Ethical Hacker 5 – Path traversal, File inclusion and Command injection

* **What is path traversal and how does it work?**

Path traversal is an attack through which the content of files outside the root directory is shown. The most common method is using the “../” sequence. Path traversal is not as common as SQL injection, for example, but is still a threat for the web applications.

* **What is remote file inclusion and how does it work?**

Remote file inclusion is a method used by attackers to get the web application to include a remote file. Malicious code can also be entered for the web application to execute it if there is no security in place for such input. Below there are some examples of file inclusion attacks:

Modifying the URL (page=*file4.php*) to find a hidden file:



Modifying the URL (using the “../” sequence repeatedly) to get the user account:

Graphical user interface, text, application, Word

Description automatically generated

Modifying the URL to get the OS type:

Text

Description automatically generated

Modifying the URL to find the TCP connections:

Graphical user interface, application

Description automatically generated

Modifying the URL to find the UDP connections:

Graphical user interface, text

Description automatically generated

Modifying the URL to include the Google search page to the initial web page:

Graphical user interface, text, application, chat or text message

Description automatically generated

* **What is command injection and how does it work?**

Command injection is a form of attack in which the commands are transmitted by exploiting one of the application’s vulnerabilities, most commonly through user input, when the input validation is not sufficient or non-existent. Below, there are a few examples of command injection attacks:

Browsing the directory using the *ls*

Text

Description automatically generated

Using the *cat*  command and index.php to create a new form:

Text

Description automatically generated

Using command injection to find the name of the user, the host name, and the IP address:

Text

Description automatically generated

* **How are path traversal, remote file inclusion and command injection related?**

All of these methods can be used on web applications, via the user input. They mainly make use of the lack of input validation, which is relatively easy to solve but it still is an important security issue among many web applications.

* **Resources:**
* [**https://www.acunetix.com/blog/articles/path-traversal/**](https://www.acunetix.com/blog/articles/path-traversal/)
* [**https://www.acunetix.com/blog/articles/remote-file-inclusion-rfi/**](https://www.acunetix.com/blog/articles/remote-file-inclusion-rfi/)
* [**https://www.imperva.com/learn/application-security/command-injection/**](https://www.imperva.com/learn/application-security/command-injection/)