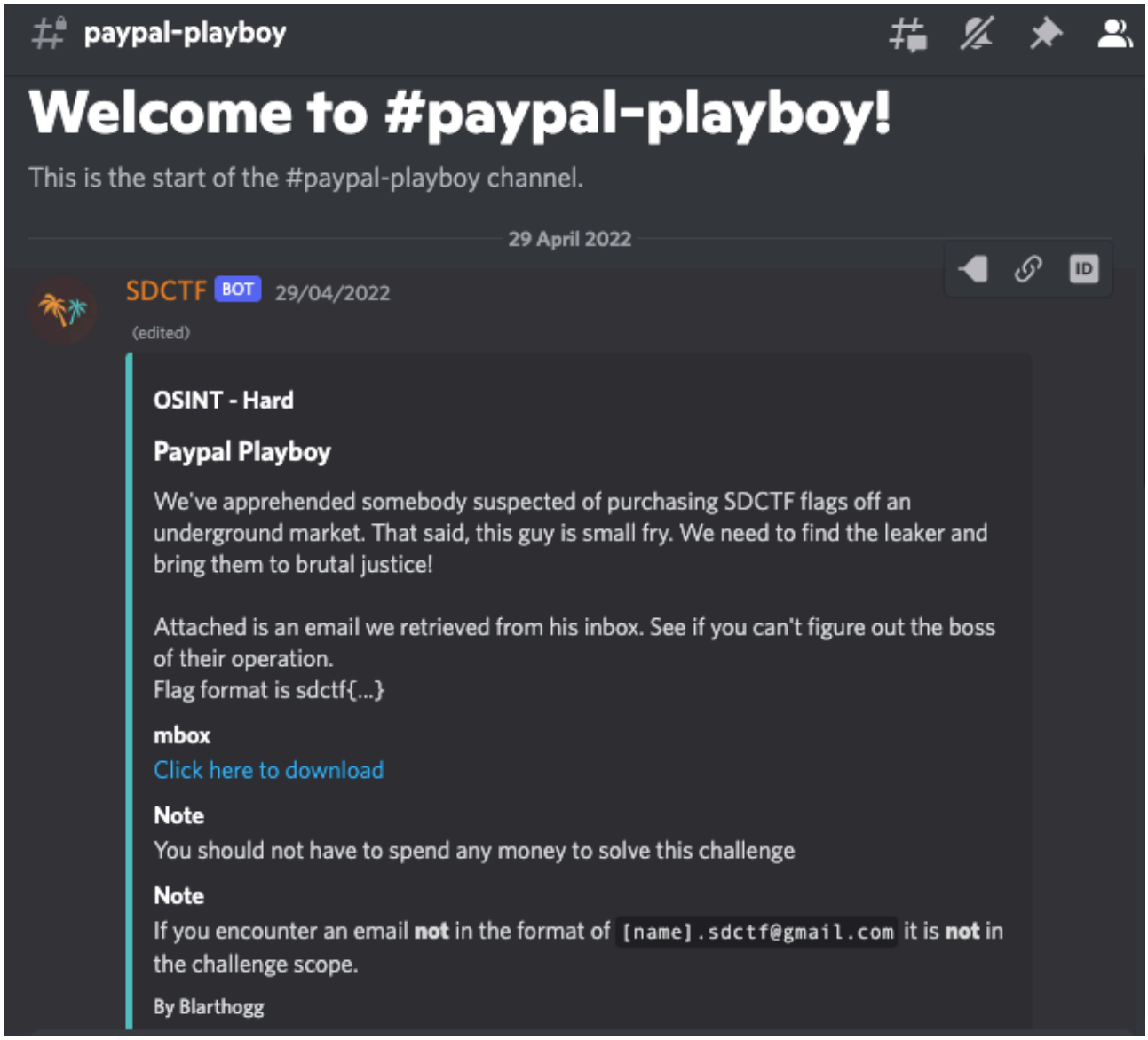
Write-up on ‘Paypal-Playboy’, an OSINT challenge at San Diego CTF 2022 (May 6-8)

by Warren Wu (wcw231@stern.nyu.edu)

‘Paypal-Playboy’ is a 300-point challenge at SDCTF 2022. The goal is straightforward: find the bad guy behind the black market sale of SDCTF flags. The story begins with the capture of an email between a buyer and this illegal operation. From that piece of information, we need to trace the origin of the boss in order to capture the flag.

Below is a screenshot of the opening of this detective story.



Instead of simply explaining the steps to retrieve the flag and then self-congratulate, this write-up will focus on 2 parts to explore the deeper meaning of this CTF challenge:

I. Solving the Mystery
II. Lessons and Insights

Let’s start with the only attachment provided in this challenge - the email, which is created with Emkei's Mailer to introduce fake info like the sender address. The email origin is traced back to a web hosting company called Shinjiru out of Malaysia.

mbox (1)

