How to use OWASP Zed Attack Proxy (zaproxy)

Motivation

Finally, after writing the papers, How to securely isolate Damn Vulnerable Linux with VirtualBox and How to securely isolate Kali Linux with VirtualBox, this paper is dedicaated to the execution of attacking the Web and DataBase services on Damn Vulnerable Linux with Zed Attack Proxy.
If you are not familiar with this beautiful, free tool, review it here:
http://tools.kali.org/web-applications/zaproxy

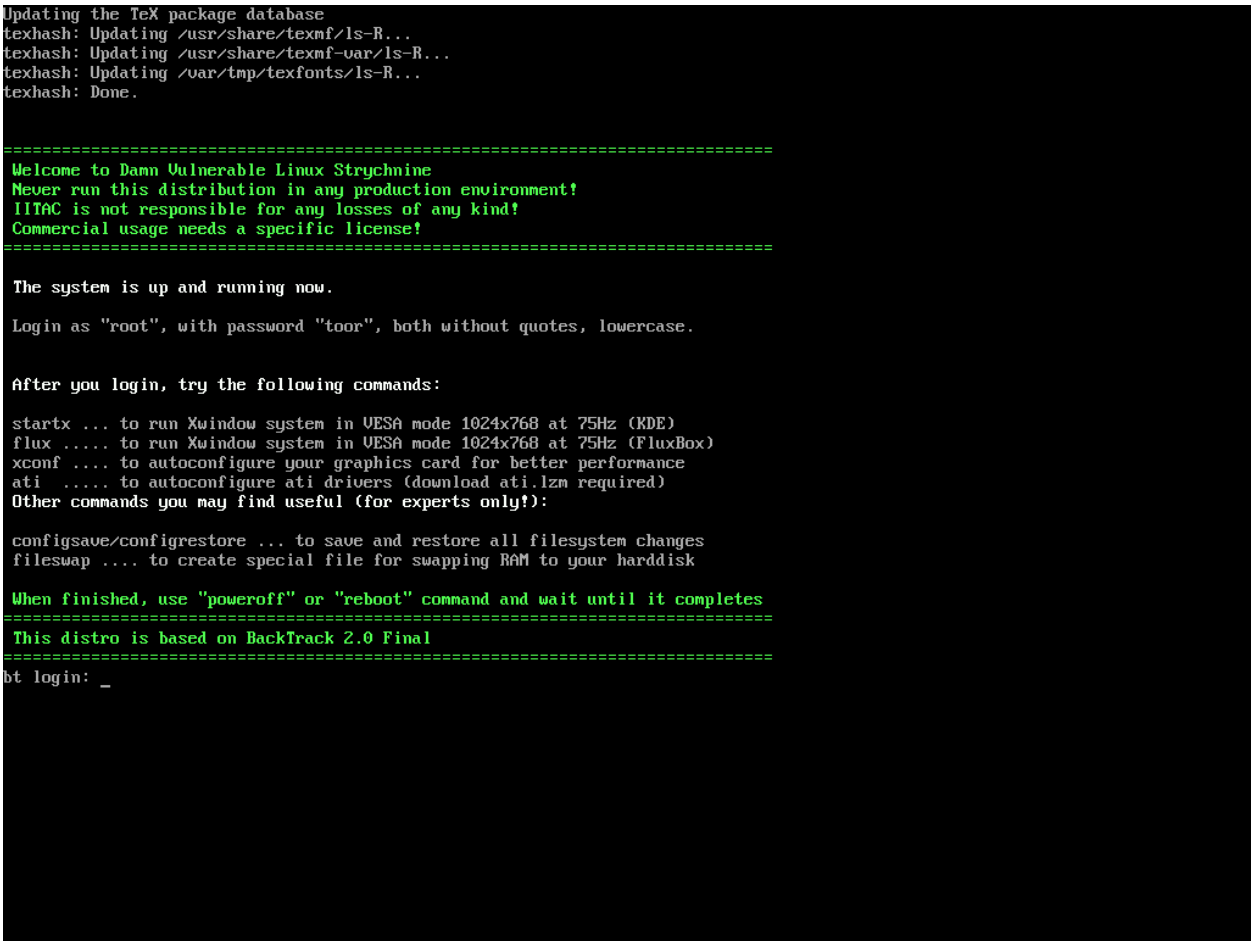
Basically, this tool enables Pen Testers an automated method to attack web servers and validate the security level of said.

Test environment layout

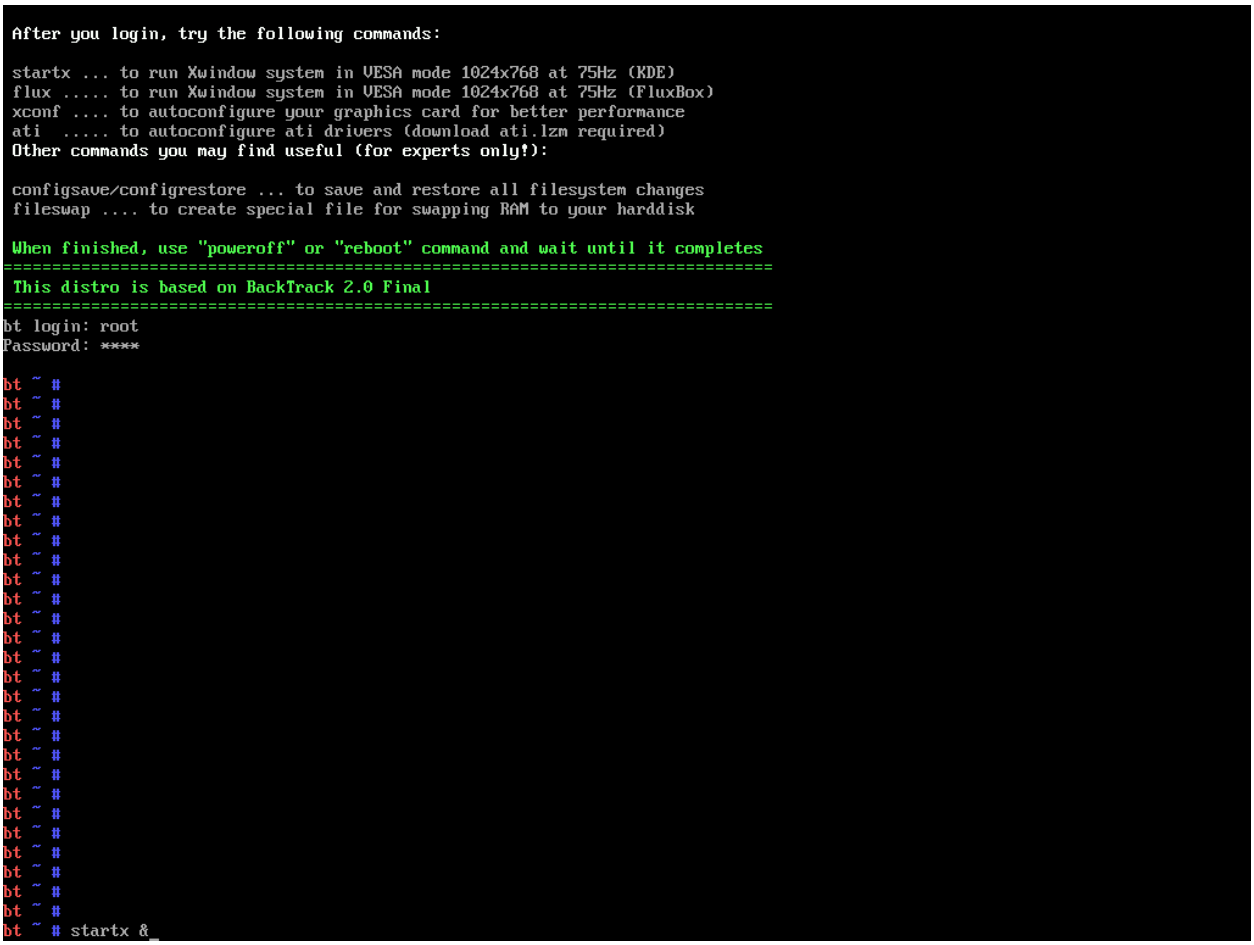
My workstation is running Ubuntu 16.10.
I am first installing VirtualBox 5.1.6 for Ubuntu, using method 2 below.
Damn Vulnerable Linux 1.5 running inside of VirtualBox 5.1.
Kali Linux running in inside VirtualBox 5.1.

Setup and deployment

Asuming you followed the previous papers mentioned in Motivation, go ahead and start both virtual machines now.

