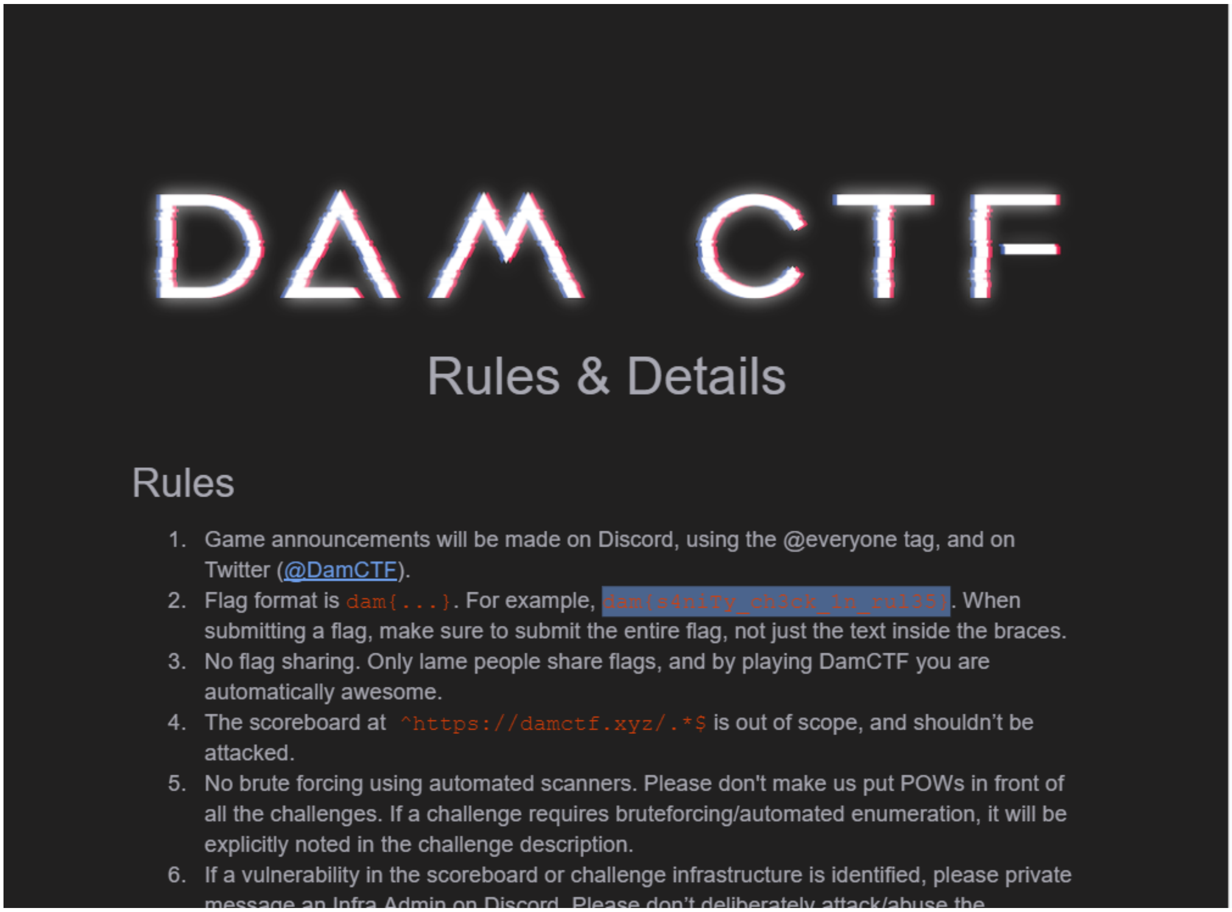
DAMCTF

Misc

rules

签到题，看rules就可以拿到flag



Rules & Details

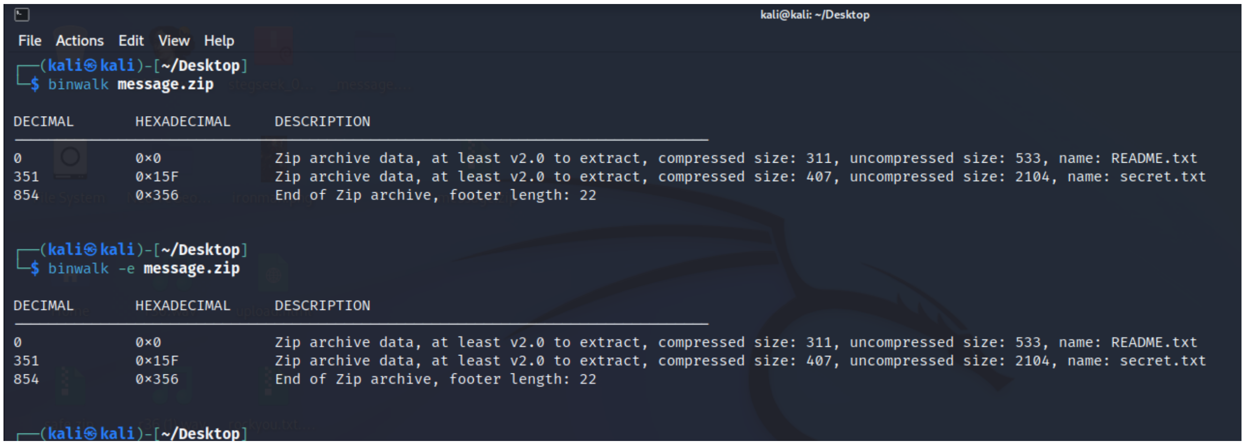
Rules

1. Game announcements will be made on Discord, using the @everyone tag, and on Twitter (@DamCTF).
2. Flag format is `dam{...}`. For example, `dam{s4niTy_ch3ck_1n_rul35}`. When submitting a flag, make sure to submit the entire flag, not just the text inside the braces.
3. No flag sharing. Only lame people share flags, and by playing DamCTF you are automatically awesome.
4. The scoreboard at `^https://damctf.xyz/.*$` is out of scope, and shouldn't be attacked.
5. No brute forcing using automated scanners. Please don't make us put POWs in front of all the challenges. If a challenge requires bruteforcing/automated enumeration, it will be explicitly noted in the challenge description.
6. If a vulnerability in the scoreboard or challenge infrastructure is identified, please private message an Infra Admin on Discord. Please don't deliberately attack/abuse the

