A

API HACKING CHECKLIST

Testing Approach (see Chapter 0)

- ☐ Determine approach: black box, gray box, or white box? (pages 4–6)

Passive Reconnaissance (see Chapter 6)

- ☐ Conduct attack surface discovery (pages 124–132)
- ☐ Check for exposed secrets (pages 133–136)

Active Reconnaissance (see Chapter 6)

- ☐ Scan for open ports and services (page 138)
- ☐ Use the application as intended (page 137)
- ☐ Inspect web application with DevTools (pages 139–142)
- ☐ Search for API-related directories (pages 143–146)
- ☐ Discover API endpoints (pages 146–148)

Endpoint Analysis (see Chapter 7)

- ☐ Find and review API documentation (pages 156–159)
- ☐ Reverse engineer the API (pages 161–164)
- ☐ Use the API as intended (pages 167–168)
- ☐ Analyze responses for information disclosures, excessive data exposures, and business logic flaws (pages 169–174)

Authentication Testing (see Chapter 8)

- ☐ Conduct basic authentication testing (pages 180–186)
- ☐ Attack and manipulate API tokens (pages 187–197)

Conduct Fuzzing (see Chapter 9)

- ☐ Fuzz all the things (pages 202–218)

Authorization Testing (see Chapter 10)

- ☐ Discover resource identification methods (pages 224–225)
- ☐ Test for BOLA (pages 225–227)
- ☐ Test for BFLA (pages 227–230)

Mass Assignment Testing (see Chapter 11)

- ☐ Discover standard parameters used in requests (pages 238–240)
- ☐ Test for mass assignment (pages 240–243)

Injection Testing (see Chapter 12)

- ☐ Discover requests that accept user input (page 250)
- ☐ Test for XSS/XAS (pages 251–253)
- ☐ Perform database-specific attacks (pages 253–259)
- ☐ Perform operating system injection (pages 259–260)

Rate Limit Testing (see Chapter 13)

- ☐ Test for the existence of rate limits (page 276)
- ☐ Test for methods to avoid rate limits (pages 276–278)
- ☐ Test for methods to bypass rate limits (pages 278–284)

Evasive Techniques (see Chapter 13)

- ☐ Add string terminators to attacks (pages 270–271)
- ☐ Add case switching to attacks (pages 271–272)
- ☐ Encode payloads (page 272)
- ☐ Combine different evasion techniques (pages 273–275)
- ☐ Rinse and repeat or apply evasive techniques to all previous attacks (page 322)