OPIVM - Vulnerability Report

Date: 13-08-2024 17:31

Host Scopes:

- localhost:81
- localhost:8000
- localhost:8001

API Scopes:

No	Method	URL	Query Params	Body Params
1	GET	http://localhost:81/	name	None
2	GET	http://localhost:8000/api/xssnovuln	None	None
4	GET	http://localhost:8000/api/lfinovuln	None	None
5	POST	http://localhost:8000/api/lfivuln	None	filename type: JSON
6	GET	http://localhost:8000/api/rfinovuln	None	None
7	POST	http://localhost:8000/api/rfivuln	None	imagelink type: JSON
8	GET	http://localhost:8000/api/hhinovuln	None	None
9	POST	http://localhost:8000/api/hhivuln	None	email type: JSON
10	GET	http://localhost:8000/api/sstinovuln	None	None
11	POST	http://localhost:8000/api/sstivuln	None	mathexp type: JSON
12	GET	http://localhost:8000/api/sqlinovuln	None	None
13	POST	http://localhost:8000/api/sqlivuln	None	password, username type: JSON
14	GET	http://localhost:8001/api/xssnovuln	None	None

No	Method	URL	Query Params	Body Params
15	POST	http://localhost:8001/api/xssreflected	None	username type: JSON
16	GET	http://localhost:8001/api/lfinovuln	None	None
17	POST	http://localhost:8001/api/lfivuln	None	filename type: JSON
18	GET	http://localhost:8001/api/rfinovuln	None	None
19	POST	http://localhost:8001/api/rfivuln	None	imagelink type: JSON
20	GET	http://localhost:8001/api/hhinovuln	None	None
21	POST	http://localhost:8001/api/hhivuln	None	email type: JSON
22	GET	http://localhost:8001/api/sstinovuln	None	None
23	POST	http://localhost:8001/api/sstivuln	None	mathexp type: JSON
24	GET	http://localhost:8001/api/sqlinovuln	None	None
25	POST	http://localhost:8001/api/sqlivuln	None	password, username type: JSON

Infrastructures Vulnerabilities

Target: http://localhost:8001

Host: 127.0.0.1

OS: Linux 2.6.32 (Accuracy: 100%)

Port: 8001 (vcom-tunnel)

- State: open
- Service: Werkzeug/2.3.8 Python/3.11.9

No vulnerabilities found.

Target: http://localhost:8000

Host: 127.0.0.1

OS: Linux 2.6.32 (Accuracy: 100%)

Port: 8000 (http-alt)

- State: open
- Service: Werkzeug/2.3.8 Python/3.11.9

No vulnerabilities found.

Target: http://localhost:81

Host: 127.0.0.1

OS: Linux 2.6.32 (Accuracy: 98%)

Port: 81 (http)

- State: open
- Service: Apache httpd 2.4.49

Vulnerabilities:

- References: CVE-2021-41773 (https://vulners.com/cve/CVE-2021-41773)
- References: CVE-2023-31122 (https://vulners.com/cve/CVE-2023-31122)
- References: CVE-2022-23943 (https://vulners.com/cve/CVE-2022-23943)
- References: CVE-2023-27522 (https://vulners.com/cve/CVE-2023-27522)
- References: CVE-2024-40898 (https://vulners.com/cve/CVE-2024-40898)
- References: CVE-2022-30556 (https://vulners.com/cve/CVE-2022-30556)
- References: CVE-2022-26377 (https://vulners.com/cve/CVE-2022-26377)
- References: CVE-2023-45802 (https://vulners.com/cve/CVE-2023-45802)
- References: CVE-2022-29404 (https://vulners.com/cve/CVE-2022-29404)
- References: CVE-2022-28615 (https://vulners.com/cve/CVE-2022-28615)
- References: CVE-2023-25690 (https://vulners.com/cve/CVE-2023-25690)
- References: CVE-2022-22720 (https://vulners.com/cve/CVE-2022-22720)
- References: CVE-2021-42013 (https://vulners.com/cve/CVE-2021-42013)
- References: CVE-2022-22719 (https://vulners.com/cve/CVE-2022-22719)
- References: CVE-2024-27316 (https://vulners.com/cve/CVE-2024-27316)
- References: CVE-2022-28330 (https://vulners.com/cve/CVE-2022-28330)
- References: CVE-2021-44224 (https://vulners.com/cve/CVE-2021-44224)
- References: CVE-2021-44790 (https://vulners.com/cve/CVE-2021-44790)
- References: CVE-2022-37436 (https://vulners.com/cve/CVE-2022-37436)
- References: CVE-2022-31813 (https://vulners.com/cve/CVE-2022-31813)
- References: CVE-2022-28614 (https://vulners.com/cve/CVE-2022-28614)
- References: CVE-2022-36760 (https://vulners.com/cve/CVE-2022-36760)
- References: CVE-2021-41524 (https://vulners.com/cve/CVE-2021-41524)
- References: CVE-2022-22721 (https://vulners.com/cve/CVE-2022-22721)
- References: CVE-2006-20001 (https://vulners.com/cve/CVE-2006-20001)

Application Vulnerabilities

ID	Vulnerability	URL	Method	Parameter	Payload
VULN-240813-0001	XSS	http://localhost:8000/api/sstivuln	post	`mathexp` JSON Body	`<script>alert()</script>`
VULN-240813-0002	XSS	http://localhost:8001/api/xssreflected	post	`username` JSON Body	`<script>alert()</script>`
VULN-240813-0003	XSS	http://localhost:8001/api/sstivuln	post	`mathexp` JSON Body	`<script>alert()</script>`
VULN-240813-0004	RFI	http://localhost:8000/api/rfivuln	post	`imagelink` JSON Body	`https://gritty.ninja`
VULN-240813-0005	RFI	http://localhost:8001/api/rfivuln	post	`imagelink` JSON Body	`https://gritty.ninja`
VULN-240813-0006	LFI	http://localhost:8000/api/lfivuln	post	`filename` JSON Body	`../../../../../../../etc/passwd`
VULN-240813-0007	LFI	http://localhost:8001/api/lfivuln	post	`filename` JSON Body	`../../../../../../../etc/passwd`
VULN-240813-0008	SQLI	http://localhost:8000/api/sqlivuln	post	`username` JSON Body	`' union select hex(123),hex(245) --`

ID	Vulnerability	URL	Method	Parameter	Payload
VULN-240813-0009	SQLI	http://localhost:8001/api/sqlivuln	post	`username` JSON Body	`' union select hex(123),hex(245) --`
VULN-240813-0010	SSTI	http://localhost:8000/api/sstivuln	post	`mathexp` JSON Body	`{{69*69}}`
VULN-240813-0011	SSTI	http://localhost:8001/api/sstivuln	post	`mathexp` JSON Body	`{{69*69}}`
VULN-240813-0012	HHI	http://localhost:8000/api/hhivuln	post	`?` Query	`Host: evil.com`
VULN-240813-0013	HHI	http://localhost:8001/api/hhivuln	post	`?` Query	`Host: evil.com`