Web Application Analysis Lab

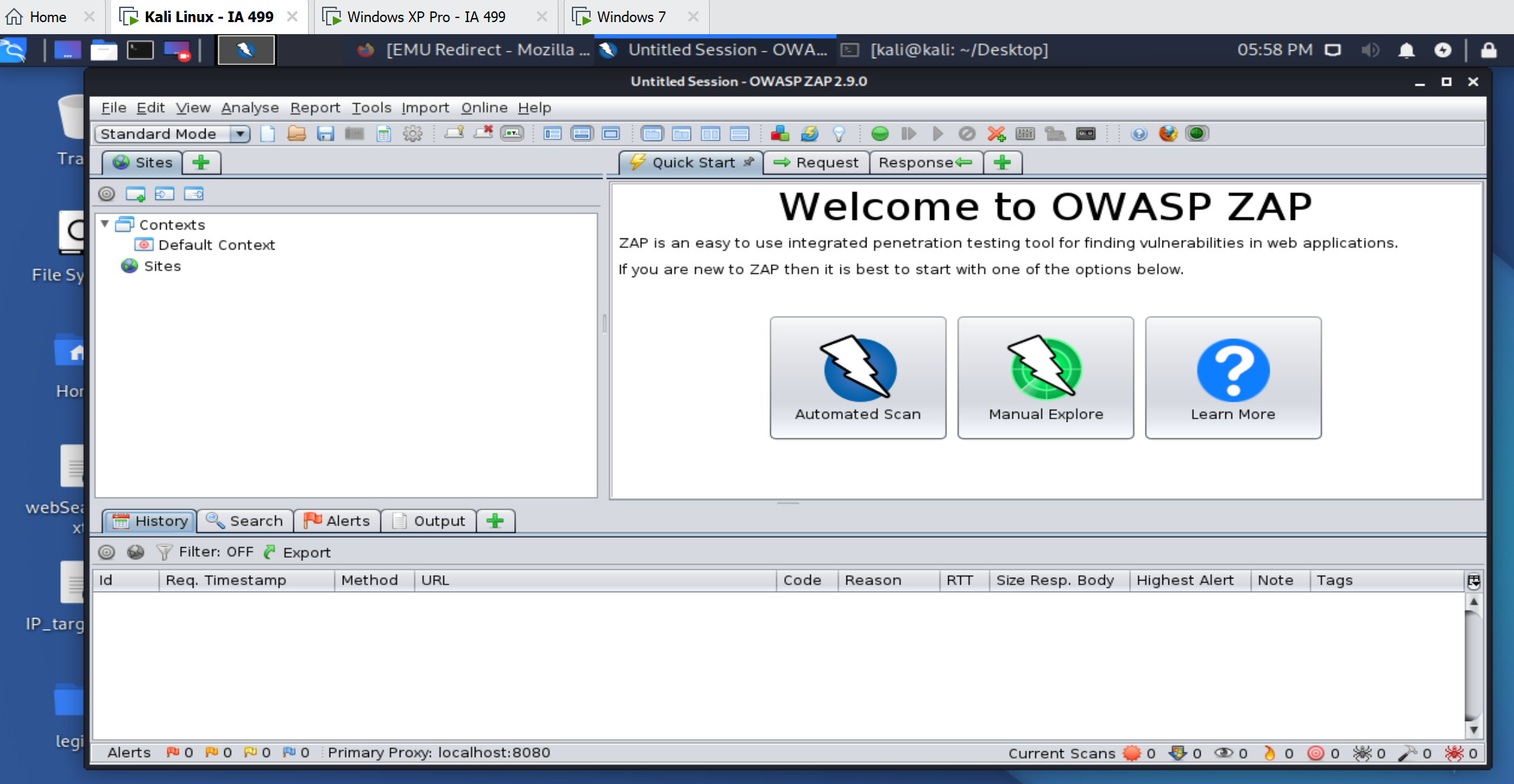
Web application analysis is the process of using tools to collect data on web servers and using that data to exploit them. This lab covers three of these types of tools which are built into Kali: Zap, WhatWeb, and DirBuster. Before you begin, you must understand that using any of these tools against actual web servers without authorization is completely illegal and may get you into trouble. Instead, this lab will target web servers or webpages that were created by cyber security firms with the goal to be intentionally targeted on for academic and research purposes.

Before starting the pen-testing, it’s best to download and install Kali Linux as a virtual machine on a Type 2 Hypervisor using either VMware, Hyper-V, or Virtual Box. Kali can be downloaded from https://www.kali.org/downloads/. It is recommended to install the 64-Bit version of Kali and allocate two cores of the processor, 4GB of Ram, and at least 40 GB of storage space, but this will come down to the specification of the host system.

Zap:

OWASP ZAP is a tool created in Java which comes in a GUI format. Security testers can use this to perform scripting, proxying, spidering, and fuzzing to attack web applications.

