KaozhengPro

IT認證考試題庫

專業平臺

考證寶提供最新考古題與模擬試題
協助您高效通過認證考試

www.kaozhengpro.com

Exam : **C-APIPen**

Title : Certified API Pentester (C-APIPen)

Version : DEMO

1.Locate potential sensitive operations in a Swagger (OpenAPI) definition.
A. See the Explanation.
Answer: A
Explanation:
1. Download the Swagger JSON/YAML file from the API documentation or endpoint (e.g., /v2/api-docs).
2. Open the file in Swagger Editor (https://editor.swagger.io/).
3. Search for HTTP methods like DELETE, PUT, and POST.
4. Focus on endpoints such as /admin, /users/{id}, or anything with role/permission keywords.
5. Document any endpoints that can change, delete, or expose sensitive data for further testing.

2.Use Swagger UI to execute a GET request and analyze the response for excessive data exposure.
A. See the Explanation.
Answer: A
Explanation:
1. Open the Swagger UI interface for the target API.
2. Locate a GET endpoint like /users, /accounts, or /orders.
3. Click “Try it out” and execute the request.
4. Inspect the returned JSON for internal fields like passwordHash, token, or internalId.
5. Report any unnecessary sensitive fields returned to unauthenticated users.

3.Identify broken access control by testing role-protected endpoints via Swagger.
A. See the Explanation.
Answer: A
Explanation:
1. Use Swagger UI and authenticate as a low-privileged user (e.g., via Bearer Token).
2. Try accessing endpoints like /admin/users, /config, or /roles.
3. Execute GET, PUT, or DELETE methods.
4. Check if you receive a 200 OK instead of 403 Forbidden.
5. If successful, document the broken access control for reporting.

4.Modify and test query parameters to check for SQL Injection via Swagger.
A. See the Explanation.
Answer: A
Explanation:
1. Open Swagger UI and locate endpoints with query parameters (e.g., /search?name=).
2. Click “Try it out” and enter payloads like ' OR 1=1-- or ' UNION SELECT NULL--.
3. Execute the request and observe the response.
4. Look for errors like SQL syntax, unclosed quotation, or unexpected data returns.
5. Log successful payloads as injection vectors.

5.Discover undocumented endpoints using the Swagger file structure.
A. See the Explanation.
Answer: A
Explanation:

1. Download the Swagger JSON file.
2. Look for $ref references that point to external paths or schemas.
3. Manually follow these references to hidden or extended files.
4. Also inspect custom tags or vendor extensions like x-internal.
5. Use curl or Postman to test discovered paths for valid responses.