misc

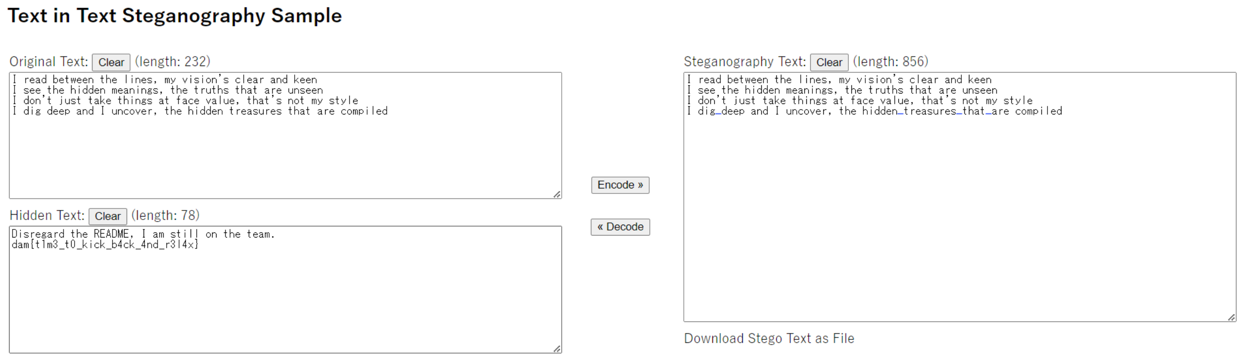
de-compressed

010发现隐藏的文件，提取压缩包，binwalk和foremost都没有成功，dd提取。



```
┌──(kali㉿kali)-[~/Desktop]
└─$ binwalk message.zip

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             Zip archive data, at least v2.0 to extract, compressed size: 311, uncompressed size: 533, name: README.txt
351           0x15F           Zip archive data, at least v2.0 to extract, compressed size: 407, uncompressed size: 2104, name: secret.txt
854           0x356           End of Zip archive, footer length: 22


┌──(kali㉿kali)-[~/Desktop]
└─$ binwalk -e message.zip

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             Zip archive data, at least v2.0 to extract, compressed size: 311, uncompressed size: 533, name: README.txt
351           0x15F           Zip archive data, at least v2.0 to extract, compressed size: 407, uncompressed size: 2104, name: secret.txt
854           0x356           End of Zip archive, footer length: 22


┌──(kali㉿kali)-[~/Desktop]
```

使用winrar修复，获得secret.txt，宽字节隐写。


Text in Text Steganography Sample
Clear
Encode »
« Decode
Download Stego Text as File

Original Text: (length: 232)

```
I read between the lines, my vision's clear and keen
I see the hidden meanings, the truths that are unseen
I don't just take things at face value, that's not my style
I dig deep and I uncover, the hidden treasures that are compiled
```

Hidden Text: (length: 78)

```
Disregard the README, I am still on the team.
dam{t1m3_t0_kick_b4ck_4nd_r3l4x}
```

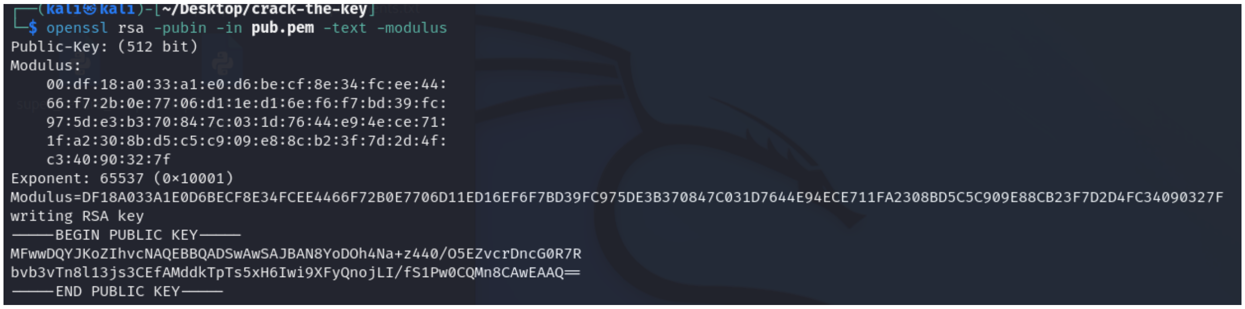
Steganography Text: (length: 856)

```
I read between the lines, my vision's clear and keen
I see the hidden meanings, the truths that are unseen
I don't just take things at face value, that's not my style
I dig deep and I uncover, the hidden treasures that are compiled
```

