XCTF新手练习区 writeup

原创

Mitch311 于 2020-12-20 21:53:00 发布 276 收藏
分类专栏： CTF

目录

第一题.view_source

原题链接

key:查看网页源代码

查看网页源代码的几种途径：

①ctrl+U

②F12

③在地址前面加上view-source后再访问

④设置->更多工具->开发者工具

第二题.robots

原题链接

key:查看robots协议

查看网页robots协议的方法：直接在地址后加上robots.txt

知识补充：robots协议的相关知识

第三题.backup

原题链接

key:查看网页的备份数据

如果网站存在某个文件的备份文件，在地址栏末尾加上/文件名.bak，即可得到备份文件

第四题.cookie

原题链接

key:网页cookie

知识补充：
有关cookie的介绍

有关cookie的应用

> **cookie的查看：**
>
> **①burpsuite抓包查看cookie**
>
> **②F12→开发者工具→网络(network)→cookie**

第五题.disabled_button

原题链接

key:js的disabled功能

F12查看源代码，把按钮中的disabled=""属性项删除后按钮就可以点击了，点击后获得flag。

第六题.weak_auth

原题链接

key:弱密码爆破

> **常见的管理员账号：admin，root等**
>
> **常见的弱密码：123456、12345678、admin、root、toor等**

第七题.simple_php

原题链接

key:掌握php的弱类型比较

> **知识补充：**php类型比较表

```php
<?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;
}
?>
```

如果$a是个字符串，$a==0会自动进行类型转换从而结果为true，$a本身类型转换后也会是0即true

如果$b=1235c，这样$b既不是数字而且还比1234大

第八题.get_post

原题链接

key:get传参+post传参

> **get传参方法：直接在网址后面加?xxx=xxx**
>
> **注意：GET传递的变量都是字符串string**
>
> **post传参方法：用firefox中的hackbar**

第九题.xff_referer

原题链接

key:掌握有关X-Forwarded-For和Referer的知识

> **X-Forwarded-For:简称XFF头，它代表客户端，也就是HTTP的请求端真实的IP，只有在通过了HTTP 代理或者负载均衡服务器时才会添加该项**
>
> **HTTP Referer是header的一部分，当浏览器向web服务器发送请求的时候，一般会带上Referer，告诉服务器我是从哪个页面链接过来的**

①打开firefox和burpsuite，使用burpsuite对firefox进行代理拦截，在请求头添加`X-Forwarded-For: 123.123.123.123`，然后放包go一下

②接着继续在请求头内添加`Referer: https://www.google.com`，再go一下即可获得flag

第十题.webshell

原题链接

key:掌握webshell相关知识

> **webshell就是以asp、php、jsp或者cgi等网页文件形式存在的一种命令执行环境，也可以将其称做为一种网页后门。黑客在入侵了一个网站后，通常会将asp或php后门文件与网站服务器WEB目录下正常的网页文件混在一起，然后就可以使用浏览器来访问asp或者php后门，得到一个命令执行环境，以达到控制网站服务器的目的。**

方法一：打开蚁剑，新建链接，密码为shell（因为小宁已经上传了木马，使得密码为shell，直接使用即可）

方法二：①在HackBar中输入相应URL和请求参数，请求参数为需要执行的shell：shell = system(“find / -name ‘flag*’”); 查看每个文件路径

②继续在Hackbar中执行命令：shell= system(“cat /var/www/html/flag.txt”);

方法三：①burpsuite抓包，将其转到Repeater，并在最下方加入请求参数：shell = system(“find / -name ‘flag*’”); go一下

②查看Response，最下方有目标文件路径

③修改Repeater中的请求参数为：shell= system(“cat /var/www/html/flag.txt”); go一下

第十一题.command_execution

原题链接

key:ping命令的使用

> **知识补充：**
>
> ping命令的使用方法及功能
>
> ping命令执行详解

①先ping一下自身IP——127.0.0.1

②Ping列出自身IP下的文件——127.0.0.1 | ls

③Ping列出自身IP下根目录的文件——127.0.0.1 | ls \

④Ping出名称带有flag的文件——127.0.0.1 & find / -name flag.txt

⑤Ping打开找到的flag文件——127.0.0.1 | cat /home/flag.txt

第十二题.simple_js

原题链接

原题的JS代码如下：

```
function dechiffre(pass_enc){
        var pass = "70,65,85,88,32,80,65,83,83,87,79,82,68,32,72,65,72,65";
        var tab  = pass_enc.split(',');
                var tab2 = pass.split(',');var i,j,k,l=0,m,n,o,p = "";i = 0;j = tab.length;
                        k = j + (l) + (n=0);
                        n = tab2.length;
                        for(i = (o=0); i < (k = j = n); i++ ){o = tab[i-l];p += String.fromCharCode((o = ta
                                if(i == 5)break;}
                        for(i = (o=0); i < (k = j = n); i++ ){
                        o = tab[i-l];
                                if(i > 5 && i < k-1)
                                        p += String.fromCharCode((o = tab2[i]));
                        }
        p += String.fromCharCode(tab2[17]);
        pass = p;return pass;
    }
    String["fromCharCode"](dechiffre("\x35\x35\x2c\x35\x36\x2c\x35\x34\x2c\x37\x39\x2c\x31\x31\x35\x2c\x36\

    h = window.prompt('Enter password');
    alert( dechiffre(h) );
```

①进行代码审计，发现不论输入什么都会跳到假密码，真密码位于 fromCharCode

②编写python脚本将16进制转换成10进制，再把10进制ASCII码转换成字母输出得到flag（\x在python中表示16进制，作为字符串输出时可以自动进行转换）

```
s='\x35\x35\x2c\x35\x36\x2c\x35\x34\x2c\x37\x39\x2c\x31\x31\x35\x2c\x36\x39\x2c\x31\x31\x34\x2c\x31\x31\x36
print(s)
s=s.split(',')
for i in s:
    print(chr(int(i)),end='')
```