

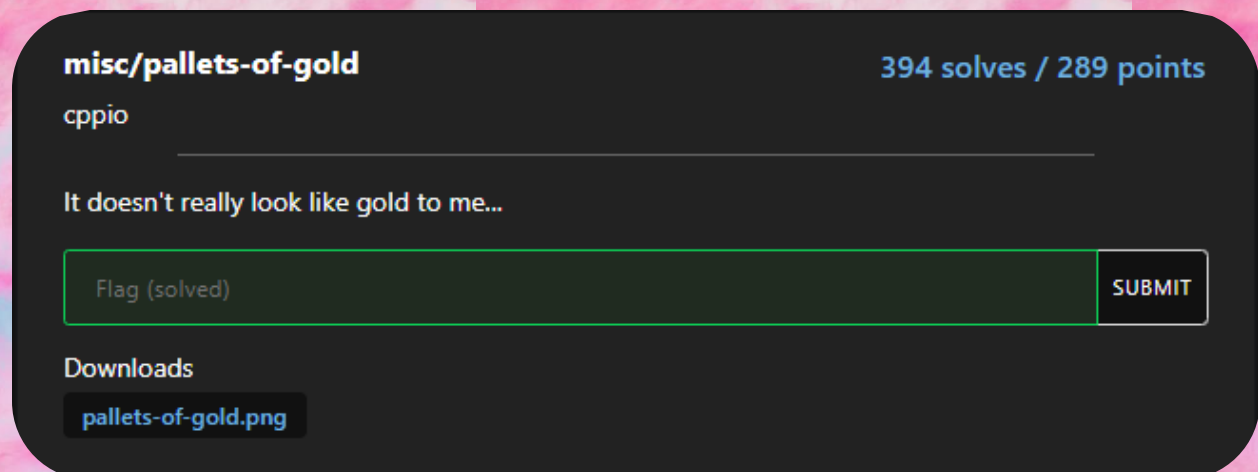
Write-up HSCCTF

Thực ra mình cũng cố gắng kiểm thêm điểm bằng mấy bài nữa nhưng không đủ thời gian :<. Có gì sai sót mong các bạn thông cảm 😊



*Misc

1. Pallets-of-gold



Mình dùng tool StegSolve online <https://stegonline.georgeom.net/image>
Chọn Browse Colour Palette

Ta-da, đã hiện flag

flag{p1te_chunks_remind_me_of_gifs}

(hơi mờ một chút, các bạn tải về ở đây

https://github.com/RepublicOfGitHub/ATTT/blob/main/Write%20up%20HSCTF%202021/files/Pallets-of-gold_solved.png rồi zoom lên xem nhé)

2. Glass-windows



misc/glass-windows

359 solves / 311 points

cpio

I found a cool glass texture.

Flag (solved)

SUBMIT

Downloads

glass-windows.png

Mình bỏ vào tool Stegsolve, chọn chế độ Colour Inversion (Xor) (bằng cách nhấn mũi tên next là được :v)

Bùm, flag hiện thân :v

3. Geographic-mapping

misc/geographic-mapping

164 solves / 429 points

JC01010

Find the coordinates of each location!

Flag format: flag{picture1 latitude,picture1 longitude,picture2 latitude,picture2 longitude}, all latitudes and longitudes to the nearest THREE decimal digits after the period. No spaces in the flag.

Example format: flag{12.862,48.066,-13.477,-48.376} The challenge author will not confirm individual locations, nor check your decimal digits. Three decimal digits gives a range of ~111 meters.

Bài này thực chất là OSINT địa điểm có trong ảnh. Trong picture 1, nhìn ở góc bên trái, ta sẽ thấy thanh điều khiển quen thuộc của Google maps => Đây chính là ảnh lấy trong Google Maps,

ở chế độ xem phổ.

Lúc đầu, mình đã cố dịch các từ xuất hiện trong ảnh và search google nhưng không được :<

Manh mỗi cuối cùng là lá cờ trắng-đỏ tung bay trong bức ảnh. Để ý kỹ góc trắng bên phải của cờ sẽ thấy có logo gì đó. Sau một hồi Google search thì mình cũng tìm thấy đó là cờ của nước Malta. Để ý kỹ hơn chút nữa, bạn sẽ thấy người dân lái xe bên trái => Đúng là ở Malta luôn.