crypto

crack-the-key

openssl分析公钥证书

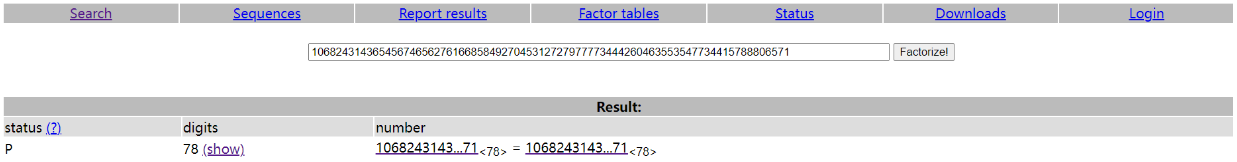


```
┌──(kali㉿kali)-[~/Desktop/crack-the-key]
└─$ openssl rsa -pubin -in pub.pem -text -modulus
Public-Key: (512 bit)
Modulus:
    00:df:18:a0:33:a1:e0:d6:be:cf:8e:34:fc:ee:44:
    66:f7:2b:0e:77:06:d1:1e:d1:6e:f6:f7:bd:39:fc:
    97:5d:e3:b3:70:84:7c:03:1d:76:44:e9:4e:ce:71:
    1f:a2:30:8b:d5:c5:c9:09:e8:8c:b2:3f:7d:2d:4f:
    c3:40:90:32:7f
Exponent: 65537 (0×10001)
Modulus=DF18A033A1E0D6BECF8E34FCEE4466F72B0E7706D11ED16EF6F7BD39FC975DE3B370847C031D7644E94ECE711FA2308BD5C5C909E88CB23F7D2D4FC34090327F
writing RSA key
-----BEGIN PUBLIC KEY-----
MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAN8YoDOh4Na+z440/O5EZvcrDncG0R7R
bvb3vTn8l13js3CEfAMddkTpTs5xH6Iwi9XFyQnojLI/fS1Pw0CQMn8CAwEAAQ==
-----END PUBLIC KEY-----
```

e是65537

16进制的n：DF18A033A1E0D6BECF8E34FCEE4466F72B0E7706D11ED16EF6F7BD39FC975DE3B370847C031D7644E94ECE711FA2308BD5C5C909E88CB23F7D2D4FC34090327F

10进制的n：116844958028890725852033105152500835722856580522709981530073782546945807066208375212876040892763414048682105946756274295080884310731251039134829262951020799



1068243143654567465627616685849270453127279777734442604635535477344157888806571

Result:		
status (?)	digits	number
P	78 (show)	1068243143...71<78> = 1068243143...71<78>

p:

1068243143654567465627616685849270453127279777734442604635535477344157888806571

q:

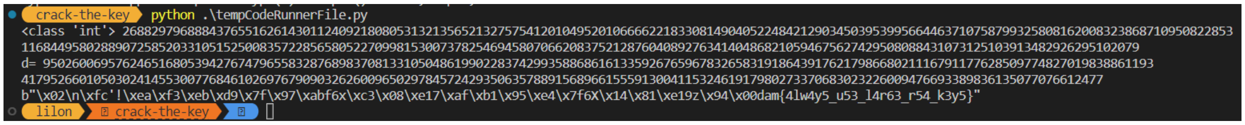
1093804895664037190149735913372113894880573887751616112836700094033933525131149

c:

base64=
M1Qgcu5TJPojVpLreDXxEPctgYG7ZSXso0bIcPWeHsorU7Z5MDViiLPMTfCkdB0UtbdZeWNNzJ5EEtqk+nZjxQ==

Hex=
0x33542072ee5324fa235692eb7835f110f72d8181bb6525eca346c870f59e1eca2b53b67930356288b3cc4df0a4741d14b5b75979634dcc9e4412daa4fa7663c5

```python
import gmpy2
from Crypto.Util.number import long_to_bytes
import base64

q = 106824314365456746562761668584927045312727977773444260463553547734415788806571
p = 109380489566403719014973591337211389488057388775161611283670009403393352513149

e = 65537
c = 0x33542072ee5324fa235692eb7835f110f72d8181bb6525eca346c870f59e1eca2b53b67930356288b3cc4df0a4741d14b5b75979634dcc9e4412daa4fa7663c5
print(type(c),c)
n = q*p
print(n)
d = gmpy2.invert(e, (p - 1) * (q - 1))
print("d=",d)
m = pow(c, d, n)
print(m)
print(long_to_bytes(m))
```

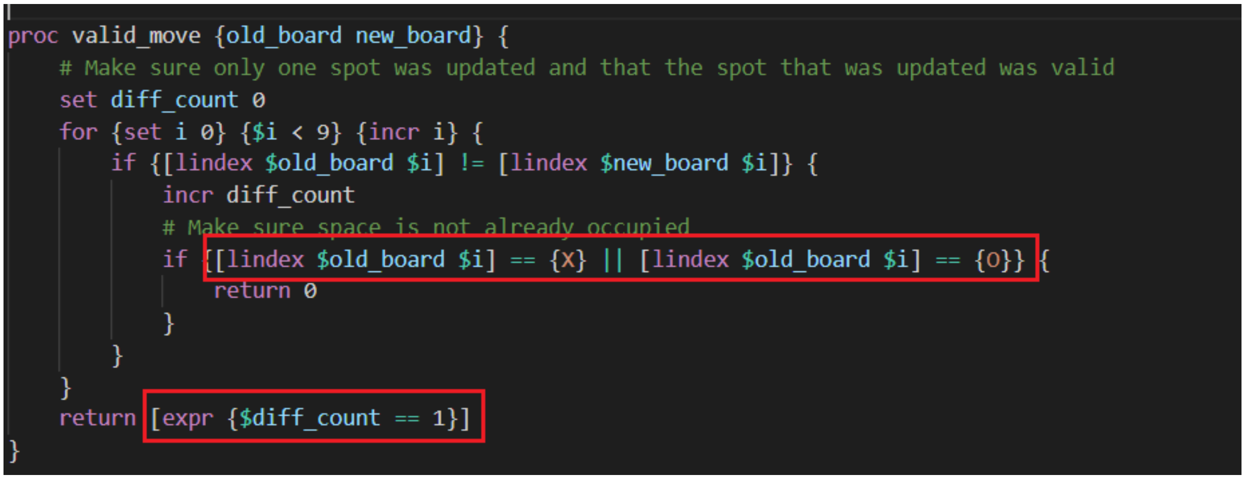


```
● crack-the-key  python .\tempCodeRunnerFile.py
<class 'int'> 2688297968884376551626143011240921808053132135652132757541201049520106666221833081490405224842129034503953995664463710758799325808162008323868710950822853
11684495802889072585203310515250083572285658052270998153007378254694580706620837521287604089276341404868210594675627429508088431073125103913482926295102079
d= 9502600695762465168053942767479655832876898370813310504861990228374299358868616133592676596783265831918643917621798668021116791177628509774827019838861193
417952660105030241455300776846102697679090326260096502978457242935063578891568966155591300411532461917980273370683023226009476693389836135077076612477
b"\x02\n\xfc'!\xea\xf3\xeb\xd9\x7f\x97\xabf6x\xc3\x08\xe17\xaf\xb1\x95\xe4\x7f6X\x14\x81\xe19z\x94\x00dam{4lw4y5_u53_l4r63_r54_k3y5}"
○ lilon  crack-the-key  
```

web

tcl-tac-toe

审计源码判断移动是否合法的函数，判断依据一：是不是只下了一步，依据二，不能下在已经被X或O标记的地方。

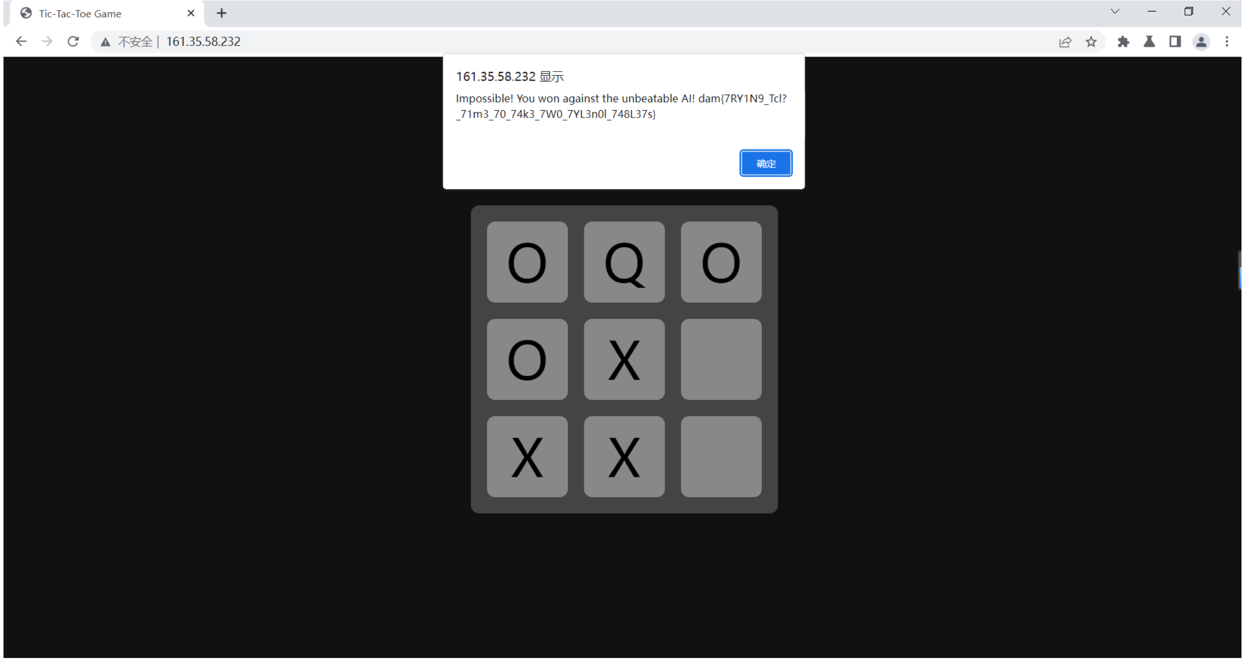


```
proc valid_move {old_board new_board} {
    # Make sure only one spot was updated and that the spot that was updated was valid
    set diff_count 0
    for {set i 0} {$i < 9} {incr i} {
        if {[lindex $old_board $i] != [lindex $new_board $i]} {
            incr diff_count
            # Make sure space is not already occupied
            if {[lindex $old_board $i] == {X} || [lindex $old_board $i] == {O}} {
                return 0
            }
        }
    }
    return [expr {$diff_count == 1}]
}
```

第一步利用其他字符例如Q占位，干扰判断，使得电脑随机下O。

第二步和第三步开始下X，制造一个2连。

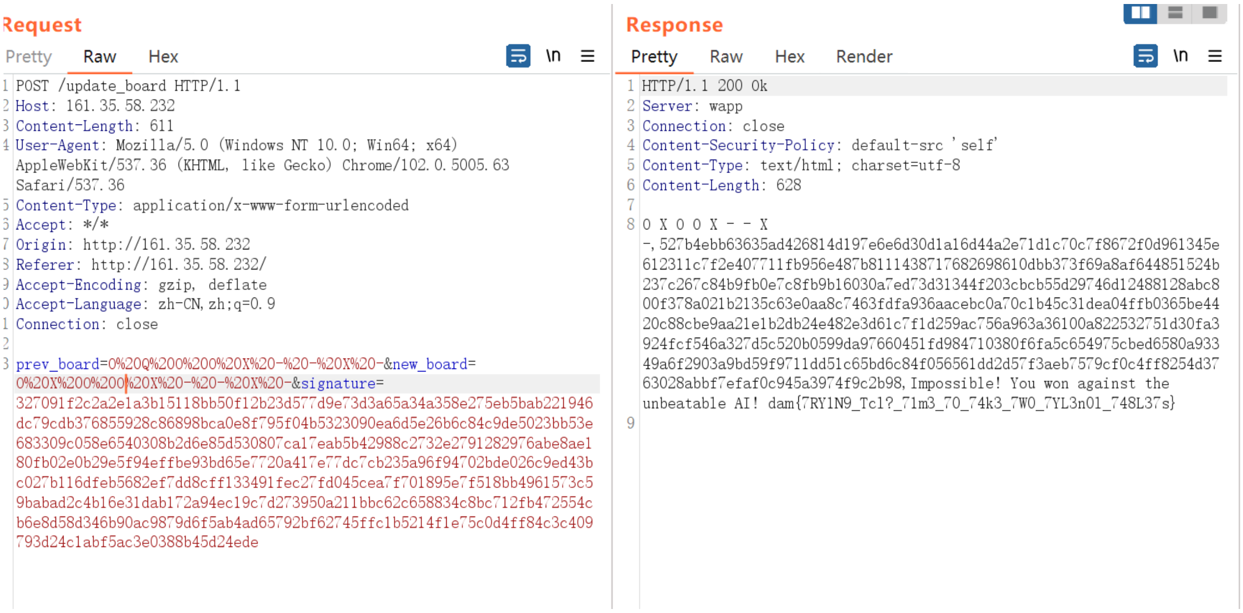
第三步，把Q改回X，因为判断移动是否合法的函数不会看是否被非X和非O字符占位。



161.35.58.232 显示

Impossible! You won against the unbeatable AI! dam{7RY1N9_Tcl?_71m3_70_74k3_7W0_7YL3n0l_748L37s}

```
O Q O
O X
X X
```



```
POST /update_board HTTP/1.1
Host: 161.35.58.232
Content-Length: 611
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: */*
Origin: http://161.35.58.232
Referer: http://161.35.58.232/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

prev_board=0%20Q%200%200%20X%20-%20-%20X%20-&new_board=0%20X%200%200%20X%20-%20-%20X%20-&signature=327091f2c2a2e1a3b15118bb50f12b23d577d9e73d3a65a34a358e275eb5bab221946dc79cdb376855928c86898bca0e8f795f04b5323090ea6d5e26b6c84c9de5023bb53e683309c058e6540308b2d6e85d530807ca17eab5b42988c2732e2791282976abe8ae180fb02e0b29e5f94effbe93bd65e7720a417e77dc7cb235a96f94702bde026c9ed43bc027b116dfeb5682ef7dd8cff133491fec27fd045cea7f701895e7f518bb4961573c59babad2c4b16e31dab172a94ec19c7d273950a211bbc62c658834c8bc712fb472554cb6e8d58d346b90ac9879d6f5ab4ad65792bf62745ffc1b5214f1e75c0d4ff84c3c409793d24c1abf5ac3e0388b45d24ede
```

```
HTTP/1.1 200 Ok
Server: wapp
Connection: close
Content-Security-Policy: default-src 'self'
Content-Type: text/html; charset=utf-8
Content-Length: 628

0 X 0 0 X - - X -,527b4ebb63635ad426814d197e6e6d30d1a16d44a2e71d1c70c7f8672f0d961345e612311c7f2e407711fb956e487b81114387176826986l0dbb373f69a8af644851524b237c267c84b9fb0e7c8fb9b16030a7ed73d31344f203cbcb55d29746d12488128abc800f378a021b2135c63e0aa8c7463fdfa936aacebc0a70c1b45c31dea04ffb0365be4420c88cbe9aa21e1b2db24e482e3d61c7f1d259ac756a963a36100a822532751d30fa3924fcf546a327d5c520b0599da97660451fd984710380f6fa5c654975cbed6580a93349a6f2903a9bd59f9711dd51c65bd6c84f056561dd2d57f3aeb7579cf0c4ff8254d3763028abbf7efaf0c945a3974f9c2b98,Impossible! You won against the unbeatable AI! dam{7RY1N9_Tcl?_71m3_70_74k3_7W0_7YL3n0l_748L37s}
```