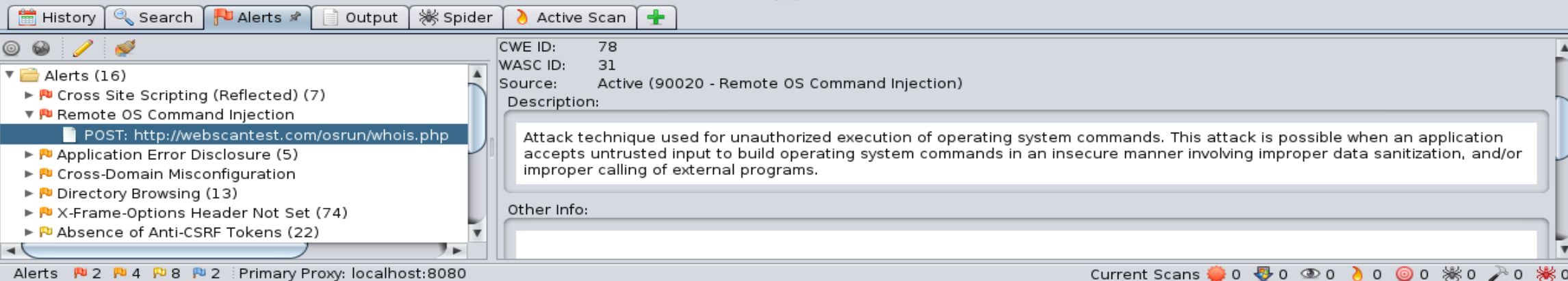
In you Kali machine, navigate to Applications menu and select Web Application Assessment. From here, select the OWASP ZAP tool to launch the application. When you first open Zap it may ask you to accept a license agreement. Accepting this is required to continue to use the application. Once you are at the main screen of Zap, you should see three windows. The left window shows the Sites tab where it will display multiple websites which can be targeted with scans. The right window is where URL’s can be entered to specifically target that website. This is also where you can specify which type of scan you would like between automated or manual scans. The bottom window will have several tabs, each with their own functions. The History tab will display websites that have been tested. The Search tab will allow us to modify searches based on what we need by specifying methods. The Alerts tab will display details about any issues and vulnerabilities that may be present on the web servers that we scan.



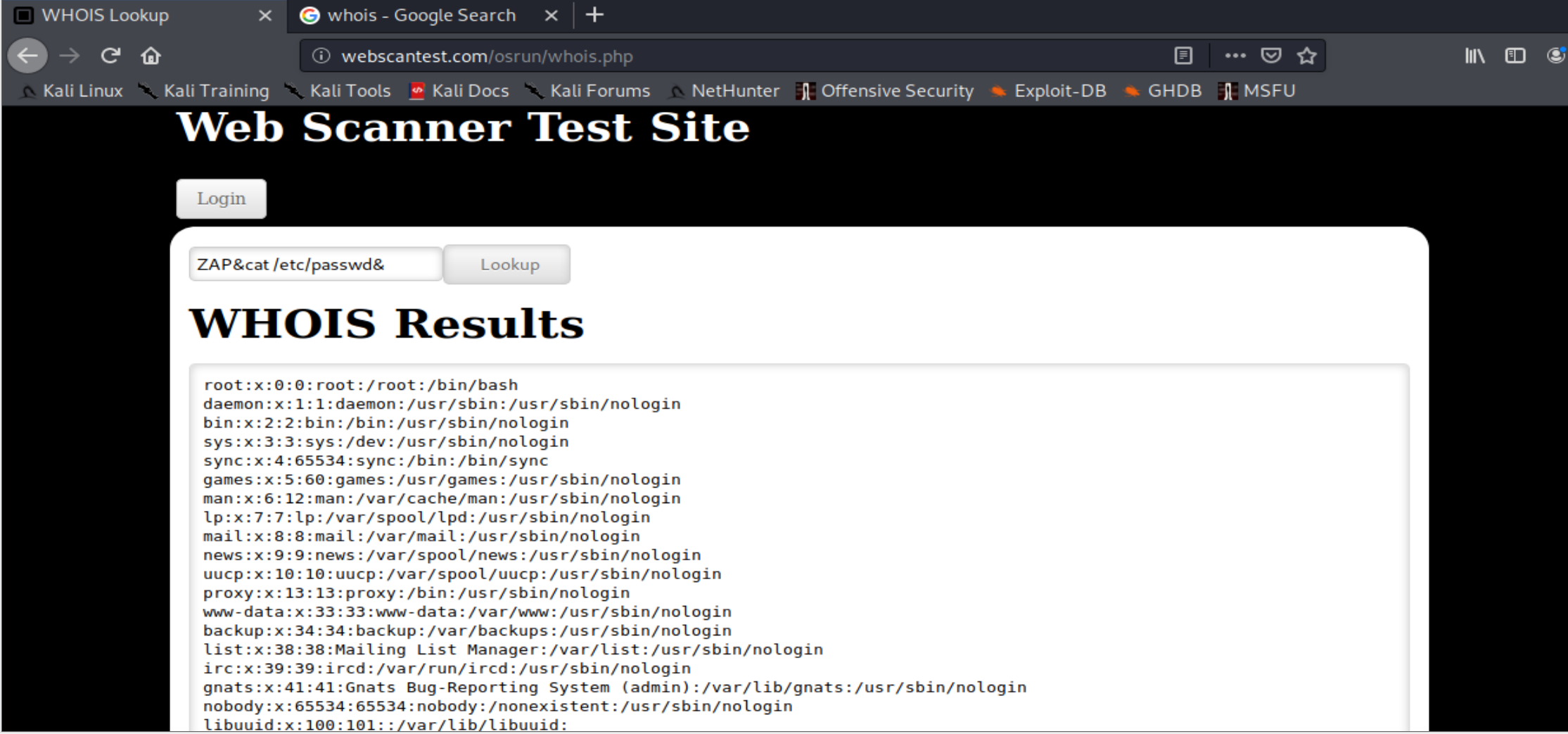
For this lab, we will target a website which was intentionally created to be attacked. Select automated scan and enter in the URL [**http://webscantest.com**](http://webscantest.com). Afterwards, select the Attack button to start scanning. Once the scan completes, you should see a whole bunch of information about the web server. Under the Response tab, we see that the server is running Apache version 2.4.7. Under the Alerts tab, we see all the issues that this web server has that could potentially lead to exploits.



