A

API HACKING CHECKLIST

Testing Approach (see Chapter 0)

- Determine approach: black box, gray box, or white box?

Passive Reconnaissance (see Chapter 6)

- Conduct attack surface discovery
- Check for exposed secrets

Active Reconnaissance (see Chapter 6)

- Scan for open ports and services
- Use the application as intended
- Inspect web application with DevTools
- Search for API-related directories
- Discover API endpoints

Endpoint Analysis (see Chapter 7)

- Find and review API documentation
- Reverse engineer the API
- Use the API as intended
- Analyze responses for information disclosures, excessive data exposures, and business logic flaws

Authentication Testing (see Chapter 8)

- Conduct basic authentication testing
- Attack and manipulate API tokens

Conduct Fuzzing (see Chapter 9)

- Fuzz all the things

Authorization Testing (see Chapter 10)

- Discover resource identification methods
- Test for BOLA
- Test for BFLA

Mass Assignment Testing (see Chapter 11)

- Discover standard parameters used in requests
- Test for mass assignment

Injection Testing (see Chapter 12)

- Discover requests that accept user input
- Test for XSS/XAS
- Perform database-specific attacks
- Perform operating system injection

Rate Limit Testing (see Chapter 13)

- Test for the existence of rate limits
- Test for methods to avoid rate limits
- Test for methods to bypass rate limits

Evasive Techniques (see Chapter 13)

- Add string terminators to attacks
- Add case switching to attacks
- Encode payloads
- Combine different evasion techniques
- Rinse and repeat or apply evasive techniques to all previous attacks