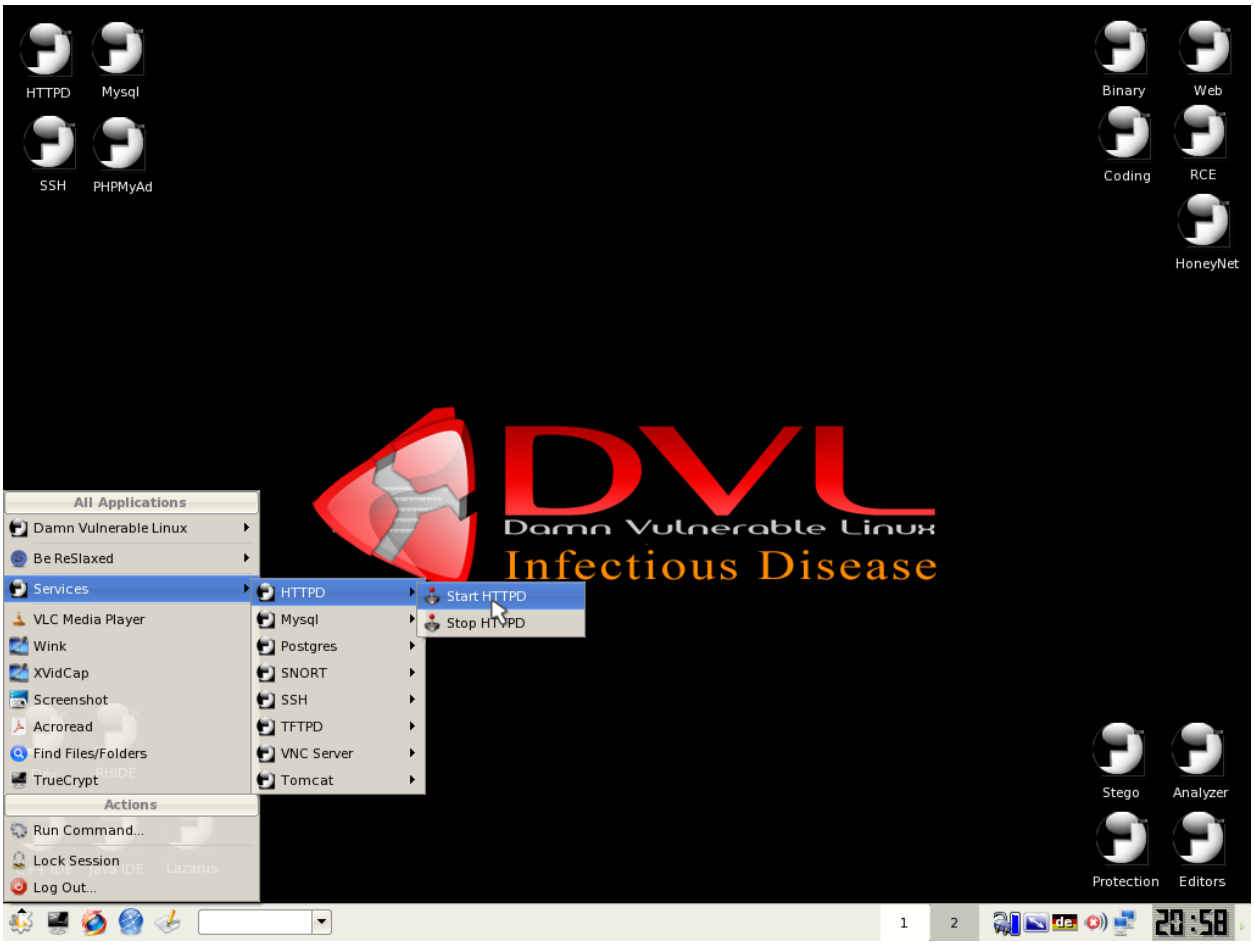


This is the login screen for Damn Vulnerable Linux. Your user name is root and the password is toor.



Type in “startx &” and hit enter.

This is the initial X11 window system.



Using the left icon, I believe KDE gears, follow the diagram and start the HTTPD service.

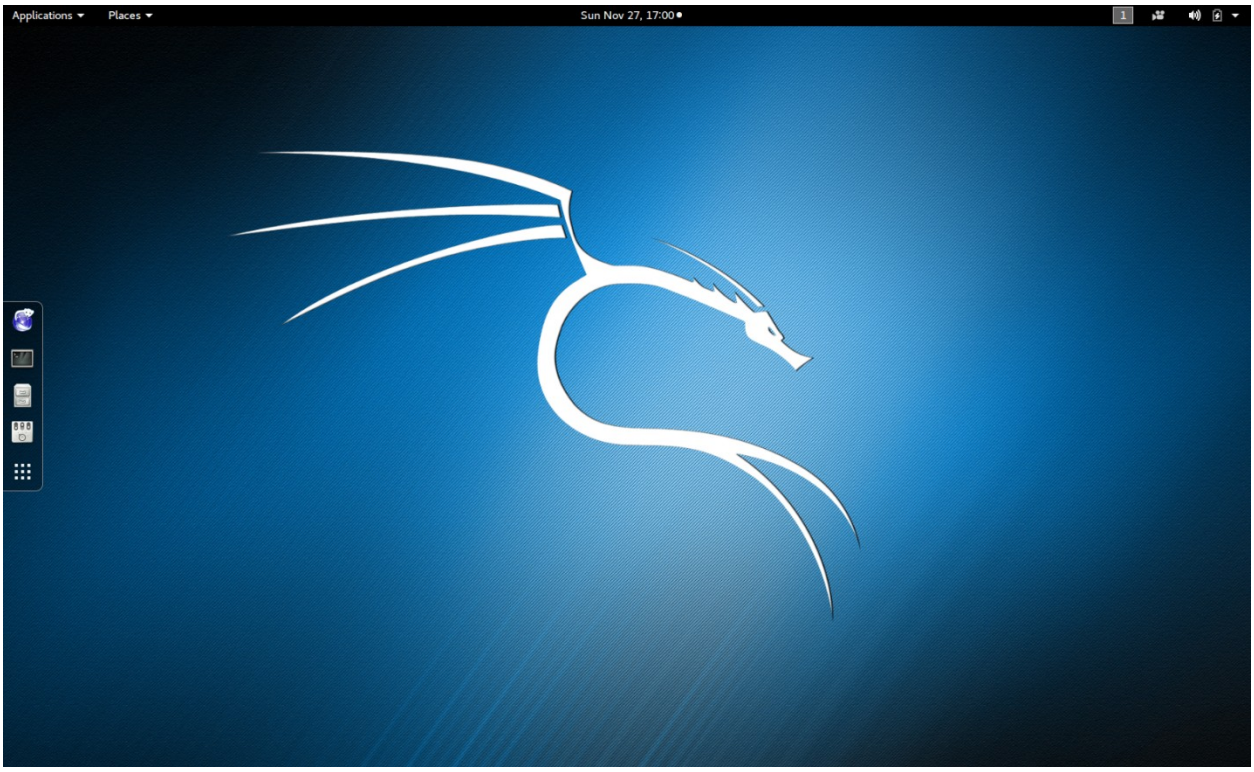
Start the MySQL service.

Start the Postgres service.

Start the SSHD service.

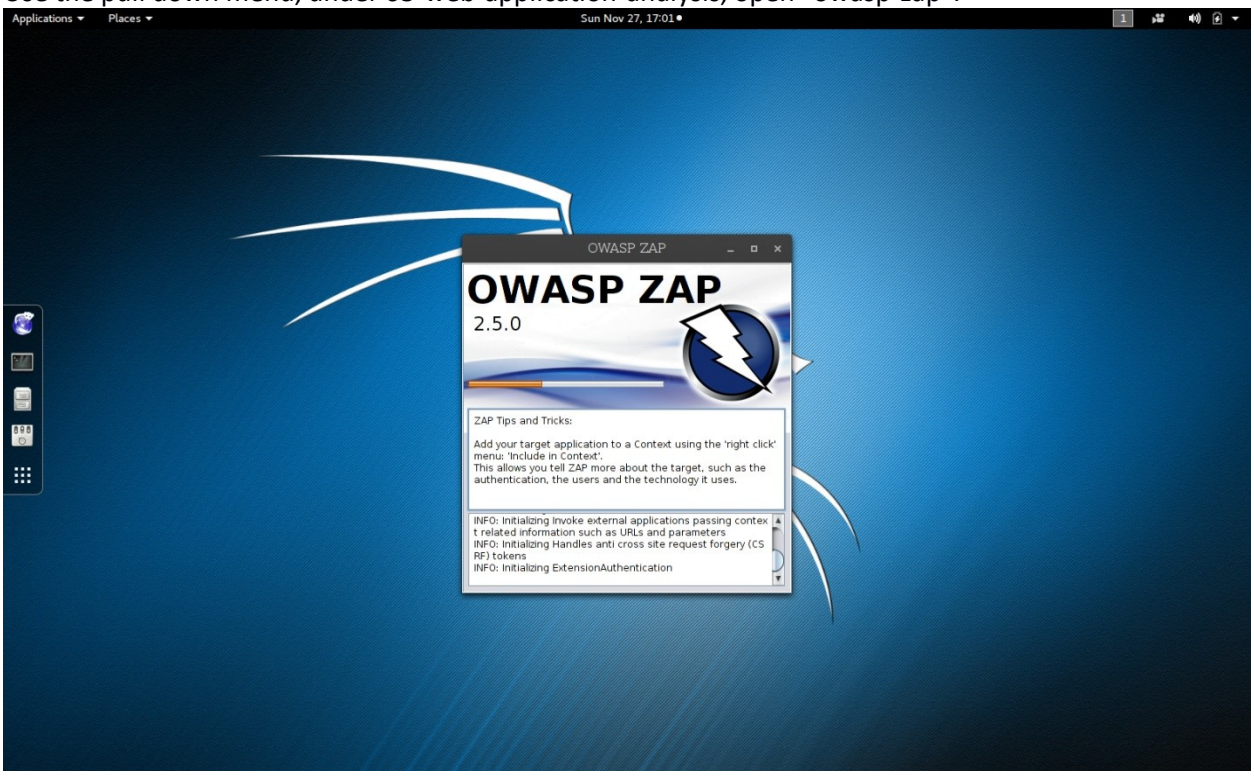
Start the Tomcat service.

