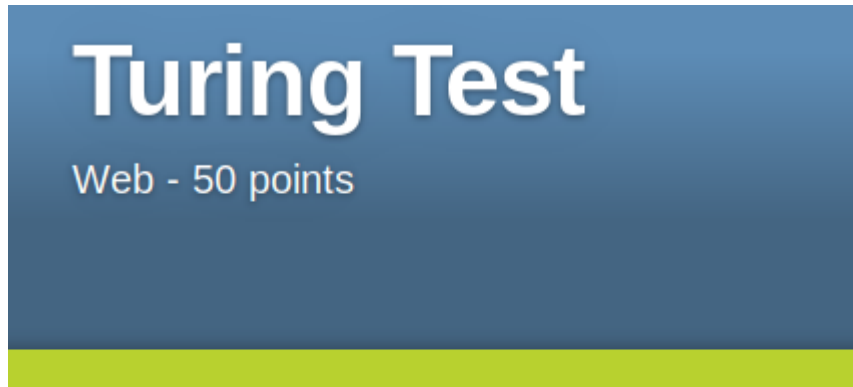


## STEM CTF: Cyber Challenge 2019 Write-ups

好久没有玩CTF，跪了(QAQ) 本文是关于web题目的解析后面两题是赛后，看着大佬的思路进行复现的，文末已经给出相应的参考文章

什么都不说了，先跪就好(Orz)

### Turing Test



## Description

Break into his account!

<http://138.247.13.111>

<http://138.247.13.111/>

这一题被称为热身题，只需要结合这个维基百科就可以得到flag:[https://en.wikipedia.org/wiki/Alan\\_Turing](https://en.wikipedia.org/wiki/Alan_Turing)

A screenshot of a web browser showing an 'Account Recovery for Alan Turing' form. The browser's address bar shows '138.247.13.111' with a warning icon and the text '不安全'. The form has a blue background with a wooden handle. The form fields are: 'Mother's Maiden Name' (Stoney), 'First School Attended' (St. Michael's), 'Favorite Primary School Subject' (science), 'Favorite Olympic Event' (marathon), '2 + 2 - 3 = ?' (1), 'Is it a leap year?' (checked), and 'I agree Security Questions are Bad' (checked). A 'Submit' button is at the bottom.

← → ↻ ⚠ 不安全 | 138.247.13.111

应用

### Account Recovery for Alan Turing

Before we are able to reset your password, you'll need to provide the answers to the following security questions.

Mother's Maiden Name

Stoney

First School Attended

St. Michael's

Favorite Primary School Subject

science

Favorite Olympic Event

marathon

$2 + 2 - 3 = ?$

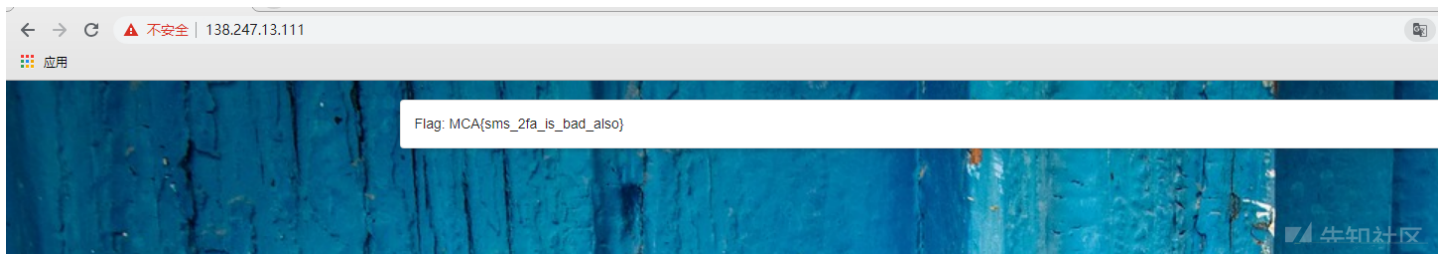
1

☒ Is it a leap year?