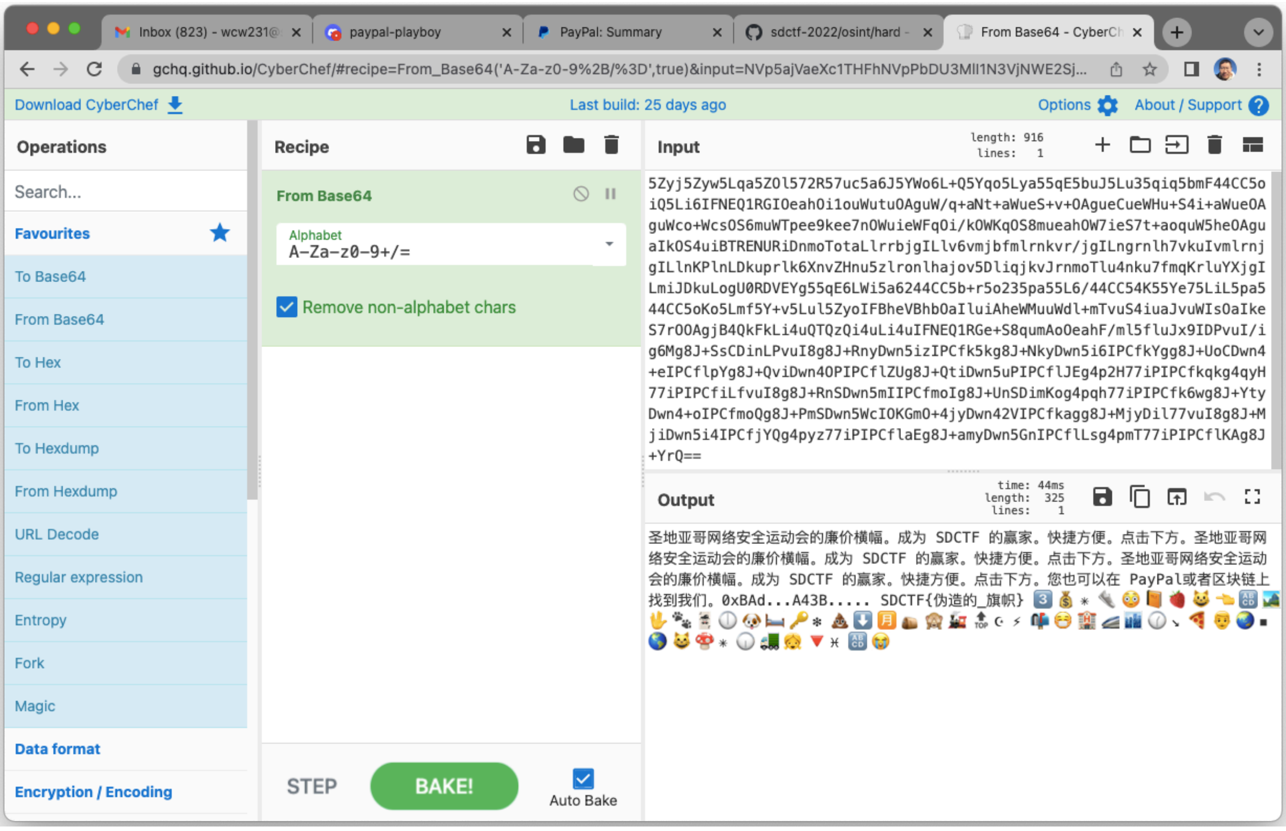
```
From flag.peddler@wehate.sdc.tf Sat Apr 23 00:39:01 2022
Delivered-To: [redacted]@gmail.com
Received: by 2002:a05:6520:266f:b0:1b9:b81b:dce2 with SMTP id il15csp1101047lkb;
        Fri, 22 Apr 2022 17:39:02 -0700 (PDT)
X-Google-Smtp-Source: ABdhPJzxwJlzfSGrxfS8BUrPyF3Rv2x9sStBn/U0tFRYMXyPsNYCyOVhWQQn7IKnPNjwjmMRrzkp
X-Received: by 2002:a05:6402:d2:b0:413:2e50:d6fd with SMTP id
i18-20020a05640200d200b004132e50d6fdmr7715550edu.171.1650674341863;
        Fri, 22 Apr 2022 17:39:01 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1650674341; cv=none;
        d=google.com; s=arc-20160816;
        b=BnpreoBKj7rM/1WsS1qGkQIpbJ5Q7glsLDD6PWDJRM4ChXRSMefEmwqElRjZAsNnxQ
         WbkErwUv9FGbI9XDj0QRlgbcKOY+zfDryej6XaZQ7/YzfTNUYFVLQ9H1tFQvNV32oI9m
         2d8eZn4LyHtp4x4M2nIplYo9EWPUObAd9/V2ajSdVBagveQXocWA28Sdcy2bflA0SplT
         gOUu1TWsT1yD1aRwIzdwyJY8J139u02P7ZIjvO0OHunde46MKIlcA50KyumhKeTCyxqJ
         YLjmgyw6Aey6PlG224L9Mslkcg739k81aUKUTMflpKGqxzM75UZepuCoKyVcwpCp+3vc
         WFug==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
        h=date:message-id:mime-version:reply-to:errors-to:importance:from
         :subject:to;
        bh=SklLFzj9D7lIOMbltmueGQUwZr9CMGutPIb3RqUNk6E=;
        b=EEGOb2Wm/rKABjU6iN1Cv+E3b6mU3Ke04PhXntTkpa7vGH8WeZg7GCfg7dmrBLGyDb
         nGC6L9utfPWqzL7tBmXDtyzqVJE/Qy82QujjnKuT5Vnxuwn1mU1ZOoAXr0KfyK8hOIe6
         jn2nQGeADRUuEedqomYGjUH6RGjuU536npXLWtqmwIwWIRv08UYkItB6ma5pDuuyEdId
         PBwv2ByfPMrReSahatKSk3FbvVuQMCqmHwSlvCIJC2fbNMVw64cQwyCP0sOl1CsFbu98
         UmtH/8ptv3tavNNjIpNqvwCFyp9pbvqZvhOUwDakqV6rY2USr51DIBFymLBllWiCHupb
         w2ZQ==
ARC-Authentication-Results: i=1; mx.google.com;
       spf=neutral (google.com: 101.99.94.116 is neither permitted nor denied by best guess record for domain of
flag.peddler@wehate.sdc.tf) smtp.mailfrom=flag.peddler@wehate.sdc.tf
Return-Path: <flag.peddler@wehate.sdc.tf>
Received: from emkei.cz (emkei.cz. [101.99.94.116])
        by mx.google.com with UTF8SMTPS id c1-20020a170906694100b006df76385bb2si7985374ejs.82.2022.04.22.17.39.01
        for <[redacted]@gmail.com>
        (version=TLS1_3 cipher=TLS_AES_256_GCM_SHA384 bits=256/256);
        Fri, 22 Apr 2022 17:39:01 -0700 (PDT)
Received-SPF: neutral (google.com: 101.99.94.116 is neither permitted nor denied by best guess record for domain of
flag.peddler@wehate.sdc.tf) client-ip=101.99.94.116;
Authentication-Results: mx.google.com;
       spf=neutral (google.com: 101.99.94.116 is neither permitted nor denied by best guess record for domain of
flag.peddler@wehate.sdc.tf) smtp.mailfrom=flag.peddler@wehate.sdc.tf
Received: by emkei.cz (Postfix, from userid 33)
        id 41BF9182372; Sat, 23 Apr 2022 02:39:01 +0200 (CEST)
To: [redacted]@gmail.com
Subject: very cheap banner
From: "cheap sdctf banner" <flag.peddler@wehate.sdc.tf>
X-Priority: 3 (Normal)
Importance: Normal
Errors-To: flag.peddler@wehate.sdc.tf
Reply-To: flag.peddler@wehate.sdc.tf
MIME-version: 1.0
Content-Type: multipart/mixed; boundary=BOUND_62634AA53D6521.02935547
Message-Id: <20220423003901.41BF9182372@emkei.cz>
Date: Sat, 23 Apr 2022 02:39:01 +0200 (CEST)
```