Now, Switch to the running Kali Linux virtual machine.

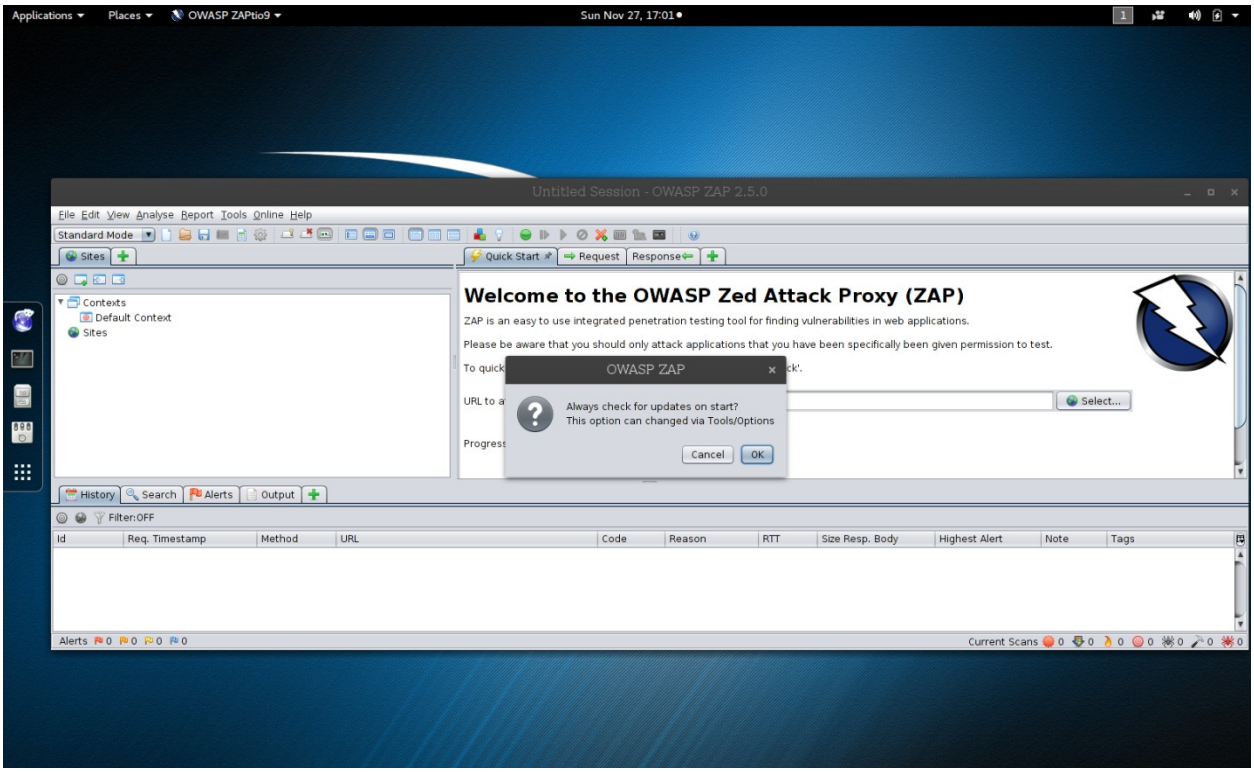


Once you authenticate in (username root, password toor), this is what you will see.

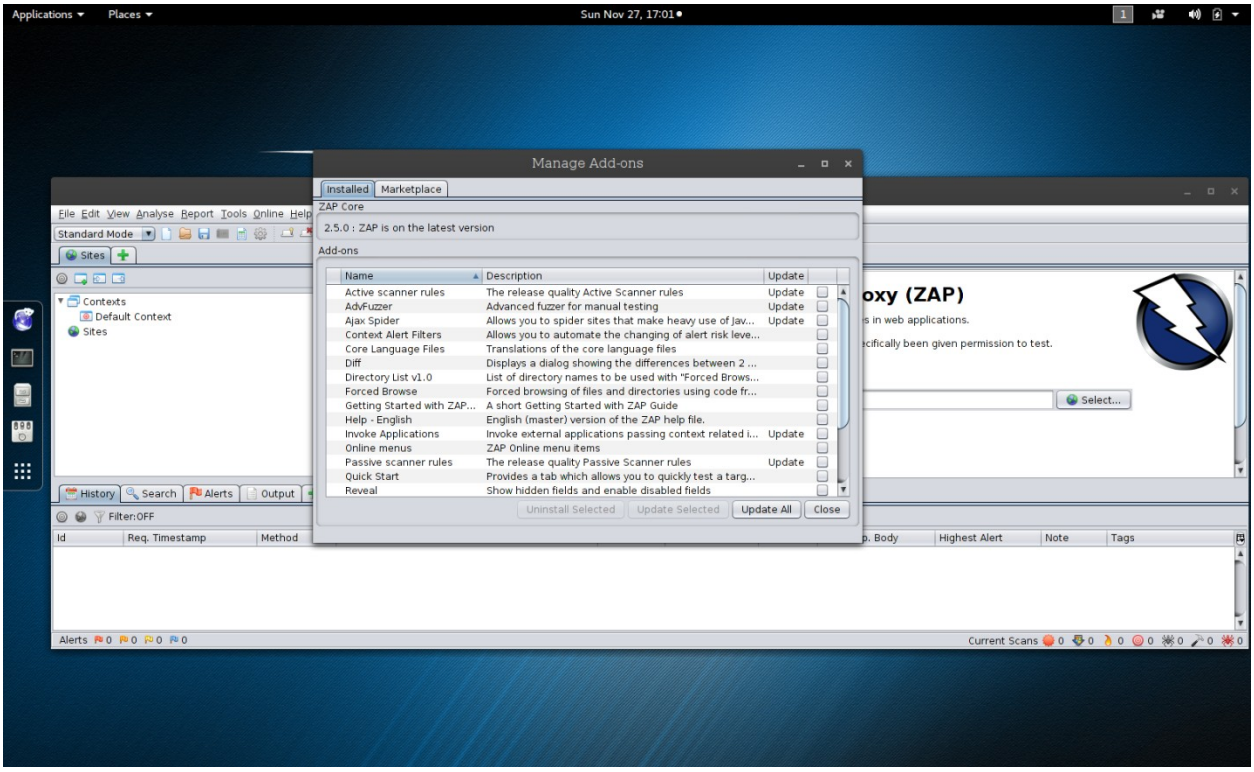
Use the pull down menu, under 03-web-application-analysis, open “owasp-zap”.



