New issue

Jump to bottom

There is a file upload vulnerability in the background settings page #161

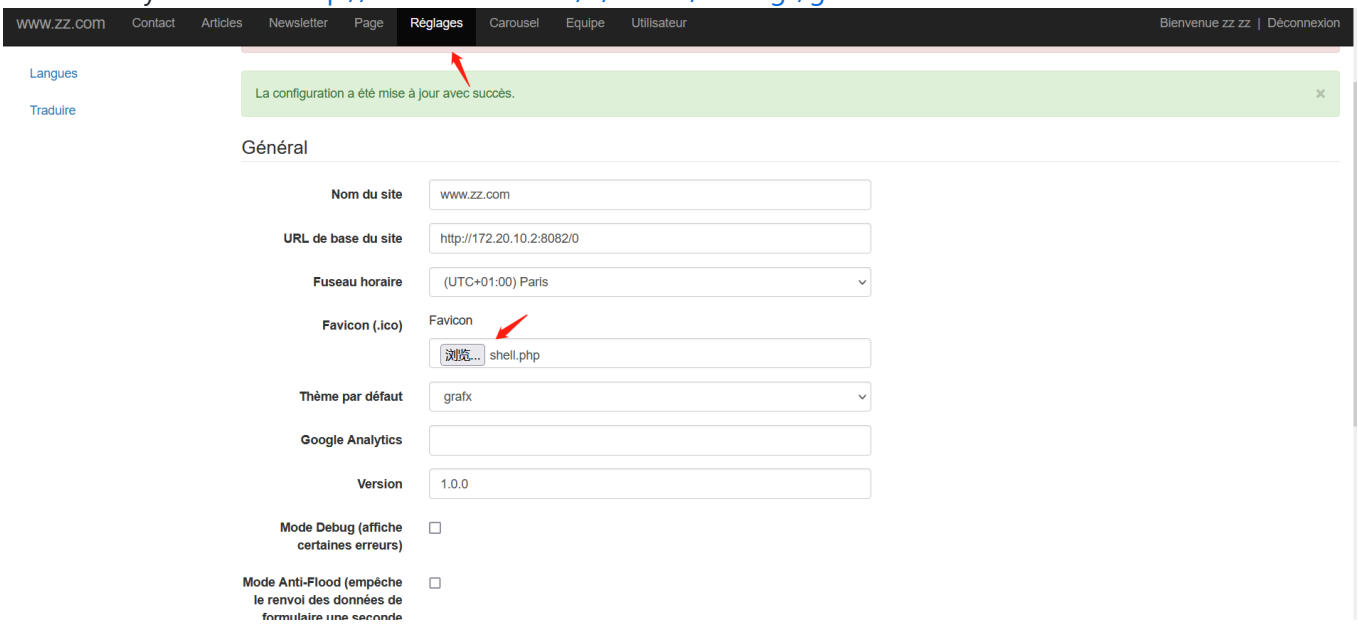
Open **code-zeng** opened this issue on Apr 22 · 0 comments

