hackerone

# Top 5 Common Security Assessment Mistakes And How To Avoid Them

Security assessments play an important role in helping organizations determine their cybersecurity readiness and learn about security gaps that should top their priorities list.

Many HackerOne customers who run security assessments, either for the first time or on a regular basis, make the same common mistakes. The following explains what they are and how to avoid them.

### 1. Lack Internal Stakeholder Buy-In and Clear Goals for Testing

Security posture testing is difficult and requires internal stakeholder buy-in, clear engagement goals, and strong internal communication. Here are a few things that can help:

- Determine expected post-engagement key deliverables across documentation and reporting.
- Confirm points of contact across the key business, technology, and compliance teams.
- Establish a schedule and timeline that does not disrupt the business.

### 2. Testing in Isolation Without Scope and Business Alignment

Continually evaluate project scope to determine what's included or excluded as it may fluctuate throughout the planning and onboarding process. Ways to avoid scope misalignment:

- Review scope in the early stages when asset awareness and experience are new.
- Involve end application owners in determining scope upfront.
- Maintain a transparent approach and strategy from the outset.
- Include all information regarding asset identification and accessibility so teams understand the testing requirements and can adequately prepare.

### 3. Lack of Communication with Ethical Hackers and Testing Participants

We often see heavy involvement during the security assessment sales and onboarding process, but this wanes after testing begins. Teams may be initially focused on meeting a vendor or customer requirement and are ultimately waiting for a final report. Maintaining communication throughout the process is important because:

- Engagements involving communicative, eager participants are more likely to end in a positive result.
- Hackers often have questions about the testing environment or accessing the application.
- Hackers perform better when they feel supported and have clarity on points of contact, testing expectations, and questions.
- Product and development teams can be prepared for remediation when internal teams have escalation procedures and clear communication channels.

### 4. Failure to Prioritize Remediation Workflows

It's important to incorporate vulnerability remediation follow-up activities and longer-term risk-reduction solutions into the testing process. Here's how to avoid tasks falling off priority lists and timeline delays:

- Task specific team members to act on final reports.
- Create a documented plan of action for triage and remediation post-engagement.
- Ensure participants are free of conflicts of interest and committed to the security assessment's goals.
- Allow hackers to integrate into the development process.

### 5. Approaching a Security Assessment as a Box to be Checked

Companies with a "check the box" mindset typically see testing as a waste of time and will try to rush through it by any means necessary. This approach results in the same mistakes mentioned above. Avoid this by following the above advice and look for opportunities to add value:

- Get endorsement from internal stakeholders and create awareness on test timelines.
- Approach testing as an opportunity to improve your security posture.
- Standardize the testing process throughout kick-off, testing, and remediation phases and make it repeatable.

Have an upcoming security assessment? Don't make these mistakes. Get in contact here to schedule a demo and learn more about HackerOne's testing approach.