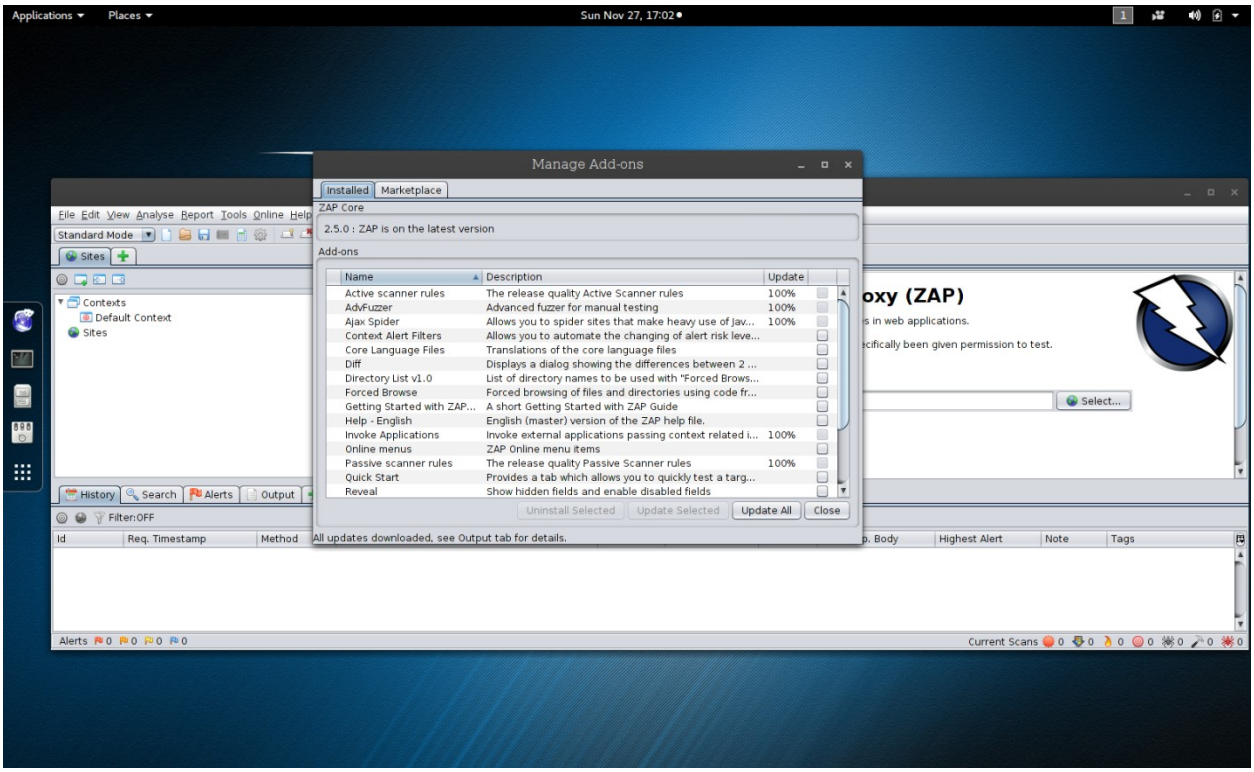
You will see this on the initial startup of the application.



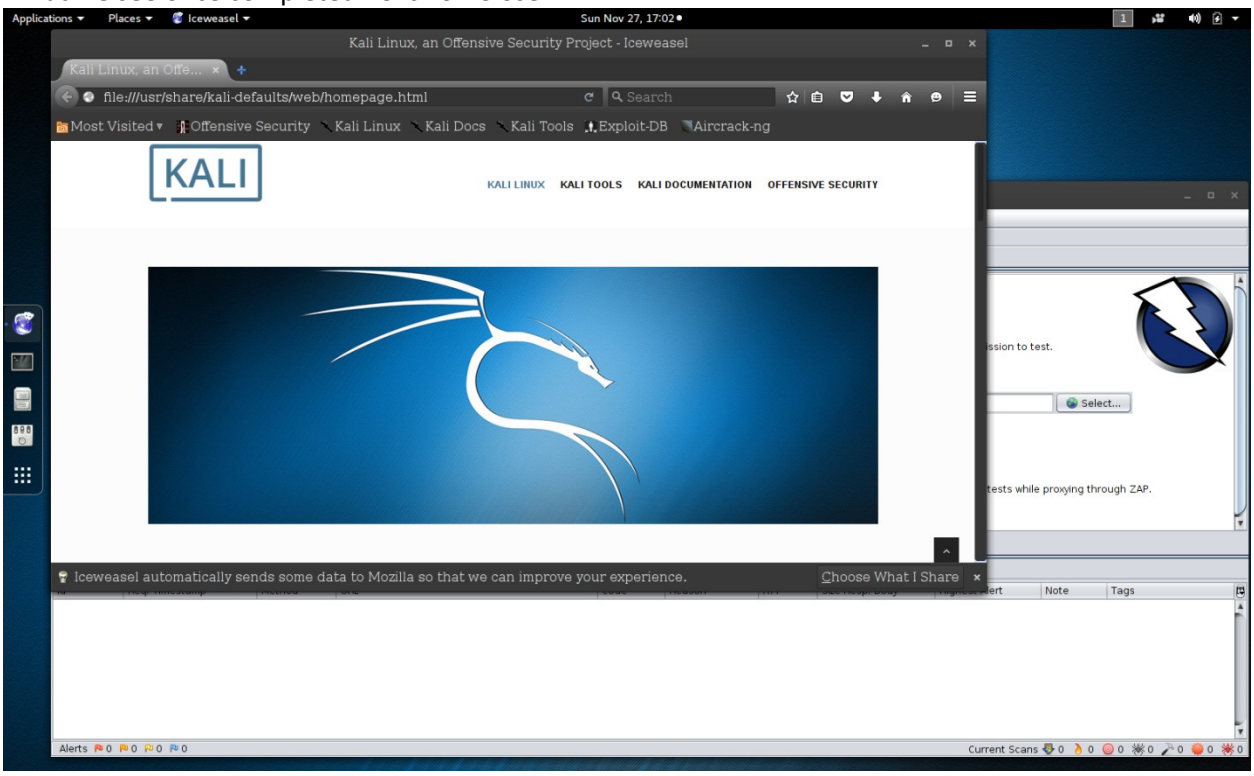
Click OK.



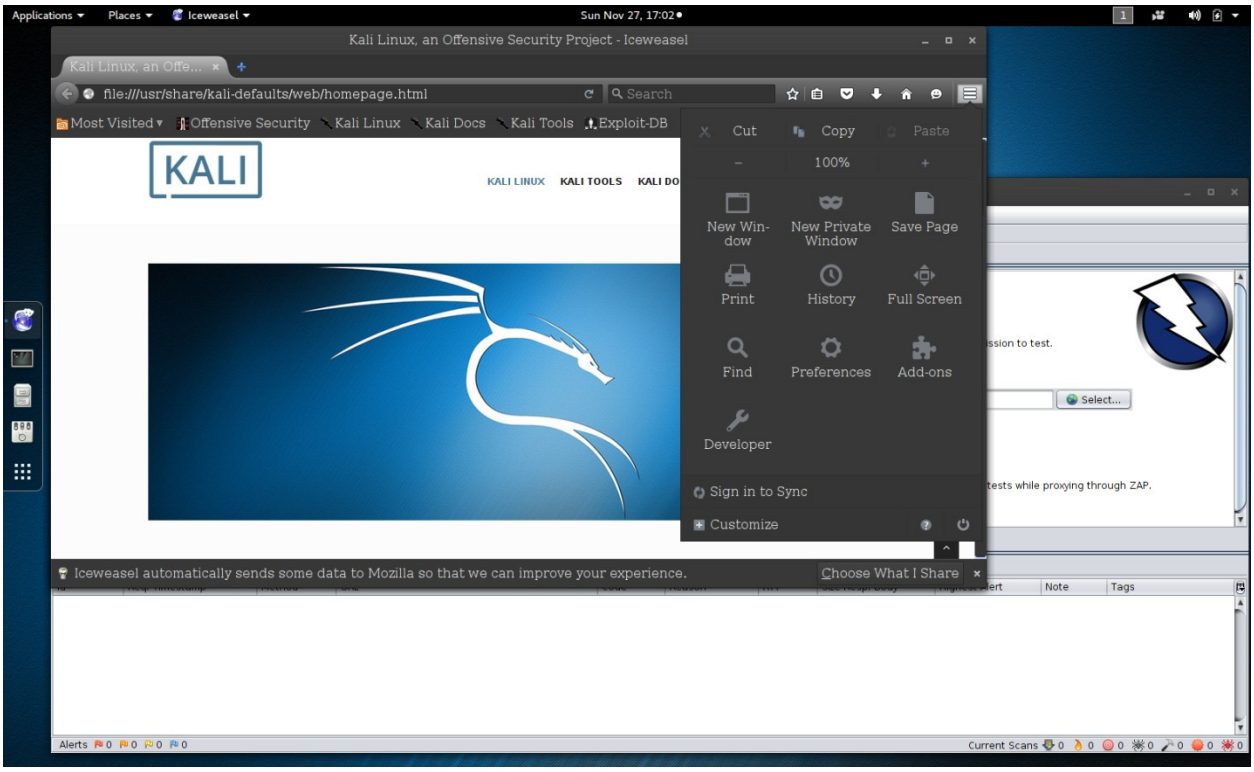
If you have internet access, click on Update All.



