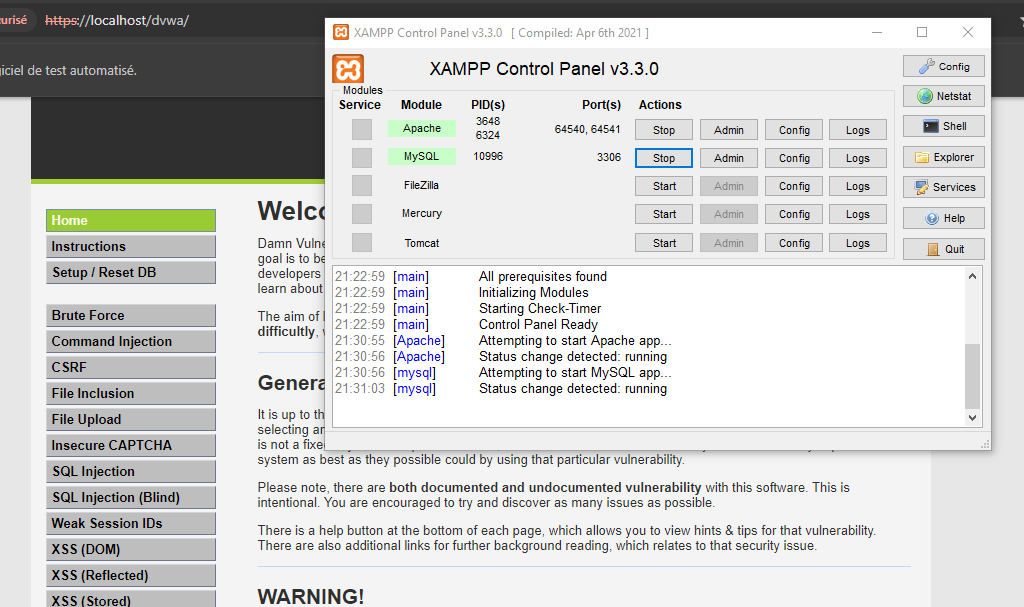
**Phase 2 : Zed Attack Proxy (zap)**

**Detect vulnerabilities in a web application using the zed attack proxy :**

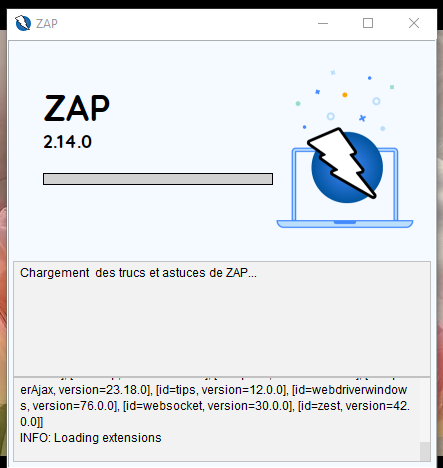
* install ZAP from the website and Configure it
* For testing we need to install Damn Vulnerable Web App (DVWA) and run it using Windows + XAMPP.

**The test :**

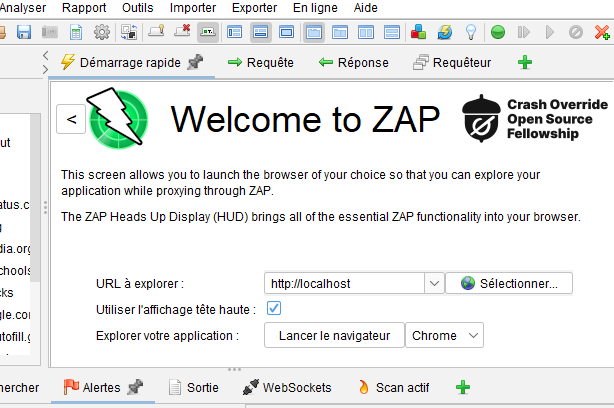
* Host DVWA on your localhost :



