ctfshow web入门 writeup 1-20(信息收集)

原创

Eph3mera1 于 2020-10-31 22:15:57 发布 833 收藏 2

信息收集系列

web1

题目：开发注释未及时删除
根据题目意思查看网页源代码，发现flag

web2

题目：js前台拦截 === 无效操作
打开页面->无法显示源代码->根据题目因为js前台拦截，右键，以及F12均无法查看源码
在url前加上view-source:，或者设置浏览器禁止JavaScript(我在chrome的设置中搜索JavaScript找到了，Firefox没找到)，即可查看源码并得到flag

web3

题目：没思路的时候抓个包看看，可能会有意外收获
根据题目提示用burpsuite抓包，在返回包中发现flag

web4

题目：总有人把后台地址写入robots，帮黑阔大佬们引路。
直接访问url/robots.txt，发现flag文件flagishere.txt
直接访问url/flagishere.txt，发现flag
Robots协议，在robots.txt中将搜索引擎抓取网站内容的范围做了约定,包括网站是否希望被搜索引擎抓取,哪些内容不允许被抓取,而网络爬虫可以据此自动抓取或者不抓取该网页内容。

web5

题目：phps源码泄露有时候能帮上忙
题目提示本题属于phps源码泄露
直接查看url/index.phps，下载文件，打开得到flag
phps文件就是php的源代码文件，通常用于提供给用户（访问者）直接通过Web浏览器查看php代码的内容。

web6

题目：解压源码到当前目录，测试正常，收工
考察源码泄露
根据常见的文件备份,在url/www.zip中得到网页源码，有一个fl000g.txt文件中显示flag{flag_here}尝试提交，发现不对，另一个文件显示flag in fl000g.txt，访问url/fl000g.txt得到flag

web7

题目：版本控制很重要，但不要部署到生产环境更重要。
考察git源码泄露，访问

```
http://7b8ee9ab-f801-4842-afa3-52711f9aa9af.chall.ctf.show/.git/
```

得到flag

web8

题目：版本控制很重要，但不要部署到生产环境更重要。
考察svn源码泄露，访问

```
http://c1727126-0f06-431e-bb7b-cd058f4650d8.chall.ctf.show/.svn/
```

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
考察vim缓存，访问

```
http://aaa843e6-7531-48ee-911c-9ea062296591.chall.ctf.show/index.php.swp
```

下载文件，打开得到flag
在vim编辑文本时会创建一个临时文件，如果程序正常退出，临时文件自动删除，如果意外退出就会保留，当vim异常退出后，因为未处理缓存文件，导致可以通过缓存文件恢复原始文件内容

```
以 index.php 为例 第一次产生的缓存文件名为 .index.php.swp
第二次意外退出后，文件名为.index.php.swo
第三次产生的缓存文件则为 .index.php.swn
注意：index前有 " . "
```

web10

题目：cookie 只是一块饼干，不能存放任何隐私数据
直接用burpsuite抓包，在cookie中得到被url编码的flag

web11

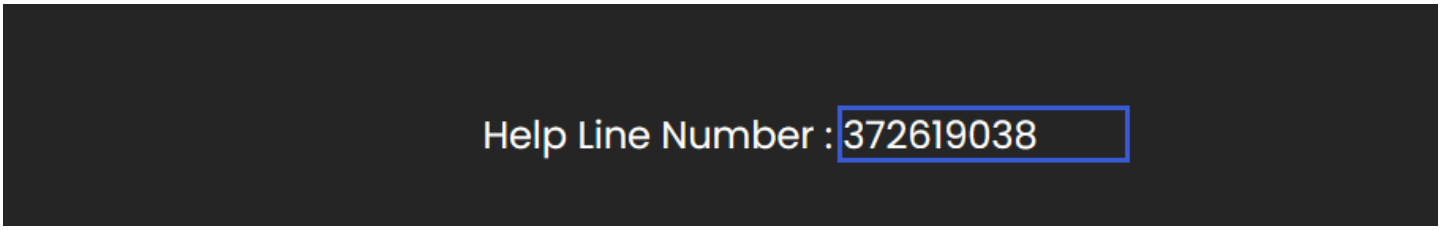
题目：域名其实也可以隐藏信息，比如ctfshow.com 就隐藏了一条信息
这道题之前在校赛HDCTF遇到过类似的，flag藏在域名的txt记录中
直接在命令控制符中输入命令

```
nslookup -qt=txt ctfshow.com
```

得到flag

web12

题目：有时候网站上的公开信息，就是管理员常用密码



在robots.txt中得到用户名为admin，尝试使用上述数字为密码登录
没找到登陆的地方，看大佬wp直接url/admin弹出登录窗口
登陆成功得到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
根据题目提示技术文档，在页面下面找到decoment，点击查看

默认后台地址：http://your-domain/system1103/login.php
默认用户名：admin
默认密码：admin1103

登录后台地址，url/system1103/login，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,默认配置害死人
题目提示泄露editor信息，直接访问url/editor
在插入文件处查看文件空间：www->html->nothinghere->fl000g.txt，双击确定得到文件路径，直接访问url/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
根据题目提示首先找到邮箱地址：

输入url：

```
http://7a20daf8-2b30-4f7b-b564-09100c23d9bf.chall.ctf.show/admin/
```

进入后台系统登陆界面，点击忘记密码，发现密保问题为我的所在地是哪个城市？
查看上述邮箱QQ号的地址位于西安，得到密码，用户名：admin，密码：admin7789登录成功，得到flag

web16

题目：对于测试用的探针，使用完毕后要及时删除，可能会造成信息泄露
题目hint：
考察PHP探针php探针是用来探测空间、服务器运行状况和PHP信息用的，探针可以实时查看服务器硬盘资源、内存占用、网卡流量、系统负载、服务器时间等信息。 url后缀名添加/tz.php 版本是雅黑PHP探针，然后查看phpinfo搜索flag

web17

题目：透过重重缓存，查找到ctfer.com的真实IP，提交flag{IP地址}
直接在命令提示符ping www.ctfer.com得到真实ip

web18

题目：不要着急，休息，休息一会儿，玩101分给你flag
查看源代码，在js/Flappy_js.js中发现Unicode编码
解码发现为：你赢了，去幺幺零点皮爱吃皮看看
访问url/110.php 得到flag

web19

题目：密钥什么的，就不要放在前端了

根据题目提示，查看源代码

```
    <!--
    error_reporting(0);
    $flag="fakeflag"
    $u = $_POST['username'];
    $p = $_POST['pazzword'];
    if(isset($u) && isset($p)){
        if($u==='admin' && $p ==='a599ac85a73384ee3219fa684296eaa62667238d608efa81837030bd1ce1bf04'){
            echo $flag;
        }
}
```


post传参：

```
username=admin&pazzword=a599ac85a73384ee3219fa684296eaa62667238d608efa81837030bd1ce1bf04
```

得到flag

web20

题目：mdb文件是早期asp+access构架的数据库文件，文件泄露相当于数据库被脱裤了

hint：mdb文件是早期asp+access构架的数据库文件 直接查看url/db/db.mdb 下载文件通过txt打开或者通过EasyAccess.exe打开搜索flag

参考：https://blog.csdn.net/a597934448/article/details/105431367