Forum:Hack Forums

Thread: Python for Security Automation: Small Scripts With Real Value

watsica12 - *October 19, 2026, 2:24 am*

I've been looking at API security testing and realized that confirming whether a user can log in is only the beginning. Object-level authorization, excessive data exposure, rate limits, input validation, and inconsistent error handling can all create problems even when authentication works correctly. APIs also tend to evolve quickly, so a check that was valid several months ago might no longer cover the current endpoints or permissions.

OpenAPI specifications can help map available routes and expected request formats, while Burp Suite and OWASP ZAP can assist with authorized testing. I'm interested in turning those specifications into repeatable checks that can run during development and flag unexpected changes. The goal is to catch security regressions early rather than discovering them during a release review.

For developers and testers, which API security issues do you encounter most frequently? How do you test whether users can access only the objects and actions their roles permit? Are there particular ways to combine API specifications, integration tests, and security tools without producing a huge number of false alarms?