code-zeng commented on Apr 22 • edited

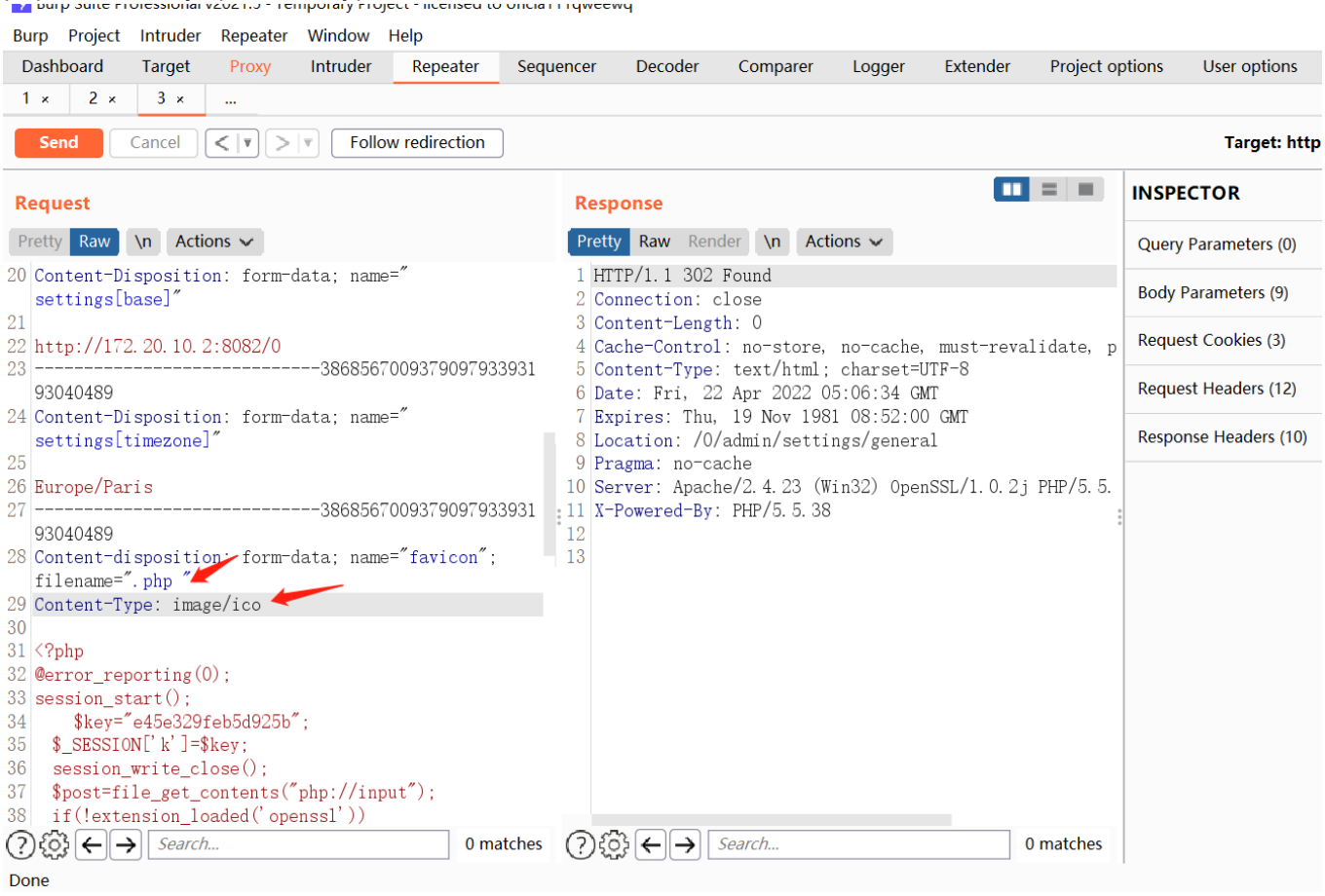
The server build environment is windows

After logging in to the background, click Settings, there is a file upload vulnerability in an ico image upload point, you can bypass the upload, upload the webshell through this point, and you can take down the server.

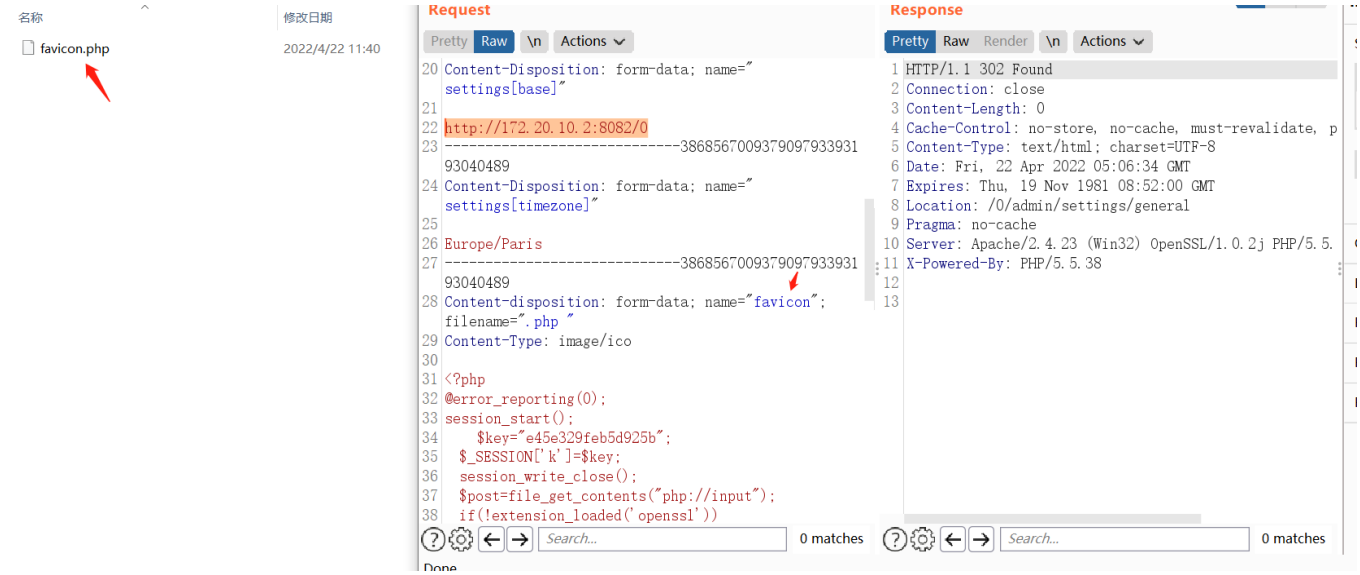
Vulnerability location：http://172.20.10.2:8082/0/admin/settings/general



