Dorkbot

Web application attacks are the #1 source of data breaches.

These exploits are caused by web application vulnerabilities such as SQLi, XSS, LFI, and RFI which collectively account for 9.1% of incidents and 18.6% of breached records[1]. For example, in recent years notable SQLi data breaches have varied from massive credit card breaches, large scale targeted attacks against universities and government agencies, as well as election related web servers and databases.

Preffered attack vectors by hackers[2]

38% XSS

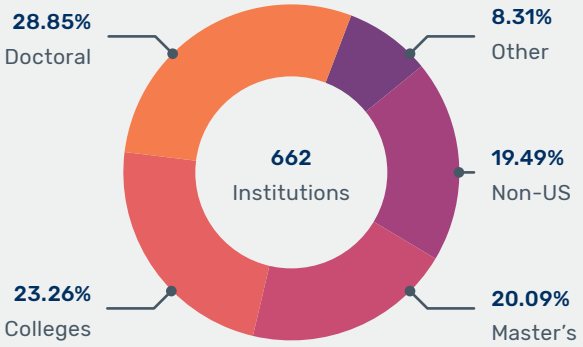
14% SQLi

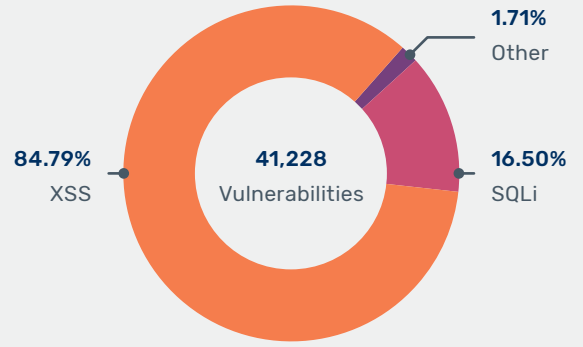
Say hello to Dorkbot.

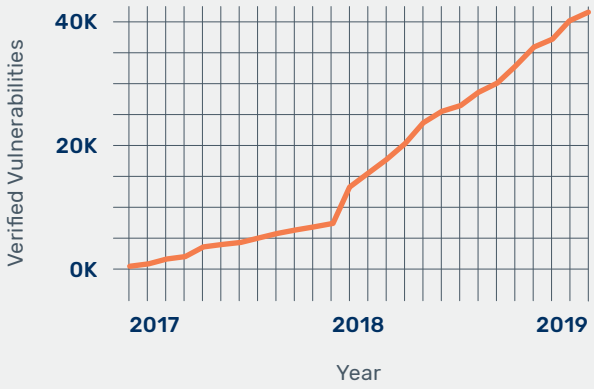
Built by The University of Texas at Austin Information Security Office, Dorkbot automates the discovery and verification of web application vulnerabilities across entire domains at scale. Specifically, Dorkbot hunts for SQLi, XSS, and other less common vulnerabilities, leveraging search engine cache and other public sources of indexed sites. Once identified vulnerabilities are verified, notices with remediation instructions are automatically sent to your security inbox. Since its launch over 2 years ago, Dorkbot coverage has grown to over 1000 institutions including 84% of the largest doctoral research institutions in the US.

"Dorkbot gives us good validation of what we do in house and augments our efforts by doing additional scans that we wish we had the time to do on an ongoing basis."

Security Analyst at Large Northeastern University







1. Verizon Data Breach Investigation Report (DBIR) 2018
2. The 2019 Hacker Report by hackerone

Ready to put Dorkbot to work at your organization? Contact us at **info@saltycloud.com**.