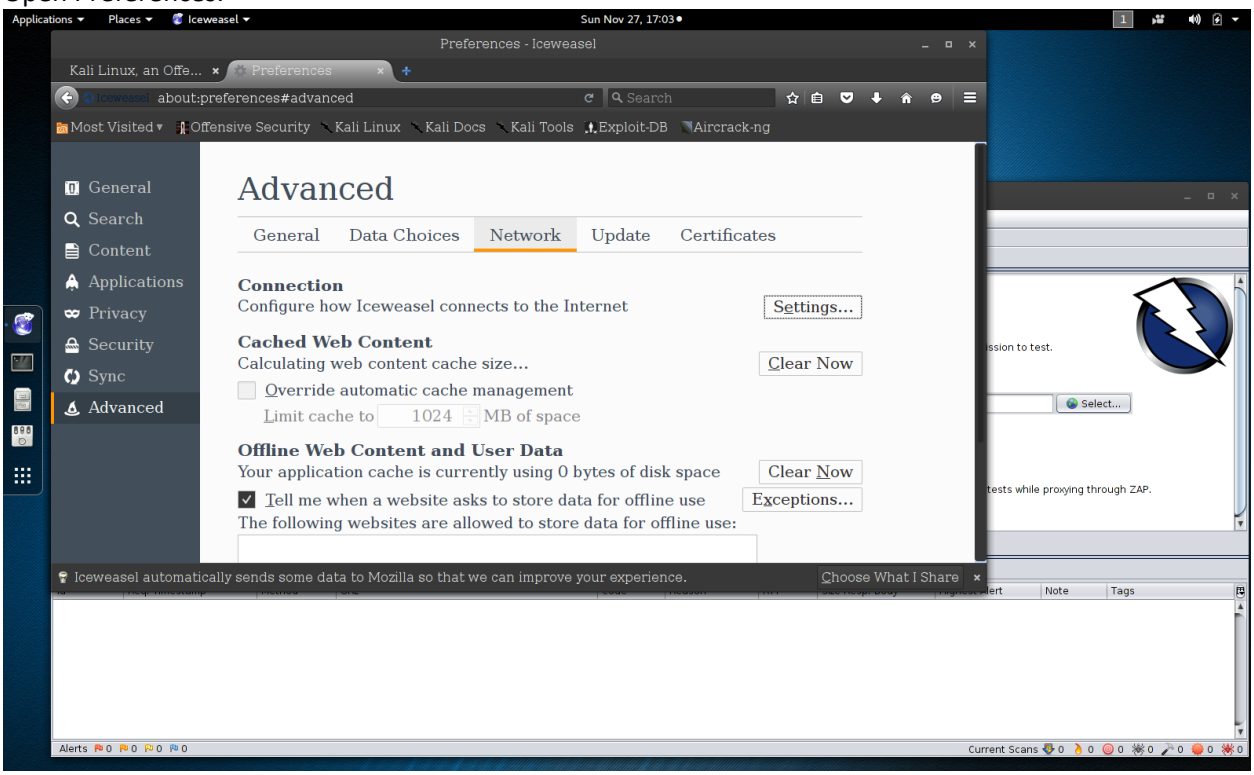
What we see once completed. Click on Close.



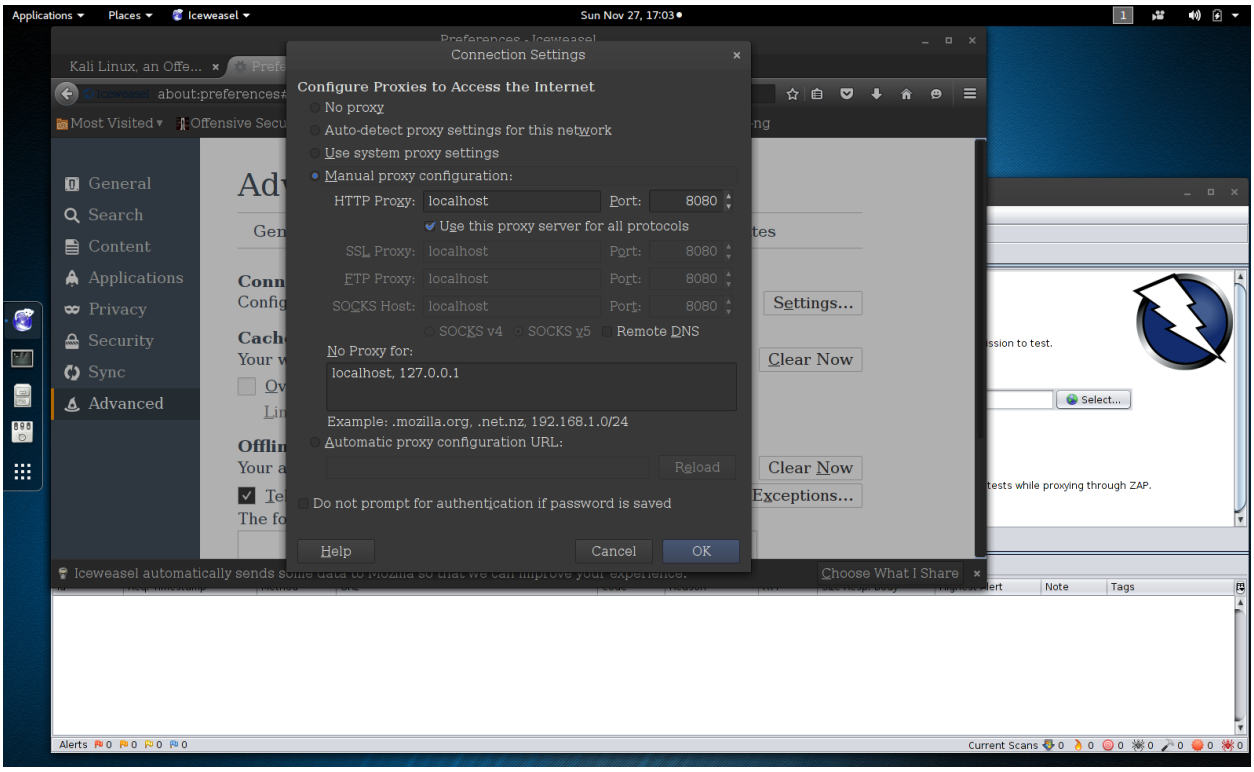
Now open the broswer Iceweasal.



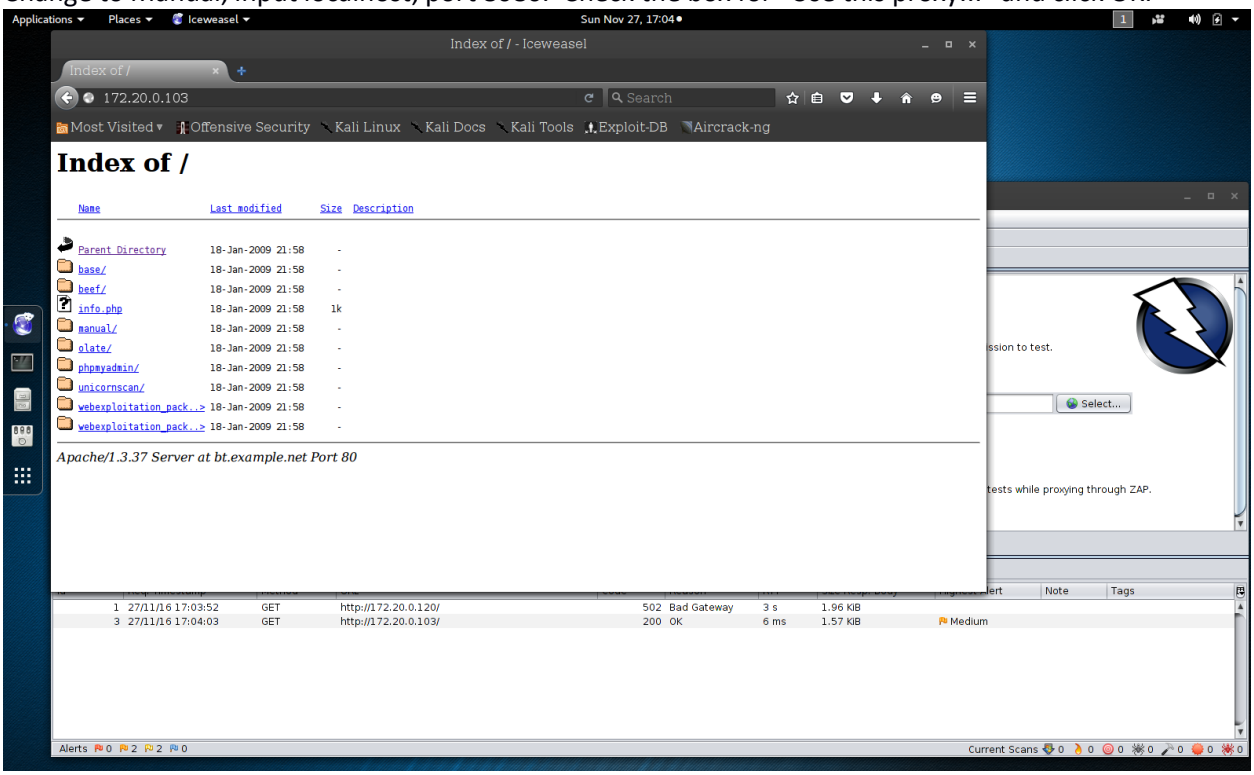
Open Preferences.



