Day 3 - Snow Flake | RIPS 2017 PHP代码安全审计挑战（RIPSTECH PRESENTS PHP SECURITY CALENDAR）/ Writeup

翻译

Ambulong 于 2018-08-31 17:10:00 发布 364 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 3 - Snow Flake

你能从下列代码中发现安全漏洞吗？

```
function __autoload($className) {
    include $className;
}

$controllerName = $_GET['c'];
$data = $_GET['d'];

if (class_exists($controllerName)) {
    $controller = new $controllerName($data);
    $controller->render();
} else {
    echo 'There is no page with this name';
}

class HomeController {
    private $data;

    public function __construct($data) {
        $this->data = $data;
    }

    public function render() {
        if ($this->data['new']) {
            echo 'controller rendering new response';
        } else {
            echo 'controller rendering old response';
        }
    }
}
```

在第8行中的`class_exists()`会检查是否存在对应的类，当调用`class_exists()`函数时会触发用户定义的`__autoload()`函数，用于加载找不到的类。