

Infosec institute n00bs CTF writeup

转载

[weixin_30448603](#)



于 2015-03-30 13:38:00 发布



199



收藏

文章标签: [php](#)

原文链接: <http://www.cnblogs.com/websec/p/4377835.html>

版权

when i browse the Infosec institute website, i saw a article about the n00bs CTF, recently i am attend some ctf like bctf and Octf

i like it so, i try the n00bs!

Home Page Levels ()

woot! \$1200 bounty available.

The Infosec Instite n00bs CTF Labs is a web application that hosts 15 mini Capture the Flag (CTF) challenges intended for beginners. The levels can be navigated in the navbar. There is no scoring or leaderboard, but to claim the bounty for each level (bounties range from \$10 to \$150) you'll need to write up the solution and any other helpful instructions or information and post that in a public place (blog, forum, etc.). If you don't have a place to post it...ask a friend!

Why? This is a learning tool and we want to promote using it as a learning tool in other places where new students of information security might be reading. After you have written up your explanation, send the link to ryan.fahey@infosecinstitute.com.

We will judge the most helpful posts, choose a winner, and post them on the [InfoSec Institute Resources](#) site. You can win up to 3 flags - we will award your highest paying 3 if you capture more. No current or former InfoSec Institute employees may enter

Happy hacking!

[< Learn More >](#)

1.Level one

Home Page Levels ()

May the source be with you!

Bounty: \$10

as we can see, the string "May the source be with you!" so we press Ctrl + u to view the source code. In the top side ,we could see the Flag is here! We got it!{infosec_flagis_welcome}

```
1 <!-- infosec_flagis_welcome -->
2 <!DOCTYPE html>
3 <html lang="en">
4   <head>
5     <meta charset="utf-8">
6     <meta name="viewport" content="width=device-width, initial-scale=1.0">
7     <meta name="description" content="a ctf for newbies">
8     <title>Infosec Institute n00bs CTF Labs</title>
9     <link href="css/bootstrap.css" rel="stylesheet">
10    <link href="css/custom.css" rel="stylesheet">
11  </head>
12
13 <body>
14   <div class="navbar navbar-inverse navbar-fixed-top">
15     <div class="navbar-inner">
16       <div class="container-fluid">
17         <a class="brand" href="index.php">Home Page</a>
18         <ul class="nav nav-pills">
19           <li class="dropdown">
20             <a href="#" class="dropdown-toggle" role="menu" data-toggle="dropdown"> Le
21             <ul class="dropdown-menu">
22               <li>
23                 <a href="levelone.php">Level 1</a>
24               </li>
25               <li>
26                 <a href="leveltwo.php">Level 2</a>
27               </li>
28               <li>
29                 <a href="levelthree.php">Level 3</a>
30               </li>
31               <li>
32                 <a href="levelfour.php">Level 4</a>
33               </li>
34               <li>
35                 <a href="levelfive.php">Level 5</a>
36               </li>
37               <li>
38                 <a href="levelsix.php">Level 6</a>
39               </li>
40               <li>
41                 <a href="404.php">Level 7</a>
42               </li>
43               <li>
```

2.Level two

Address:<http://ctf.infosecinstitute.com/leveltwo.php>

open the url above, i saw a broken image, so i download the weard img file to my computer, then i use the hex editor to open the img file, i saw a base64 string: `aW5mb3NIY19mbGFnaXNfd2VhcmVqdXN0c3RhcnRpbmc=`

and we decode the string and get the flag is : `infosec_flagis_wearejuststarting`

3.Level three

Address:<http://ctf.infosecinstitute.com/img/qrcode.png>

open the url above, we could see a qrcode, so first we decode the qrcode and see what secret hide in it.