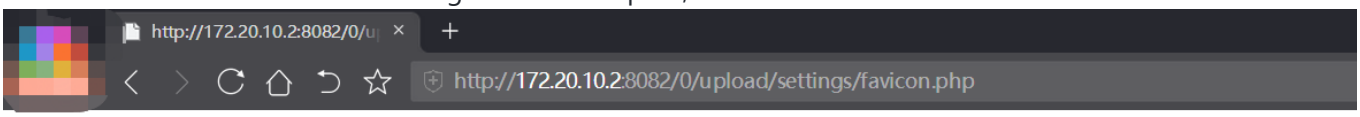
1.Upload the shell file and capture the package。Modify Content-Type to image/ico, filename to .php and php followed by spaces to bypass



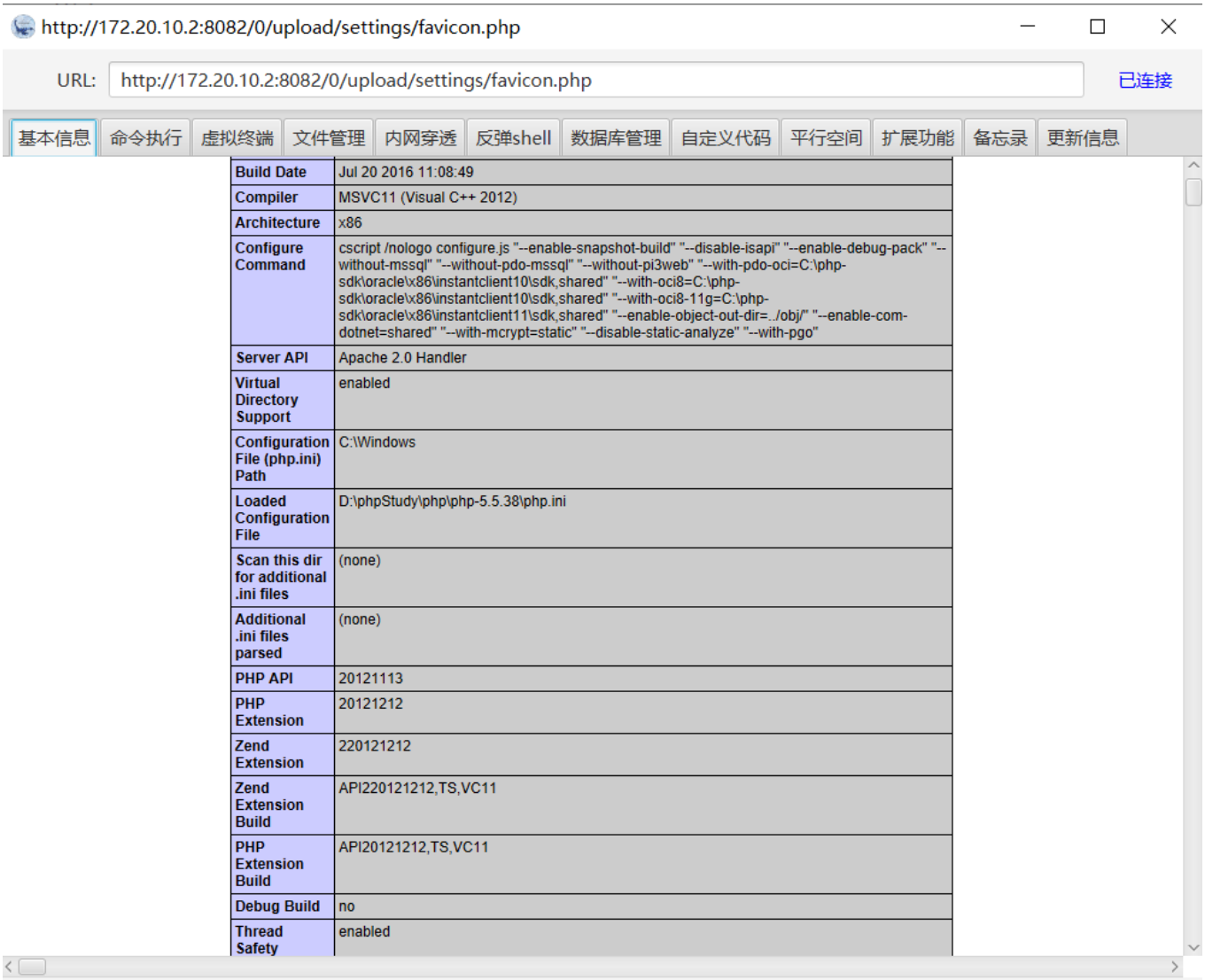
2.Although the response packet is 302, the file itself has been uploaded successfully。The uploaded file is located in the \upload\settings directory, named favicon.php