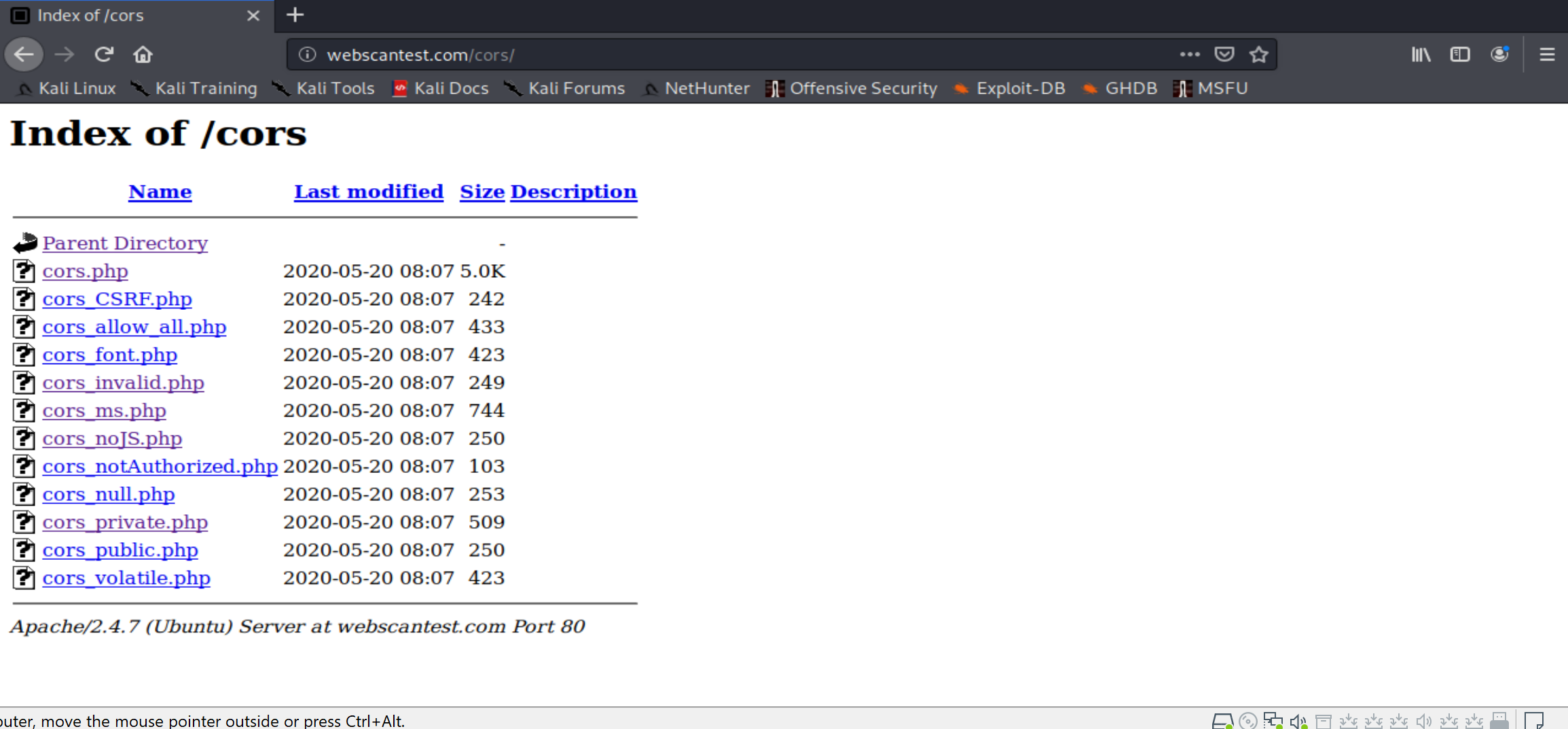
The color of the flags indicates the severity of each alert. As you can see, there are several critical, high, and medium alerts, making this web server prone to many different types of attacks. Try selecting the Remote OS Command Injection vulnerability to learn a little about it. An attacker exploiting this vulnerability could lead them to execute operating system commands on the server due to improper data sanitation by the web server.