mbox (1)

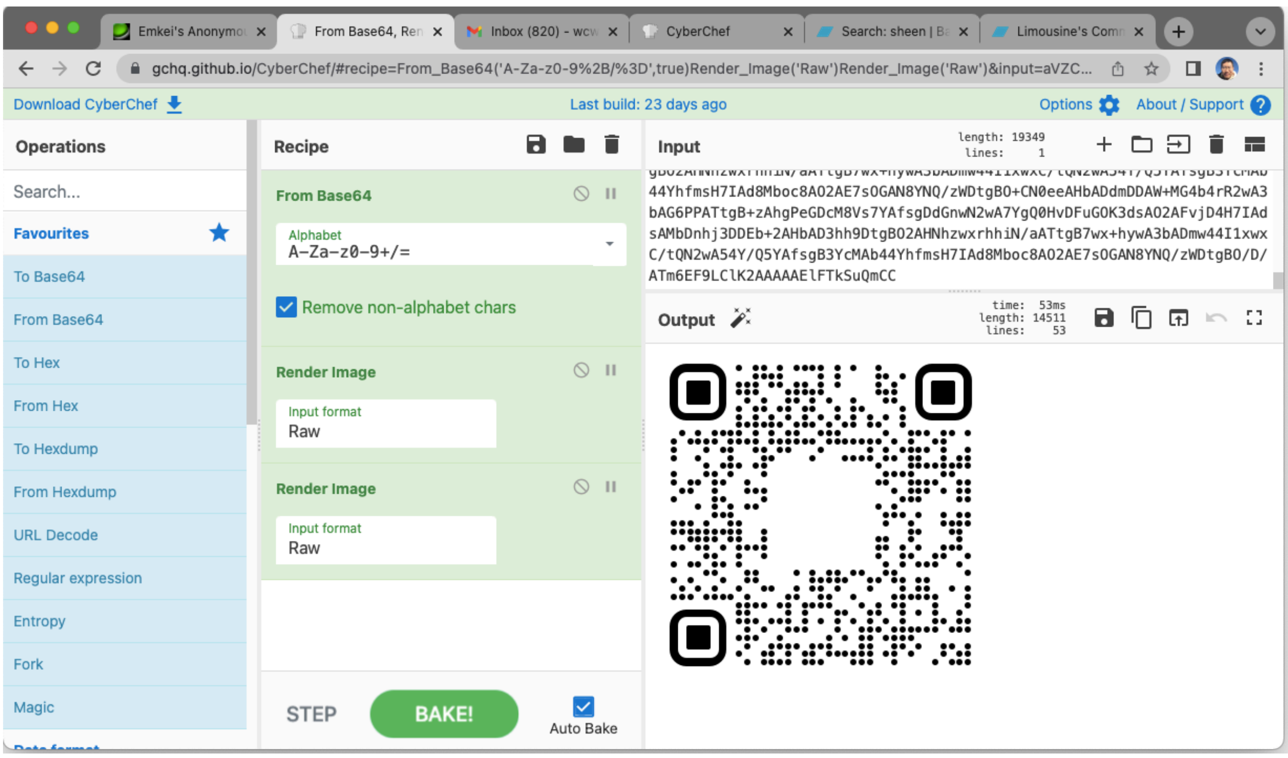
```
Reply-To: flag.peddler@wehate.sdc.tf
MIME-version: 1.0
Content-Type: multipart/mixed; boundary=BOUND_62634AA53D6521.02935547
Message-Id: <20220423003901.41BF9182372@emkei.cz>
Date: Sat, 23 Apr 2022 02:39:01 +0200 (CEST)

--BOUND_62634AA53D6521.02935547
Content-Type: text/plain; charset=utf-8
Content-Transfer-Encoding: base64

5Zyj5Zyw5Lqa5ZOl572R57uc5a6J5YWo6L+Q5Yqo5Lya55qE5buJ5Lu35qiq5bmF44CC5oiQ5Li6
IFNEQ1RGIOeahOi1ouWutuOAguW/q+aNt+aWueS+v+OAgueCueWHu+S4i+aWueOAguWco+WcsOS6
muWTpee9kee7nOWuieWFqOi/kOWKqOS8mueahOW7ieS7t+aoquW5heOAguaIkOS4uiBTRENURiDn
moTotaLlrrbjgIllv6vmjbfmlrnkvr/jgILngrnlh7vkuIvmlrnjgILlnKPlnLDkuprlk6XnvZHn
u5zlronlhajov5DliqjkvJrnmoTlu4nku7fmqKrluYXjgILmiJDkuLogU0RDVEYg55qE6LWi5a62
44CC5b+r5o235pa55L6/44CC54K55Ye75LiL5pa544CC5oKo5Lmf5Y+v5Lul5ZyoIFBheVBhbOaI
luiAheWMuuWdl+mTvuS4iuaJvuWIsOaIkeS7rOOAgjB4QkFkLi4uQTQzQi4uLi4uIFNEQ1RGe+S8
qumAoOeahF/ml5fluJx9IDPvuI/ig6Mg8J+SsCDinLPvuI8g8J+RnyDwn5izIPCfk5kg8J+NkyDw
n5i6IPCfkYgg8J+UoCDwn4+eIPCflpYg8J+QviDwn4OPIPCflZUg8J+QtiDwn5uPIPCflJEg4p2H
77iPIPCfkqkg4qyH77iPIPCfiLfvuI8g8J+RnSDwn5mIIPCfmoIg8J+UnSDimKog4pqh77iPIPCf
k6wg8J+YtyDwn4+oIPCfmoQg8J+PmSDwn5WcIOKGmO+4jyDwn42VIPCfkagg8J+MjyDil77vuI8g
8J+MjiDwn5i4IPCfjYQg4pyz77iPIPCflaEg8J+amyDwn5GnIPCflLsg4pmT77iPIPCflKAg8J+Y
rQ==


--BOUND_62634AA53D6521.02935547
Content-Type: image/png; name="支付.png"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="支付.png"

iVBORw0KGgoAAAANSUhEUgAAAUYAAAFOCAYAAAD6hLSdAAABPmlDQ1BJQ0MgUHJvZmlsZQAAKJFj
YGASSCwoyGFhYGDIzSspCnJ3UoiIjFJgf8bAwiDMIMigxcCXmFxc4BgQ4ANUwgCjUcG3awyMIPqy
