*Security is everywhere*



# BSides San Francisco CTF 2017 - Write-ups

MONDAY 13 FEBRUARY 2017 (2017-02-13)
#CRYPTO #CTF #FORENSICS #MISC #REVERSING #SECURITY #WEB #WRITEUPS

## Informations

## Version

| By | Version | Comment |
|---|---|---|
| noraj | 1.0 | Creation |

## CTF

- **Name** : BSides San Francisco CTF 2017
- **Website** : ctf.bsidessf.com
- **Type** : Online
- **Format** : Jeopardy
- **CTF Time** : link

## 1 - Hackers - Misc

CATEGORIES

- linux (30)
  - archlinux (8)
  - debian (1)
  - opensuse (7)
  - ubuntu (1)
- misc (4)
- news (7)
  - security (4)
  - warez (1)
- programming (3)
  - python (2)
  - ruby (1)
- security (121)
  - centos (2)
  - windows (4)
  - writeups (109)
- windows (3)

TAG CLOUD

anonymity apache archlinux backdoor bsd centos crypto ctf debian firefox forensics git graphic guessing hyper-v install joy kvm lfi linux misc netbios network news opensuse pentest php piracy privacy programming proxy pwn python qemu recon reverse reversing ruby security ssh stegano system tor trivia ubuntu update usenet

> *Hack the _ _ !*

Answer: `planet`

## 20 - NOP - Misc

> *x86's NOP is actually another instruction. What is the Intel syntax representation of the assembly of the other instruction?*
>
> *Include a space between operands, if applicable.*

Answer: `xchg eax, eax`

Details

# 1 - Ancient Hop Grain Juice - Misc

> *This beverage, brewed since ancient times, is made from hops and grains?*

Answer: `beer`

# 1 - The Wrong Cipher - Misc

virtualbox virtualization vulnerability warez web webshell windows writeups

ARCHIVES

- April 2017 (10)
- March 2017 (7)
- February 2017 (8)
- January 2017 (2)
- December 2016 (12)
- November 2016 (28)
- October 2016 (4)
- September 2016 (11)
- August 2016 (26)
- July 2016 (26)
- June 2016 (6)
- May 2016 (5)
- April 2016 (8)
- March 2016 (2)
- December 2015 (2)
- October 2015 (1)
- September 2015 (1)
- November 2014 (1)
- October 2014 (1)
- September 2014 (1)
- August 2014 (5)
- December 2012 (1)

> *This cipher was used incorrectly in WEP*

Answer: `RC4`

Details

# 1 - The Right Cipher - Misc

> *This cipher was correctly used in TKIP*

Answer: `RC4`

Details

# 1 - Let's play a game - Misc

> *This is the name of the game that a young hacker thinks he's playing with the WOPR Supercomputer. [Spaces expected]*

Answer: `Global Thermonuclear War`

Details

LINKS

- Hexo
- FOSS
- Torrent is not a crime

# 1 - Quote - Misc

> *This movie featured the memorable phrase "My voice is my passport"*

Answer: `Sneakers`

Movie

# 20 - Zumbo 1 - Web

> *Welcome to ZUMBOCOM....you can do anything at ZUMBOCOM.*
>
> *Three flags await. Can you find them?*
>
> *http://zumbo-8ac445b1.ctf.bsidessf.net*
>
> *Stages 2 and 3 - coming soon!*

View source of http://zumbo-8ac445b1.ctf.bsidessf.net/index.temp

```
1  <!-- page: index.template, s
```

Let's check the `/code/server.py` path: http://zumbo-8ac445b1.ctf.bsidessf.net/code/serve
We get an error:

```
1  [Errno 2] No such file or d
2  <!-- page: code/server.py, s
```

Every non-existing page give the same error. We need to do a directory traversal: http://zumbo-8ac445b1.ctf.bsidessf.net/../../../../coc
But unfortunately the `../../../../` part is automatically removed.

So I just URLencoded this part to bypass the filter: http://zumbo-8ac445b1.ctf.bsidessf.net/..%2F..%2F..

