CTF解题思路笔记

原创

山兔1 于 2021-09-13 19:12:11 发布 578 收藏 5

分类专栏： CTF 文章标签： php python

本文链接：https://blog.csdn.net/m0_53008479/article/details/120270571

1.直接查看网页源码，即可找到 `flag`。

2.robots.txt

3.查看 `http` 请求/响应。

4.302跳转的中转网页有信息。

5.查看开发者工具控制台。

6. `javascript` 代码绕过。

7. `.bash_history`。

8. `Webshell`：

9. `ctf` 之流量分析： `Referer` 来源伪造；

10. `X-Forwarded-For`： `ip` 伪造 。

11. `User-Agent`：用户代理（就是用什么浏览器什么的）。

12. `web` 源码泄漏：

`vim` 源码泄漏，如果发现页面上有提示 `vi` 或 `vim`，说明存在 `swp` 文件泄漏；

地址： `/.index.php.swp` 或 `index.php~`。

`Git` 源码泄露: `GitHack` 一把梭。

编码和加解密，各类编码和加密。

绕 `waf`，大小写混合，使用编码，使用注释，使用空字节。

`python` 爬虫信息处理。

13.PHP 代码审计： `$_post` //获取post数据，是一个字典；

`$_get` //获取get数据，是一个字典。

错误控制运算符 `@` 。

`0e` 开头且后面都是数字会被当作科学计数法。

`ereg` `%00` 截断。

`parse_str()` 的作用是解析字符串，并注册成变量。 `unset($bar)` 用来销毁指定的变量。

`mt_rand()` 函数是一个伪随机发生器。

`rand()` 函数在产生随机数的时候没有调用 `srand()`，则产生的随机数是有规律可询的。

反引号“`”可以调用 shell_exec正常执行代码。

`preg_replace()`。
`php://filter`读取文件。
`php://input`写入文件， 数据利用 POST 传过去。
`data://`将 `include` 的文件流重定向到用户控制的输入流。 `phar://allow_url_include=on` 的状态下，就可以考虑 `phar` 伪协议绕过。
写一个 `shell.php` 文件，里面包含一句话木马。然后，压缩成 `xxx.zip`。然后改名为`xxx.jpg` 进行上传。最后使用 `phar` 进行包含，这里的路径为上传的 `jpg` 文件在服务器的路径。
`zip://` 把`1.php`文件压缩成 `zip`，再把`zip`的后缀改为 `png`，上传上去，并且可以获得上传上去的 `png` 的地址。
`1.zip`文件内仅有`1.php`这个文件。
13.`XSS`题目
绕过`waf`长度限制，用`BurpSuite` 抓包改包绕过，也可以直接在`F12`里改页面源代码。
双写将被过滤的关键字符写两遍。
等价替代，就是不用被过滤的字符，而使用没有被过滤却会产生相同效果的字符。比如，如果`SQL`注入题目中过滤了空格，可以用`/**/`绕过对空格的限制； `XSS`题目如果过滤了`<script>`标签，可以使用其他类型的`payload`；如果需要使用`cat`命令却被过滤，可以使用`tac`、`more`、`less`命令来替代等。
`URL`编码绕过，比如，过滤了`cat`，可以使用`c%61t` 来绕，编码和加密不一样。
`Linux`命令使用反斜杠绕过， `cat` 与 `ca\t` 两条命令等价，效果完全相同。可以利用这个特性来进行一些绕过操作（当然，这个仅限于命令执行漏洞）。
`URL` 二次解码绕过 如果源码中出现了 `urldecode()`函数，可以利用`url`二次解码来绕过。
14.`SQL`注入
`xss`平台： `xssplatfrom`， `beef***`利用`xss`弹， `cookie`的方式弹出`flag`。
`php` 弱类型 `===` 在进行比较的时候，会先判断两种字符串的类型是否相等，再比较 。`==` 在进行比较的时候，会先将字符串类型转化成相同，再比较。
`md5` 绕过(`Hash` 比较缺陷)。
`json` 绕过。
`array_search is_array` 绕过。
`strcmp`漏洞绕过`php -v <5.3`。
`PHP`伪协议
1.`php://`协议-
`php://filter` 与 `php://input` 主要用于读取源代码并进行 `base64` 编码输出，访问各个输入/输出流。
`file://`协议
`file://` [文件的绝对路径和文件名]
`file:///etc/passwd` `git` 泄露`/file` 协议
`phar://`协议
`zlib://`协议
`data://`协议
文件上传漏洞