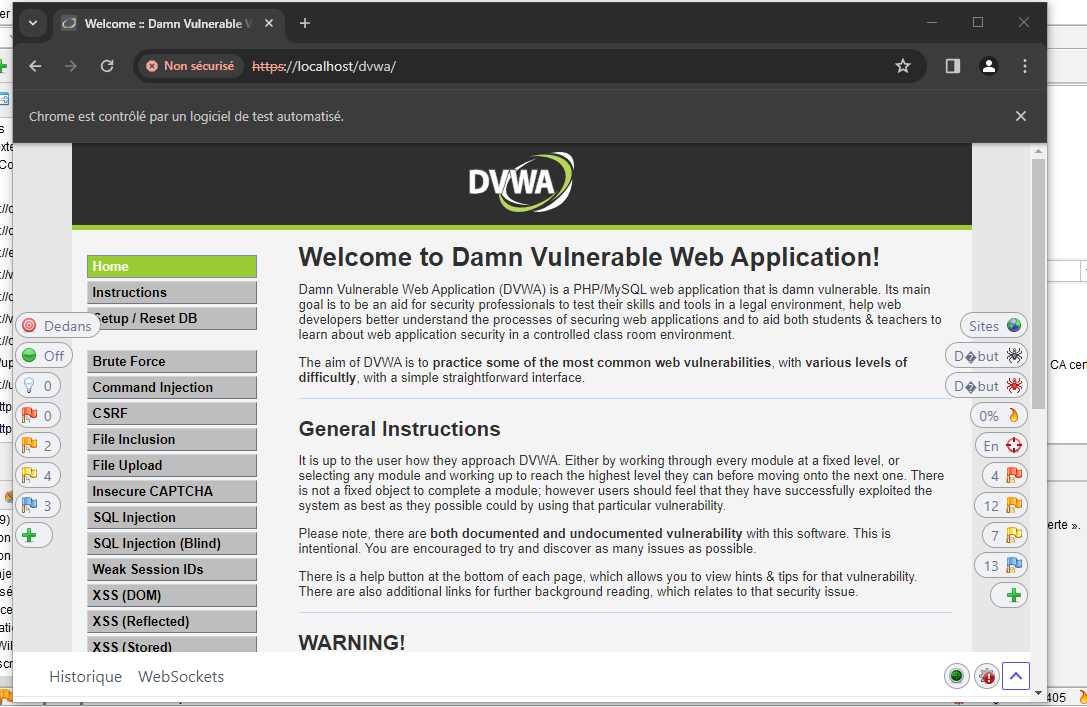
* Run ZAP :



Choose manual scan and enter your localhost link :



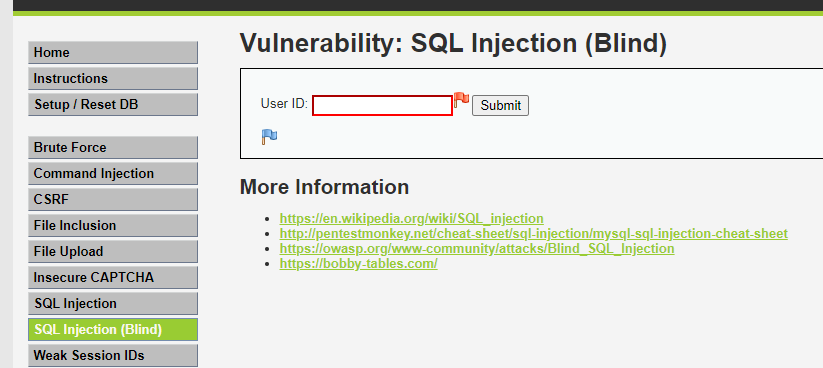
* Start testing by navigating through the website

