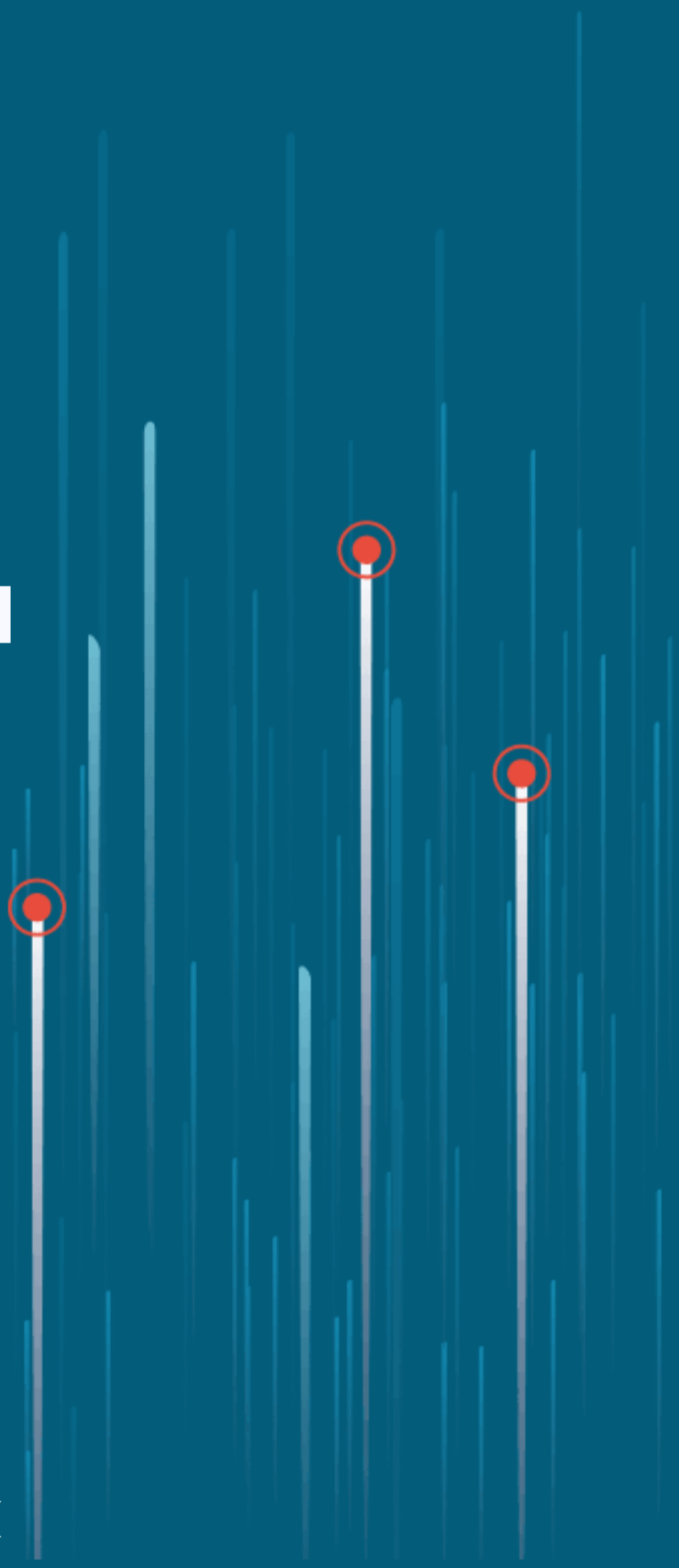
API PENETRATION TESTING REPORT



EthicalCheck

www.ethicalcheck.dev

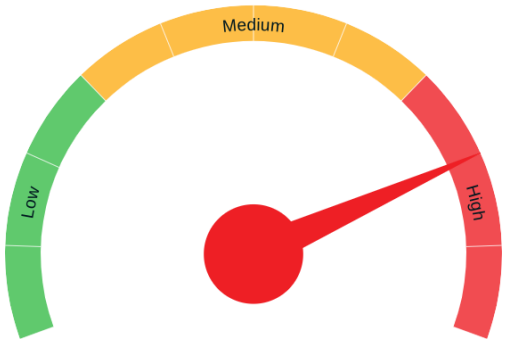
TABLE OF CONTENTS

This document is confidential and is a proprietary work product of APIsec Inc.
The information contained herein may not be copied or distributed without the specific written consent of APIsec Inc.
www.apisec.ai

