CYBER SECURITY 2021

**Mandatory Final: Study of one of the hacking subject**

# Material:

* <https://null-byte.wonderhowto.com/how-to/scan-websites-for-potential-vulnerabilities-using-vega-vulnerability-scanner-kali-linux-0181887>
* <https://subgraph.com/vega> (download Vega)
* <https://www.youtube.com/watch?v=bQykANXkM-k> (installing libwebkitgtk-1.0)
* <https://www.javahelps.com/2015/03/install-oracle-jdk-in-ubuntu.html> (installing Java version 8)
* <https://youtu.be/mKuyZY2cQrU> (example of using Vega to scan for SQL injection)

# Theory and Tools:

**Vega Vulnerability Scanner** is a free, open-source graphical web-auditing tool running on Linux, OS X and Windows, developed by the security company Subgraph. Vega can help **Alert Analyst**, people in a security operations center, or website administrators to find and validate SQL Injection, Cross-Site Scripting (XSS), inadvertently disclosed sensitive information, and other vulnerabilities.

How it works: Vega includes an automated scanner for quick tests and an intercepting proxy for tactical inspection. The Vega scanner finds XSS (cross-site scripting), SQL injection, and other vulnerabilities. It can be extended using a powerful API in the language of the web: Javascript.

# Practice:

Finally, I managed to download Vega into my Kali Linux virtual machine (through instruction in the material links). It requires Java 8 in manual mode.

A picture containing text, monitor, screenshot, electronics

Description automatically generated

Figure . Installed Vega :D

After a quick guide tour in the instruction, I scanned my own apache webserver (just newly run):

A screenshot of a computer

Description automatically generated with medium confidence

Figure . Scan my own web server

I get only 1 medium scan alert: Vega found a single filesystem path from my web server, which is the index.html file to get the server up :P

In other case, it may contain sensitive information and such absolute system path should not be sent to remote clients on production servers. However, it is OK in my server now.

Vega also provides some additional references with relevant information for the case: <https://www.owasp.org/index.php/Information_Leakage> (link no longer works)

<https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/01-Information_Gathering/01-Conduct_Search_Engine_Discovery_Reconnaissance_for_Information_Leakage>

And for the “info” section of this scan, there is a HTTP error Dectected:

Graphical user interface, application

Description automatically generated

Figure . HTTP Error Detected

Since I have one machine to scan (with my permission) and I have little knowledge about Web Server, I can only do this exercise.