API Security Checklist

Object level authorization - OWASP - A1

1. Verify that implement authorization checks with user policies and hierarchy
2. Verify that API implementation is not rely on IDs sent from client , instead API should check IDs stored object in the session.
3. Verify that server configuration is hardened as per the recommendation of the application server and framework in use.
4. Verify that , API implementation check authorization each time there is a client request to access database.
5. Verify that API is not using random guessable IDs (UUIDs)

Brocken authentication - OWASP - A2

1. Verify all possible ways to authenticate all APIs
2. Verify password reset APIs and one-time links also allow users to get authenticated and should be strictly protected.
3. Verify API implements standards authentication , token generation, password storage and Multi factor authentication.
4. Verify , API uses short lived access token.
5. Verify that , API uses stricter rate-limiting for authentication , implement lockout polices and weak password checks.

Excessive data exposure - OWASP - A3

1. Verify that , API is not relying on client to filter data.
2. Verify API responses and adapt response to what the API consumers really need.
3. Verify API specification define schemas of all request and responses.
4. Verify error API responses are clearly defined.
5. Verify that all the sensitive or PII information are used with clear justification.
6. Verify APIs enforced response checks to prevent accidental data and exception leaks.

Lack of resources and rate limiting - OWASP - A4

1. Verify that , rate limiting is configured considering API method , client and addresses.

2. Verify payload limit is configured,.
3. Verify compression ration while implementing rate limiting.
4. Verify rate limiting in the context of computing / container resources

Brocken functional level authorization - OWASP - A5

1. Verify , by default all access are denied
2. Verify that , API is not relying on App to enforce admin access
3. Verify , all the unnecessary features are disabled.
4. Verify rate limiting in the content of computing/container resources
5. Ensure roles are granted only based on specific role.
6. Verify authorization are implemented correctly in API.

Mass assignment- OWASP - A6

1. Verify API is not automatically bind incoming data and internal objects.
2. Verify API is not explicitly define all the parameters and payload you are expecting.
3. Verify that , for object schemas use the readOnly set to true for all properties that can be retrieved via APIs but should never be modified.
4. Verify that APIs are precisely define at design time the schemas , types, patterns you will accept in the requests and enforces them at runtime.

Security misconfiguration - OWASP - A7

1. Verify that APIs implementation are repeatable & hardening and patching activities are incorporated in development process
2. Verify that API ecosystem has automated process to locate configuration flaws.
3. Verify that , platform disabled unnecessary features in any API.
4. Verify that , platform restrict administrative access.
5. Ensure , define and enforce all outputs including errors .
6. Verify authorization are implemented correctly in API.

Injection OWASP - A8

1. Verify that , API are not trusting your API consumers even if internal.

2. Verify API are strictly define all input data : schemas , types , string patterns - and enforce them at runtime.
3. Verify that APIs are validating, filtering & sanitizing all incoming data.
4. Verify that APIs are define , limit and enforce API outputs to prevent data leaks.

Improper asset management - OWASP - A9

1. Verify platform capability document / inventory all API hosts.
2. Verify platform limit access to anything that should not be public.
3. Verify platform limit access to production data. Saggregate access to production and non-production data.
4. Verify , architecture implement additional external controls such as API firewall.
5. Verify that a process is considered for properly retire old versions or backport security fixes
6. Verify architecture implements strict authentication , redirects , CORs etc.

Insufficient Logging & Monitoring OWASP - A10

1. Verify API Log failed attempts , denied access , input validation failure any failure in security policy checks.
2. Verify platform ensure that logs are formatted to be consumable by other tools.
3. Verify that platform protects logs as highly sensitive.
4. Verify that platform include enough details to identify attackers.
5. Verify platform integrate with SIEM and other dashboards , monitoring alerting tools.