And we get the `server.py` source:

```
 1  import flask, sys, os
 2  import requests
 3
 4  app = flask.Flask(__name__)
 5  counter = 12345672
 6
 7
 8  @app.route('/<path:page>')
 9  def custom_page(page):
10      if page == 'favicon.ico
11      global counter
12      counter += 1
13      try:
14          template = open(pag
15      except Exception as e:
16          template = str(e)
```

```
17      template += "\n<!-- pag
18      return flask.render_ter
19
20  @app.route('/')
21  def home():
22      return flask.redirect('
23
24  if __name__ == '__main__':
25      flag1 = 'FLAG: FIRST_FL
26      with open('/flag') as f
27              flag2 = f.read(
28      flag3 = requests.get('h
29
30      print "Ready set go!"
31      sys.stdout.flush()
32      app.run(host="0.0.0.0")
33
34  <!-- page: ../../../../code
```

Flag was `FLAG: FIRST_FLAG_WASNT_HARD` .

**PS**: Only `page` is used so `http://zumbo-8ac445b1.ctf.bsidessf.net/server` also works...

# 100 - Zumbo 2 - Web

> *Welcome to ZUMBOCOM....you can do anything at ZUMBOCOM.*
>
> *Three flags await. Can you find them?*

> *http://zumbo-8ac445b1.ctf.bsidessf.net*
>
> *Stage 3 - coming soon!*

For the next part of the challenge, we already got the `server.py` source so I looked again at the flag2 part:

```
1  with open('/flag') as f:
2          flag2 = f.read()
```

Ok the flag is in `/flag` so just change `http://zumbo-8ac445b1.ctf.bsidessf.net/..%2f.` into `http://zumbo-8ac445b1.ctf.bsidessf.net/..%2f.`

And get the flag: `FLAG: RUNNER_ON_SECOND_BASE` .

# 100 - the-year-2000 - Web

> *Wait, what year is it?*
>
> *http://theyear2000.ctf.bsidessf*

The author says on this home page:

> *I made this website all by myself using these tools*

- *html*
- *notepad++*
- *git*
- *apache*

I tried `http://theyear2000.ctf.bsidessf.` and it returned me *Forbidden* error. So there is a `.git` repot here.

As usual I used GitTools to dump the repository:

```
$ ./gitdumper.sh http://the
Destination folder does not
Creating repo/.git/
Downloaded: HEAD
Downloaded: objects/info/pa
Downloaded: description
Downloaded: config
Downloaded: COMMIT_EDITMSG
Downloaded: index
Downloaded: packed-refs
Downloaded: refs/heads/mast
Downloaded: refs/remotes/or
Downloaded: refs/stash
Downloaded: logs/HEAD
Downloaded: logs/refs/heads
Downloaded: logs/refs/remot
Downloaded: info/refs
Downloaded: info/exclude
Downloaded: objects/4e/ec6b
Downloaded: objects/00/0000
Downloaded: objects/e0/39a6
Downloaded: objects/9e/9ce4
Downloaded: objects/f3/a3f8
Downloaded: objects/0c/e1cb
Downloaded: objects/bd/72ee
Downloaded: objects/e1/6b65
Downloaded: objects/7c/57d1
Downloaded: objects/7b/aff3
```

A quick `git log -p` show me this commit:

```
commit 4eec6b9c6e464c35fff
Author: Mark Zuckerberg <th
Date:   Sat Feb 11 22:54:32

    Wooops, didn't want to

diff --git a/index.html b/
index 7c57d17..e16b652 100
--- a/index.html
+++ b/index.html
@@ -15,7 +15,7 @@ pre {
 </style>
 </head>
 <body>
-<h1>Welcome to my homepage
+<h1>Welcome to my homepage
 <hr>
 <p>I made this website all
 <ul>
```

There was a rebase so let's see when it happened:

```
$ git reflog
4eec6b9 HEAD@{0}: commit: Wo
e039a66 HEAD@{1}: reset: mov
9e9ce4d HEAD@{2}: commit: F
e039a66 HEAD@{3}: commit (in
```

Ok so we have to come back before the HEAD reset:

```
$ git reset --hard HEAD@{2}
HEAD is now at 9e9ce4d Fixed
```

Now let's take a look at this fix: `git log -p -1`

```
commit 9e9ce4da43d0d2dc10ec
Author: Mark Zuckerberg <th
Date:   Sat Feb 11 22:54:27

    Fixed a spelling error

diff --git a/index.html b/i
index 7c57d17..7baff32 100
--- a/index.html
+++ b/index.html
@@ -43,3 +43,4 @@ _________
 </pre>
 </marquee>
 </body></html>
+Your flag is... FLAG:what_
```

Here is teh flag:

`FLAG:what_is_HEAD_may_never_die`

# 40 - easycap - Forensics

> *Can you get the flag from the packet capture?*
>
> - *easycap.pcap*

This is some raw tcp frames and some of them have 1 byte of additional data.

