APIsec

PENETRATION TESTING REPORT

Penetration Testing Report

Application: **spotify**

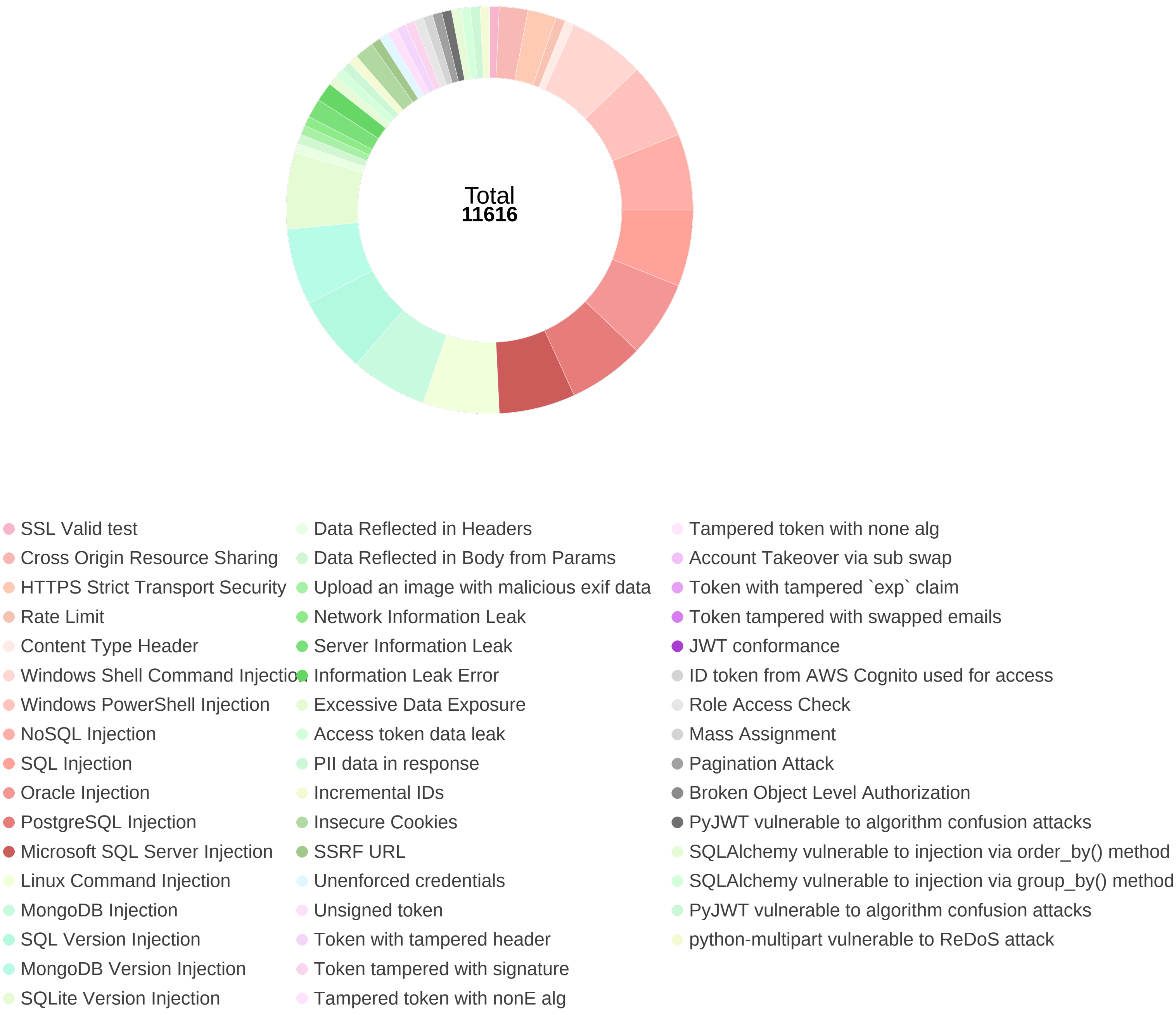
Instance: **https://api.spotify.com/v1**

Endpoints: **88**

Tests Generated: **11616**

Vulnerabilities: **1**

Coverage Overview



Vulnerabilities

Method	Endpoint	Category	Test Type	CVSS Score	Severity	Age(In days)	Status
GET	/browse/featured-playlists	Denial Of Service	Pagination Attack	CVSS:7.5	HIGH	-	RESOLVED
GET	/users/{user_id}/playlists	Indirect Object Reference	Incremental IDs	CVSS:5	MEDIUM	-	ACTIVE

Endpoints

Method	Endpoint	Sensitivity
GET	/users/{user_id}	CRITICAL
GET	/users/{user_id}/playlists	CRITICAL
POST	/users/{user_id}/playlists	CRITICAL
GET	/episodes/{id}	LOW
GET	/episodes	LOW
GET	/me/episodes	LOW
PUT	/me/episodes	LOW
DELETE	/me/episodes	LOW
GET	/me/episodes/contains	LOW
GET	/search	LOW
GET	/tracks/{id}	LOW
GET	/tracks	LOW
GET	/me/tracks	LOW
PUT	/me/tracks	LOW
DELETE	/me/tracks	LOW
GET	/me/tracks/contains	LOW
GET	/audio-features	LOW
GET	/audio-features/{id}	LOW
GET	/audio-analysis/{id}	LOW
GET	/recommendations	LOW