Cờ nước Malta

Rồi bật maps nước Malta lên, một đất nước rộng thế này thì mình bắt đầu từ đâu 😊

Để ý kỹ góc bên phải, bên ngoài bờ rào, chúng ta sẽ thấy tháp thoáng hình ảnh của biển. Vậy ta chỉ tìm khu ven biển thôi :v Để giảm tọa độ tìm kiếm, mình đã bật chế độ giao thông và chỉ tìm kiếm nơi nào có đường đi sát biển. Thêm vào đó, nhìn la bàn bắc-nam, chúng ta đoạn đường này chạy theo hướng bắc nam, mình loại hết các đoạn đường chạy theo hướng khác. Mình đã phải mò mẫm rất lâu 😓 đi dọc hết bờ biển Malta để tìm :<. Nó ở đây này:

https://www.google.com/maps/@35.8980094,14.5179499,3a,75y,334.56h,83.87t/data=!3m9!1e1!3m7!1sv4-Tz3_nciJr10A1On3UZA!2e0!7i13312!8i6656!9m2!1b1!2i28!5m1!1e1?hl=vi

Nhưng nếu bạn để ý kỹ hơn nữa, bạn sẽ thấy chỗ này ở ngã ba đấy, bạn có thể rút gọn phạm vi đi rất nhiều :<

Ở picture 2, mình cũng cố đọc chữ trên bức tường và google search nhưng chẳng ra được gì cả 😓. Manh mỗi cuối cùng là lá cờ trắng xanh, sau một hồi search google thì mình chỉ tìm thấy cờ của một số thành phố trong lịch sử (như Flag of Bavaria) và bị bí từ đoạn này. May sao mình tìm đọc được cái này https://photius.com/flags/horizontal_blue_white_stripes.html và biết được đó là cờ trước kia của San Marino 😓. Sau khi kết hợp google search San Marino castle và San Marino tourist attractions, mình biết được đây là địa điểm du lịch dùng cáp treo. Mình tiếp tục tìm kiếm và lấy được tên chỗ cáp treo đó là Funivia · Città (Libertà) rồi cùng maps bay lên đỉnh tòa nhà đó lấy tọa độ thôi 😊. Đây nè:

https://www.google.com/maps/@43.9376694,12.4458827,3a,75y,356.18h,86.85t/data=!3m7!1e1!3m5!1snYL_K8Cr0zd5Etaxh7UKKA!2e0!6shttps:%2F%2Fstreetviewpixels-pa.googleapis.com%2Fv1%2Fthumbnail%3Fpanoid%3DnYL_K8Cr0zd5Etaxh7UKKA%26cb_client%3Dmaps_sv.tactile.gps%26w%3D203%26h%3D100%26yaw%3D78.467026%26pitch%3D0%26thumbfov%3D100!7i13312!8i6656



Cờ nước San Marino

Tọa độ các bạn lấy trong link có nhé, làm tròn đến 3 chữ số thập phân (theo như đề bài yêu cầu) để ra flag nhé :v

*Web

Lúc mình vào chơi các cao thủ đã giải xong hết rồi 😩. Mãi về sau họ mới bổ sung challenge mới mình mới tranh thủ solve được.

1. Big-blind

web/big-blind

136 solves / 444 points

cppio

<https://big-blind.hsc.tf>

Flag (solved)

SUBMIT

Đề bài đã nói lên tất cả

web/big-blind
cppio



Mình nghĩ ngay đến Blind-Sql Injection. Và quả thực như vậy, đề bài cho 1 trang login, mình phải đăng nhập thôi :v

Mình chọn user là admin. Trong pass mình thử payload ' UNION SELECT null, sleep(10)-- - và ngay lập tức server ngủ 10s => MySQL Injection rồi. Nhưng mình không đăng nhập được, vẫn phải mò pass vậy :v

Nếu table hoặc column không tồn tại, server sẽ trả về lỗi 500. Thế là mình lần lượt đoán và check được table tên là “users” có 2 trường là “user” và “pass”, trong trường “user” có 1 record với user là “admin”.

Đến đây thì mình tự viết script brute-force pass thôi, lợi dụng lỗi sleep :v

Flag: flag{any_info_is_good_info}

*Rev

1. Multidimensional

rev/multidimensional

140 solves / 442 points

wooshi

It's time to break through portals and get multidimensional! Can you cross through all 3 (or 4?) dimensions?

Flag (solved)

SUBMIT

Downloads

Multidimensional.java

Sau khi chạy file Java người ta yêu cầu nhập flag. Đọc source code, họ biến đổi 1 xâu kí tự thành flag; mình đoán mình phải reverse ngược lại để đọc biến chứa flag thôi :v

Đến đây thì mình làm như thế này: Cái nào chạy trước thì mình đảo về sau, đảo ngược thứ tự function và các lệnh trong function lại. Đồng thời, đảo ngược vòng lặp for, các phép tính cộng trừ nhân chia phức tạp chứa biến đã biết ta quay về như bài toán tìm x (tìm cái chưa biết).

Code tham khảo:

<https://github.com/RepublicOfGitHub/ATTT/blob/main/Write%20up%20HSCTF%202021/Multidimensional.java>

Flag: flag{th3_g4t3w4y_b3t233n_d1m3n510n5}