Let's extract that with *tshark*:

```
$ tshark -r easycap.pcap -T
464c41473a33383562383761666
```

Now translate hex to ASCII with a little ruby trick:

```
irb(main):008:0> ['464c4147
=> "FLAG:385b87afc8671dee07
```

Flag is `FLAG:385b87afc8671dee07550290d1`

# 10 - Easy - Reversing

> *This one is easy.*

- *easy-32*
- *easy-64*

```
$ strings easy-64 | grep -i
FLAG:db2f62a36a018bce28e46d
```

# 30 - easyauth - Web

> *Can you gain admin access to this site?*
>
> *http://easyauth-afee0e67.ctf.bsidessf.net*
>
> - *easyauth.php*

Hint say to log in with: guest/guest

We have a cookie like this:

```
1  auth=username=guest&date=20
```

If we click on the link we get the following message:

> *It's cool that you logged in, but unfortunately we can only give the flag to 'administrator'. :(*

Configure proxy and launch burpsuite.

Then change `guest` into `administrator` in the cookie and send. You now get the flag:

> *Congratulations, you're the administrator! Here's your reward:*
>
> *FLAG:0076ecde2daae415d7e5*

# 450 - vhash - Crypto

> *---- Due to a bug, the challenge might be easier than intended. Enjoy the free points! ----*
>
> *Can you gain admin access to this site?*
>
> *(The vhash binary is what's used for signing the cookie)*
>
> *http://vhash-c6bb0e85.ctf.bsidessf.net:929*
>
> - *vhash.zip*

The zip contain the `vhash` ELF executable and the `index.php` source:

```
1  <?php
2    require_once('./auth.php'
3
4    function do_hash($data) {
5      $filename = tempnam(sys
6      file_put_contents($file
7
8      $hash = substr(`/home/c
9      unlink($filename);
10
11     return $hash;
12   }
13
14   function create_hmac($dat
```

```
15      return do_hash(SECRET .
16    }
17
18    if(isset($_GET['action'])
19      setcookie('auth', '');
20      header('Location: inde
21    }
22
23    if(isset($_POST['username
24      # Do pagey stuff
25      if(is_valid($_POST['use
26        # Create the cookie
27        $cookie = 'username='
28        $cookie .= 'date=' .
29        $cookie .= 'secret_le
30
31        # Sign the cookie
32        $cookie = create_hmac
33        setcookie('auth', $co
34        print "<h1>Login succ
35        print "<p>Setting coo
36      } else {
37        print "<h1>Username c
38      }
39      print "<p>Click <a href
40      exit(0);
41    }
42
43    if(!isset($_COOKIE['auth'
44      require_once('./login_f
45      exit(0);
46    }
47
48    list($hmac, $cookie) = ex
49    if(create_hmac($cookie) !
50      setcookie('auth', '');
51      print "<p>Something was
52      print "<p>Click <a href
53      exit();
54    }
55
56    $pairs = explode('&', $co
57    $args = array();
58    foreach($pairs as $pair)
59      if(!strpos($pair, '='))
60        continue;
```

```
61      list($name, $value) = e
62      $args[$name] = $value;
63    }
64    $username = $args['usern
65
66    print "<h1>Welcome back,
67    if($username == 'adminis
68      print "<p>Congratulatic
69      print "<p>" . FLAG . "<
70    } else {
71      print "<p>It's cool tha
72    }
73    print "<p><a href='/inde
74  ?>
75
```

Description says the challenge is more easy due to a bug, here it is:

```
1  if($username == 'administra
```

So the challenge is exactly like the previous **30 - easyauth - Web**.

Configure proxy and launch burpsuite.

Then change `guest` into `administrator` in the cookie and send. You now get the flag:

> *Congratulations, you're the administrator! Here's your reward:*
>
> *FLAG:180e2300112ef5a4f23c*

---