

攻防世界web篇writeup

原创

卡面来打01 于 2021-02-23 14:39:31 发布 247 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/qq_51954912/article/details/113882224

版权

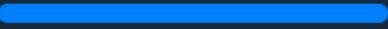
view_source  151 最佳Writeup由Healer_aptx • Anchorite提供

难度系数:  1.0

题目来源: [Cyberpeace-n3k0](#)

题目描述: X老师让小宁同学查看一个网页的源代码, 但小宁同学发现鼠标右键好像不管用了。

题目场景:  <http://111.200.241.244:49206>

 [删除场景](#)

倒计时: 03:59:42 [延时](#)

题目附件: 暂无

https://blog.csdn.net/qq_51954912

1.

打开场景发现

FLAG is not here

我们先查看网页源码

```
<!-- cyberpeace{90974ac5b2ffa6e4431635213f38b5a9} -->
```

发现

经过查询, cyberpeace为网络安全的意思, 即明白, 此为flag

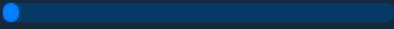
robots  166 最佳Writeup由MOLLYMY提供

难度系数:  1.0

题目来源: [Cyberpeace-n3k0](#)

题目描述: X老师上课讲了Robots协议, 小宁同学却上课打了瞌睡, 赶紧来教教小宁Robots协议是什么吧。

题目场景:  4%



题目附件: 暂无

https://blog.csdn.net/qq_51954912

2.

先了解什么是robots协议

发现只需在url后添加robots.txt即可查看robots协议

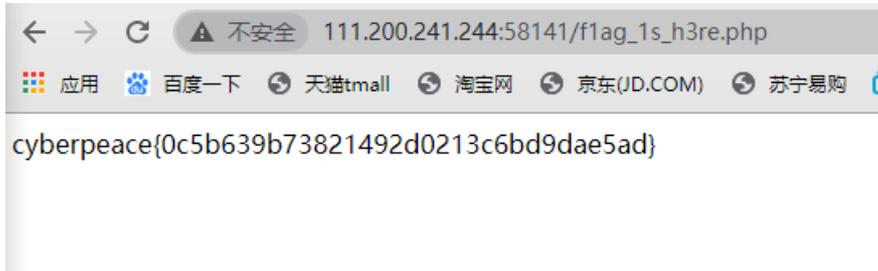
Robots协议是什么?

很简单,在网站的根目录域名后加上/robots.txt就可以了。例如,通过<https://www.douban.com/robots.txt>这个链接可以查看淘宝的 **Robots 协议**。

```
User-agent: *
Disallow:
Disallow: flag_1s_h3re.php
```

发现

本以为flag_1s_h3re.php, 为flag, 结果提交错误想到robots协议的特点, 将flag_1s_h3re.php放到url后, 即发现flag



3.

