Day 7 - Bells | RIPS 2017 PHP代码安全审计挑战（RIPSTECH PRESENTS PHP SECURITY CALENDAR）/ Writeup

翻译

Ambulong 于 2018-08-31 17:13:03 发布 321 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 7 - Bells

你能从下列代码中发现安全漏洞吗？

```
function getUser($id) {
    global $config, $db;
    if (!is_resource($db)) {
        $db = new MySQLi(
            $config['dbhost'],
            $config['dbuser'],
            $config['dbpass'],
            $config['dbname']
        );
    }
    $sql = "SELECT username FROM users WHERE id = ?";
    $stmt = $db->prepare($sql);
    $stmt->bind_param('i', $id);
    $stmt->bind_result($name);
    $stmt->execute();
    $stmt->fetch();
    return $name;
}

$var = parse_url($_SERVER['HTTP_REFERER']);
parse_str($var['query']);
$currentUser = getUser($id);
echo '<h1>'.htmlspecialchars($currentUser).'</h1>';
```

看到了`parse_str`就知道这是一个变量覆盖的漏洞。同时`$_SERVER['HTTP_REFERER']`也是可控的，那么就存在变量覆盖的漏洞了。