Day 1 - Wish List | RIPS 2017 PHP代码安全审计挑战（RIPSTECH PRESENTS PHP SECURITY CALENDAR）/Writeup

翻译

Ambulong 于 2018-08-31 17:05:20 发布 411 收藏
文章标签： 代码审计

RIPSTECH PRESENTS PHP SECURITY CALENDAR 是由 RIPS 团队出品的PHP代码安全审计挑战系列题目，RIPSTECH PRESENTS PHP SECURITY CALENDAR 2017 共包含24道题目（Day 1 ~ 24），每道题目将包含一个较新颖的知识点供大家学习。

VULNSPY 提供在线实验环境让您可以在线进行模拟渗透测试，在线体验 RIPSTECH PRESENTS PHP SECURITY CALENDAR。

在线实验环境和Writeup: http://www.vulnspy.com/cn-ripstech-presents-php-security-calendar-2017/

查看更多内容，点击右上角 `START TO HACK` 可以快速访问在线实验环境。

Day 1 - Wish List

你能从下列代码中发现安全漏洞吗？

```
class Challenge {
    const UPLOAD_DIRECTORY = './solutions/';
    private $file;
    private $whitelist;

    public function __construct($file) {
        $this->file = $file;
        $this->whitelist = range(1, 24);
    }

    public function __destruct() {
        if (in_array($this->file['name'], $this->whitelist)) {
            move_uploaded_file(
                $this->file['tmp'],
                self::UPLOAD_DIRECTORY . $this->file['name']
            );
        }
    }
}

$challenge = new Challenge($_FILES['solution']);
```

在代码的 13 行存在任意文件上传漏洞。 在 12 行代码通过 `in_array()` 来判断文件名是否为整数，可是未将 `in_array()` 的第三个参数设置为 `true` 。`in_array()`的第三个参数在默认情况下是`false`，因此 PHP 会尝试将文件名自动转换为整数再进行判断，导致该判断可被绕过。比如使用文件名为 `5vulnspy.php` 的文件将可以成功通过 `in_array($this->file['name'], $this->whitelist)` 判断，从而将恶意的 PHP 文件上传到服务器。