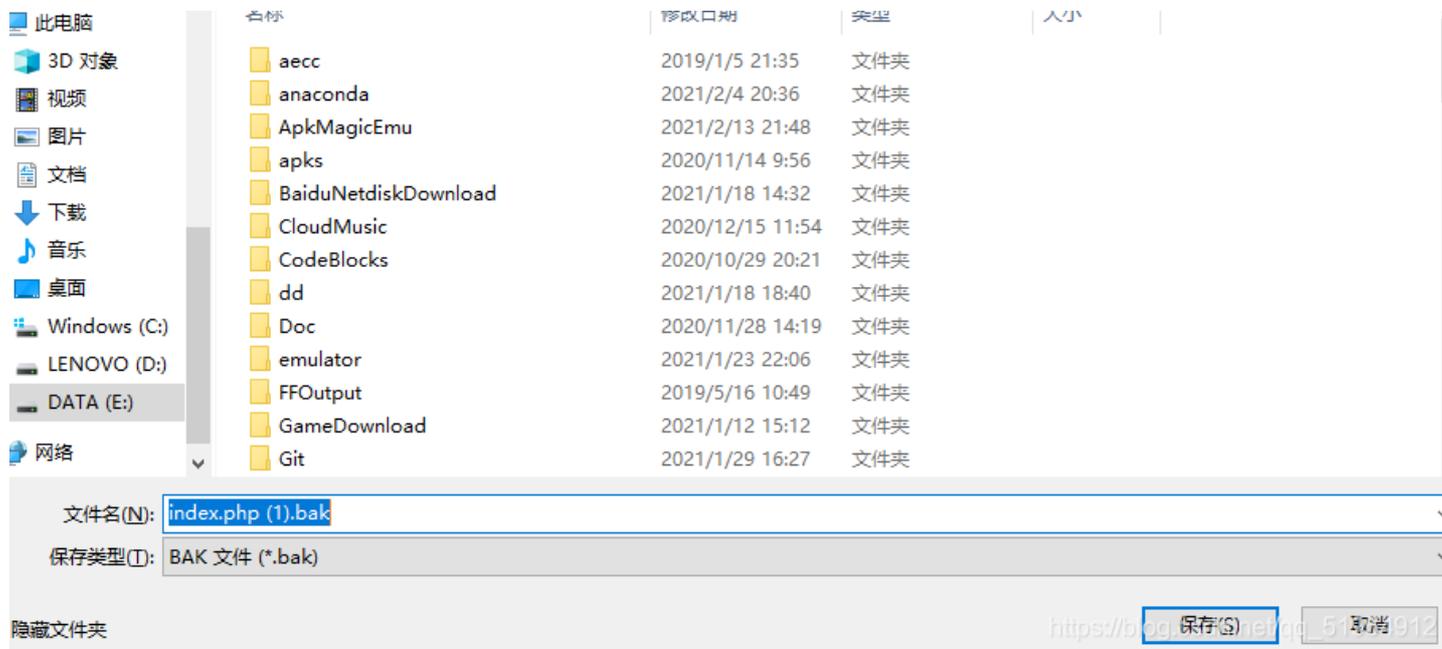


首先了解一个知识点

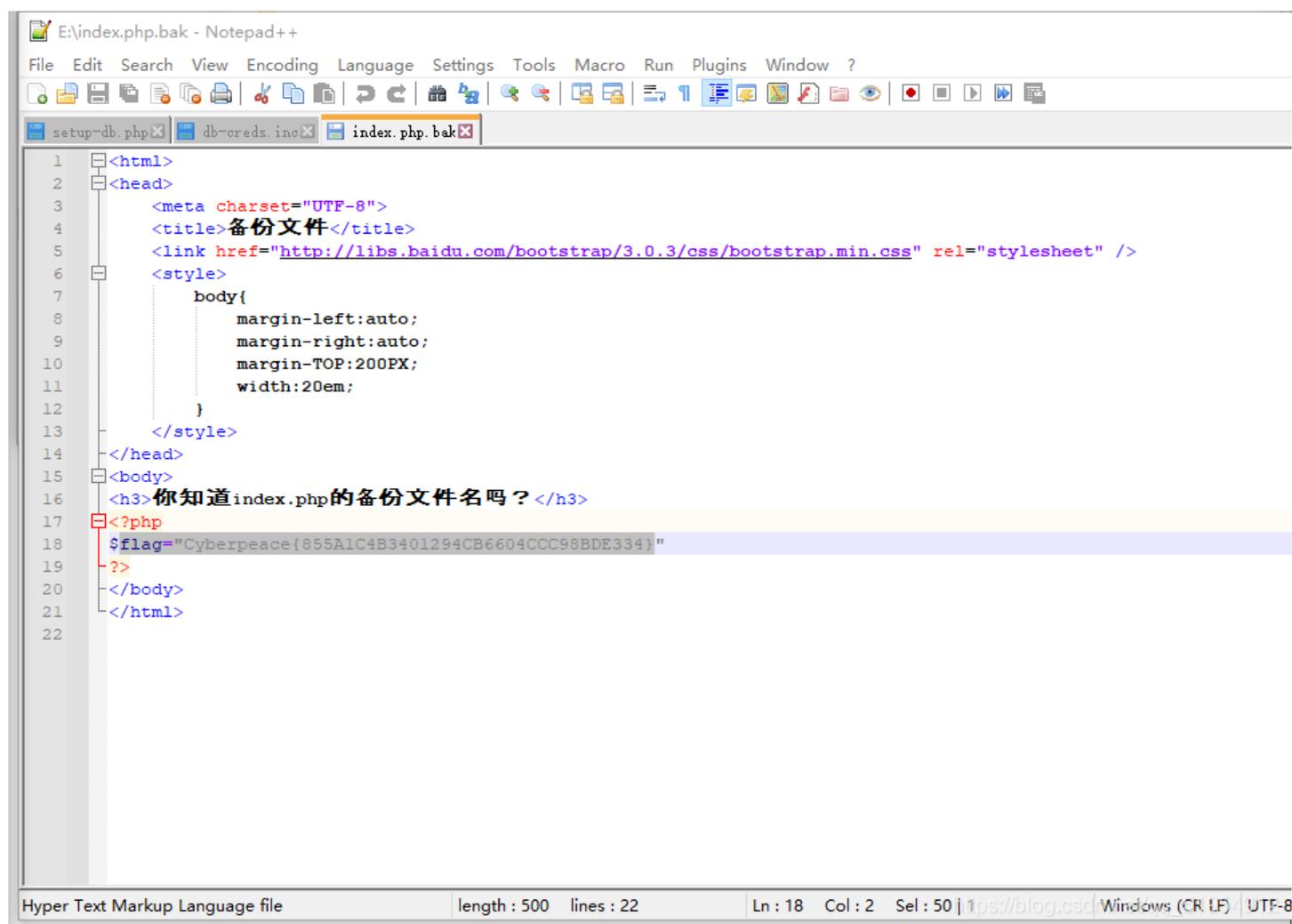
如果网站存在备份文件, 常见的备份文件后缀名有: “.git”、“.svn”、“.swp”、“.”、“.bak”、“.bash_history”、“.bkf” 尝试在URL后面, 依次输入常见的文件备份扩展名。

