# BILAL SIDDIQUI

## PERSONAL INFORMATION

| | |
|---|---|
| *email* | bilal.s12@protonmail.com |
| *website* | http://bsssq.xyz |
| *phone* | (437) 882 6733 |

## ABOUT ME

I am a database security researcher and penetration tester, with more than **2** years of professional experience and **2** years of independent self-teaching and pursuit of bleeding-edge tactics, techniques, and procedures (**TTPs**). Combined with **4** years of former software and database development experience, I possess a total of **8** years of working with, developing, and reverse engineering the latest in database technology. I look forward to expanding my skill set and experience in the cyber and information security space, and bringing my passion and diligence to your organization!

*"The only way out, is through."*

## CORE COMPETENCIES

*Hard Skills*

**Operating Systems**: Windows, macOS, Kali Linux, Ubuntu Server

**Networking**: TCP/UDP/IP, FTP, SSH, NFS, SMTP, Routing, DNS, PKI, SSL/TLS, Wireshark

**Databases**: MS SQL Server, MySQL/MariaDB/Percona Server, PostgreSQL, MongoDB, Amazon Aurora/RDS, Oracle, CosmosDB, Teradata, Cassandra, DynamoDB, AzureDB

**Cloud + DevOps**: Git, Apache SVN, Kubernetes, Redhat OpenShift, Docker, Terraform, Jenkins, AWS ECS/EC2/S3, Azure DevOps, Jira, SAST/DAST, NUnit

**Scripting + Programming**: Shell (zsh, Bash, Powershell), Python, C++, C#, PHP, XML, SQL, Javascript, Ruby, Go

**Web**: Cookie stealing, Session hijacking, Burp Suite (credential stuffing, fuzzing, proxy)

**Information Gathering**: Subdomain/Directory/File Enumeration, sublist3r, amass, dirb, dirbuster, netcat

**Footprinting + Scanning**: nmap, enum4linux, smbclient, sqlmap, Shodan, linPEAS

**Vulnerability Assessment**: Nessus, Nexpose, GFI LANGuard, dbProtect

**Attacks**: Brute-force/dictionary attacks (john, Hydra, hashcat), Buffer Overflow, Active Directory, XSS, SQL Injections, Null Sessions, ARP Poisoning/Spoofing, Backdoors, Local/Remote File Inclusion, Remote Code Execution, Privilege Escalation, Metasploit, Shellcodes, Reverse Engineering, **OWASP Top 10**

**Defense**: Firewalls, Logging, IPS/IDS, SIEM, SOAR, System and Device Hardening

**Frameworks + Principles**: NIST, SOC2, FISMA, GDPR, ISO 27001/2, DISA-STIG, CIS Benchmark, Zero-Trust (Data Loss Prevention), CIA

## WORK EXPERIENCE

### *Trustwave* Database Security Researcher — Toronto, ON

*December 2021 – Present*

Responsible for **discovery and investigation** of the latest **attacks and**

**vulnerabilities** pertaining to **17** (and counting) major relational database management systems on behalf of our clients, who occupied key sectors such as telecommunications, energy, and national security & defense.

Provided the Engineering team with hard technical research and data gleaned from the vulnerability assessment engine and other automation platform, based on various needs communicated by the Product team, to develop full protection against current and future threats.

Developed and improved our **vulnerability assessment engine**, by adding over **300** unique check scripts and over **66** framework scripts. The engine is implemented in **C#**, running under the .NET platform, and uses IronPython to execute **Python** scripts (checks) that look for vulnerabilities and report the findings in an event-driven manner.

Developed and tested our **automation platform** that parses software vendor security advisories (**ETL**) and extends project functionality to better support new platforms, by leveraging vast amounts of **threat intelligence** and **telemetry data** to develop new **automation patterns and algorithms** and provide **critical patch updates** to clients.

Closely studied the most current **DISA-STIGs** and **CIS Benchmarks** to close any gaps in our clients' **compliance requirements**. Personally added detection and support for MongoDB 4.x/5.x/6.x, PostgreSQL 13.x, MariaDB 10.x, Oracle 12c, and more.

In-depth **research** of whitepapers, statistics, conference presentations and blog articles to bolster both work-related and individual research efforts. Published internal research pertaining to MongoDB Buffer Overflows, Honeypots and Malware Analysis, Attacks on the Healthcare Sector, and more.

### *Veryon* Lead Database Developer — Toronto, ON

*June 2018 – December 2021*

Authored, validated, and maintained high-quality, **guided troubleshooting solutions** for a **reasoning engine** based on several maintenance manuals for a variety of equipment and systems.

Developed entire **libraries and databases**, Powershell scripts, and Tableau data visualizations to collect **analytics** and deliver **engagement reports** to our clients.

Worked well with a wide range of personalities and roles, and actively participated in project roadmaps and discussions, **providing technical suggestions**, including estimates and priorities.

Gained ability to be flexible to shifting priorities and workloads, and to work on **multiple time-sensitive projects**.

## EDUCATION

### *B.Eng* Western University — London, ON

*2013–2018*

Major: Electrical Engineering; Specialization: Information Communication and Transmission

*Certifications*

2023 · INE Professional Penetration Tester (eCPPT)
2021 · INE Junior Penetration Tester (eJPT)
2021 · TryHackMe Offensive Pentesting Path
2020 · Microsoft Azure Fundamentals (AZ-900)

## OTHER INFORMATION

*Languages*

| | |
|---|---|
| English · | Native |
| Hindi · | Native |
| Urdu · | Native |
| Arabic · | Intermediate |
| French · | Intermediate |
| Mandarin | Basic (simple words and phrases) |