Executive Summary

EthicalCheck : API Penetration Testing Report			
OAS URL	https://raw.githubusercontent.com/apisec-inc/Netbanking-Specs/main/ethicalcheck-netbanking-spec.json		
End Points	58	Security Tests	59
Vulnerabilities	5	Date	Apr 04, 2023
Review Required	3	Project Name	Online Banking REST API YaZd

Business Risk



High-security risk. Several critical and high severity and commonly exploited vulnerabilities are active.

Medium-security risk. Several high-severity and commonly exploited vulnerabilities are active.

Low-security risk. Several medium and low severity vulnerabilities that impact API availability and security are active.

Vulnerabilities by severity

Severity	Critical	High	Medium	Low
# of issues	4	0	1	0

Severity scoring

Critical - Immediate threat to key business processes

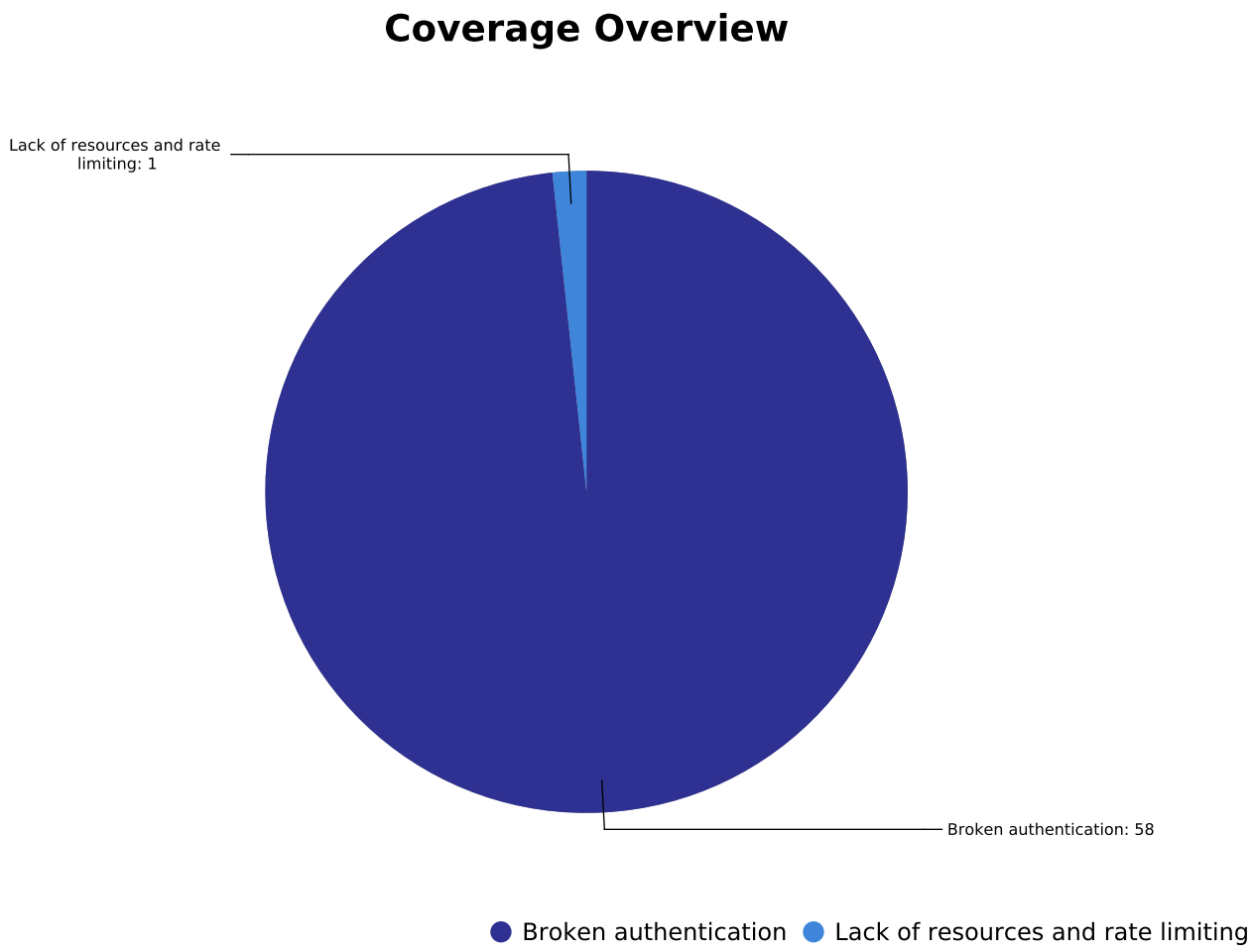
High - Direct threat to key business processes