LsisncmnB3+YKdt7w+KqjrKaJjemehTAlZJanAyk/wBxYnJBUQkDA2MCkK1cXlIAYrcA2SJFQEcB
2TNA7HQIew2InQRhHwCrCQlyBrKvANkCyRmJKUD2EyBbJwlJPB2JDbUXBNiNzH0DjI0JuJQMUJJa
UQKinfMLKosy0zNKFByBIZSq4JmXrKejYGRgZMTAAApviOrPN8DhyCjGgRArBPrPypOBgSkXIZYQ
wMCw4wPImwgxVR0GBp7jDAwHYgsSixLhDmD8xlKcZmwEYXNvZ2Bgnfb//+dwoJc1GRj+Xv////f2
////LmNgYL4F1PsNABfNXW1QnDRZAAAAYmVYSWZNTQAqAAAACAACARIAAwAAAAEAAQAAh2kABAAA
AAEAAAAmAAAAAAADkoYABwAAABIAAABQoAIABAAAAAEAAAFGoAMABAAAAAEAAAFOAAAAAEFTQ0lJ
AAAAU2NyZWVuc2hvdNuRKQwAAAI9aVRYdFhNTDpjb20uYWRvYmUueG1wAAAAAA8eDp4bXBtZXRh
IHhtbG5zOng9ImFkb2JlOm5zOm1ldGEvIiB4OnhtcHRrPSJYTVAgQ29yZSA2LjAuMCI+CiAgIDxy
ZGY6UkRGIHhtbG5zOnJkZj0iaHR0cDovL3d3dy53My5vcmcvMTk5OS8wMi8yMi1yZGYtc3ludGF4
LW5zIyI+CiAgICAgIDxyZGY6RGVzY3JpcHRpb24gcmRmOmFib3V0PSIiCiAgICAgICAgICAgICAg
bG5zOmV4aWY9Imh0dHA6Ly9ucy5hZG9iZS5jb20vZXhpZi8xLjAvIgogICAgICAgICAgICAgICB4bWxu
czp0aWZmPSJodHRwOi8vbnMuYWRvYmUuY29tL3RpZmYvMS4wLyI+CiAgICAgICAgICAgICAgICA8ZXhpZjpV
c2VyQ29tbWVudD5TY3JlZW5zaG90PC9leGlmOlVzZXJDb21tZW50PgogICAgICAgICAgICAgICAgPC9yZGY6RGVzY3JpcHRpb24+
aXhlbFhEaW1lbnNpb24+MzI2PC9leGlmOlBpeGVsWERpbWVuc2lvbj4KICAgICAgICAgICAgICAgIDxleGlmOlBpeGVsWURpbWVu
T3JpZW50YXRpb24+MTwvdGlmZjpPcmllbnRhdGlvbj4KICAgICAgICAgICAgICAgIDx0aWZmOlJlc29sdXRpb25Vbml0PjI8L3Rp
CiAgICAgICAgICAgICAgICAgIDx0aWZmOlJlc29sdXRpb25Vbml0PjI8L3RpZmY6UmVzb2x1dGlvblVuaXQ+CiAgICAgICAgICAg
CwxsMEizYDXyAswLIIRsWXgPfgDDgmFniR0LRuCHYM+fnyWweAEkSyDYsEACsQBjIVkY2NhejO9X
55ocanqyIrI78lT1n0hpqO6MjDgnI6vyVnUf7r3tbGyDmx2wA3bADtxw4Cc3XvmFHbADdsAOnDvg
jdEngh2wA3ZgwwFvjBuG+K0dsAN2wBujzwE7YAfswIYD3hg3DPFbO2AH7IA3Rp8DdsAO2IENB7wx
bhiit3bADtqBb4w+B+vAHbADGw54Y9wwxG/tqB2wA94YfO7YATtqBzYc8Ma4YYif2qE7YAe8Mfoc
```

