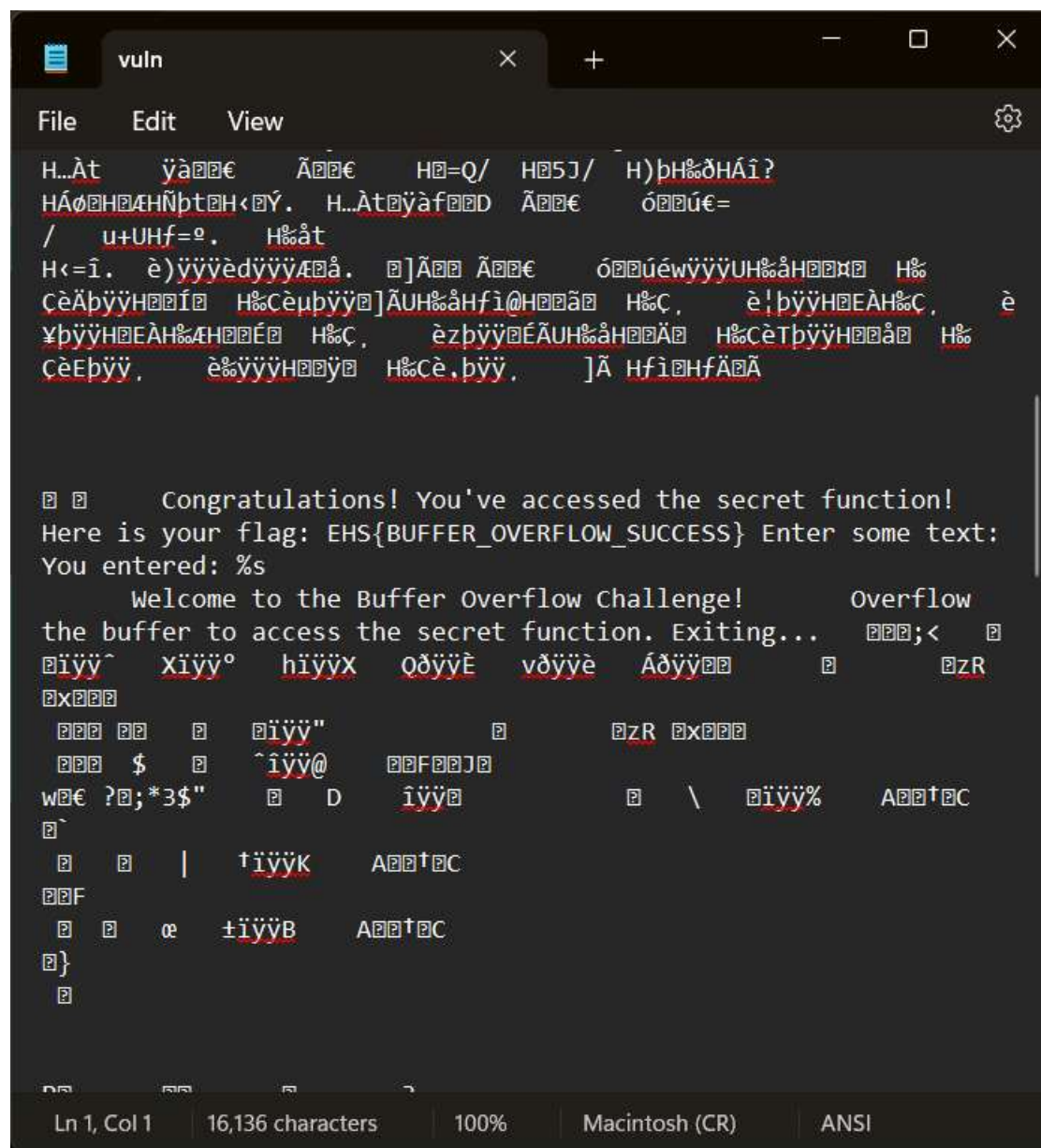


Get me s

Monday, November 18, 2024

4:18 PM



```
File Edit View
H...Àt ỳà€ Ầ€ H=Q/ H5J/ H)h%đHÁi?
HÁøHMHÑptH<Y. H...ÀtỳàfHĐD Ầ€ óHú€=
/ u+UHf=°. H%ât
H<=î. è)yyəèyyə€å. ]ẢẢẢ Ầ€ óHúéwyyəUH%åHẢẢẢ H%
CèẢyyəHẢẢẢ H%Cèmyyə]ẢUH%åHfi@HẢẢẢ H%Ç, è!yyəHẢẢẢH%Ç, è
YyyəHẢẢẢH%CHẢẢẢ H%Ç, èzyyəHẢẢẢUH%åHẢẢẢ H%CèTyyəHẢẢẢ H%
CèEyyə, èyyəHẢẢẢ H%Cè.yyə, ]Ả HfiHfẢẢẢ

Congratulations! You've accessed the secret function!
Here is your flag: EHS{BUFFER_OVERFLOW_SUCCESS} Enter some text:
You entered: %s

Welcome to the Buffer Overflow Challenge! Overflow
the buffer to access the secret function. Exiting... <
^ xıy° hıyX ođyÈ vđyè ÁđyẢẢẢ zR
xẢẢẢ
ẢẢẢ ẢẢ Ầy" zR xẢẢẢ
ẢẢẢ $ Ầy@ ẢẢẢẢẢ
w€ ?;*3$" D ıy \ Ầy% AẢẢ†C
~
| †ıyK AẢẢ†C
ẢẢF
æ ±ıyB AẢẢ†C
}
```

با باز کردن فایل توی نوتپد، میتونیم فلگ رو ببینیم

No to math

Monday, November 18, 2024

4:29 PM

دنباله حسابی، جمله اول برابر ۵- و قدرنسبت برابر ۸ است. کدام جمله دنباله برا

$$a - + 1 = \frac{555 - (-5)}{8} + HT1!; 5; L08ukxK0 - jvf2; \#73$$

ن جمله دنباله حسابی زیر برابر ۱۴۵- است؟
-6)
-۱۳ ،

توی اسلاید 4 فلگ رو میبینیم. همین رو با فرمت فلگ تایپ میکنیم

Easy in hard appearance

Monday, November 18, 2024

4:30 PM

The screenshot shows a presentation viewer interface. On the left, a vertical list of slides is visible, numbered 13 through 17. Slide 16 is highlighted with a red border and a small speech bubble icon containing the number 1. The main area on the right displays the content of slide 16, which features a diagram of a water treatment process. The diagram includes a flowchart with boxes labeled 'آلودگی' (Pollution), 'تصفیه' (Purification), and 'توزیع' (Distribution), connected by arrows. Below the flowchart is a table with numerical data. The interface also includes a 'Comments' panel on the right, with a 'New' button and a comment by 'Amiro' with the ID 'EHS{74br1k_b3_70_d00573_4z1z}'.