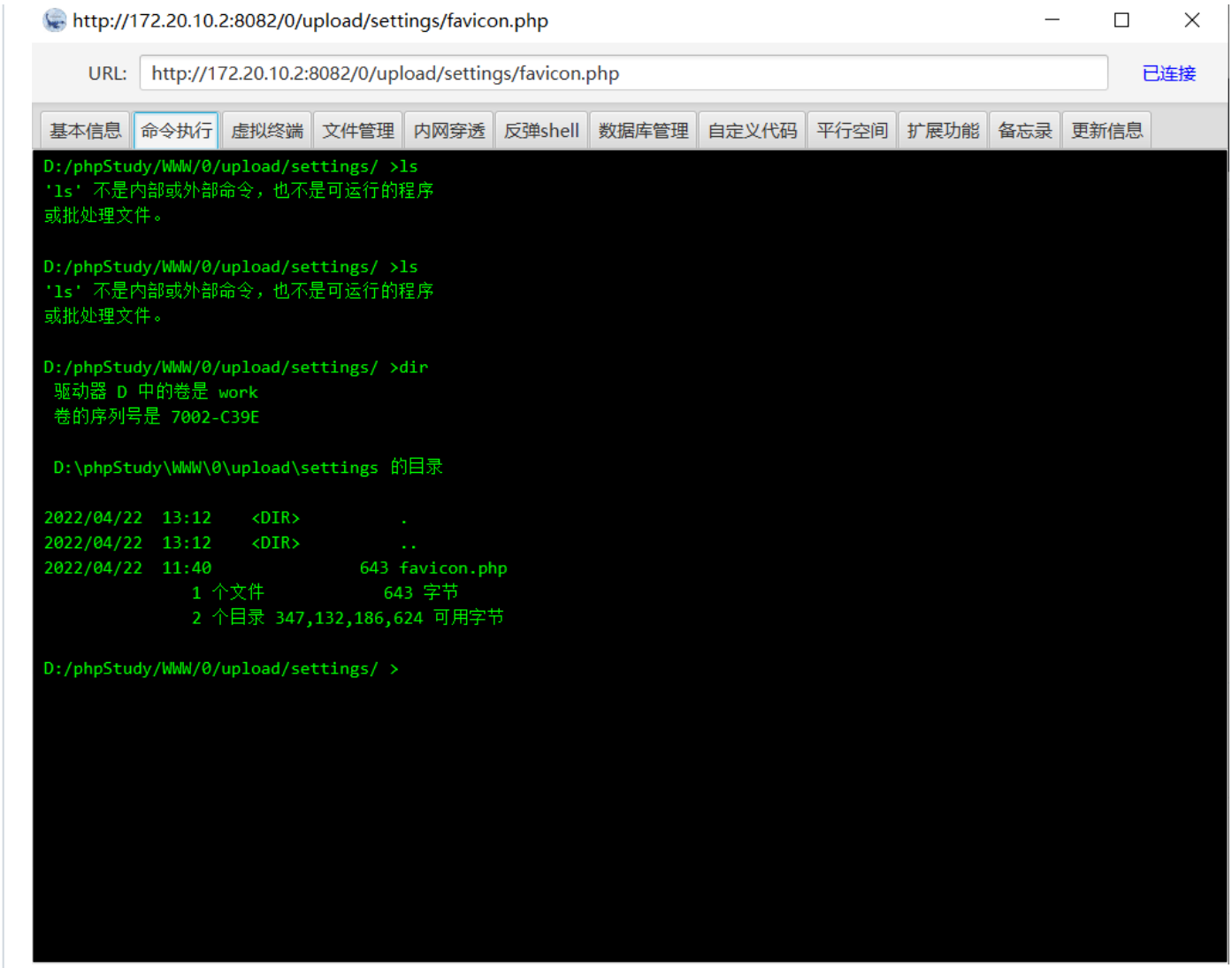
3.The connection is successful through the ice scorpion, and the server shell is obtained.



Notice: Undefined offset: 1 in **D:\phpStudy\WWW\0\upload\settings\favicon.php** on line **23**



Build Date	Jul 20 2016 11:08:49
Compiler	MSVC11 (Visual C++ 2012)
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\x86\instantclient10\sdk,shared" "--with-oci8=C:\php-sdk\oracle\x86\instantclient10\sdk,shared" "--with-oci8-11g=C:\php-sdk\oracle\x86\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-5.5.38\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20121113
PHP Extension	20121212
Zend Extension	220121212
Zend Extension Build	API220121212,TS,VC11
PHP Extension Build	API20121212,TS,VC11
Debug Build	no
Thread Safety	enabled



Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant