

CTFSHOW-WEB入门 writeup

原创

abtgu 于 2020-09-29 16:30:21 发布 1199 收藏

分类专栏: [CTF WEB安全](#) 文章标签: [web](#)

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/weixin_43790779/article/details/108870852

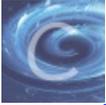
版权



[CTF 同时被 2 个专栏收录](#)

22 篇文章 1 订阅

订阅专栏



[WEB安全](#)

6 篇文章 0 订阅

订阅专栏

web1

题目: 开发注释未及时删除

解题思路: 右键查看源代码即可得到flag。

web2

题目: js前台拦截 === 无效操作

解题思路: 火狐浏览器禁止JavaScript之后, 右键查看源代码, 得到flag。

web3

题目: 没思路的时候抓个包看看, 可能会有意外收获

解题思路: burp抓包, 查看响应头, 得到flag。

web4

题目:

解题思路: 根据提示访问<http://a03708c9-ff09-457d-9688-676ccb7997ce.chall.ctf.show/robots.txt>。得到提示信息, flagishere.txt,

访问<http://a03708c9-ff09-457d-9688-676ccb7997ce.chall.ctf.show/flagishere.txt>。得到flag。

web5

题目: phps源码泄露有时候能帮上忙

解题思路: 根据提示, 访问index.phps, 将文件下载下来, 打开即可看到flag。

web6

题目: 解压源码到当前目录, 测试正常, 收工

解题思路: 访问[www.zip](#), 下载源代码, 查看index.php内容, 发现flag在fl000g.txt中, **这里注意压缩包里fl000g.txt中的flag不正确, 应该访问题目环境中的fl000g.txt。**

web7

题目：版本控制很重要，但不要部署到生产环境更重要。

解题思路：根据提示版本控制，想到常用的版本控制工具git, svn, 尝试访问.git和.svn, 在.git中发现flag。

web8

题目：版本控制很重要，但不要部署到生产环境更重要。

解题思路：上一题访问.git得到flag, 这一题首先想到.svn, 果然得到flag。

web9

题目：发现网页有个错别字？赶紧在生产环境vim改下，不好，死机了

解题思路：提示vim异常关闭，想到linux下vi/vim异常关闭是会存留.swp文件，尝试访问index.php.swp, 得到flag。

web10

题目：cookie 只是一块饼干，不能存放任何隐私数据

解题思路：查看网页的cookie发现flag。

web11

题目：域名其实也可以隐藏信息，比如ctfshow.com 就隐藏了一条信息

解题思路：在域名解析查询网站查询，<http://dbcha.com/>，逐个尝试，在Txt中发现flag。

web12

题目：有时候网站上的公开信息，就是管理员常用密码

解题思路：访问后台，<http://a811a9ef-0d5c-45d8-8162-e98e26a7d3e9.chall.ctf.show/admin/>，提示登录，猜想用户名为admin，密码应该在网站中，观察到页面底部有“Help Line Number : 372619038”，尝试输入数字，成功登录，得到flag。

web13

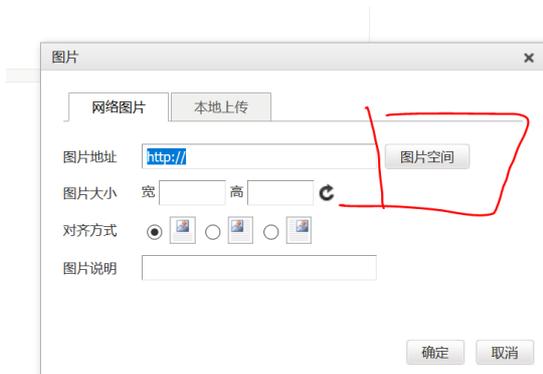
题目：技术文档里面不要出现敏感信息，部署到生产环境后及时修改默认密码

解题思路：在网站中寻找技术文档（查看源代码寻找较为方便），在底部找到document，点击即可查看到默认用户名，密码，访问<http://299bf98c-7cb9-4bdc-826d-c25a285a61df.chall.ctf.show/system1103/login.php>。输入用户名和密码，即可得到flag。

web14

题目：有时候源码里面就能不经意间泄露重要(editor)的信息,默认配置害死

解题思路：根据提示访问editor，出现文本编辑器，点击图片，



https://blog.csdn.net/weixin_43790779

可以看到文件目录，`/var/www/html/nothinghere` 中有一个`fl000g.txt`，访问 <http://6ce4a2ea-ac6a-4c12-84fa-40a347055991.chall.ctf.show/nothinghere/fl000g.txt> 得到flag。

web15

题目： 公开的信息比如邮箱，可能造成信息泄露，产生严重后果

解题思路： 在网站底部发现一个qq邮箱，访问后台，发现可以有忘记密码选项，点击，密保问题是所在地城市，查找qq所在地为西安，输入，返回修改后的密码，登录即可得到flag。

web16

题目： 对于测试用的探针，使用完毕要及时删除，可能会造成信息泄露

解题思路： 提到探针，就想到雅黑探针，访问/tz.php，点击PHP参数，点击下图红框中文字

PHP相关参数	
PHP信息 (phpinfo) :	PHPINFO
PHP运行方式:	FPM-FCGI
PHP安全模式 (safe_mode) :	×
上传文件最大限制 (upload_max_filesize) :	2M
脚本超时时间 (max_execution_time) :	30秒
PHP页面根目录 (doc_root) :	×
dl()函数 (enable_dl) :	https://blog.csdn.net/weixin_43790779

跳转到网站的phpinfo页面，在页面搜索flag，即可找到flag。（关于php探针的内容可参考https://blog.csdn.net/weixin_43790779/article/details/108834213）

web17

题目： 透过重重缓存，查找到ctfer.com的真实IP，提交flag{IP地址}

解题思路： <https://icplishi.com> 查询www.ctfer.com 的IP地址，得到IP地址即为flag。

web18

题目： 不要着急，休息，休息一会儿，玩101分给你flag

解题思路： 查看网页源代码，发现Flappy_js.js文件，访问可看到

```
if(score>100)
{
var result=window.confirm("\u4f60\u8d62\u4e86\u4f0c\u53bb\u5e7a\u5e7a\u96f6\u70b9\u76ae\u7231\u5403\u770b\u770b");
}
else
{
var result=window.confirm("GAMEOVER\n是否从新开始");
if(result){
location.reload();}
}
```

将 `\u4f60\u8d62\u4e86\u4f0c\u53bb\u5e7a\u5e7a\u96f6\u70b9\u76ae\u7231\u5403\u770b\u770b` 进行Unicode解码得到“你赢了，去么么零点皮爱吃皮看看”。访问110.php得到flag。

web19

题目： 密钥什么的，就不要放在前端了

解题思路： 查看页面源代码，发现一段注释代码，代码中已经给出了用户名和密码，但是若有表单提交密码就会被加密，所以用hackbar工具，POSTA提

交 `username=admin&pazzword=a599ac85a73384ee3219fa684296eaa62667238d608efa81837030bd1ce1bf04` ，得到flag。