

Gabb1337

Security Researcher · Bug Bounty Hunter

Investigate the edge. Prove the impact.

Independent security research across applications, APIs, mobile clients, firmware and smart contracts. I combine code review, differential testing and reproducible proof of concept development, with explicit evidence boundaries.

RESEARCH FOCUS

APPLICATIONS & APIS

Object authorization, authentication, stored XSS and business logic.

IDENTITY & SESSIONS

Revocation, token renewal, devices and persistent channels.

MOBILE & SYSTEMS

Android, WebViews, SSRF, binary analysis and emulation.

SMART CONTRACTS

State and accounting invariants; Move and Solidity code review.

WORKING METHOD

1. Define scope, actors and the expected boundary.
2. Compare a baseline, negative control and narrow variant.
3. Record reproducible observations and limitations.
4. Deduplicate, report precisely and clean up.

KNOWLEDGE SYSTEM

Obsidian research notes connect hypotheses, session records, evidence and decisions to their sources.

Platform workflows: Bugcrowd · HackerOne · HackenProof

CONNECT

X / @Gabbsec1337

LinkedIn / gabb1337ro

GitHub / gabb1337sky

SELECTED RESEARCH

SEC-01 / OBJECT AUTHORIZATION

Project permissions across an integration

Controlled identities and private test objects were used to compare a host application's access rejection with an integration response. The reviewed records document a private-data read and a Bugcrowd submission.

Authenticated access is required. A recorded submission is not a claim of final acceptance or reward.

SEC-04 / SESSION LIFECYCLE

Revocation across credentials and channels

Differential tests compare behavior before and after a device revocation, with separate observations for sessions, renewal paths and established connections.

Validation is limited to a test environment; channel-specific observations are not generalized to production.

SEC-08 / FIRMWARE ANALYSIS

Following configuration data through a binary

A fixed firmware artifact and instrumented execution were used to reconstruct and observe a relevant binary path. Simulated dependencies and hardware-validation limits are recorded explicitly.

Emulation evidence is distinct from physical-device or over-the-air reproduction.

PUBLIC MATERIALS

The portfolio contains nine anonymized research files, three standalone teaching models and selected public research updates.

The lab uses synthetic data and runs locally in the browser or Node.js. It does not contact real targets or reproduce a private report.

Disclosure boundary. Program names, target identities, endpoints, payloads, credentials and original report evidence are withheld. Submission, duplicate and local-validation states are distinguished. No unverified award, severity or production-impact claim is implied.