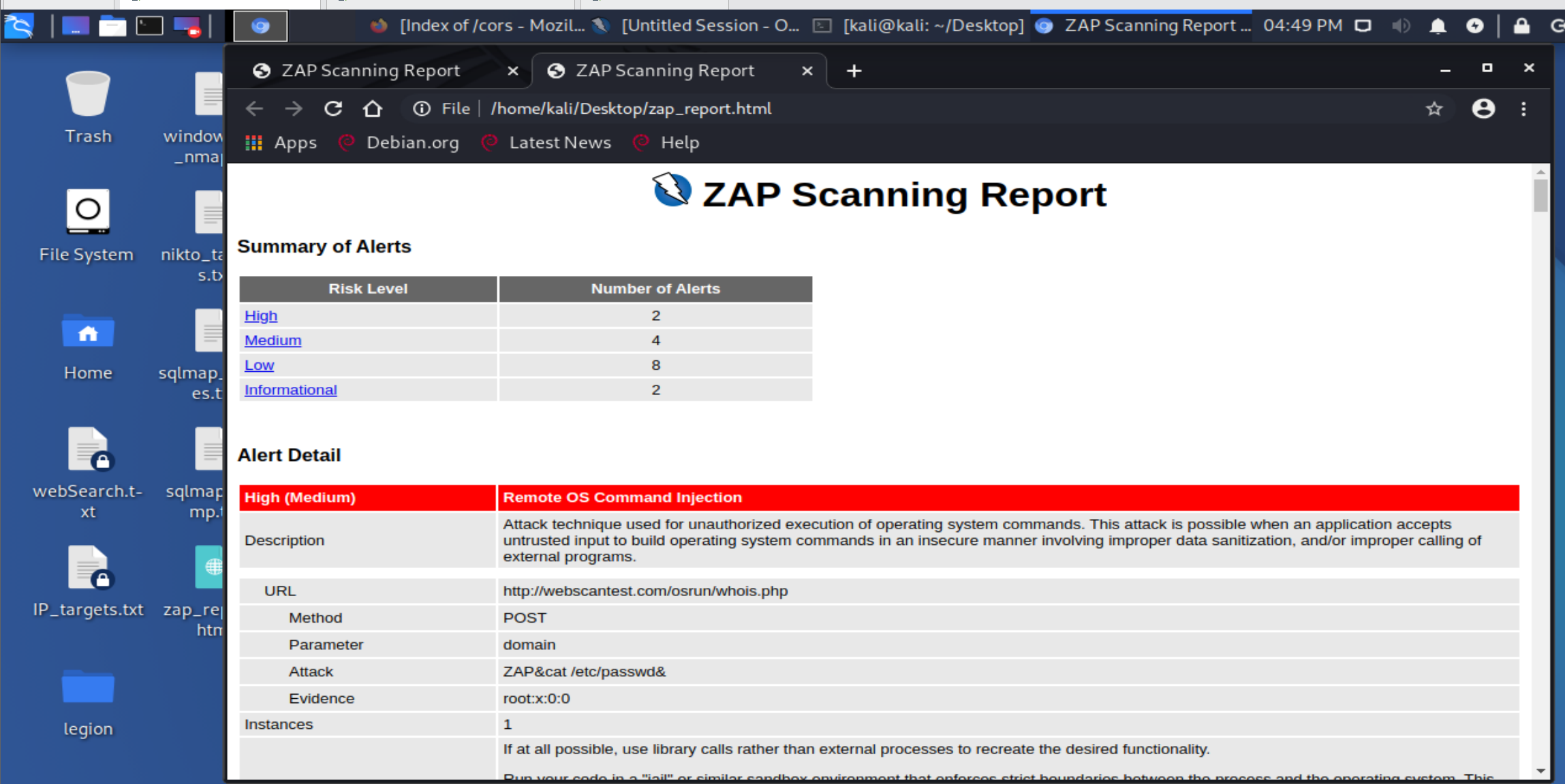
Another vulnerability of extreme severity is the Cross-Site Scripting (Reflected), which may allow an attacker to inject malicious JavaScript code into the input fields. Open a web browser and type into the URL **webscantest.com/osrun/whois.php**. A web page with a WHOIS lookup should appear, but instead of typing an ip address into the input field, type **ZAP&cat /etc/passwd&**.