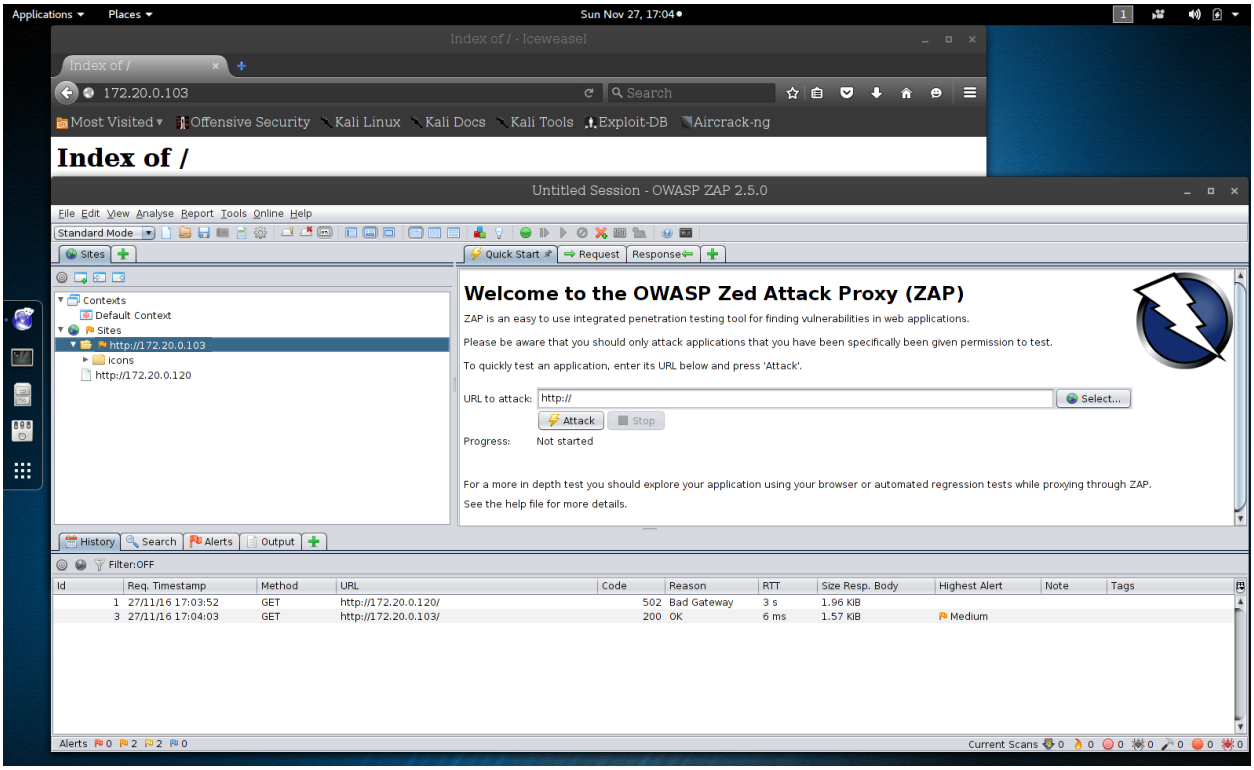
Under Advanced, Network, click on Settings.



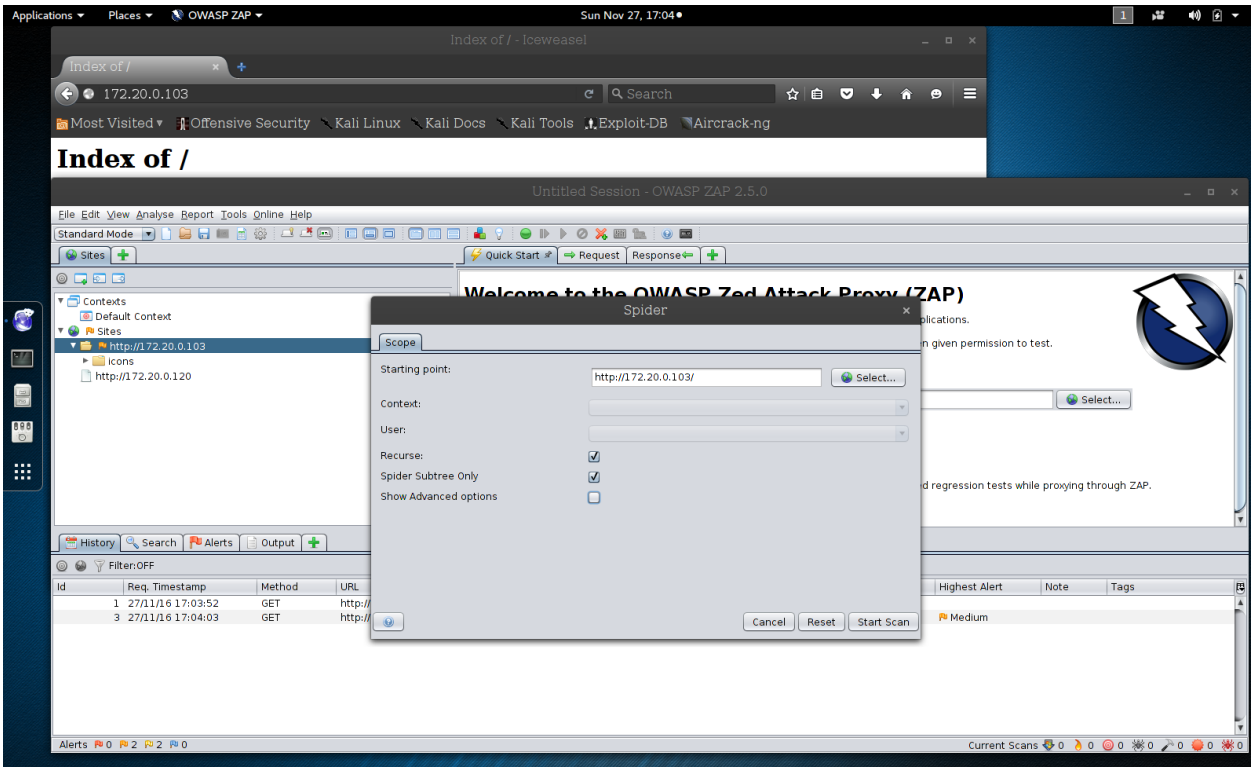
Change to Manual, input localhost, port 8080. Check the box for “Use this proxy...” and click OK.



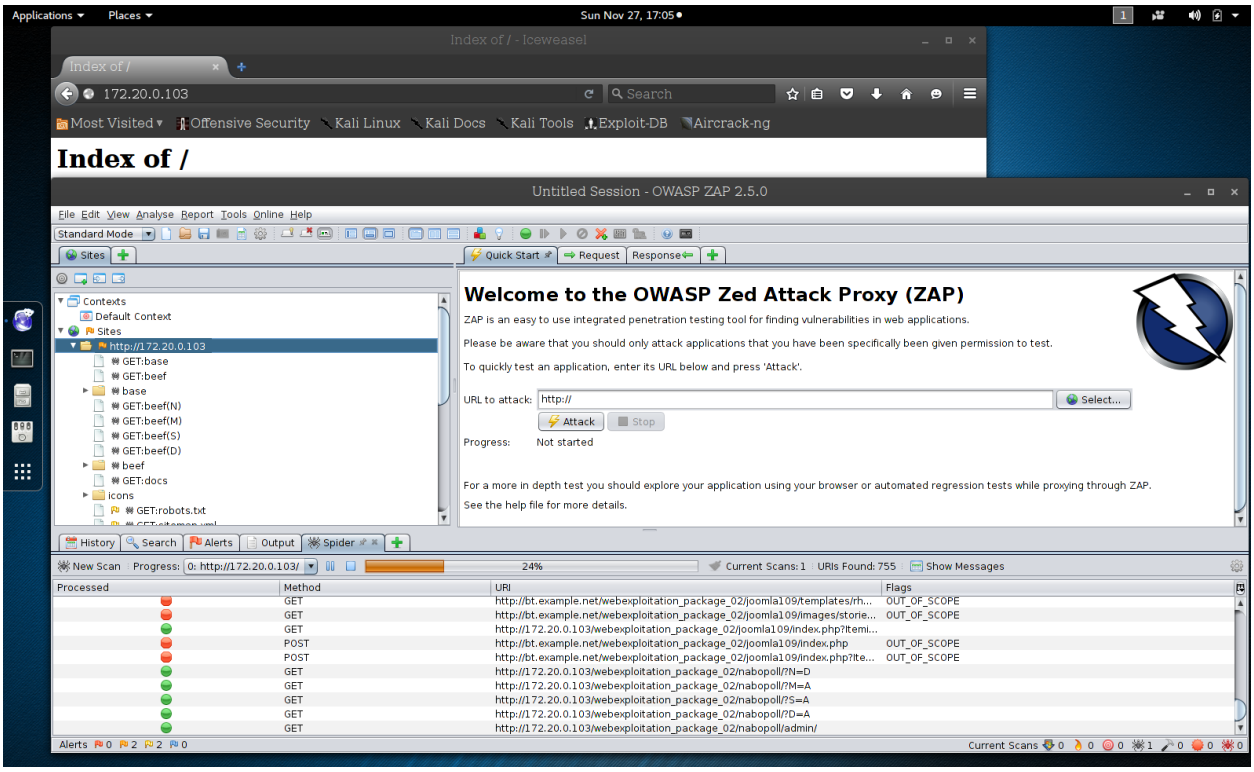
Now, in the browser, put the IP address of the Damn Vulnerable Linux server, here I have 172.20.0.103. To check, open a terminal and type in “ip a” this will show the address on the DVL virtual machine. Plug that result in here.