Medium - Indirect threat to key business processes

Low - No direct threat exists

This document is confidential and is a proprietary work product of APIsec Inc.
The information contained herein may not be copied or distributed without the specific written consent of APIsec Inc.
www.apisec.ai

Coverage Overview



This chart aims in creating awareness for the project's risk coverage and test areas completion. APIsec aims at covering all the OWASP Top 10 security risks in its automated test cycles and being a stepping stone for development teams' cultural changes to ensure secure coding as a continuous process.

This document is confidential and is a proprietary work product of APIsec Inc.
The information contained herein may not be copied or distributed without the specific written consent of APIsec Inc.
www.apisec.ai

Discovered Vulnerabilities

S/N	OWASP	Category	Endpoint	CVSS 3.1	Severity	Logged on
1	#2	Broken authentication	DELETE:/api/v1/primary-transaction/{id}	9.1	Critical	Apr 04 2023
2	#2	Broken authentication	PUT:/api/v1/primary-transaction	9.1	Critical	Apr 04 2023
3	#2	Broken authentication	GET:/api/v1/primary-transaction/{id}	9.1	Critical	Apr 04 2023
4	#2	Broken authentication	GET:/api/v1/primary-transaction	9.1	Critical	Apr 04 2023
5	#4	Lack of resources and rate limiting	GET:/api/v1/transfers	6.5	Medium	Apr 04 2023

This document is confidential and is a proprietary work product of APIsec Inc.
The information contained herein may not be copied or distributed without the specific written consent of APIsec Inc.
www.apisec.ai

Review/False-Positives

False-Positives occurs when an AI Bot flags a security vulnerability, It needs to reviewed/validated whether it is a true vulnerability.

S/N	OWASP	Category	Endpoint	AI comment	Logged on
1	#2	Broken authentication	POST:/api/v1/users/team-sign-up	Failed	Apr 04 2023
2	#2	Broken authentication	POST:/api/v1/users/enterprise-sign-up	Failed	Apr 04 2023
3	#2	Broken authentication	POST:/api/v1/users/personal-sign-up	Failed	Apr 04 2023

This document is confidential and is a proprietary work product of APIsec Inc.
The information contained herein may not be copied or distributed without the specific written consent of APIsec Inc.
www.apisec.ai

Tested/Discovered Endpoints

S/N	Endpoint	Tested
1	POST : /api/v1/bank-account	OK
2	PUT : /api/v1/bank-account	OK
3	GET : /api/v1/bank-account	OK
4	PUT : /api/v1/bank-account/deposit-amount	OK
5	PUT : /api/v1/bank-account/withdraw-	OK
6	GET : /api/v1/bank-account/{id}	OK
7	DELETE : /api/v1/bank-account/{id}	OK
8	GET : /api/v1/branches	OK
9	POST : /api/v1/branches	OK
10	PUT : /api/v1/branches/update	OK
11	GET : /api/v1/branches/{id}	OK
12	DELETE : /api/v1/branches/{id}	OK
13	GET : /api/v1/orgs	OK
14	POST : /api/v1/orgs	OK
15	GET : /api/v1/orgs/allorgs	OK
16	GET : /api/v1/orgs/by-user	OK
17	GET : /api/v1/orgs/find-by-name/{name}	OK
18	GET : /api/v1/orgs/login-status	OK
19	GET : /api/v1/orgs/search	OK
20	GET : /api/v1/orgs/{branchId}/branch-user/	OK
21	POST : /api/v1/orgs/{branchId}/users/add-	OK
22	PUT : /api/v1/orgs/{branchId}/users/	OK
23	POST : /api/v1/orgs/{branchId}/users/	OK
24	GET : /api/v1/orgs/{id}	OK
25	PUT : /api/v1/orgs/{id}	OK
26	DELETE : /api/v1/orgs/{id}	OK
27	GET : /api/v1/orgs/{id}/users	OK
28	PUT : /api/v1/primary-account/deposit-	OK
29	POST : /api/v1/primary-account/primary-	OK
30	GET : /api/v1/primary-account/primary-	OK
31	PUT : /api/v1/primary-account/primary-	OK