☒ I agree Security Questions are Bad

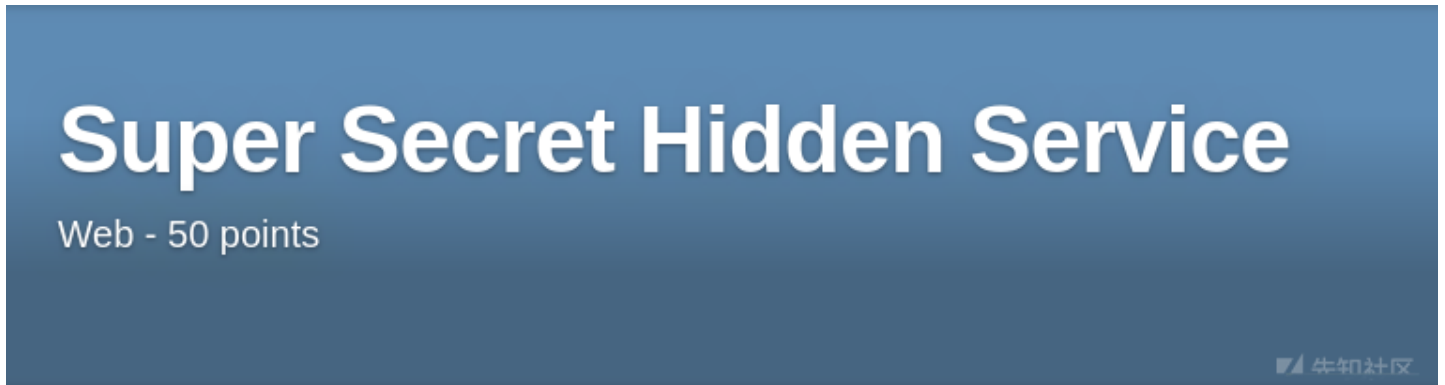
Submit

成功拿到flag：



Flag: MCA{sms\_2fa\_is\_bad\_also}

Super Secret Hidden Service



<https://138.247.13.115/>

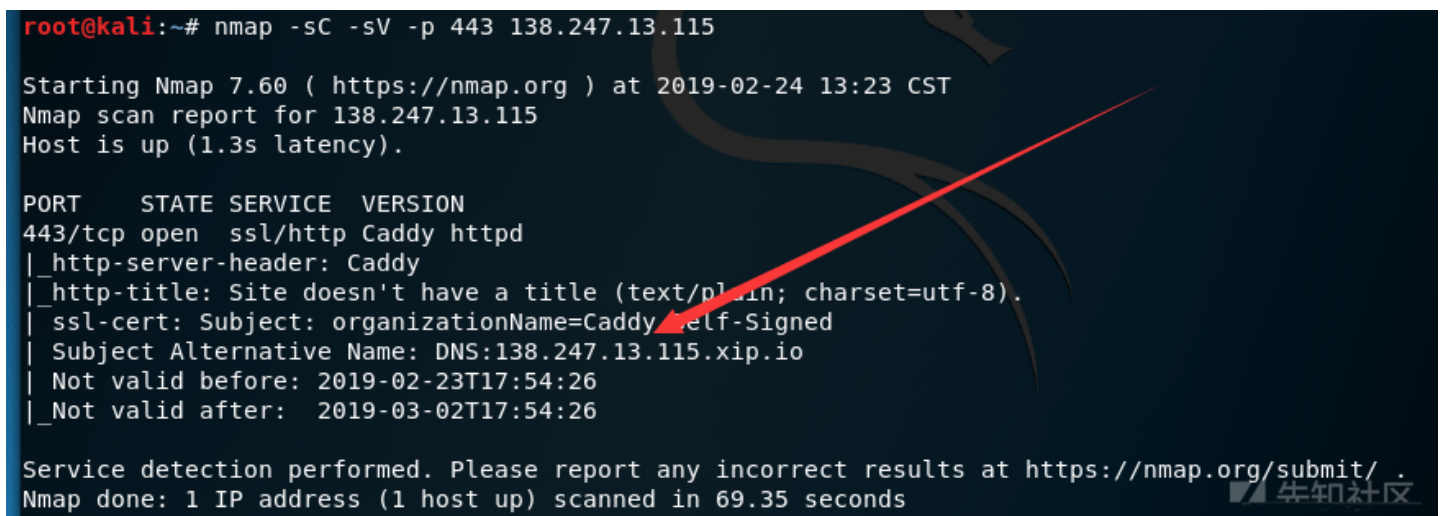
由给出的链接进入网站发现Google对于这个网站的返回报错处理：



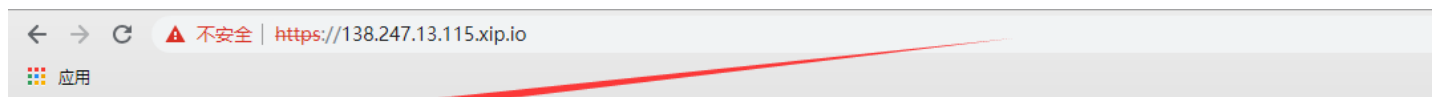
这只是意味着caddy服务响应客户端发送的服务器名称，因为我们发送了这个IP，我们得到了错误响应，所以我们需要知道这个域名。