I . Solving the Mystery

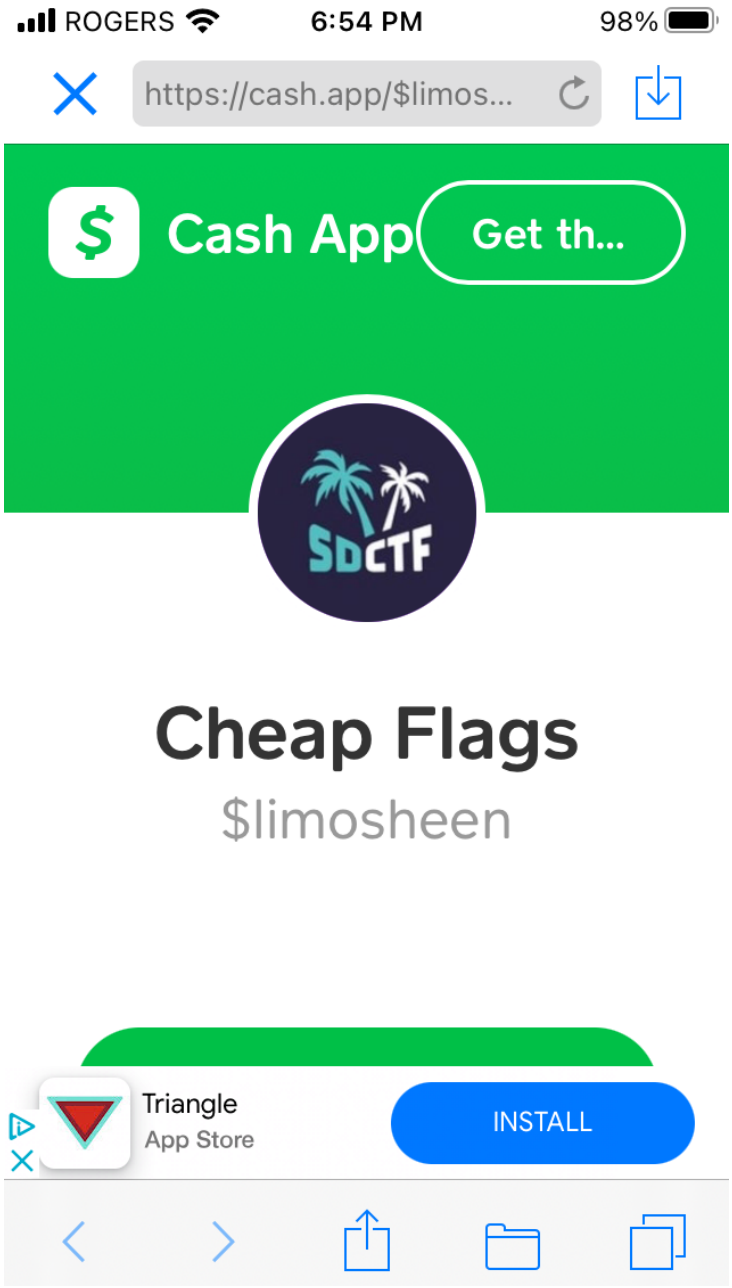
The main content of the captured email is not human readable plain text but 2 parts of long alphanumeric texts that need decoding. Using CyberChef, we can decode these base-64 texts as a message and a QR code:



The message consists of some Chinese slogans promoting the sale of SDCTF flags via Paypal and blockchain. Note that the display of 0xBAd…A34B… and the lines of emojis (which seem to require further decoding) are nothing but distractions.



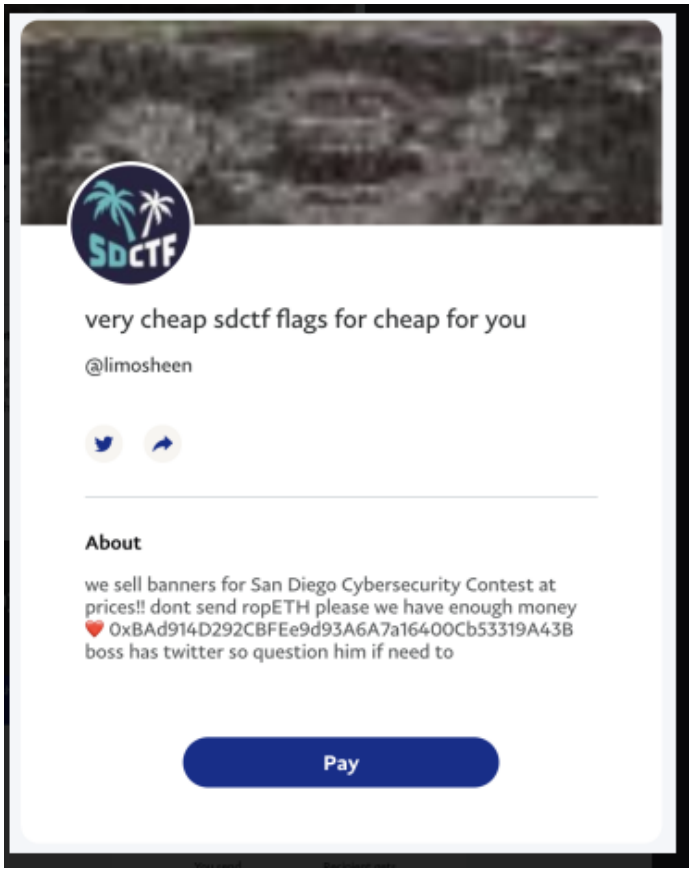
The decoded QR code leads to the site of Cash App for payment purpose:



Here we clearly see that $limosheen is the bad guy. By logging in to the site as the user $limosheen, we notice that the app will ask for email validation and expose the email format as jacxxxxx@gmail.com. This is where the challenge itself may be hacked as the CTF description says only email format of xxxxx.sdctf@gmail.com will be used. So a simple test has exposed that jack.sdctf@gmail.com is in fact the real email of $limosheen in Cash App. However, extensive online investigation on this gmail address turns out to be futile.