The ZAP&cat /etc/passwd& is a malicious payload that we injected into the input field, allowing us access to the contents of a password file located at /etc/password. We can take advantage of another vulnerability and access directories that are not intended to be accessed. In the web browser’s URL type **webscantest.com/cors/**. This will allow us access to directory on the back end of the server will files that contain code.



This is most likely due to not having enough permissions set in place to prevent non-authorized people access. The last thing we can look at is Zap’s ability to generate reports on servers that have been scanned. This can be done by selecting Report from the menu bar and then choosing to generate a HTML report.



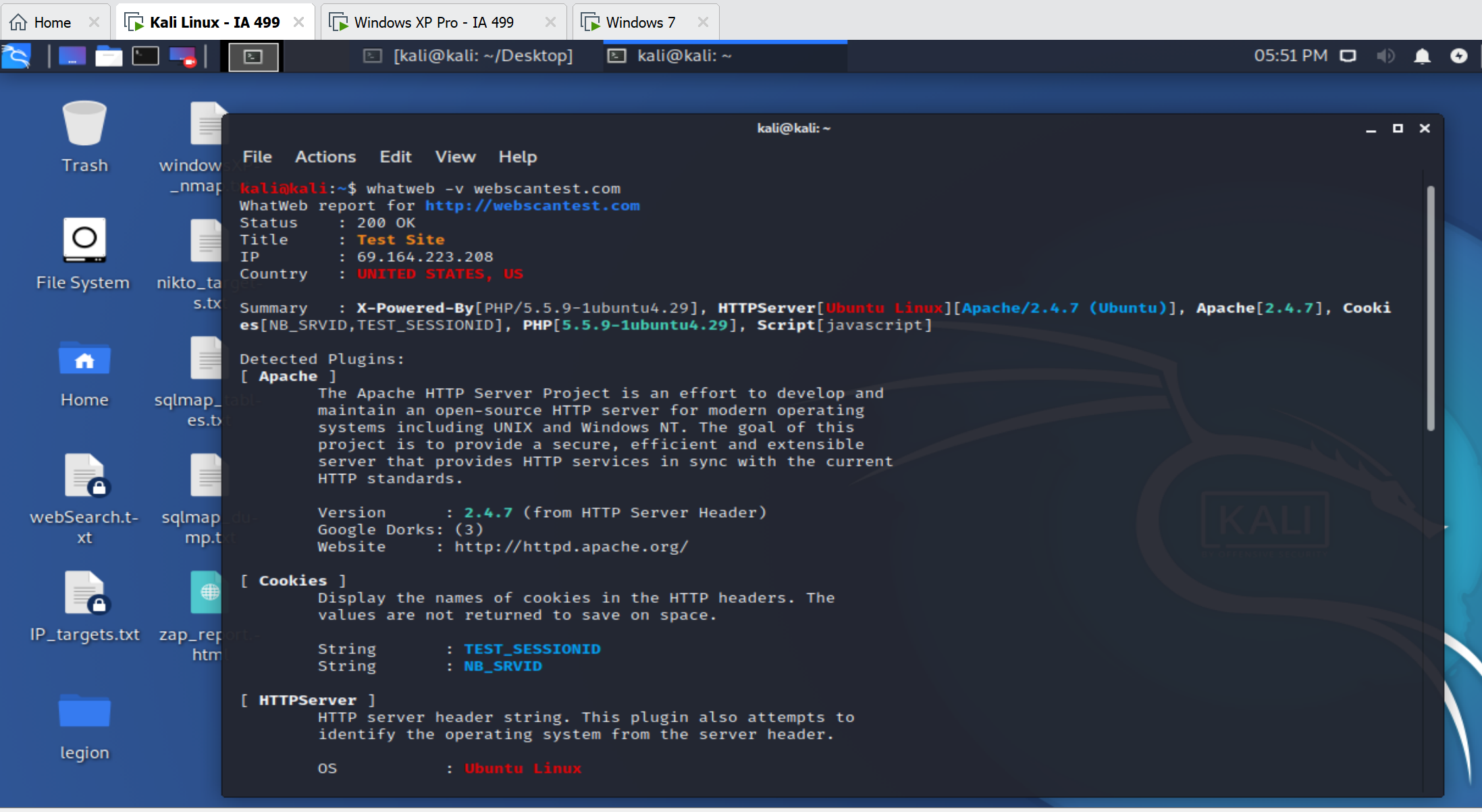
This report can be useful to save for later as it contains important information, such as a summary of alerts and descriptions on the different types of vulnerabilities.

Whatweb:

Whatweb is a scanning tool which will identify all sorts of information on websites. Some of this information includes the IP address, country of origin, the platform, and other analytics. Whatweb is built into Kali and can used within the terminal.

