , Indeed , Skyscanner , AlienVault , Dutch National Cyber Security Centre (NCSC) and 40+ others.

CORE SKILLS

Application Security Threat modelling, Authentication & authorisation design, API security, SAST / DAST, OWASP Top 10 & ASVS, Dependency and supply-chain review, Secrets management

Offensive Security Web application penetration testing, Network penetration testing, Vulnerability research & coordinated disclosure, Exploit development, Binary analysis & reverse engineering, Malware triage

Frameworks OWASP Top 10 / ASVS, CWE, CVSS, MITRE ATT&CK, NIST Cybersecurity Framework, CIS Controls, PCI DSS, GDPR / ePrivacy

Tools Burp Suite | Nessus | Qualys | Rapid7 | Nmap | Wireshark | Ghidra | x64dbg | GDB | ELK | Sysmon | TheHive | MISP | Linux | REMnux

Engineering JavaScript | Node.js , Express , React/NextJs | MongoDB | Python | Bash | SQL | REST APIs | Git

PROFESSIONAL EXPERIENCE

In-House Developer & Retail Associate | SWEPAK HB

Feb 2022 - Present | Stockholm, Sweden

- Design, build and secure commerce systems for retail operations; ERP, e-commerce storefront, B2B wholesale portal and in-store tooling.
- Delivered B2B wholesale portals with role-based access control, tiered pricing and ordering.
- Built an internal ERP covering inventory, purchasing, pricing and order flow, replacing manual spreadsheet processes.
- **Productised the in-house tooling into butiksmanager.se**, a retail-operations platform now used by other small Swedish shops.
- Work the retail floor and customer service alongside development, giving direct daily insight into the operational problems the software is built to solve.

Freelance Developer | Self-employed

Stockholm, Sweden

- Build and ship full-stack web applications for private clients, React / Node.js / threejs, REST APIs, from requirements to deployment.

Information Technology Analyst | Earth Retail

Feb 2021 - Dec 2021 | Abu Dhabi, United Arab Emirates

- Owned vulnerability management across - servers, POS endpoints, cloud services and network devices, including pre-launch secure configuration review and VAPT.
- Hardened and operationalised **~80** assets to secure baselines, closing the highest-risk exposures in the estate.
- Integrated security tooling into the operational stack; scoped engagements and drove proofs of concept through to implementation, including third-party assessments.

Security Researcher (Contract) | Graana

Aug - Nov 2020 , 3-month engagement | Remote (Pakistan)

- Sole tester on a full-scope VAPT of Graana's real-estate platform, the main web application, admin panel, ad server, error-tracking and blog subdomains. Identified **25 vulnerabilities** (3 high, 15 medium, 7 low).
- Highest-impact findings included a user account takeover via insecure direct object reference, broken access control granting full control over any property listing, a blind SSRF, unauthenticated mass-scraping of user PII, and an email-verification bypass.
- Delivered proof-of-concept reports with severity ratings and remediation guidance, then re-tested and verified fixes through to production; findings drove the platform's adoption of rate limiting on authentication endpoints.

Data Analyst | 7-Eleven

Apr 2019 - Dec 2020 | Dubai, United Arab Emirates

- Forecast sales across the store network, set store-level targets and built annual budgets; delivered category analysis and monthly P&L reporting to management.
- Applied data mining, cleansing and structuring (SQL, Excel, Power BI) to turn raw operational data into decision-ready reporting.

SOC Analyst | National Bank of Ras Al Khaimah

Sep 2018 – Apr 2019 | Ras Al Khaimah, United Arab Emirates

- Ran patch and vulnerability management across ~4,000 bank assets using Nessus, Qualys and Microsoft tooling.
- Conducted secure configuration testing on ~2,000 assets and delivered PCI DSS Requirement 11 assessments.
- Designed and rolled out the SOC scanning and reporting strategy, automating the reporting workflow and cutting manual effort.
- Ran attack simulations against internal systems and web applications to surface exploitable flaws; documented findings and drove remediation with engineering teams.
- Reverse-engineered and analysed triaged malicious code in sandboxed virtual machines, assessing behaviour and updating the bank IOC database.
- Performed SIEM operations, ELK and Sysmon threat hunting and detection-rule tuning; led TheHive and MISP integration with the bank security stack.

SELECTED PROJECTS

- **TheHive |** open-source SOC platform deployed and integrated with MISP and surrounding security tooling.
- **Malicious Hash Identifier |** threat-hunting tooling built on Sysmon telemetry for rapid IOC triage.
- **sparlos.se |** cookie-free, GDPR-aligned web analytics for the Swedish market. Server-side measurement, no cross-site tracking, no consent banner requirement, EU-only data residency.
- **butiksmanager.se |** retail operations platform I built and run, helping Swedish shop owners manage day-to-day store operations. Full-stack product: authentication, role-based access and business workflow and online shop management.

CERTIFICATIONS

OffSec Exploit Developer (OSED) in progress. Windows user-mode exploit development: stack overflows, SEH, egghunters, and bypassing modern mitigations.

Microsoft Certified: Azure Security Engineer Associate (AZ-500) in progress. Identity and access, platform protection, security operations and data/application security on Azure.

EDUCATION

Associate Degree, Computer Science & Networking | Virtual University of Pakistan · in progress

Higher Secondary Education | BISP, Pakistan

AWARDS & COMPETITION

- Top 3, Hacker's Academy Capture the Flag (CTF), Dubai.
- Hack The Box | active competitor, focused on the pwn and takeovers (hackthebox.com/profile/16012).

LANGUAGES

English (fluent) | Urdu (native) | Swedish (Basic)