【CTFhub】web-信息泄露-PHPINFO_WriteUp

原创

KUSIA_ 于 2021-11-02 23:00:05 发布 67 收藏

分类专栏： ctfhub-writeup 文章标签： php 前端 开发语言

本文链接：https://blog.csdn.net/weixin_45633243/article/details/121111434

目录导航

开启题目

得到FLAG

可以手动浏览，也可以 `ctrl+F` 搜索 flag 或者 ctfhub

$_ENV['APACHE_LOCK_DIR']	/var/lock/apache2
$_ENV['LANG']	C
$_ENV['APACHE_RUN_USER']	www-data
$_ENV['APACHE_RUN_GROUP']	www-data
$_ENV['APACHE_LOG_DIR']	/var/log/apache2
$_ENV['PWD']	/
$_ENV['FLAG']	ctfhub{c2054fece4cfcbcc6a0671d2}

PHP Credits

PHP Group
Thies C. Arntzen, Stig Bakken, Shane Caraveo, Andi Gutmans, Rasmus Lerdorf, Sam Ruby, Sascha Schumann, Zeev Suraski, Jim Winstead, Andrei Zmievski

Language Design & Concept
Andi Gutmans, Rasmus Lerdorf, Zeev Suraski, Marcus Boerger

可以看到 $_ENV[‘FLAG’] 即为flag

扩展_phpinfo

> 什么是 phpinfo

phpinfo是php内置的函数，用于以网页的形式输出 php的具体配置信息。

使用：phpinfo — 输出关于 PHP 配置的信息

```
bool phpinfo([ int $what = INFO_ALL])
```

输出 PHP 当前状态的大量信息，包含了 PHP 编译选项、启用的扩展、PHP 版本、服务器信息和环境变量（如果编译为一个模块的话）、PHP环境变量、操作系统版本信息、path 变量、配置选项的本地值和主值、HTTP 头和PHP授权信息(License)。

> 从 phpinfo 中可获得什么信息

phpinfo()函数返回的信息中包含了服务器的配置信息，包括：

1）PHP编译选项以及文件扩展名的相关信息；

2）php的版本信息

3）php的配置信息；

4）数据库信息；等敏感信息。这些敏感信息会帮助攻击者展开进一步的攻击。

> php各个版本的差异

该篇文章介绍的很详细： https://xz.aliyun.com/t/6131

> phpinfo为什么能被利用

【待更新】

参考：

https://www.php.cn/php-ask-434716.html

https://blog.csdn.net/weixin_39934520/article/details/107022162