Open a terminal and start looking at some of the options and features Whatweb offers by just typing its name: **whatweb**. Whatweb can change its types of scans based on the level of aggression. The higher the level, the slower but more reliable the scan is. The default level of Whatweb is the stealthiest but also the fastest, which is what we will stick to for this lab. Start ascan against webscantest.com using the following command:

**whatweb -v webscantest.com**

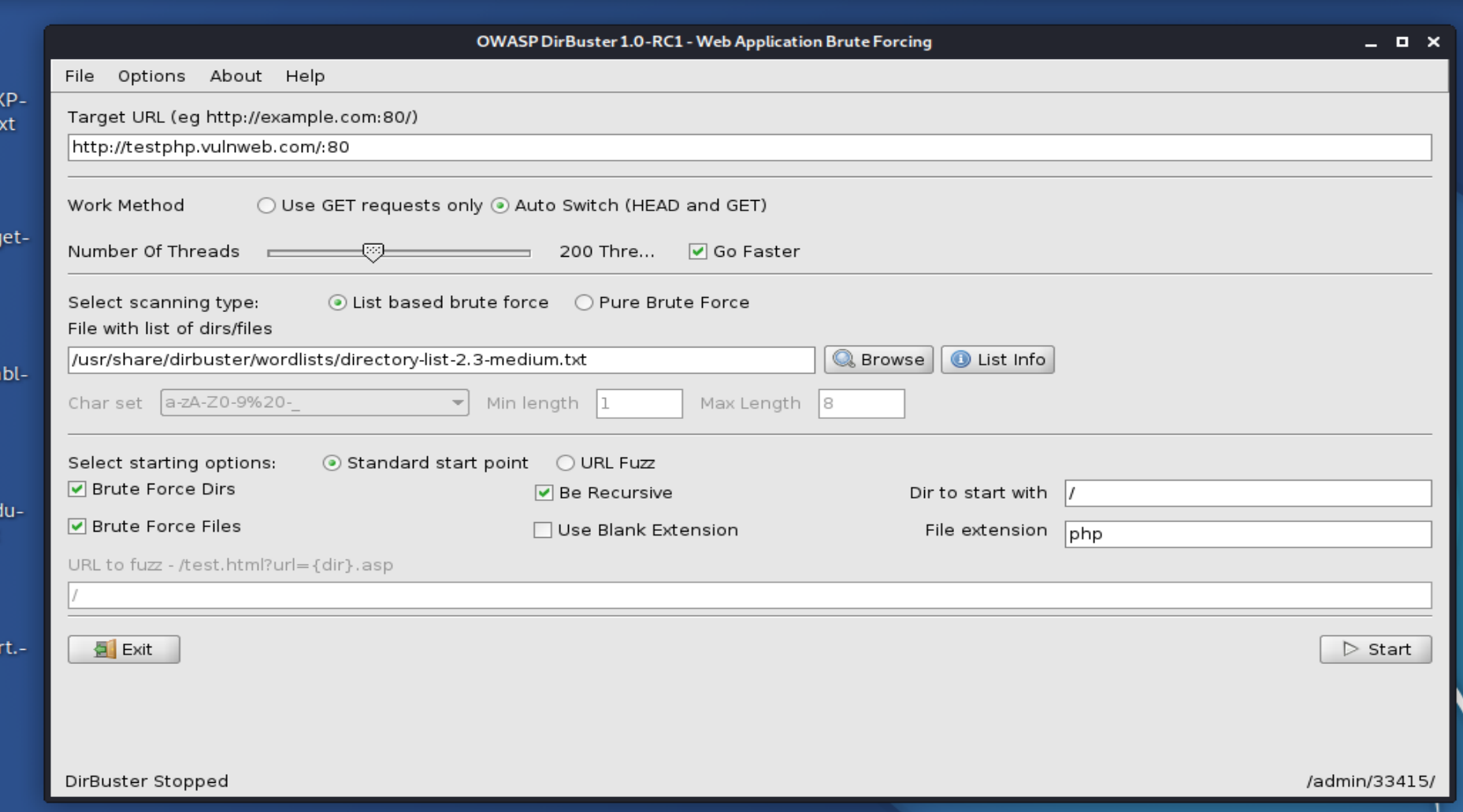


Just like it is show, Whatweb provides all kinds of information. We can grab the ip address (69.164.223.208), the location of the server (United States), the version of PHP (5.5.9), the version of Apache (2.4.7) and the cookie information.

