Mahmud Hasan Sizan

OFFENSIVE SECURITY RESEARCHER · BUG BOUNTY HUNTER

mahmudhasan3801@gmail.com · hackerone.com/twistedmock · bugcrowd.com/twistedmock
github.com/Twistedmock · linkedin.com/in/twistedmock · Remote worldwide or relocating · GMT+6

Top-1,000 all-time researcher on **HackerOne** with six years hunting web-application vulnerabilities. **102 reports resolved** across **67 programs**, 100+ paid bounties, and **HackerOne Clear** (background-checked). **84% of my reputation sits in 28 private, invitation-only programs** — including one where I rank **#1 of every hunter on it**. Publicly credited by **Apple, Goldman Sachs, SpaceX, GitHub** and **Adobe**.

3,447	#807	102	67	100+	81st	84th	6 yrs
REPUTATION	GLOBAL RANK · TOP 1,000	REPORTS RESOLVED	PROGRAMS	PAID BOUNTIES	SIGNAL PERCENTILE	IMPACT PERCENTILE	HUNTING

PLATFORMS

HackerOne — twistedmock
3,447 reputation · rank #807 · 102 resolved · 67 programs · signal 81st / impact 84th percentile · HackerOne Clear · 18 badges across 6 OWASP categories. **28 private programs hold 2,896 reputation (84%)**, including a flagship where I am **#1 overall — 48 valid reports of 94, 1,075 reputation**.

Bugcrowd — twistedmock
64 valid findings · rank #2,381 · 86% accuracy. Public hall of fame at SpaceX/Starlink, Atlassian, Twilio, Bitdefender, Coca-Cola, United Airlines, Lenovo, Ibotta, Monash University and the U.S. Dept. of Veterans Affairs.

PUBLIC ACKNOWLEDGEMENTS

—**Apple** — credited ×3 in official security acknowledgements (Feb 2026, Aug 2025, Jul 2025).

—**Goldman Sachs** — two bounties awarded, May 2026.

—**GitHub** — report resolved 2021; GitHub Security Researcher.

—**Adobe** — 5 valid reports (4 resolved in six weeks, 2023).

—**30+ HackerOne programs** — incl. PayPal, Palantir, Databricks, Hostinger, Stellar, UPS, Xiaomi, Roblox, Spotify, Kubernetes.

FOCUS AREAS

—**Broken Access Control** — IDOR, privilege escalation.

—**Injection** — SQL and command injection.

—**Cross-Site Scripting** — stored, reflected, DOM-based.

—**Broken Authentication** — session & identity, account takeover.

—**XML External Entities** & **Security Misconfiguration**.

Web Application Security | Recon at scale | API testing | Attack-surface mapping

TOOLING (open source, Rust)

—**qshodan** — extracts hosts from Shodan, defeating the 1,000-result cap by recursively subdividing queries.

—**qport** — passive port discovery via Shodan InternetDB; maps an estate without a packet touching the target.

—**Attack Surface Monitoring** (SaaS, in development) — Crunchbase, Shodan, Censys, crt.sh and Whoxy in one picture.

LANGUAGES

—**English** — IELTS 8.0 · **Bengali** (native) · **Hindi** · **Urdu**.

ROLES SOUGHT

Penetration testing · red teaming · application security · vulnerability research. Available now, full-time or contract.

Every figure is drawn from the HackerOne and Bugcrowd APIs (retrieved 15 August 2026) and each vendor's own acknowledgements page — not self-reported. Only public programs are named; private programs are withheld as their terms require. Portfolio: 144.91.96.148:7777