具体原因可以参考：<https://nvd.nist.gov/vuln/detail/CVE-2018-19148>

我们使用nmap进行简单的扫描就会得到



访问扫描得到的DNS:138.247.13.115.xip.io就可以得到flag：



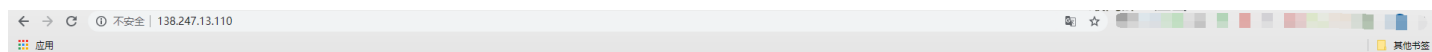
Flag is: MCA{shuHeimoowaiF5a}

先知社区

TODO



<http://138.247.13.110/>



TODOLIST

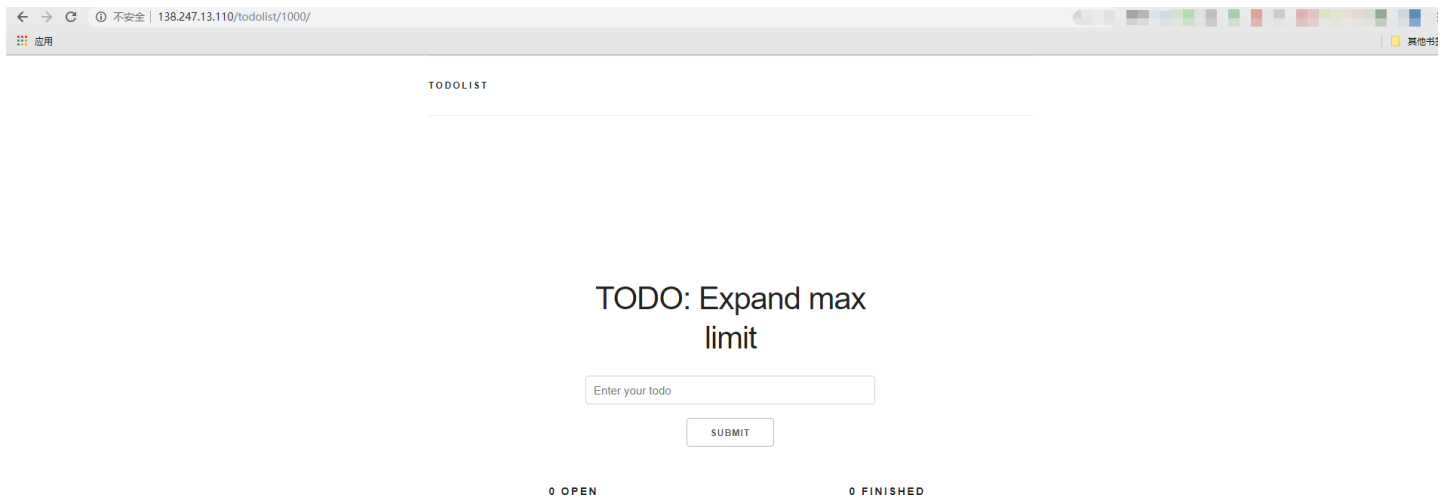
Dead simple Todolists.

