Day 8 - Candle | RIPS 2017 PHP代码安全审计挑战（RIPSTECH PRESENTS PHP SECURITY CALENDAR）/ Writeup

翻译

Ambulong 于 2018-08-31 17:14:10 发布 352 收藏

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 8 - Candle

你能从下列代码中发现安全漏洞吗？

```
header("Content-Type: text/plain");

function complexStrtolower($regex, $value) {
    return preg_replace(
        '/(' . $regex . ')/ei',
        'strtolower("\\1")',
        $value
    );
}

foreach ($_GET as $regex => $value) {
    echo complexStrtolower($regex, $value) . "\n";
}
```

这道题目也十分的简单，出现了`preg_replace('/e','')`这种代码，`preg_replace`在`/e`模式下能够执行代码如下：

```
preg_replace('/(.*)/e','phpinfo();','xxx');
```

这样就能够执行`phpinfo()`。