经过依次对url后添加后缀, 并不能得到flag, 或者文件。

但是页面中有index.php, 尝试将其输入到url后, 再依次输入以上后缀, 最终发现



然后用
notepad++打开，发现flag



4.

cookie 最佳Writeup由神秘人·孔雀翎提供 WP 建议

难度系数：★ 1.0

题目来源：Cyberpeace-n3k0

题目描述：X老师告诉小宁他在cookie里放了些东西，小宁疑惑地想：‘这是夹心饼干的意思吗？’

题目场景： 删除场景

倒计时：03:56:49 延时

题目附件：暂无

题目已答对

分享wp点赞赚金币哦 马上去写

https://blog.csdn.net/qq_51954912

打开场景，进行抓包，发现下图

Set-Cookie: look-here=cookie.php



See the http response

https://blog.csdn.net/qq_51954912

进行图片操作，查到flag

```
^Cpowered by: PHP/5.3.3-1ubuntu4.20
flag: cyberpeace{1777724ea3c5eed63a127aafdfb6ba44}
Vary: Accept-Encoding
```

5.

disabled_button

👍 62 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？

题目场景：🖥️ http://111.200.241.244:42980

删除场景

倒计时：03:49:47

延时

题目附件：暂无

https://blog.csdn.net/qq_51954912

一个不能按的按钮

https://blog.csdn.net/qq_51954912

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

html \ body \ form

删去disabled

一个不能按的按钮

cyberpeace{dc8d59895a31f995dc813c896c9e10c0}

https://blog.csdn.net/qq_51954912

按钮可按，即得flag

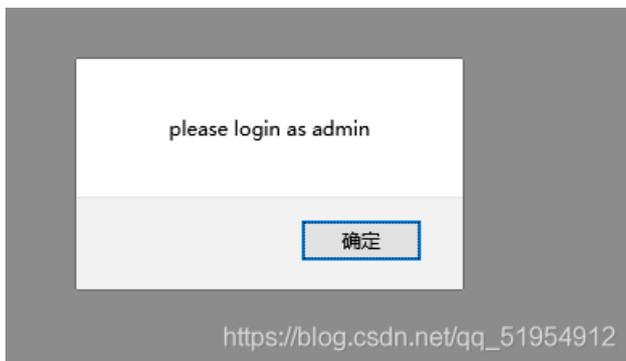
The screenshot shows a CTF challenge interface for 'weak_auth'. It features a title 'weak_auth' with a thumbs-up icon and the number '102'. A badge indicates '最佳Writeup由小太阳的温暖提供'. The difficulty level is '★ 1.0'. The source is 'Cyberpeace-n3k0'. The description reads: '小宁写了一个登陆验证页面，随手就设了一个密码。'. The scenario is 'http://111.200.241.244:55893'. There is a progress bar, a '删除场景' button, and a timer showing '03:48:26' with a '延时' button. The attachments section is empty. A URL 'https://blog.csdn.net/qq_51954912' is visible at the bottom right.

6.

Login

https://blog.csdn.net/qq_51954912

尝试一些简单的密码用户名



发现用户名是admin，这里我想到了爆破密码，但是在使burp查看过程中，偶然发现

http://111.200.241.244:55893

- /
- check.php
 - username=admin&password=123456
 - username=wrfq&password=awef
 - username=wsss&password=wda
- http://adu.g-fox.cn
- http://libs.baidu.com
- http://ocsp.dccosp.cn
- http://ocsp.digicert.com
- http://ocsp.globalsign.com
- http://ocsp.pki.goog
- http://ocsp.sectigo.com
- http://ocsp2.globalsign.com
- http://status.rapidssl.com

Contents

Host	Method	URL
http://111.200.241.2...	POST	/check.php
http://111.200.241.2...	POST	/check.php
http://111.200.241.2...	POST	/check.php
http://111.200.241.2...	GET	/check.php

Request Response

Raw Headers Hex HTML Render

```
HTTP/1.1 200 OK
Date: Tue, 23 Feb 2021 06:29:11 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.26
Vary: Accept-Encoding
Connection: close
Content-Type: text/html
Content-Length: 225

<!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <title>weak auth</title>
</head>
<body>

cyberpeace{3d32b7ebdb70a9168806d62847637c40}<!--maybe you need a dictionary-->

</body>
</html>
```

https://blog.csdn.net/qq_51954912

直接得出flag