Enter your todo

START ONE NOW

先知社区

随手输入内容进行简单的测试，发现输入的内容重定向到：<http://138.247.13.110/todolist/1000/>



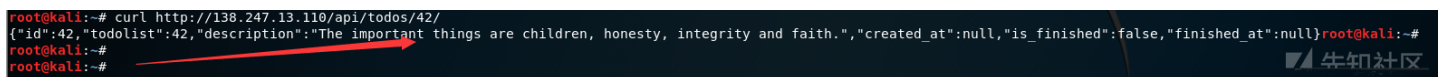
查看网页源代码发现两个自定义的js脚本



lists.js 这个是对我们有用的脚本，仔细读取后面的内容可以发现

```
// send put request using the data of the get for the same id
var todoURL = '/api/todos/' + todoID + '/'
$.getJSON(todoURL, function(data) {
data.is_finished = isFinished;
if (isFinished) {
data.finished_at = moment().toISOString();
} else {
data.finished_at = null;
}
$.ajax({
url: todoURL,
type: 'PUT',
contentType: 'application/json',
data: JSON.stringify(data),
success: function() {
location.reload();
}
});
```

我们可以访问这里面的数据



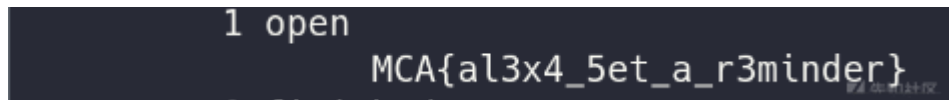
因此我们只需要使用burp，对<http://138.247.13.110/api/todos/<id>> /其中的id从1遍历到1000即可</id>

得到flag：MCA{al3x4\_5et\_a\_r3minder}

或者写一个脚本：

```
import requests
import re
url = 'http://138.247.13.110/todolist/'

for i in range(1,1001):
    print('Requesting ' + url + str(i))
    response = requests.get(url + str(i))
    stripped = re.sub('<[^<]+?>', '', response.text)
    if 'MAC' in stripped:
        print(stripped.strip())
        break
```



## My First Blog

由于能力原因，本题并未能够做出，这一题的思路后面将会给出参考文章

<http://138.247.13.106/>



Bazaar - 世界上最好的版本控制！是一个线索，我们可以使用工具dvcs-ripper 找到Bazaar的源码

工具链接：<https://github.com/kost/dvcs-ripper>

```
% ~/CTF/tools/dvcs-ripper/rip-bzr.pl -v -u http://138.247.13.106/.bzr/
[i] Downloading bzr files from http://138.247.13.106/.bzr/
[i] Auto-detecting 404 as 200 with 3 requests
[i] Getting correct 404 responses
[d] found branch-format
[d] found branch/branch.conf
[d] found branch/format
[d] found branch/last-revision
[d] found branch/tags
[d] found checkout/conflicts
[d] found checkout/dirstate
[d] found checkout/format
[!] Not found for checkout/merge-hashes: 404 Not Found
[d] found checkout/views
[d] found repository/format
[d] found repository/pack-names
[i] Running bzr check to check for missing items
[i] Getting repository/indices/c325a543411b3717bd63b6cc879e3d50.rix
[d] found repository/indices/c325a543411b3717bd63b6cc879e3d50.rix
[i] Got items with bzr check: 1
[i] Items fetched: 1
[i] Running bzr check to check for missing items
```

```
[i] Getting repository/packs/c325a543411b3717bd63b6cc879e3d50.pack
[d] found repository/packs/c325a543411b3717bd63b6cc879e3d50.pack
[i] Got items with bzd check: 1
[i] Items fetched: 1
[i] Running bzd check to check for missing items
[i] Getting repository/indices/c325a543411b3717bd63b6cc879e3d50.iix
[d] found repository/indices/c325a543411b3717bd63b6cc879e3d50.iix
[i] Got items with bzd check: 1
[i] Items fetched: 1
[i] Running bzd check to check for missing items
[i] Getting repository/indices/c325a543411b3717bd63b6cc879e3d50.cix
[d] found repository/indices/c325a543411b3717bd63b6cc879e3d50.cix
[i] Got items with bzd check: 1
[i] Items fetched: 1
[i] Running bzd check to check for missing items
[i] Getting repository/indices/c325a543411b3717bd63b6cc879e3d50.tix
[d] found repository/indices/c325a543411b3717bd63b6cc879e3d50.tix
[i] Got items with bzd check: 1
[i] Items fetched: 1
[i] Running bzd check to check for missing items
[i] Got items with bzd check: 0
[i] Items fetched: 0
[i] Finished fetching (5/5)
[i] Checking out/Reverting source by calling bzd revert
N index.php
```