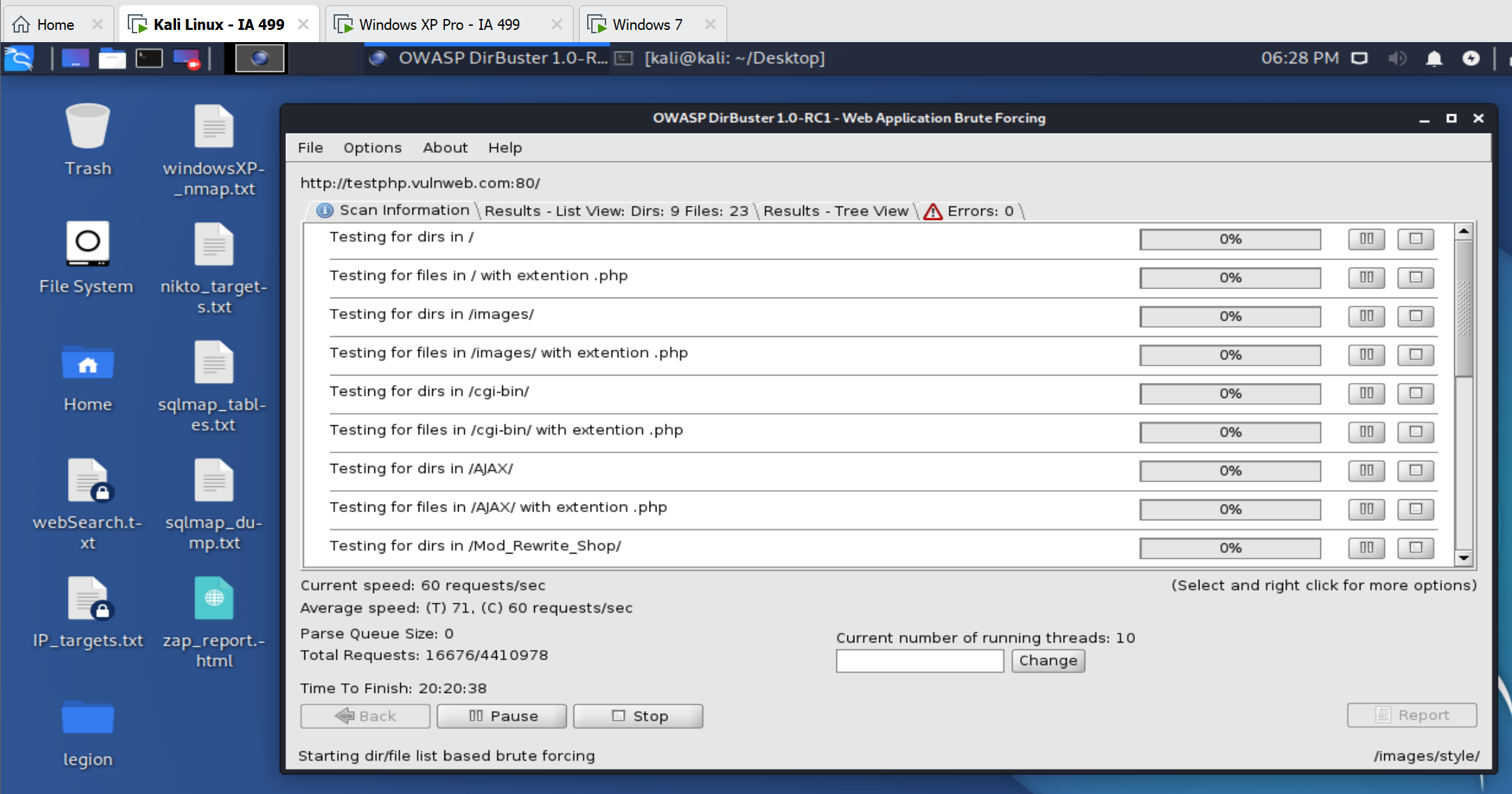
DirBuster:

DirBuster is a java tool with a GUI format which can target websites and brute force their directories and files. This can reveal directories, files, and even applications which are meant to be hidden. This tool can be useful for web developers to test their own websites for vulnerabilities to see if they are prone to their unlinked directories and files of being revealed by others. The downside to DirBuster is that it can be extremely slow especially if the Kali virtual machine is configured with an inefficient amount of computing resources. For this reason, it is recommended that your host system contains a processor with at least four cores and the system memory has at least 8GB RAM. Your Kali VM should be configured to take at least two cores from the processor and 4GB of RAM.