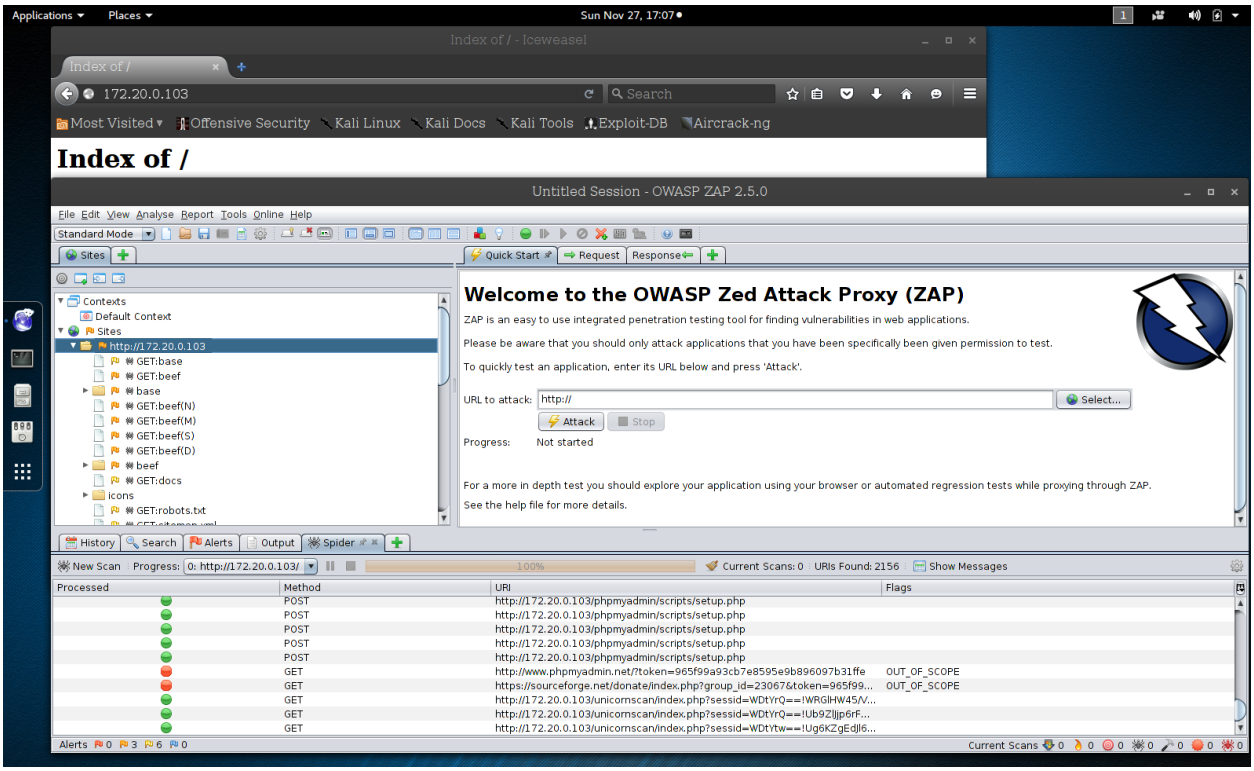
In OWASP ZAP, you will see the IP address populate under Sites.



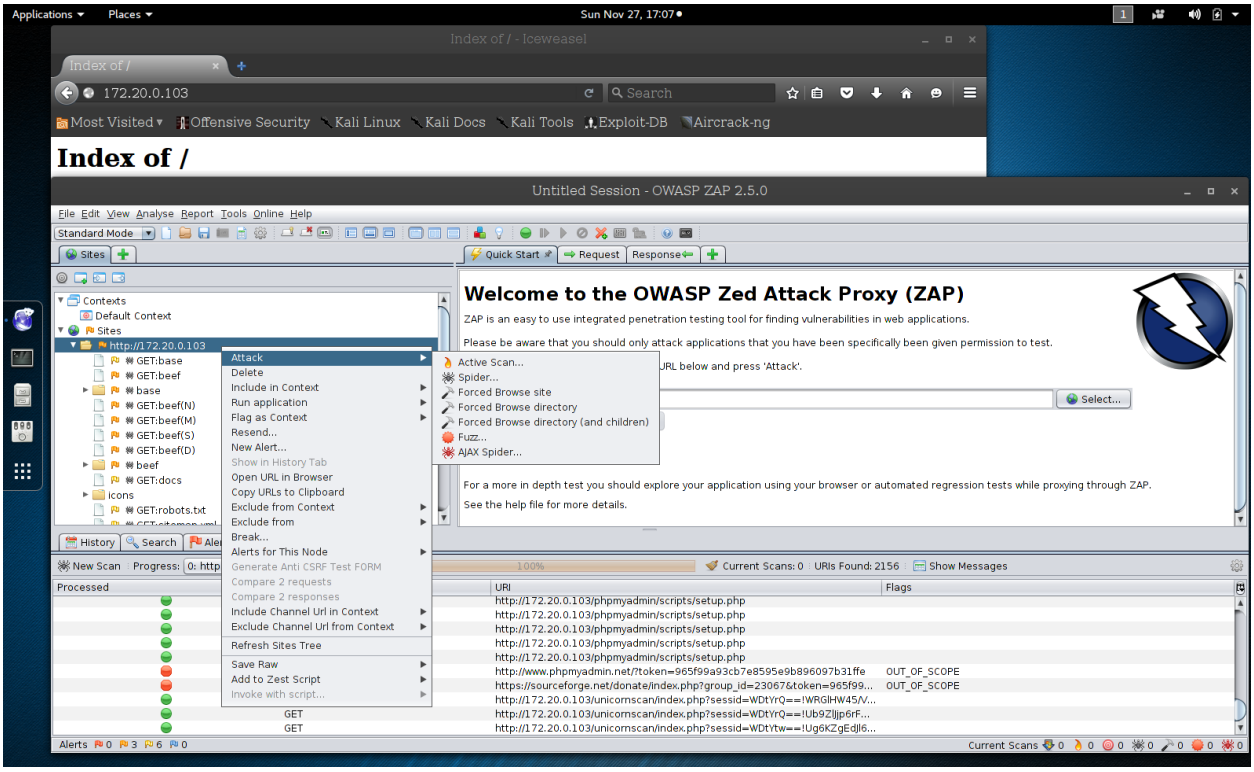
Most items in ZAP are right-click sensitive, meaning you can right click to open additional dialogues. Right click under Sites on the IP address and choose: Attack, Spider. Check the box for Spider Subtree Only, and hit Start Scan.