现在我们可以看到以前提交的源代码文件

```
% bzd log
-----
revno: 1
committer: BZR Lover
branch nick: filePathTraversalEasy
timestamp: Thu 2018-12-06 13:48:25 -0500
message:
  BZR is so cool!

% bzd revert

% cat index.php|grep MCA
// Flag is MCA{canonical_is_literally_my_favorite_company_in_the_whole_world}
```

Medium is overrated

<http://138.247.13.104/>

← → ↻ 不安全 | 138.247.13.104 应用 其他书签

## My Blog

Just a spot for me to talk about how much I love Canonical

### CentOS is just RedHat

A friend of mine was explaining how the company he works for pays for RedHat. I don't understand why they are LITERALLY throwing their money away since CentOS is just RedHat. In fact, CentOS is even better than RedHat since it discovers the fastest mirror automatically. I'm applying for one of their open job reqs just to give them a piece of my mind.

### I love Canonical

As someone who is just getting started with Linux, I love Canonical. They build the easiest to use Linux distribution I can find, and they build so many useful tools. So far I've tried out

- Juju - The worlds best configuration management tool!
- Bazaar - The worlds best version control!
- Ubuntu - The worlds best OS!
- Launchpad - GitHub? Gross!

### Learning PHP

I recently learned about PHP and I can't stop switching everything over to it. In fact, this blog is now powered by PHP, I think! I changed the file extension at least, and added a little PHP code below here. That should pretty much do it right? I have the PHP code commented out for now since I can't seem to get it to work right. I'll have to look into it later.

这一题我们可以使用与上面一题同样的方式进行解答

```
$ ~/CTF/tools/dvcs-ripper/rip-bzr.pl -v -u http://138.247.13.104/.bzr/
```

