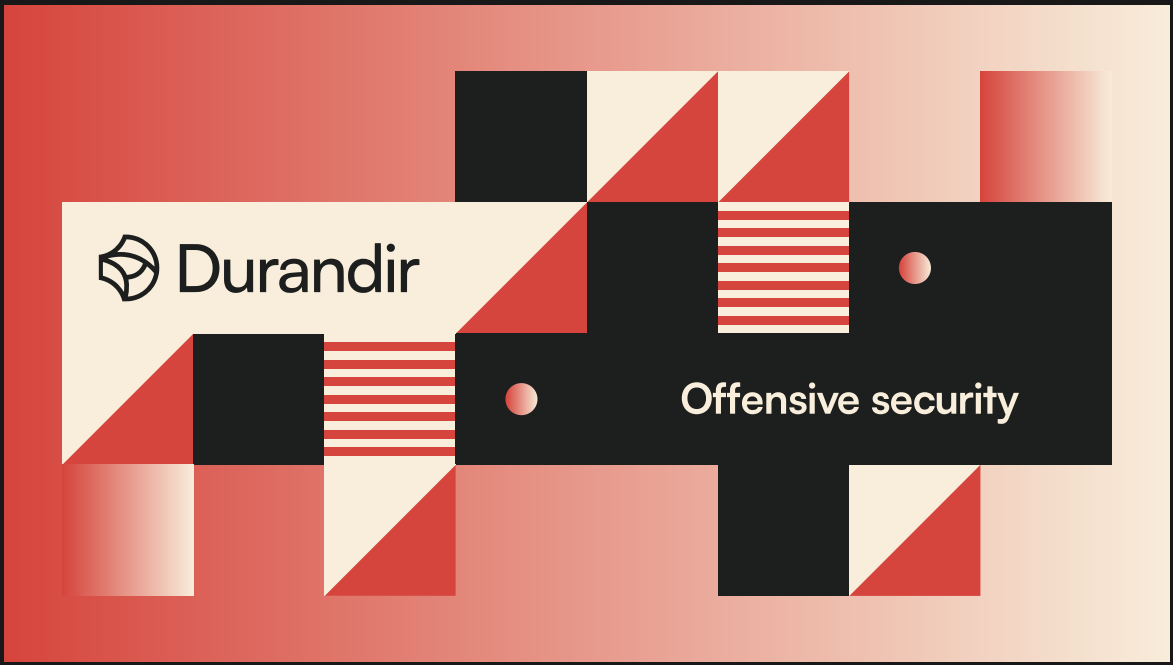
Offensive security



Published	Nov 13, 2026
Last updated	Nov 16, 2026
Category	Research

How attackers get in, and how to find and prove it before they do.

Our team carries out authorised security assessments and builds the software it uses for them. Research in this area goes into Durandir Cybersecurity and into our Red team engagements.

What we study

- Vulnerability discovery in websites, APIs and networks, from access control and injection to server-side request forgery and path traversal.
- Verification: confirming that a finding is real and reproducible before it reaches a report, so that teams do not chase false positives.
- Attack chains: how small weaknesses combine into real impact, mapped to MITRE ATT&CK.
- Reporting: findings that state the impact, the evidence and the fix in terms the people who must act can use.

How we work

All of this work happens within a written scope and an authorisation, following recognised methodologies such as the OWASP Web Security Testing Guide, NIST SP 800-115 and PTES. Our responsible use commitments apply to our own work as much as to our customers.