This document is confidential and is a proprietary work product of APIsec Inc.
The information contained herein may not be copied or distributed without the specific written consent of APIsec Inc.
www.apisec.ai

Tested/Discovered Endpoints

S/N	Endpoint	Tested
32	GET : /api/v1/primary-account/primary-	OK
33	DELETE : /api/v1/primary-account/primary-	OK
34	PUT : /api/v1/primary-account/withdraw-	OK
35	PUT : /api/v1/primary-transaction	X
36	GET : /api/v1/primary-transaction	X
37	POST : /api/v1/primary-transaction	OK
38	GET : /api/v1/primary-transaction/{id}	X
39	DELETE : /api/v1/primary-transaction/{id}	X
40	GET : /api/v1/savings-account/savings-	OK
41	POST : /api/v1/savings-account/savings-	OK
42	PUT : /api/v1/savings-account/savings-	OK
43	GET : /api/v1/savings-account/savings-	OK
44	DELETE : /api/v1/savings-account/savings-	OK
45	PUT : /api/v1/savings-transaction	OK
46	GET : /api/v1/savings-transaction	OK
47	POST : /api/v1/savings-transaction	OK
48	DELETE : /api/v1/savings-transaction/{id}	OK
49	GET : /api/v1/savings-transaction/{id}	OK
50	GET : /api/v1/transfers	X
51	PUT : /api/v1/transfers	OK
52	POST : /api/v1/transfers	OK
53	GET : /api/v1/transfers/{id}	OK
54	DELETE : /api/v1/transfers/{id}	OK
55	POST : /api/v1/users/enterprise-sign-up	OK
56	POST : /api/v1/users/personal-sign-up	OK
57	GET : /api/v1/users/status	OK
58	POST : /api/v1/users/team-sign-up	OK

This document is confidential and is a proprietary work product of APIsec Inc.
The information contained herein may not be copied or distributed without the specific written consent of APIsec Inc.
www.apisec.ai

Tested Categories

OWASP Coverage

This document is confidential and is a proprietary work product of APIsec Inc.
The information contained herein may not be copied or distributed without the specific written consent of APIsec Inc.
www.apisec.ai

Remediations

Lack of resources and rate limiting

Based on the business need of the company, the following RateLimiting techniques may be employed.

- User Rate Limiting: Associating the number of user requests made either from their API Key or IP address.
- Geographic Rate Limiting: Rate limits can be set for particular regions and particular time periods.
- Server Rate Limiting: Rate limits can be set on server level basis to ensure servers handle certain aspects of application.

Broken authentication

The following techniques may be utilized for having Secured Endpoints [3][5][6].

- Session Management and Authentication
- API Keys
- OpenID Connect, OAuth2, and SAML
- Access Controls
- Rate Limits
- Input Validation and HTTP Return Codes

This document is confidential and is a proprietary work product of APIsec Inc.
The information contained herein may not be copied or distributed without the specific written consent of APIsec Inc.
www.apisec.ai

About APIsec Inc.

APIsec is build to address fundamental security challenge - 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.

APIsec offers

Continuous Security

Continuous testing that keeps up with Development

Automated Testing

Automated test creation ensures APIs are fully examined

Complete Coverage

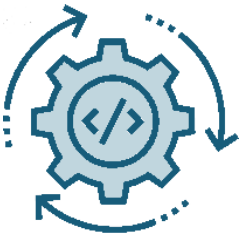
Tests every endpoint and method against OWASP risks

Speed

Executes complete API test suites in minutes

BUSINESS VALUE

Compliance mandate



Secure Releases

Avoid Manual Security Penetration Effort

This document is confidential and is a proprietary work product of APIsec Inc.
The information contained herein may not be copied or distributed without the specific written consent of APIsec Inc.
www.apisec.ai