然后我们可以为index.php文件显示提交历史记录 ( -p : 显示每个修订版本的不同 ) :

```
% bzr log -p index.php
```

```
-----
revno: 167
committer: BZR Lover
branch nick: filePathTraversalHard
timestamp: Thu 2018-12-06 18:00:21 -0500
message:
  Oops
diff:
=== modified file 'index.php'
--- index.php      2018-12-06 23:00:02 +0000
+++ index.php      2018-12-06 23:00:21 +0000
@@ -28,5 +28,4 @@
?>
</div>
</body>
-</html>
-<!-- 6fb3b5b05966fb06518ce6706ec933e79cfaea8f12b4485cba56321c7a62a077 --->
\ No newline at end of file
+</html>
\ No newline at end of file
-----
revno: 166
committer: BZR Lover
branch nick: filePathTraversalHard
timestamp: Thu 2018-12-06 18:00:02 -0500
message:
  CentOS is just RedHat
diff:
=== modified file 'index.php'
--- index.php      2018-12-06 22:54:52 +0000
+++ index.php      2018-12-06 23:00:02 +0000
@@ -10,6 +10,8 @@
<h1 class="display-4">My Blog</h1>
<p class="lead">Just a spot for me to talk about how much I love Canonical</p>
</div>
+<h1>CentOS is just RedHat</h1>
+<p>A friend of mine was explaining how the company he works for pays for RedHat. I don't understand why they are LITERALLY th
<h1>I love Canonical</h1>
<p>As someone who is just getting started with Linux, I love Canonical. They build the easiest to use Linux distribution I can
<ul>
@@ -26,4 +28,5 @@
?>
</div>
</body>
-</html>
\ No newline at end of file
+</html>
+<!-- 6fb3b5b05966fb06518ce6706ec933e79cfaea8f12b4485cba56321c7a62a077 --->
\ No newline at end of file
-----
revno: 156
committer: BZR Lover
branch nick: filePathTraversalHard
timestamp: Thu 2018-12-06 17:54:52 -0500
message:
  Nevermind on the blog post
diff:
=== modified file 'index.php'
--- index.php      2018-12-06 22:52:42 +0000
+++ index.php      2018-12-06 22:54:52 +0000
@@ -10,11 +10,6 @@
<h1 class="display-4">My Blog</h1>
<p class="lead">Just a spot for me to talk about how much I love Canonical</p>
```

```
</div>
-<h1>Encryption is so cool!</h1>
-<p>It's so cool that I can paste a block of text here and if its encrypted then none of you will EVER be able to read it! Aft
-<p>NWEyYTk5ZDNiYWFEwN2JmYmQwOGI5NjEyMDVkyY2FlODg3ZmIwYWNmOWYyNzI5MjliYWE3OTExZmFhNGFlNzclMQ==</p>
-<p>There's like a whole 3 Bitcoin in there, but none of you will ever be able to get it!</p>
-<hr>
<h1>I love Canonical</h1>
<p>As someone who is just getting started with Linux, I love Canonical. They build the easiest to use Linux distribution I can
<ul>
-----

revno: 155
committer: BZR Lover
branch nick: filePathTraversalHard
timestamp: Thu 2018-12-06 17:52:42 -0500
message:
  Add a new blog post!
diff:
=== modified file 'index.php'
--- index.php      2018-12-06 18:48:25 +0000
+++ index.php      2018-12-06 22:52:42 +0000
@@ -10,6 +10,11 @@
<h1 class="display-4">My Blog</h1>
<p class="lead">Just a spot for me to talk about how much I love Canonical</p>
</div>
+<h1>Encryption is so cool!</h1>
+<p>It's so cool that I can paste a block of text here and if its encrypted then none of you will EVER be able to read it! Aft
+<p>NWEyYTk5ZDNiYWFEwN2JmYmQwOGI5NjEyMDVkyY2FlODg3ZmIwYWNmOWYyNzI5MjliYWE3OTExZmFhNGFlNzclMQ==</p>
+<p>There's like a whole 3 Bitcoin in there, but none of you will ever be able to get it!</p>
+<hr>
+<h1>I love Canonical</h1>
+<p>As someone who is just getting started with Linux, I love Canonical. They build the easiest to use Linux distribution I can
+<ul>
-----

revno: 1
committer: BZR Lover
branch nick: filePathTraversalEasy
timestamp: Thu 2018-12-06 13:48:25 -0500
message:
  BZR is so cool!
diff:
=== added file 'index.php'
--- index.php      1970-01-01 00:00:00 +0000
+++ index.php      2018-12-06 18:48:25 +0000
@@ -0,0 +1,29 @@
+<html>
+<head>
+<title>My Blog</title>
+<link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0/css/bootstrap.min.css" integrity="sha384-Gn5384x
+</head>
+<body>
+
+<div class="container">
+<div class="jumbotron">
+<h1 class="display-4">My Blog</h1>
+<p class="lead">Just a spot for me to talk about how much I love Canonical</p>
+</div>
+<h1>I love Canonical</h1>
+<p>As someone who is just getting started with Linux, I love Canonical. They build the easiest to use Linux distribution I ca
+<ul>
+<li>Juju - The worlds best configuration management tool!</li>
+<li>Bazaar - The worlds best version control!</li>
+<li>Ubuntu - The worlds best OS!</li>
+<li>Launchpad - GitHub? Gross!</li>
+</ul>
+<hr>
+<h1>Learning PHP</h1>
+<p>I recently learned about PHP and I can't stop switching everything over to it. In fact, this blog is now powered by PHP, I
+<?php
+// Flag is MCA{canonical_is_literally_my_favorite_company_in_the_whole_world}
```



```
+?>
+</div>
+</body>
+</html>
\ No newline at end of file
```