Method	Endpoint	Sensitivity
GET	/recommendations/available-genre-seeds	LOW
GET	/me	LOW
GET	/me/top/{type}	LOW
PUT	/playlists/{playlist_id}/followers	LOW
DELETE	/playlists/{playlist_id}/followers	LOW
GET	/me/following	LOW
PUT	/me/following	LOW
DELETE	/me/following	LOW
GET	/me/following/contains	LOW
GET	/playlists/{playlist_id}/followers/contains	LOW
GET	/chapters/{id}	LOW
GET	/chapters	LOW
GET	/shows/{id}	LOW
GET	/shows	LOW
GET	/shows/{id}/episodes	LOW
GET	/me/shows	LOW
PUT	/me/shows	LOW
DELETE	/me/shows	LOW
GET	/me/shows/contains	LOW
GET	/audiobooks/{id}	LOW
GET	/audiobooks	LOW
GET	/audiobooks/{id}/chapters	LOW
GET	/me/audiobooks	LOW
PUT	/me/audiobooks	LOW
DELETE	/me/audiobooks	LOW
GET	/me/audiobooks/contains	LOW
GET	/playlists/{playlist_id}	LOW

Method	Endpoint	Sensitivity
PUT	/playlists/{playlist_id}	LOW
GET	/playlists/{playlist_id}/tracks	LOW
POST	/playlists/{playlist_id}/tracks	LOW
PUT	/playlists/{playlist_id}/tracks	LOW
DELETE	/playlists/{playlist_id}/tracks	LOW
GET	/me/playlists	LOW
GET	/browse/featured-playlists	LOW
GET	/browse/categories/{category_id}/playlists	LOW
GET	/playlists/{playlist_id}/images	LOW
PUT	/playlists/{playlist_id}/images	LOW
GET	/artists/{id}	LOW
GET	/artists	LOW
GET	/artists/{id}/albums	LOW
GET	/artists/{id}/top-tracks	LOW
GET	/artists/{id}/related-artists	LOW
GET	/browse/categories	LOW
GET	/browse/categories/{category_id}	LOW
GET	/markets	LOW
GET	/me/player	LOW
PUT	/me/player	LOW
GET	/me/player/devices	LOW
GET	/me/player/currently-playing	LOW
PUT	/me/player/play	LOW
PUT	/me/player/pause	LOW
POST	/me/player/next	LOW
POST	/me/player/previous	LOW
PUT	/me/player/seek	LOW

Method	Endpoint	Sensitivity
PUT	/me/player/repeat	LOW
PUT	/me/player/volume	LOW
PUT	/me/player/shuffle	LOW
GET	/me/player/recently-played	LOW
GET	/me/player/queue	LOW
POST	/me/player/queue	LOW
GET	/albums/{id}	LOW
GET	/albums	LOW
GET	/albums/{id}/tracks	LOW
GET	/me/albums	LOW
PUT	/me/albums	LOW
DELETE	/me/albums	LOW
GET	/me/albums/contains	LOW
GET	/browse/new-releases	LOW

Vulnerability by OWASP Categories

OWASP Coverage	Vulnerabilities	CVSS Score
Broken Object Level Authorization	1	CVSS : 5
Broken Authentication	-	-
Broken Object Property Level Authorization	-	-
Unrestricted Resource Consumption	-	CVSS : 7.5
Broken Function Level Authorization	-	-
Unrestricted Access to Sensitive Business Flows	-	-
Server Side Request Forgery	-	-
Security Misconfiguration	-	-
Improper Inventory Management	-	-

OWASP Coverage	Vulnerabilities	CVSS Score
Unsafe Consumption of APIs	-	-
Injection	-	-

Remediations

Category	Test Type	Remediation
Pagination Attack	Denial Of Service	The API's response time to this request was higher than usual. The average response time during the dry run was 34.5 ms, while the response time to this request was 64.0. This suggests that the API may have been vulnerable to this test's pagination exploit. The test sent a request with the following query parameters: * limit: 1000000 * offset: 1 Threat actors can take advantage of this vulnerability to bring down your service availability.
Incremental IDs	Indirect Object Reference	Do not use integer-based, auto-incremental identifiers such as those generated by SQL databases by default on primary key columns. Instead, use alternative identifiers such as UUIDs. If that's not possible, consider using a method for masking the primary key value, such as [Sqids](https://sqids.org/).

About APIsec Inc.

APIsec is built to address fundamental security challenges - APIs are breached on a scale never seen before with web and mobile applications. Attackers abuse business logic flaws and loopholes in APIs to expose and exploit the sensitive data of millions of people across the globe every year. APIsec addresses the critical need to secure APIs before they reach production, providing the industry's only automated and continuous API security testing platform.