Day 4 - False Beard | RIPS 2017 PHP代码安全审计挑战（RIPSTECH PRESENTS PHP SECURITY CALENDAR）/ Writeup

翻译

Ambulong 于 2018-08-31 17:10:53 发布 207 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 4 - False Beard

你能从下列代码中发现安全漏洞吗？

```
class Login {
    public function __construct($user, $pass) {
        $this->loginViaXml($user, $pass);
    }

    public function loginViaXml($user, $pass) {
        if (
            (!strpos($user, '<') || !strpos($user, '>')) &&
            (!strpos($pass, '<') || !strpos($pass, '>'))
        ) {
            $format = '<xml><user="%s"/><pass="%s"/></xml>';
            $xml = sprintf($format, $user, $pass);
            $xmlElement = new SimpleXMLElement($xml);
            // Perform the actual login.
            $this->login($xmlElement);
        }
    }
}

new Login($_POST['username'], $_POST['password']);
```

虽然这道题目出现了`XML`，但是考察的确实`strpos`的用法和PHP的自动类型转换的问题。