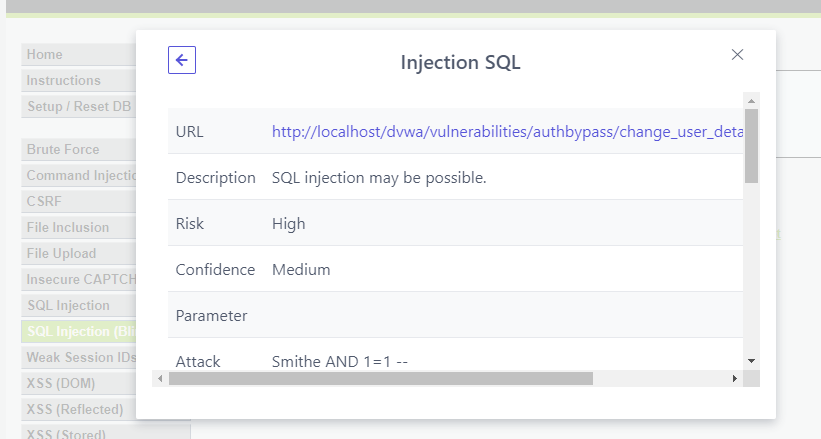


**The vulnerabilities found in DVWA using ZAP:**

* **Injection SQL :**
  + - URL : http://localhost/dvwa/vulnerabilities/authbypass/change\_user\_details.php
    - RISK : High
    - Attaque : Smithe AND 1=1 –

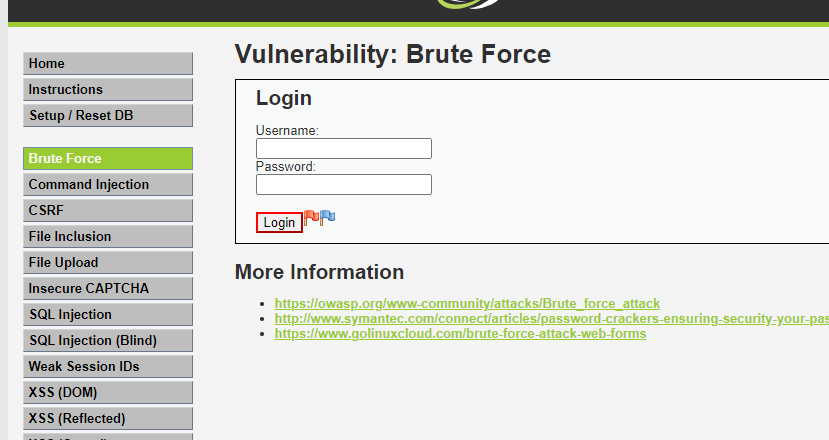
The page results were successfully manipulated using the boolean conditions [Smithe AND 1=1 -- ] and [Smithe AND 1=2 -- ] The parameter value being modified was NOT stripped from the HTML output for the purposes of the comparison.

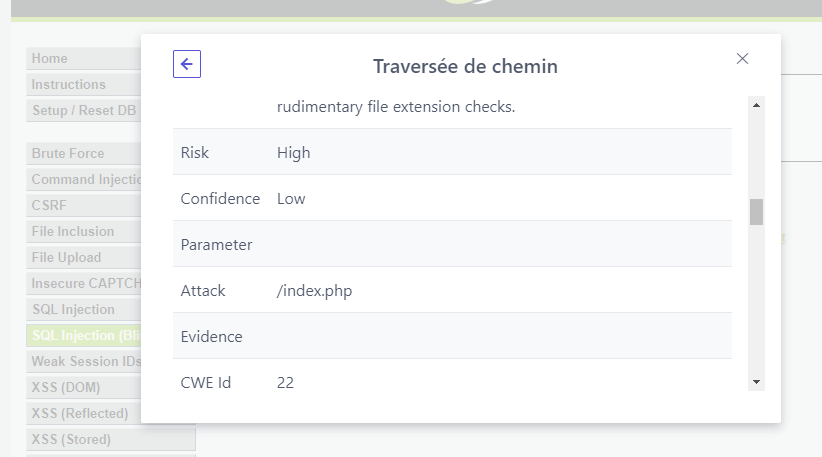




* **path traversal attack :**
  + - URL :http://localhost/dvwa/vulnerabilities/brute/index.php
    - RISK : High
    - Attaque : /index.php

The path traversal attack technique allows a hacker to access files, directories, and commands potentially residing outside the root directory of internet documents. An attacker can manipulate a URL in such a way that the website will execute or reveal the content of arbitrary files located anywhere on the web server.





* **Cross Site Scripting :**
  + - URL :http://localhost/dvwa/vulnerabilities/view\_source.php
    - RISK : High

Cross-site Scripting (XSS) is an attack technique that involves injecting code provided by the attacker into a user's browser instance. A browser instance can be a standard browser or a browser object embedded in a software product. When a hacker manages to execute their code through a user's browser, the code runs within the security context (or zone) of the hosting website.