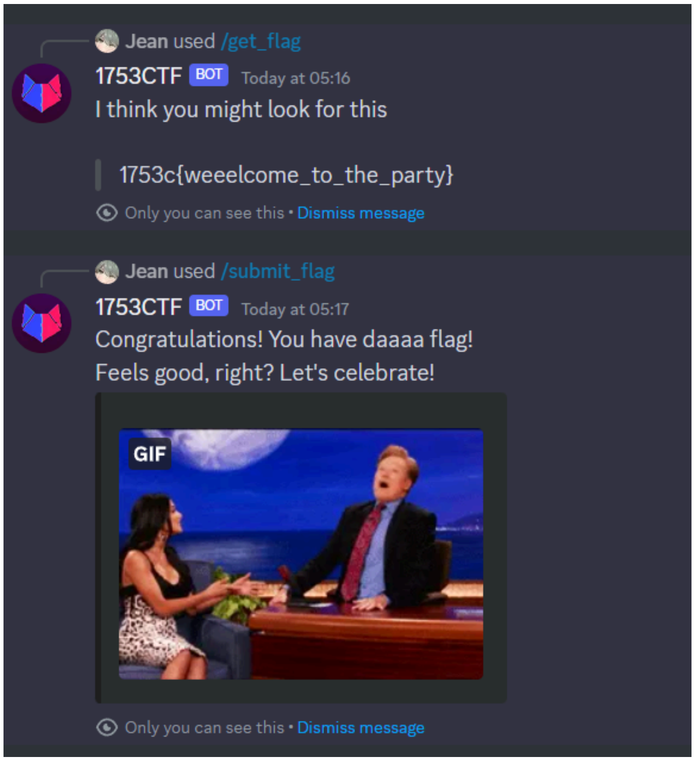
1735 CTF (2024) Writeup

—---Start Here—---

MISC // 🤖 Sanity Check



Jean used /get_flag

1753CTF BOT Today at 05:16

I think you might look for this

> 1753c{weeelcome_to_the_party}

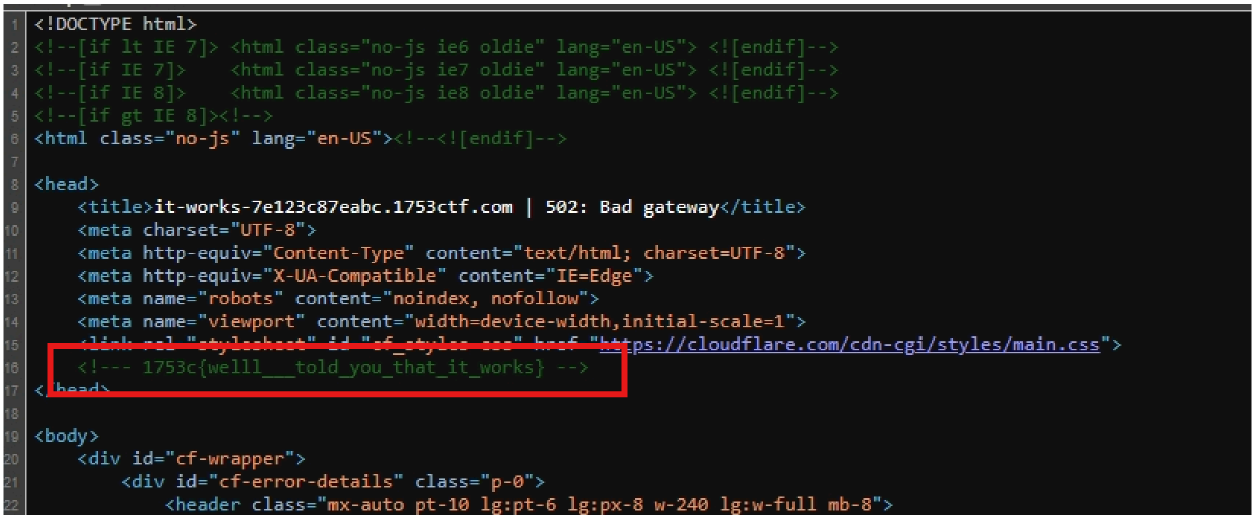
Only you can see this • Dismiss message

Jean used /submit_flag

1753CTF BOT Today at 05:17

Congratulations! You have daaaa flag! Feels good, right? Let's celebrate!

Only you can see this • Dismiss message

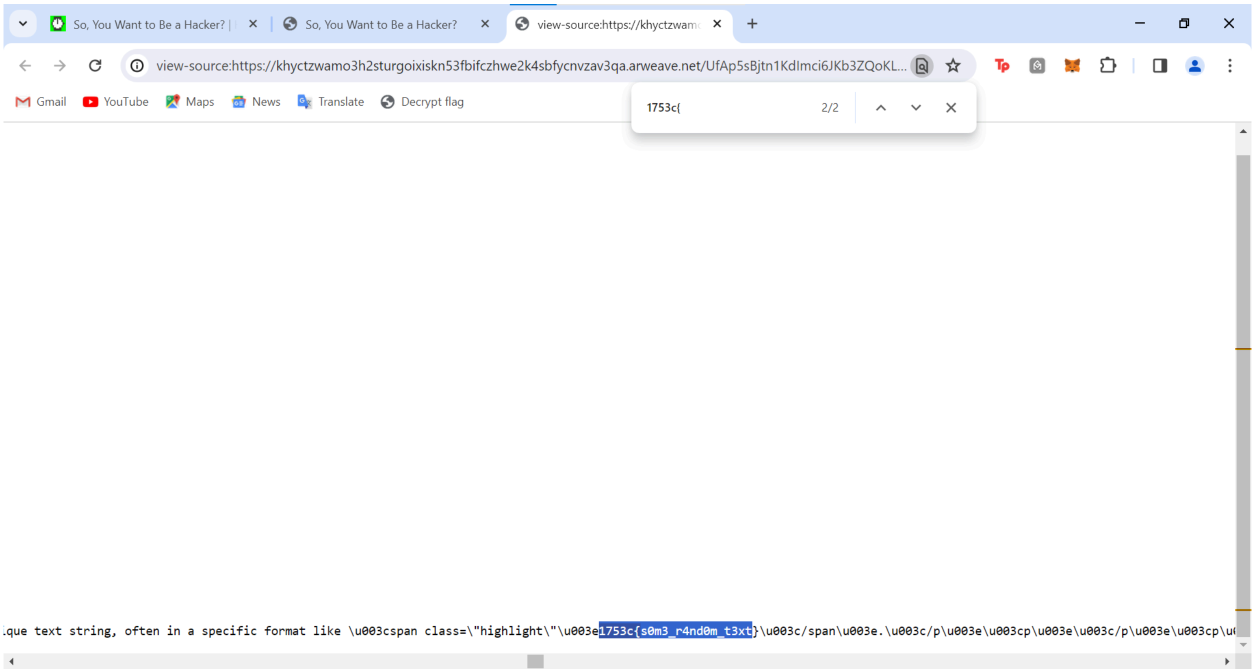


```
<!DOCTYPE html>
<!--[if lt IE 7]> <html class="no-js ie6 oldie" lang="en-US"> <![endif]-->
<!--[if IE 7]>    <html class="no-js ie7 oldie" lang="en-US"> <![endif]-->
<!--[if IE 8]>    <html class="no-js ie8 oldie" lang="en-US"> <![endif]-->
<!--[if gt IE 8]><!-->
<html class="no-js" lang="en-US"><!--<![endif]-->

<head>
    <title>it-works-7e123c87eabc.1753ctf.com | 502: Bad gateway</title>
    <meta charset="UTF-8">
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
    <meta http-equiv="X-UA-Compatible" content="IE=Edge">
    <meta name="robots" content="noindex, nofollow">
    <meta name="viewport" content="width=device-width,initial-scale=1">
    <link rel="stylesheet" id="cf_styles-css" href="https://cloudflare.com/cdn-cgi/styles/main.css">
    <!--- 1753c{welll___told_you_that_it_works} -->
</head>

<body>
    <div id="cf-wrapper">
        <div id="cf-error-details" class="p-0">
            <header class="mx-auto pt-10 lg:pt-6 lg:px-8 w-240 lg:w-full mb-8">
```

https://flag-vault-5a37f69100fc.1753ctf.com/backups/phpinfo.php flag valut challange

OSINT // Fixed Mistake

Found a link by Hackernoon where they featured an article about 1753 CTF , scrolled down and clicked on Permanent on Arweave. Used the Find tool in its page source to obtain the flag

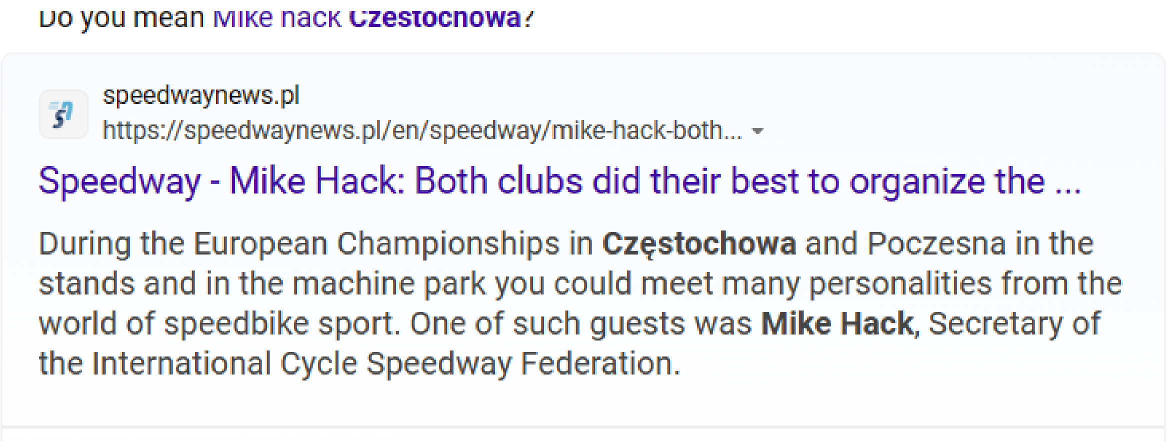

So, You Want to Be a Hacker? |
So, You Want to Be a Hacker?
view-source:https://khyctzwam
Gmail
YouTube
Maps
News
Translate
Decrypt flag
1753c{
2/2

view-source:https://khyctzwamo3h2sturgoixiskn53fbifczhwe2k4sbfycnvzav3qa.arweave.net/UfAp5sBjtn1KdImci6JKb3ZQoKL...

```
ique text string, often in a specific format like \u003cspan class=\"highlight\"\u003e1753c{s0m3_r4nd0m_t3xt}\u003c/span\u003e.\u003c/p\u003e\u003cp\u003e\u003c/p\u003e\u003cp\u
```

MISC // Resume

Googled Mike Hack's name with his Highschool location and found an article that mentions his workplace.



Do you mean Mike hack Czestochowa?

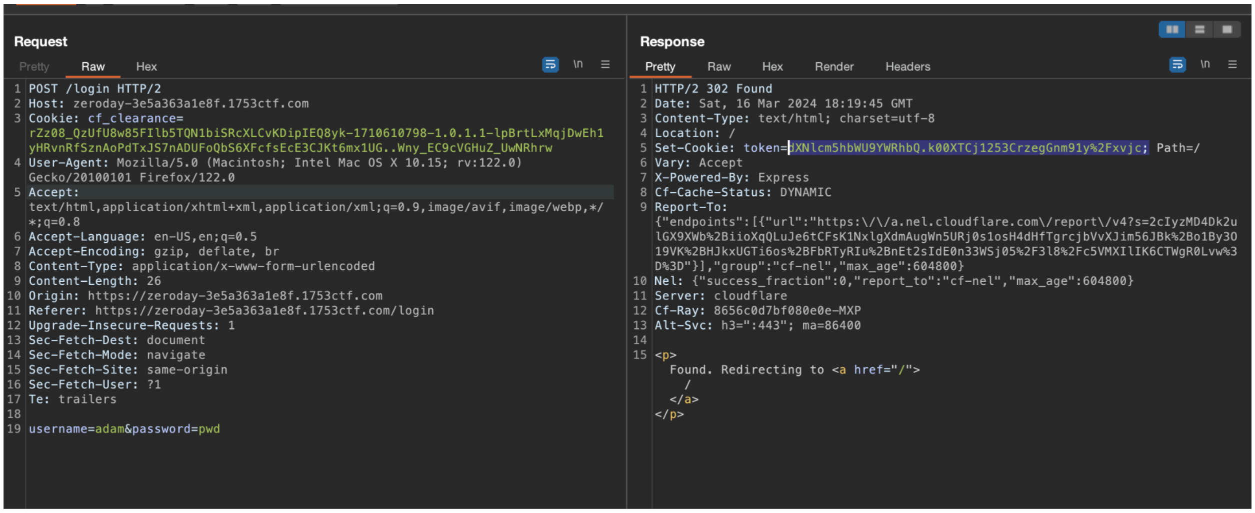
speedwaynews.pl
https://speedwaynews.pl/en/speedway/mike-hack-both...