The next clue is Paypal and so we try to solicit any familiar flag seller. It turns out there is a user known as @limosheen in Paypal doing exactly that. Through further investigating the profile of this user in Paypal, we find some details of blockchain transaction related to the sale. In particular, the address 0xBAd914D292CBFEe9d93A6A7a16400Cb53319A43B is exposed (which echoes 0xBAd…A43B mentioned in the decoded email content). Another important hint is that the crime boss has something to do with twitter. The steps leading to this discovery in Paypal, however, is not straightforward, as the user interface of conducting a Paypal transaction may not expose this profile description of @limosheen. Instead, one has to query through paypal.me in order to dig up such details. This is not intuitive and requires an experienced PayPal user some hacking skills

either to navigate a myriad of UI or write a URL query to retrieve (https://paypal.me/limosheen?country.x=US&locale.x=en_US).



Etherscan searches on the address of 0xBAd914D292CBFEe9d93A6A7a16400Cb53319A43B will lead to a bunch of transactions that expose the destination address of the potential flag sales operation: 0x949213139D202115c8b878E8Af1F1D8949459f3f.

Etherscan

Ropsten Testnet Network

All Filters | Search by Address / Txn Hash / Block / Token / Ens

Home | Blockchain | Tokens | Misc | Ropsten

Address 0xBAd914D292CBFEe9d93A6A7a16400Cb53319A43B

Overview

