THE STATE OF PENTESTING 2023 Download the Report Here

Cobalt

# Pentest Preparation Checklist

Practical steps on how to prepare for each test and extract maximum value, guided by insights from the Cobalt Core — our community of 400+ skilled and vetted pentesting professionals.

## Setting the pentest's objective and scope (pg 21)

- [ ] 1) Align all internal stakeholders on what the goal of your pentest is and what assets should be in scope.
- [ ] 2) Describe the in-scope assets with information on endpoints, URLs, number of static and dynamic pages.
- [ ] 3) Include information on the complexity of your asset, covering the questions we suggest on page 21 of The State of Pentesting 2023.

## Familiarize the pentesters with how things are supposed to work (pg 22)

- [ ] 4) Decide if you want to have a black-, gray-, or white-box pentest.
- [ ] 5) If you want a gray- or white-box pentest, share documentation (walkthrough videos, demos, process diagrams, data flow charts, user role breakdowns, access control matrices) on how your asset(s) are built, how they are meant to function, where data flows, etc.

## Prepare a staging environment and your colleagues for the test (pg 23)

- [ ] 6) Set up a mirror image of your production environment and back up critical data.
- [ ] 7) Set up and share credentials with the testers.
- [ ] 8) Whitelist pentesters' IP addresses.
- [ ] 9) Inform affected colleagues a pentest will take place and which IP addresses will be making requests.

## Collaborate with the pentesters for a more productive test and better insights into your vulnerabilities (pg 24)

- [ ] 10) Establish a point of contact (POC) from your team who can liaison with the testers.
- [ ] 11) That POC should be responsive to the results of a pentest, analyze results, and ask questions if more info is needed.
- [ ] 12) The POC should also be available to help remove blockers slowing down the testers.