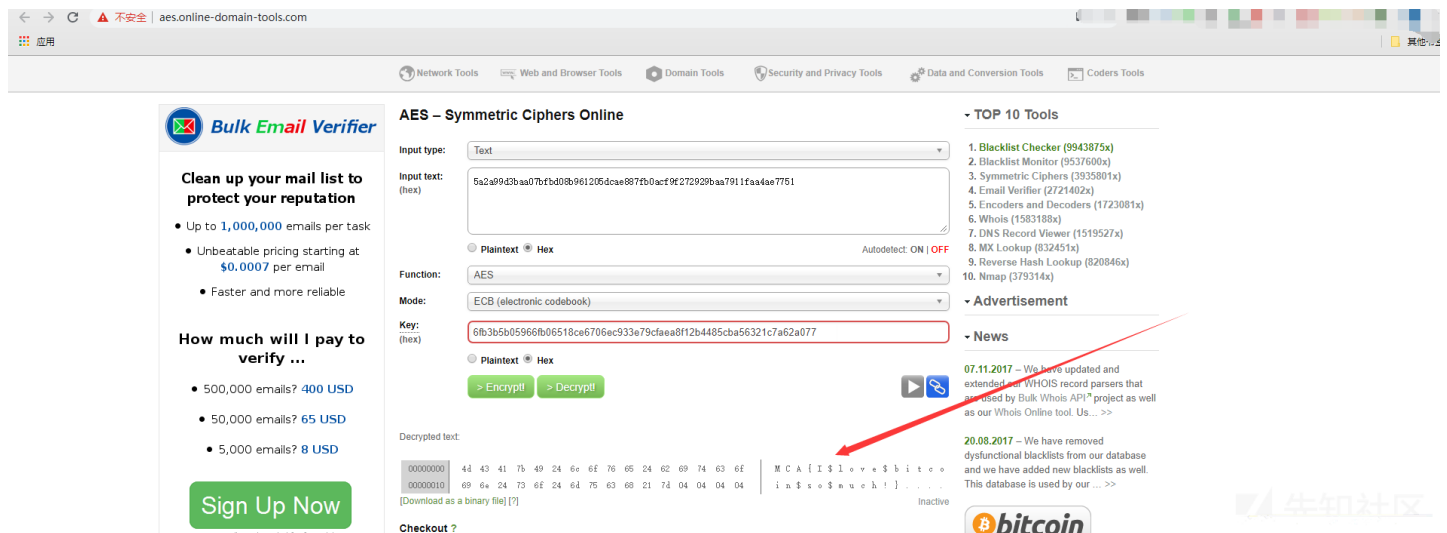
所以很容易拿到私钥：NWEyYTk5ZDNiYWwN2JmYmQwOGI5NjEyMDVhY2F1ODg3ZmIwYWNmOWYyNzI5MjliYWE3OTExZmFhNGF1Nzc1MQ==

使用base64进行解密就会得到：



由于AES ECB密钥必须是：6fb3b5b05966fb06518ce6706ec933e79cf8a8f12b4485cba56321c7a62a077

使用在线解密工具：<http://aes.online-domain-tools.com/>



得到flag:MCA{I\$love\$bitcoin\$so\$much!}

参考资料：

<https://rawsec.ml/en/STEM-CTF-2019-write-ups/>

点击收藏 | 0 关注 | 1

[上一篇：如何使用PowerShell Em...](#) [下一篇：如何使用PowerShell Em...](#)

1. 0 条回复

- 动动手指，沙发就是你的了！

[登录](#) 后跟帖

先知社区

[现在登录](#)

热门节点

[技术文章](#)

[社区小黑板](#)

[目录](#)

[RSS](#) [关于社区](#) [友情链接](#) [社区小黑板](#)