

Appendix C. Remote Command Execution Cheat Sheet

This table provides a handy list of techniques that can be used for remote command execution, by language.

Table C-1. Remote Command Execution Cheat Sheet		
<i>Web Application Environment</i>	<i>Source Code</i>	<i>Additional Information</i>
Java Servlet	<pre>class Example extends HttpServlet { . . . void function() { Runtime r = Runtime.getRuntime(); Process p = r.exec("<command>", <arguments>); } . . . }</pre>	http://java.sun.com/j2se/1.4/docs/api/java/lang/Run
Java Server Pages (JSP)	<pre><% Runtime r = Runtime.getRuntime(); Process p = r.exec("<command>", <arguments>); %></pre>	http://java.sun.com/j2se/1.4/docs/api/java/lang/Run
Active Server Pages (ASP)	If Windows Scripting Host is installed on the target system: <pre><% Set wsh = Server.CreateObject("Wscript.shell") wsh.run("<command>"); %></pre>	http://msdn.microsoft.com/library/default.asp?url=/us/script56/html/wsMthRun.asp
PERL	In PERL, commands are executed by wrapping them with the backtick symbol (`)	http://www.perldoc.com/perl5.6/pod/perlfunc.html

Table C-1. Remote Command Execution Cheat Sheet

Web Application Environment	Source Code	Additional Information
	<pre>\$result = `<command>`; or system("<command>"); or open(IN, "<command> ");</pre>	
PHP	<pre><? system("<command>") ?> or <? shell_exec("<command>") ?></pre>	http://www.php.net/manual/en/function.shell-exec.
MS SQL	EXEC master..xp_cmdshell" <command>"	