توی اسلاید 16 یه کامنت هست که فلگ توش نوشته شده

Abnormal

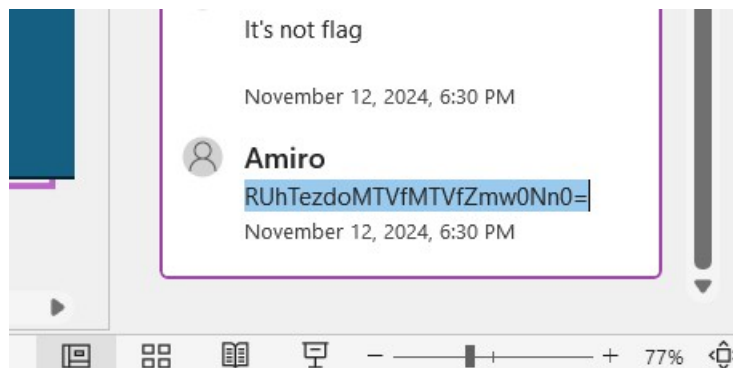
Monday, November 18, 2024 4:34 PM



عدد 24 به جای 2 نوشته شده

Not too easy

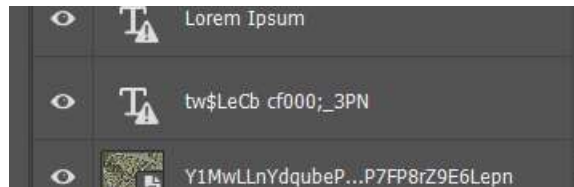
Monday, November 18, 2024 4:36 PM



توی آخرین کامنت یک استرینگ وجود داره که با Base64 رمزنگاری شده که میتونیم با CyberChef اون رو رمزگشایی کنیم و به فلگ برسیم: EHS{7h15_15_fl46}

Look at the Whole Picture!

Monday, November 18, 2024 4:40 PM



آخرین لایه ی عکس توی فوتوشاپ، یک متن هست که با متد Rot47 رمزنگاری شده و بعد از رمزگشایی، به این فلگ میرسیم: EHS{6r3 47__j0b!}

Nuclear is not interesting

Monday, November 18, 2024 4:44 PM

نفاذ قرار می گیرد.
دارانرژی آزاد شده در یک راکتور هسته ای با تعداد شد
پارید!)(circle's hexcolor)DAR SLIDE 18ت ها
نترل کردن تعداد نوترون های که برای انجام عمل
روش های رسیدن به چنین کنترلی، این است که ماده
نمیتواند به راحتی کنترل شود، اما تنظیم مقدار این ماده

توی اسلاید 2 به نشونه به اسلاید 18 هست

Microsoft Word ribbon: Shape Styles, WordArt Styles, Accessibility, Arrange.

Colors dialog box (Custom tab):

- Color model: RGB
- Red: 183
- Green: 192
- Blue: 175
- Hex: #B7C0AF
- Transparency: 0%

Background image: A technical diagram of a nuclear reactor system with various pipes, tanks, and components.

توان حرارتی	3000 مگاوات	قطر خارجی پوسته راکتور	4/525 متر
توان الکتریکی <th>1000 مگاوات</th> <th>ضخامت دیواره پوسته راکتور</th> <th>20 سانتی متر</th>	1000 مگاوات	ضخامت دیواره پوسته راکتور	20 سانتی متر
نوع سوخت <th>Sintered Uranium dioxide</th> <th>طول پوسته راکتور</th> <th>11/185 متر</th>	Sintered Uranium dioxide	طول پوسته راکتور	11/185 متر
وزن کلی سوخت <th>80 تن</th> <th>دبی سیستم خنک کننده راکتور</th> <th>21200-4 متر مکعب در ساعت</th>	80 تن	دبی سیستم خنک کننده راکتور	21200-4 متر مکعب در ساعت
تعداد مجتمع های سوخت <th>163</th> <th>درجه حرارت در ورودی به قلب راکتور</th> <th>291 درجه سانتی گراد</th>	163	درجه حرارت در ورودی به قلب راکتور	291 درجه سانتی گراد
تعداد میله های سوخت در هر مجتمع <th>311</th> <th>درجه حرارت در خروجی از قلب راکتور</th> <th>321 درجه سانتی گراد</th>	311	درجه حرارت در خروجی از قلب راکتور	321 درجه سانتی گراد
طول مجتمع سوخت <th>4/57 متر</th> <th>فشار مدار اول</th> <th>157 بار</th>	4/57 متر	فشار مدار اول	157 بار
قطر قرص سوخت <th>7/57 میلی متر</th> <th>قطر داخلی کره فولادی</th> <th>56 متر</th>	7/57 میلی متر	قطر داخلی کره فولادی	56 متر
ارتفاع قرص سوخت <th>17 میلی متر</th> <th>ضخامت دیواره کره فولادی</th> <th>3-5 سانتی متر</th>	17 میلی متر	ضخامت دیواره کره فولادی	3-5 سانتی متر
قطر قلب راکتور <th>3/16 متر</th> <th>ضخامت فونداسیون ساختمان راکتور</th> <th>4 متر</th>	3/16 متر	ضخامت فونداسیون ساختمان راکتور	4 متر
ارتفاع قلب راکتور <th>3/55 متر</th> <th>ضخامت پوشش بتنی</th> <th>1/75-2 متر</th>	3/55 متر	ضخامت پوشش بتنی	1/75-2 متر

توی اسلاید 18 رنگ دایره رو به صورت hex توی فرمت فرگ میذاریم.

EHS{#B7C0AF}

Congratulations

Monday, November 18, 2024 4:49 PM

با به سرچ توی اینترنت، سایت هایی پیدا میشن که رنگ رو از Hex به γxy تغییر بدن.

Pcap-1

Monday, November 18, 2024

4:51 PM

```
Accept: */*
Content-Length: 27
Content-Type: application/x-www-form-urlencoded

EHS{uh_605h_pc4p_15_50_fun}
HTTP/1.1 404 Not Found
Server: nginx/1.18.0 (Ubuntu)
Date: Tue, 29 Oct 2024 19:53:32 GMT
Content-Type: text/html
Content-Length: 162
Connection: keep-alive

<html>
```

فایل رو توی wireshark باز میکنیم و روی توی بخشی از پیام هایی که رد و بدل شده، فلگ رو میبینیم

Howl

Monday, November 18, 2024 4:55 PM

طبق هینت، با یه سرچ توی گوگل به نرم افزار هایی مثل DeepSound و با اون میتونیم متن پنهان شده توی فایل رو ببینیم و فلگ رو استخراج کنیم.

DumpNo1se

Monday, November 18, 2024 4:57 PM

فایل رو توی سایت های مختلف استخراج متن مورس کد از فایل صوتی آپلود میکنیم و فلگ رو میگیریم

Pcap-2

Monday, November 18, 2024

4:58 PM

این دفعه یک استرینگ رمزنگاری شده رو میبینیم که اون رو رمزگشایی میکنیم (Base64) و به فلگ میرسیم.

```
User-Agent: curl/8.9.1
Accept: */*
Content-Length: 64
Content-Type: application/x-www-form-urlencoded

RUhTe3VoX2dvc2hfcGNhcF9pc19zb19mdW5fYW5kX2l0X2dldHNfZnVubml1cn0=
HTTP/1.1 404 Not Found
Server: nginx/1.18.0 (Ubuntu)
Date: Tue, 29 Oct 2024 20:02:17 GMT
Content-Type: text/html
Content-Length: 162
Connection: keep-alive

<html>
<head><title>404 Not Found</title></head>
<body>
<center><h1>404 Not Found</h1></center>
<hr><center>nginx/1.18.0 (Ubuntu)</center>
</body>
</html>
```

EHS{uh_gosh_pcap_is_so_fun_and_it_gets_funnier}

Pcap-3

Monday, November 18, 2024 5:05 PM

تمام request های http رو نگاه میکنیم و تیکه تیکه متن ها رو کپی میکنیم و به صورت Base64 رمزگشایی میکنیم.

```
RUhTe3VoX2dvc2hfcGNhcF9pc19zb19mdW5fYW5kX2l0X2dldH  
NfZnVubmllcl9Pb29vb2hfTm93X2lfY2FuX2dvX3NvX2Zhcn0=
```

```
EHS{uh_gosh_pcap_is_so_fun_and_it_gets_funnier_Ooooooh_N  
ow_i_can_go_so_far}
```

Pcap-4

Monday, November 18, 2024 5:09 PM

```
Accept: */*
Content-Length: 833
Content-Type: application/x-www-form-urlencoded
```

```
.....RUF{1_4z_601a6_s0e_4_e07_0a3}.....
.....tell.....em.....davis.....was.....he
re.....
```

```
HTTP/1.1 404 Not Found
Server: nginx/1.18.0 (Ubuntu)
Date: Tue, 29 Oct 2024 20:14:03 GMT
Content-Type: text/html
Content-Length: 162
Connection: keep-alive
```

```
<html>
<head><title>404 Not Found</title></head>
<body>
<center><h1>404 Not Found</h1></center>
<hr><center>nginx/1.18.0 (Ubuntu)</center>
</body>
</html>
```

یک استرینگ وسط متن هست که اون رو کپی میکنیم و با Rot13 اون رو رمزگشایی میکنیم:

EHS{1_4m_601n6_f0r_4_r07_0n3}

Wired Code

Monday, November 18, 2024 5:12 PM

فرمت کد رو سرچ میکنیم و میبینیم که چیزی به اسم G code وجود داره که کدی برای طراحی با cnc هست. اون رو توی سایت های مختلفی که هستند میزنیم و فلگ رو میخوانیم

Magic Byte

Monday, November 18, 2024 5:13 PM

میدونیم 4 بایت اول هر فایل یک چیز مشخص به اسم File Signature هست که توی این فایل، درست نیست. با یک Hex Editor 4 بایت اول عکس رو به File Signature اکستنشن png که این پایین هست تغییر میدیم و فایل رو باز و فلگ رو میخونیم.
89 50 4E 47

ROT

Monday, November 18, 2024 5:17 PM

فلگ رمزنگاری شده رو با استفاده از ROT13 و تغییر مقدار تا جایی که به فرمت
فلگ تبدیل بشه (مقدار -3) رمزگشایی میکنیم:

HKV{4u3_b0x_eo1qg_0u_5p7_?}

EHS{4r3_y0u_bl1nd_0r_5m7_?}

Base

Monday, November 18, 2024 5:20 PM

با base64 استرینگ رو رمزگشایی میکنیم تا به فلگ برسیم:

RUhTe20wcjMzMzMzX2ZsNDY1fQ==

EHS{m0r33333_fl465}

Another ROT

Monday, November 18, 2024 5:21 PM

فلگ رو با ROT47 رمزگشایی میکنیم:

tw\$Lc?_f9bC07=ce09bCbN
EHS{4n07h3r_fl46_h3r3}

Copy me

Monday, November 18, 2024

8:39 PM

فایل txt رو دانلود و فلگ رو کپی و submit کردم

Find me

Monday, November 18, 2024

8:41 PM

بعد از خواندن description چالش وارد بخش rules شدم و فلگ رو کپی و submit کردم

Search Me

Monday, November 18, 2024 8:47 PM

اول فایل رو دانلود کردم و اون رو توی notepad بازش کردم و با `ctrl + f` سرچ رو باز کردم و EHS رو سرچ کردم و فلگ رو پیدا کردم.

Not1ce

Monday, November 18, 2024

8:50 PM

بعد از یک ساعت و نیم نگاه کردن به اون ویدیوی آموزشی متوجه تغییر رنگ Cursor شدم.

Paintonawall

Monday, November 18, 2024 8:51 PM

عکس رو وارد گوگل لنز کردم و متوجه شدم این یک نقاشی معروف خیابانی از آقای banksy هست و بعد از گشتن درباره اطلاعات بیشتر درباره عکس به سایت ویکی پدیا برخوردم که مدل گوشی و اطلاعات بیشتر در ته صفحه ویکی پدیا در بخش metadeta بود.

Res1st

Monday, November 18, 2024 8:52 PM

دقیقا خود سوال رو از هوش مصنوعی پرسیدم و به من جواب داد که 10 اهم مقاومت دارد و من 10000 را در فرمت فلگ قرار دادم

Just Do It!