Balance: 1.300000028708218 Ether

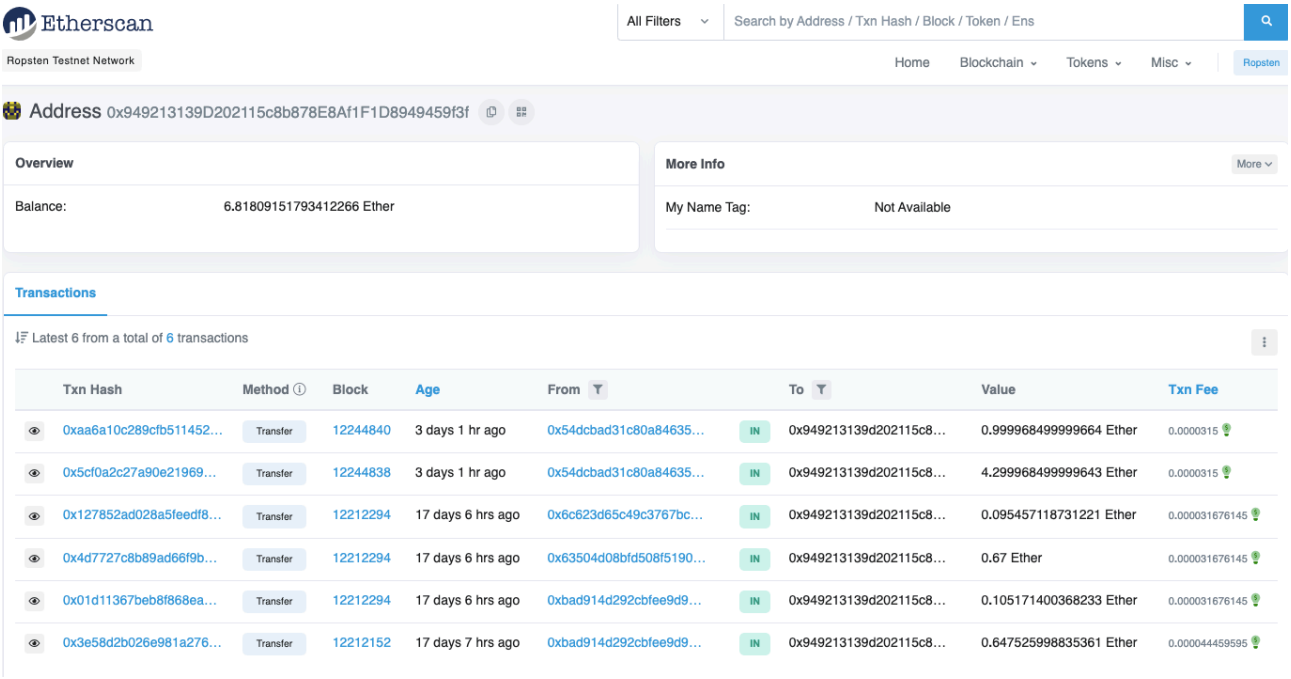
More Info

My Name Tag: Not Available

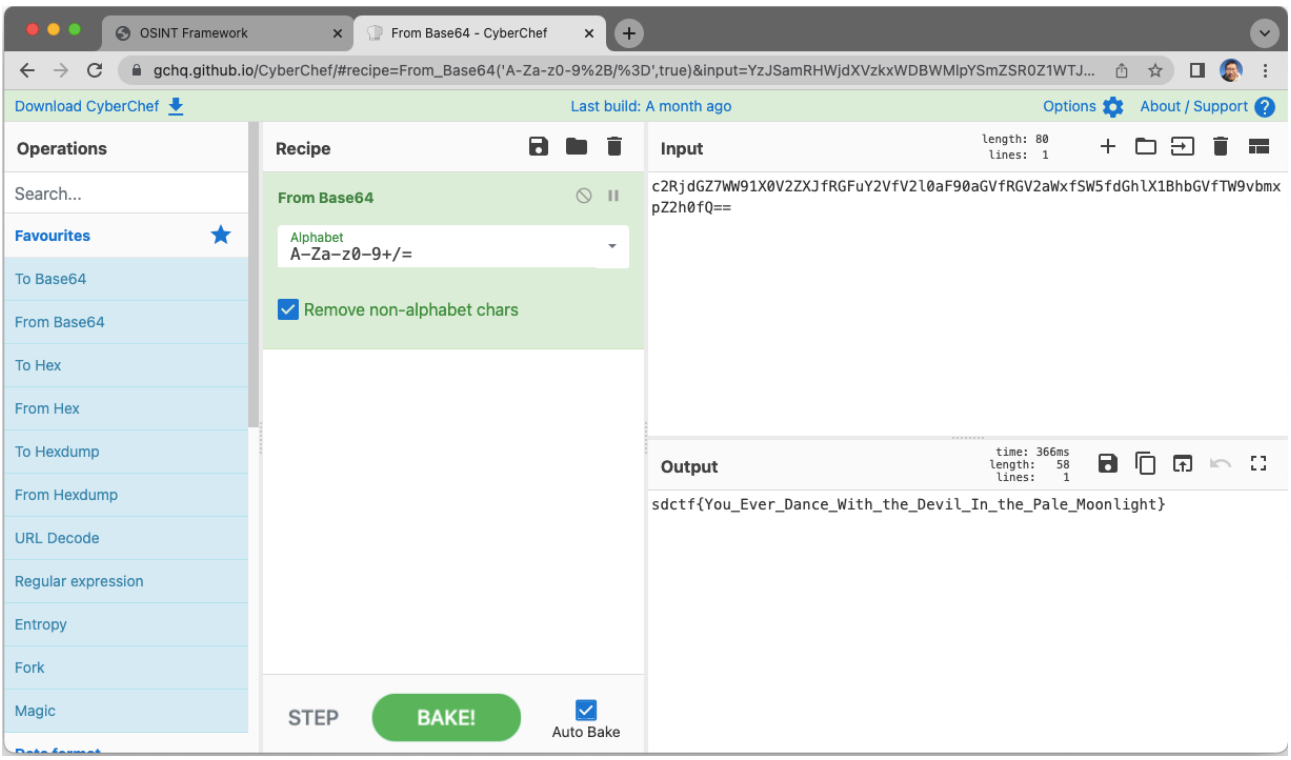
Transactions | Internal Txns

Latest 7 from a total of 7 transactions

Txn Hash	Method	Block	Age	From		To	Value	Txn Fee
0x32dcf32595755f16d34…	Transfer	12248448	1 day 21 hrs ago	0x78c115f1c8b7d0804fb…	IN	0xbad914d292cbfee9d9…	1 Ether	0.00105
0x01d11367beb8f868ea…	Transfer	12212294	17 days 6 hrs ago	0xbad914d292cbfee9d9…	OUT	0x949213139d202115c8…	0.105171400368233 Ether	0.000031676145
0x3e58d2b026e981a276…	Transfer	12212152	17 days 7 hrs ago	0xbad914d292cbfee9d9…	OUT	0x949213139d202115c8…	0.647525998835361 Ether	0.000044459595
0x8f58a54503dfa7ce4a8…	Transfer	12212152	17 days 7 hrs ago	0x63504d08bfd508f5190…	IN	0xbad914d292cbfee9d9…	0.1 Ether	0.000044459595
0x7f40600ddfc858ae7b7…	Transfer	12212152	17 days 7 hrs ago	0x63504d08bfd508f5190…	IN	0xbad914d292cbfee9d9…	0.0032 Ether	0.000044459595
0x24bc789aae244a9a0d…	Transfer	12212152	17 days 7 hrs ago	0x63504d08bfd508f5190…	IN	0xbad914d292cbfee9d9…	0.002 Ether	0.000044459595
0xebb14a4274db5ddbd4…	Transfer	12212050	17 days 8 hrs ago	0x766c94a76f3652b853…	IN	0xbad914d292cbfee9d9…	0.64757356365306 Ether	0.000090204487

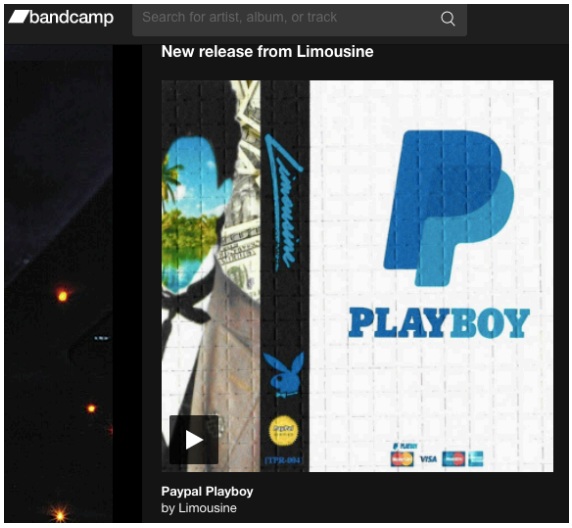


With this destination address, plus the hint that the boss is on twitter, a search in the site will locate this guy together with an encoded flag mentioned in his comments.