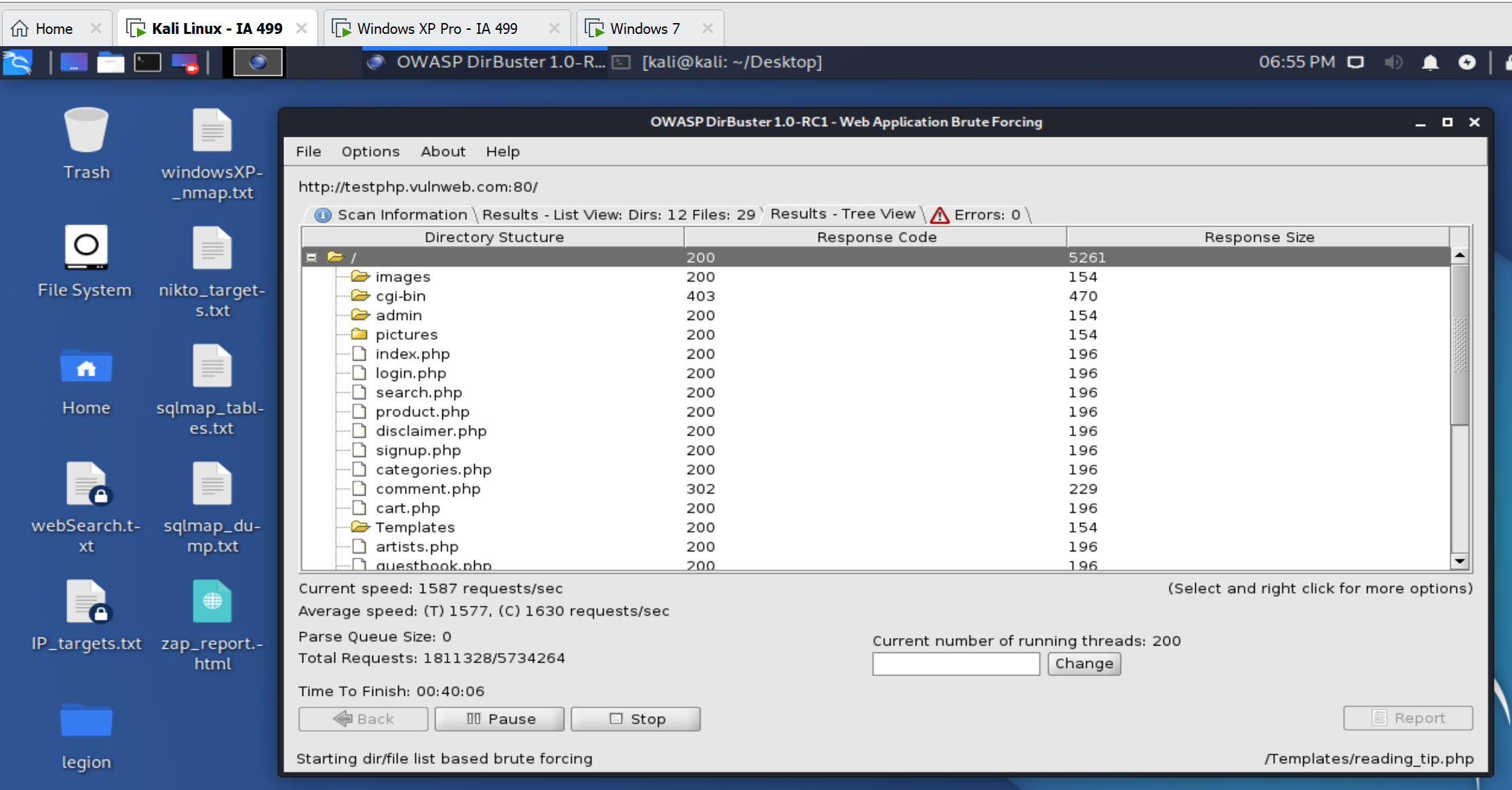
Start DirBuster by simply typing **dirbuster** in the terminal. DirBuster can also be started by navigating to the Application menu and locating it within the Web Application Analysis category. A window will open showing various settings and options for targeting URL’s. We will be targeting the website <http://testphp.vulnweb.com>, a website intentionally created to be targeted by anyone for educational purposes. In the Target URL input field, type [**http://testphp.vulnweb.com/:80**](http://testphp.vulnweb.com/:80). Next, change the number of threads by selecting the Go Faster button to speed up the brute force process. If this is not checked or the number of threads is not increased, this whole process would be extremely slow to the point where you may not see any progress for hours. The last thing we must do is to point DirBuster to a file which contains a list of word for DirBuster to compare to for the scan. Lucky for us, we do not have to create a text file, instead, DirBuster comes installed with several of these. So, where it says, “file with list of dirs/files,” select browse and navigate to the directory /usr/share/dirbuster/wordlists and select the file “directory-list-2.3-medium.txt.” For the rest of the options, leave the defaults on and select start.



DirBuster will start the scanning process and create the directory tree detailing every directory and file, including the hidden ones.



To fully complete the scan and recreation of the files and directories, it would mostly likely take DirBuster hours. Instead, let it scan for about 20 to 30 minutes or until it reaches about 20% of the scan and then select to pause the scan. You should see the results of what it was able to find. You can select the Results – Tree View tab to look at the directories and files in a tree like format.



This will provide information on the types of the files and the size of them as well. If you get any errors during the scan, you can use the Errors tab to view them. Lastly, DirBuster allows you to generate a report on what it discovers. Reports can be generated in either a text file, an XML file, or a CSV file.