Monday, November 18, 2024 8:52 PM

ابتدا فایل پاورپوینت رو دانلود کردم و Editing رو enable کردم و نوار زرد رو برداشتم و پشت نوار زرد فلگ رو که به رنگ سفید نوشته شده بود رو پیدا کردم

Pr03

Monday, November 18, 2024 8:53 PM

وقتی فایل رو دانلود کردم حتی نیازی ندیدم که درباره اون کدی بنویسم چون میشد فقط با شمردن حروف فلگ رو پیدا کرد

Key "Bored"

Monday, November 18, 2024 8:53 PM

فایل رو دانلود کردم و اون رو باز کردم و طبق دستورالعملی که خودش گفته بود عمل کردم و عبارت SUCHALONGFLAG! که بدست آمده بود را در فرمت فلگ قرار دادم

Office Master

Monday, November 18, 2024 8:54 PM

فایل pptx رو دانلود کردم و وقتی به کل اسلاید ها یه نگاه کلی انداختم f5 رو زدم و اون رو گذاشتم روی اسلایدشو و اسپم کلیک کردم تا یه چیز غیر عادی ، به عکس کج قرار داده شده و یا کدی پیدا کنم. در یکی از اسلاید ها کد باینری پیدا کردم. اون رو کپی کردم و وارد سایت rapidtables کردم تا باینری رو به textبرام تغییر بده و فلگ پیدا شد

$F(F(F(F(F(x))))))$

Monday, November 18, 2024 8:55 PM

کد رو وارد cyberchef کردم و output ای رو که بهم داد رو دوباره وارد input کردم تا دوباره خروجی بده و این کار رو چند بار تکرار کردم تا بهم فلگ رو داد.

Not1ce 3

Monday, November 18, 2024 8:56 PM

راستش من این مدل نوشتن رو به leet speak میشناسم و دربارش میدونستم ولی دیدم وقتی که leet_speak رو داخل فرمت فلگ قرار میدم و فلگ اشتباه میشه فهمیدم باید دربارش تحقیق کنم. بعد از یکم فهمیدم که این مدل نوشتن به leet و speak 1337 هم معروفه و این دو رو تست کردم و leet وارد فرمت فلگ شد و درست بود.

PR02

Monday, November 18, 2024 8:57 PM

طبق دستورالعملی که داده کلمه احسان رو با اعداد به طوری که گفته شده در notepad سرچ کردم) با f + ctrl تعداد کاراکترهایی که قبل اون عبارت عددی هست رو وارد سایت wordcounter کردم و تعداد کاراکترهایی که قبل اون متن بود ۱۹۵ تا بود پس اولین کاراکتر عبارت ۱۹۶ امین کاراکتر بود. از اونجایی که کل عبارت باید ۲۵ کاراکتر باشه آخرین کاراکتر عبارت ۲۱۰ امین کاراکتر هست.

Trojan_Horse

Monday, November 18, 2024 8:57 PM

فایل رو دانلود کردم و داخل notepad بازش کردم. حتی نیازی نبود که EHS رو سرچ کنم چون خود فلگ داخلش نوشته شده بود اون رو کپی و submit کردم

Notepad.img

Monday, November 18, 2024 8:58 PM

فایل رو دانلود کردم و اون رو داخل notepad باز کردم و EHS رو سرچ کردم و فلگ رو کپی و submit کردم.

Metadata is so OP

Monday, November 18, 2024 8:58 PM

دوباره فایل رو دانلود و اون رو توی notepad باز کردم و EHS رو سرچ کردم و فلگ رو کپی و submit کردم.

Fly

Monday, November 18, 2024 8:59 PM

رایتاپ: fly (این چالش در عین آسونیش بسیار وقت من و تیمم رو گرفت) بلافاصله بعد از دیدن عدد ها فهمیدم که این یک نوع مختصاته اون رو وارد گوگل مپ کردم و یه دریاچه قلب شکل رو نشون داد پس از تلاش های بسیار زیاد متوجه شدم که [اولین چیزی که میتونیم ببینیم] اسم خیابونی که این دریاچه در اون وجود داره ، هست. برای همین اسم خیابون رو تست کردیم و شد.

Find the recycle bin

Monday, November 18, 2024 8:59 PM

از روی ظاهر باغ حدس زدم که این باغ جهان نما هست ولی چون مختصاتشو نداشتم نتونستم فلگ رو پیدا کنم. برای همین داخل گوگل مپ نقطه به نقطه باغ جهان نما و street view رو گشتم تا تونستم اون مکان رو پیدا کنم و مختصاتشو وارد فلگ کنم.