Speedway - Mike Hack: Both clubs did their best to organize the ...

During the European Championships in **Częstochowa** and Poczesna in the stands and in the machine park you could meet many personalities from the world of speedbike sport. One of such guests was **Mike Hack**, Secretary of the International Cycle Speedway Federation.

This way I was able to google his email as well

Web/crypto zeroday



```
POST /login HTTP/2
Host: zeroday-3e5a363a1e8f.1753ctf.com
Cookie: cf_clearance=
rZz08_QzUfU8w85FIlb5TQN1biSRcXLCvKDipIEQ8yk-1710610798-1.0.1.1-lpBrtLxMqjDwEh1
yHRvnRfSznAoPdTxJS7nADUFoQbS6XFcfsEcE3CJKt6mx1UG..Wny_EC9cVGHuZ_UwNRhrw
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:122.0)
Gecko/20100101 Firefox/122.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/
*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 26
Origin: https://zeroday-3e5a363a1e8f.1753ctf.com
Referer: https://zeroday-3e5a363a1e8f.1753ctf.com/login
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers

username=adam&password=pwd
```

```
HTTP/2 302 Found
Date: Sat, 16 Mar 2024 18:19:45 GMT
Content-Type: text/html; charset=utf-8
Location: /
Set-Cookie: token=dXNlcm5hbWU9YWRhbQ.k00XTCj1253CrzegGnm91y%2Fxvjc; Path=/
Vary: Accept
X-Powered-By: Express
Cf-Cache-Status: DYNAMIC
Report-To:
{"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?s=2cIyzMD4Dk2u
lGX9XWb%2BiioXqQLuJe6tCFsK1NxlgXdmAugWn5URj0s1osH4dHfTgrcjbVvXJim56JBk%2Bo1By3O
19VK%2BHJkxUGTi6os%2BFbRTyRIu%2BnEt2sIdE0n33WSj05%2F3l8%2Fc5VMXIlIK6CTWgR0Lvw%3
D%3D"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 8656c0d7bf080e0e-MXP
Alt-Svc: h3=":443"; ma=86400

<p>
  Found. Redirecting to <a href="/">
    /
  </a>
</p>
```

The token encoded base64

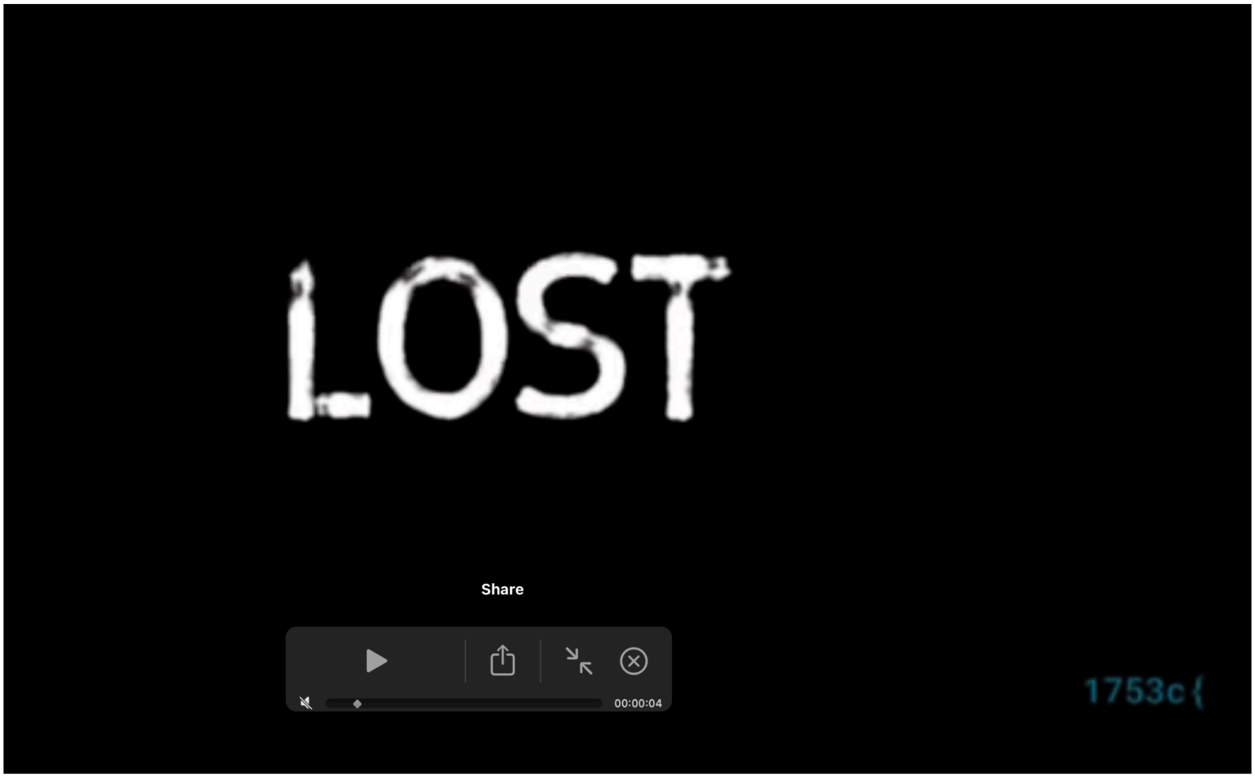
dXNlcm5hbWU9YWRhbQ.k00XTCj1253CrzegGnm91y%2Fxvjc;

After decoding : username=adabQ.“ML(õÛ Â¯7 y½1y%Ø\ojc;

Though if we changed the username to admin and encoded again the whole token and sent the request it should log us in as admin and print the flag ., for some reason it didn’t work for me.

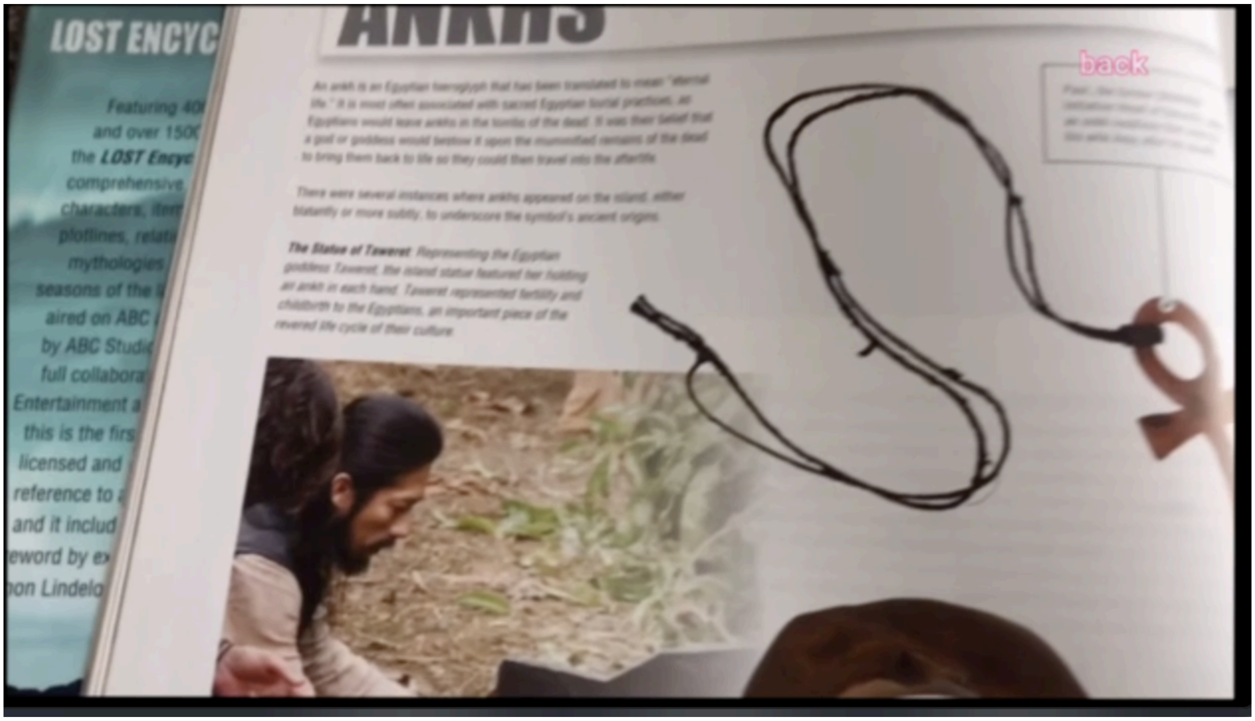
STEGANO // The Constant

Tried the usual steganography techniques to see if the flag hidden somewhere as a string in the video file , doesn’t seem like it , instead watched the video slowly and looks like the flag or a part of it is in the video ??



1753c{

The beginning of the flag



An ankh is an Egyptian hieroglyph that has been translated to mean "eternal life." It is most often associated with sacred Egyptian burial practices, as Egyptians would leave ankhs in the tombs of the dead. It was their belief that a god or goddess would bestow it upon the mummified remains of the dead to bring them back to life so they could then travel into the afterlife.

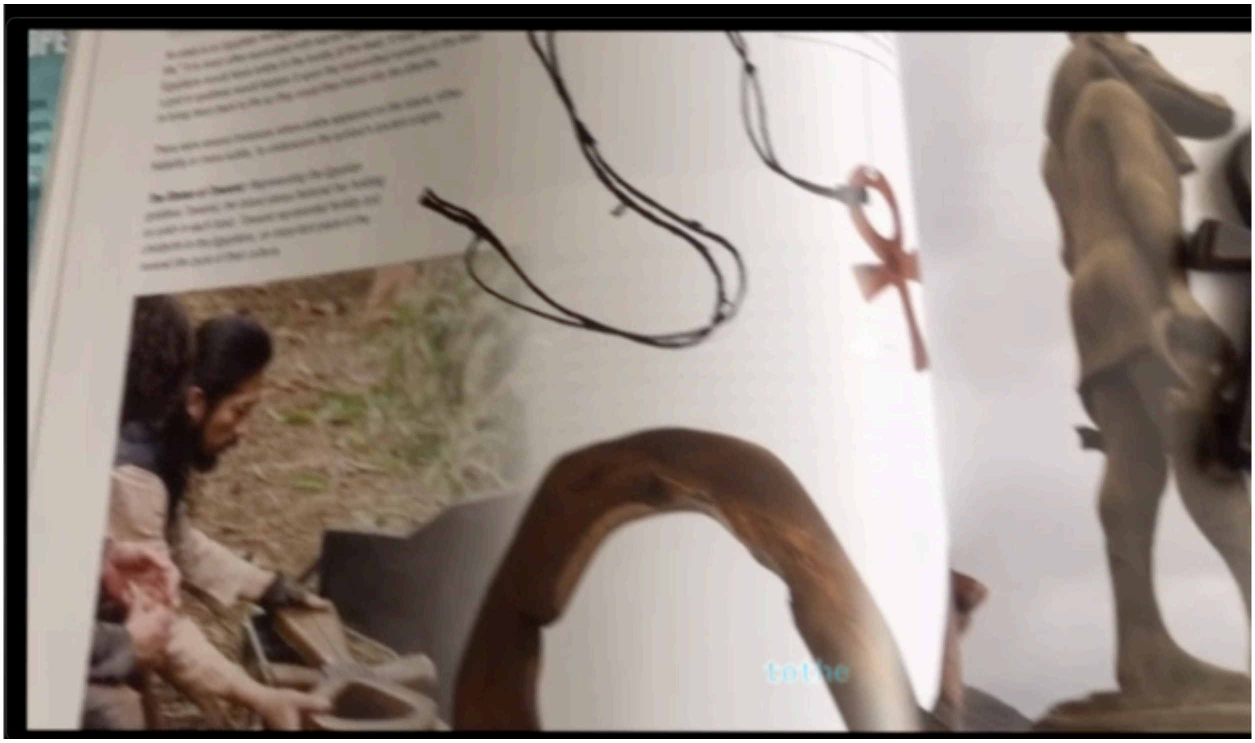
There were several instances where ankhs appeared on the island, either blatantly or more subtly, to underscore the symbol's ancient origins.

The Statue of Taweret: *Representing the Egyptian goddess Taweret, the island statue featured her holding an ankh in each hand. Taweret represented fertility and childbirth to the Egyptians, an important piece of the revered life cycle of their culture.*

back

The word back ?

To the ?



Island} and a closing bracket , that feels like end of the flag

1753c{backto theisland}
Tried submitting it in diff formats but wasn’t valid