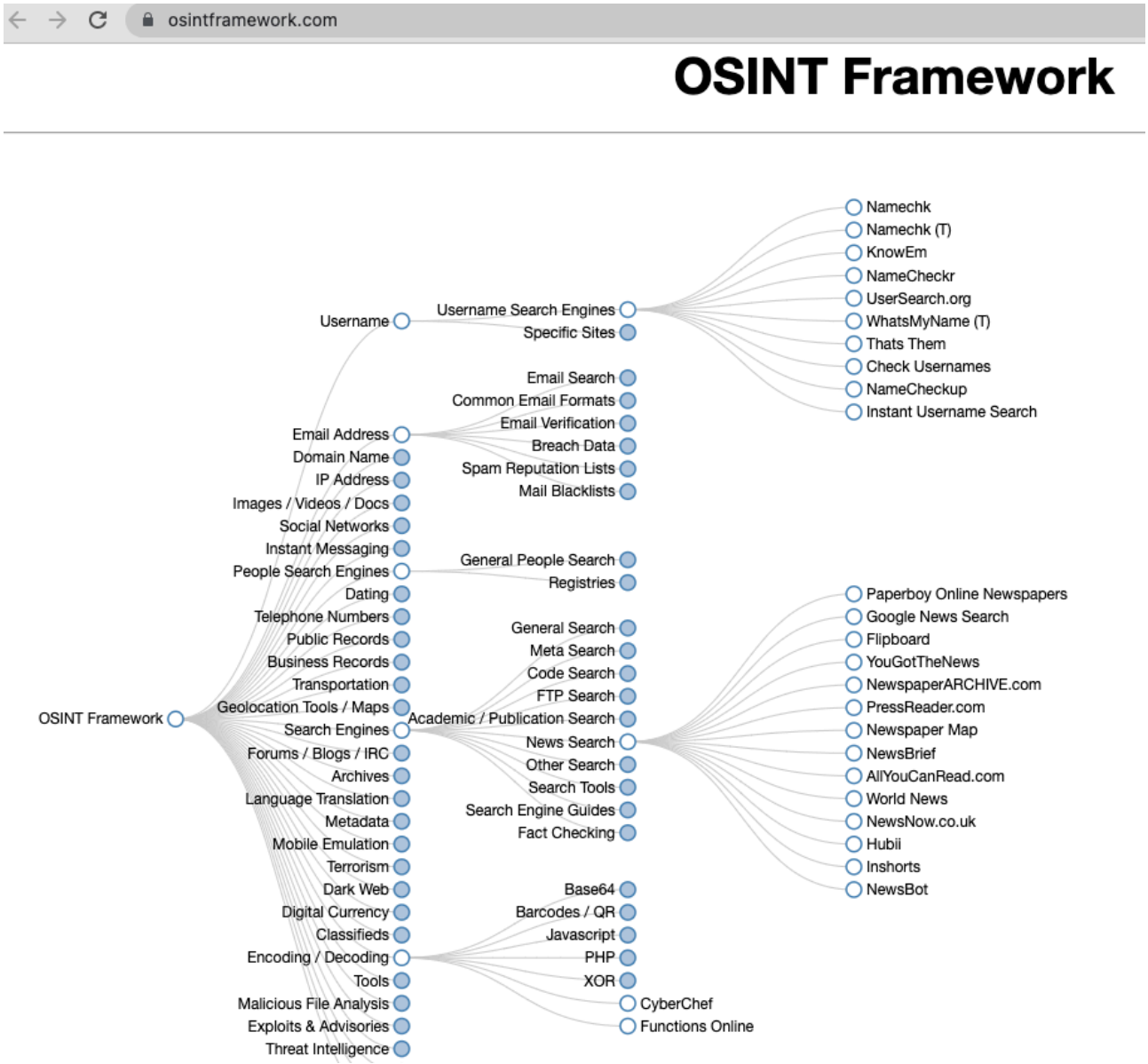
II. Lessons and Insights

There is a clear thought process behind this CTF challenge: the author wants to test the participants' skills in base64 decoding, language translation, Cash App, Paypal, blockchain transaction tracking and twitter. But what is not clear is that the author introduces a lot of noises, whether intentional or not, that may lead many clear-mind participants to many rabbit holes unnecessarily. First and foremost, the name of this challenge, Paypal-Playboy, is misleading. Where is the playboy in the grand scheme of things? There is, however, an album called Paypal-Playboy by the band Limousine, the name of which very much resembles that of @limosheen or $limosheen, which is the bad user created in Paypal and Cash App respectively. This unfortunately can lead to someone with a reasonable detective mind to dig through the bandcamp site hoping to find more clues in the fan base. It turns out that the author is a fan and nothing else.



Perhaps the most interesting question everyone should ask is this: if a bad dude is so secretive as to send out emails with encoded contents and fake addresses, why would the same criminal mind post detail instructions and sensitive addresses on Paypal and twitter openly for the world to query? Isn't the dark web a more reasonable channel for communication after all?

After all, this challenge is about finding the bad boss. But more often than not, CTF designers are more obsessed with finding the flag than achieving the goal. One would argue that finding the real email behind a payment gateway is more reliable intel than anything posted on twitter, let alone plain text description on any covert operation. In hunting down the boss, we have used a very useful site to leverage on online resources related to the OSINT framework:



While this framework may help in the real world, it often leads to information paralysis in CTF situations. Throughout this 'Paypal-Playboy' challenge, we have seen multiple instances when obvious clues are in fact rabbit holes and what seemingly credible intel leads to nowhere (e.g. exactly 0x100 emojis sitting in an encoded email message yawning for decoding, a suspicious FB user named limo sheen posting a likely encrypted picture, questionable profiles in LinkedIn / Instagram / HackerNews associated with the email account recovered from the Cash App user $limosheen, a fan in the bandcamp site trying to sell Paypal fake credits…). Perhaps the real lesson behind all these decoys and false alarms is that in the world of offensive security, it is absolutely necessary to understand your counterparts and nemesis: what they want, how they think, where they come from, when will they do what and if not…. coz in today's CTF scene will come tomorrow's cyber warfare operators. To fight for a flag will once again capture its true meaning: protecting our universal values against digital tyranny. The stakes have never been higher.