BUUCTF web

原创

Catch_1t_AlunX 于 2020-06-20 18:17:48 发布 171 收藏
文章标签： php python linux 安全 laravel

一、打开靶机页面是一个滑稽图片，查看一下源代码，得到提示source.php

```
</head>
<body>
    <!--source.php-->

    <br><img src="https://i
```

二、访问source.php可以看到高亮源码，搜索相应内容,是CVE-2018-12613 PhpMyadmin后台文件包含漏洞的简化版本

针对关键代码分析如下：

（1）白名单验证，三次验证，任何一次通过即视为通过。

（2）第一次验证，在白名单里通过。这里可以看到hint.php也在白名单，访问得到提示ffffllllaaaagggg。

```
$whitelist = ["source"=>"source.php","hint"=>"hint.php"];
if (! isset($page) || !is_string($page)) {
        echo "you can't see it";
        return false;
}

if (in_array($page, $whitelist)) {
        return true;
}
```

（3）第二次验证，原漏洞原因是为避免传入的参数还有参数，例如传入a.php?b=xxx,此时截取？前的部分以验证是否在白名单里。

（4）第三次验证，原漏洞原因是为避免参数被url编码，先解码再截取？号前的部分验证是否在白名单内。

（5）漏洞产生情况：由于第三次验证时进行了解码，所以$page参数可以是被url编码的参数，即在外层判断时,file可以是url编码后的形式，而include(xx.php%3f/../yyy)时由于%截断，会把3f当成一个目录，这时候使用3f/../就到xx.php所在目录，然后可以尽情的目录穿越。

根据提示向上穿越3层即可，payload:file=source.php%253f/../../../ffffllllaaaagggg

注：在做题时发现了一个非预期的情况，payload:file=source.php？/../../../ffffllllaaaagggg竟然也可以得出flag，暂时不知道原因。

include(?/)应该是不能包含的。