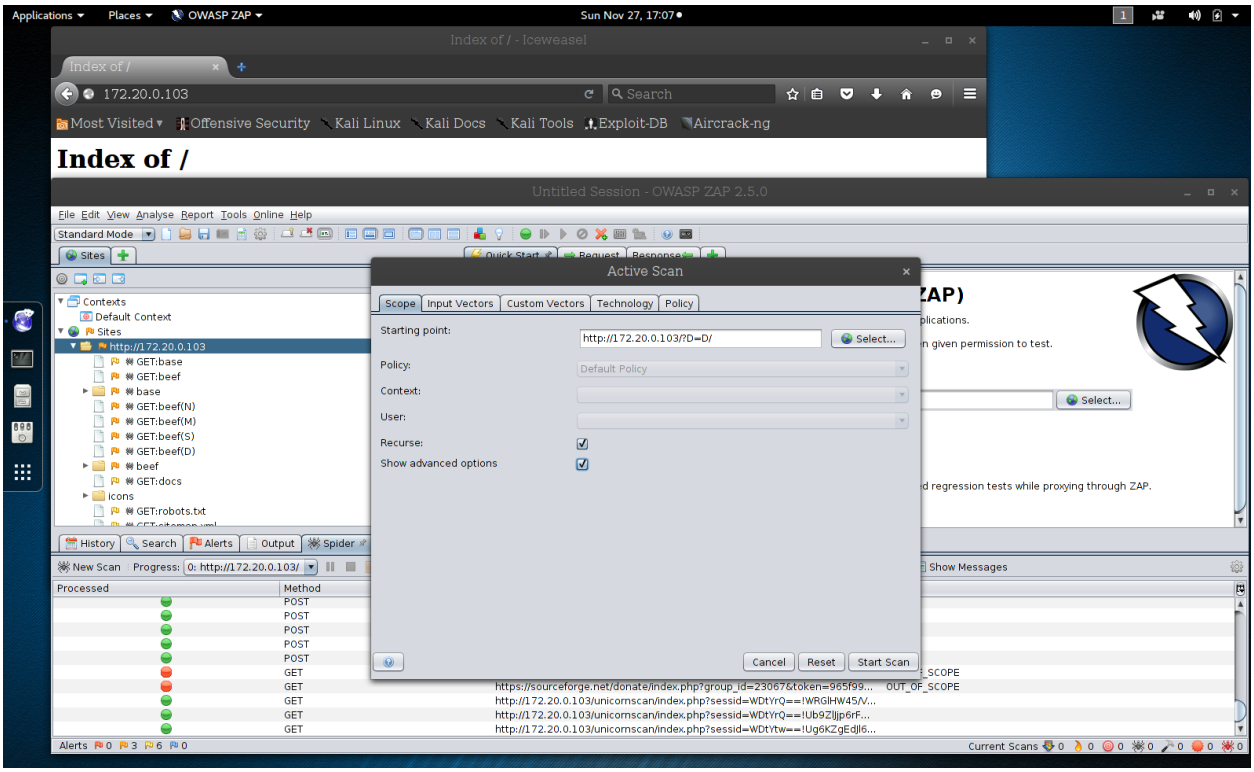
Spider in progress.



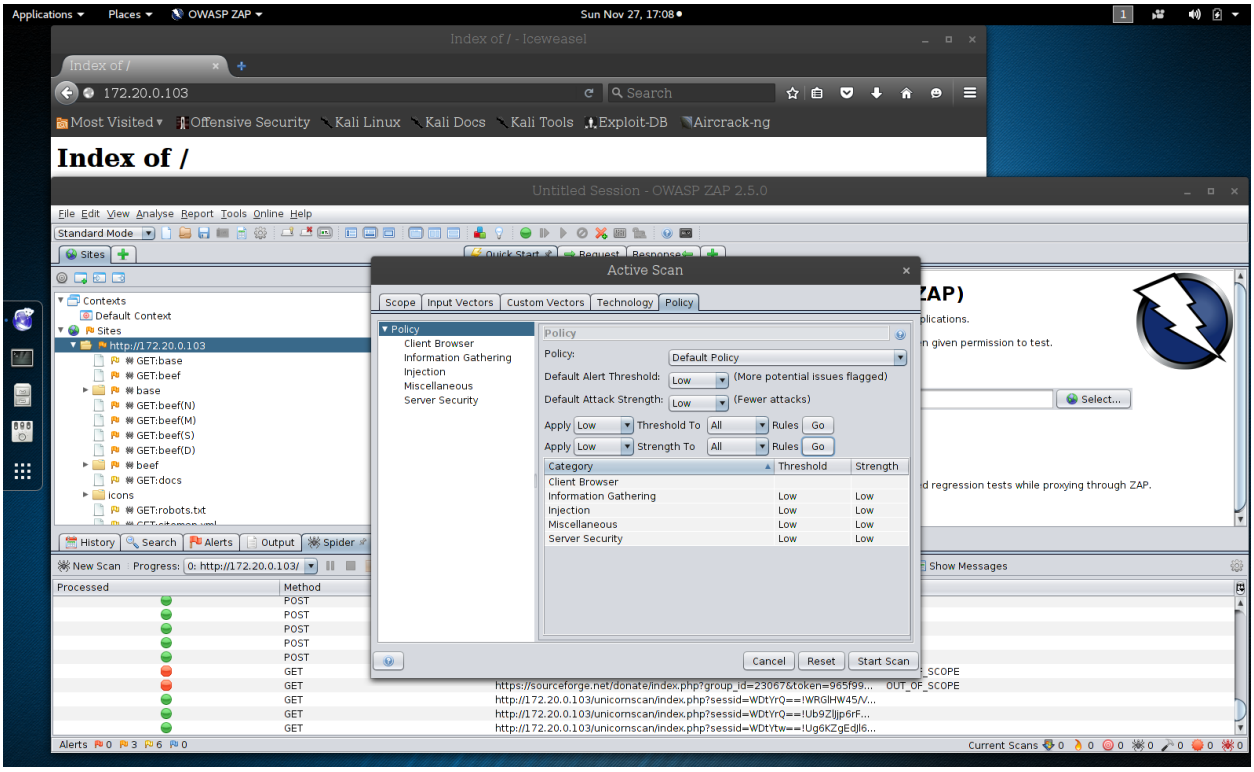
Spider finished.



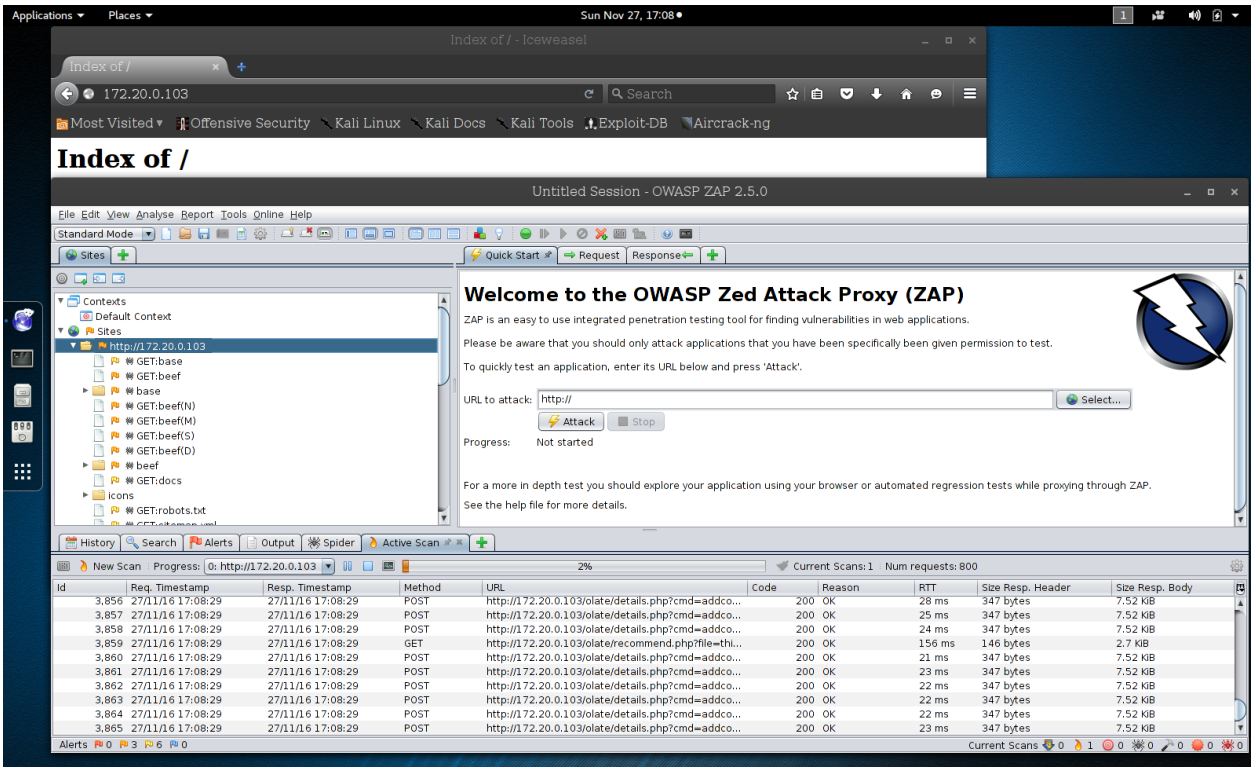
Right click on the IP, Choose: Attack, Active Scan.



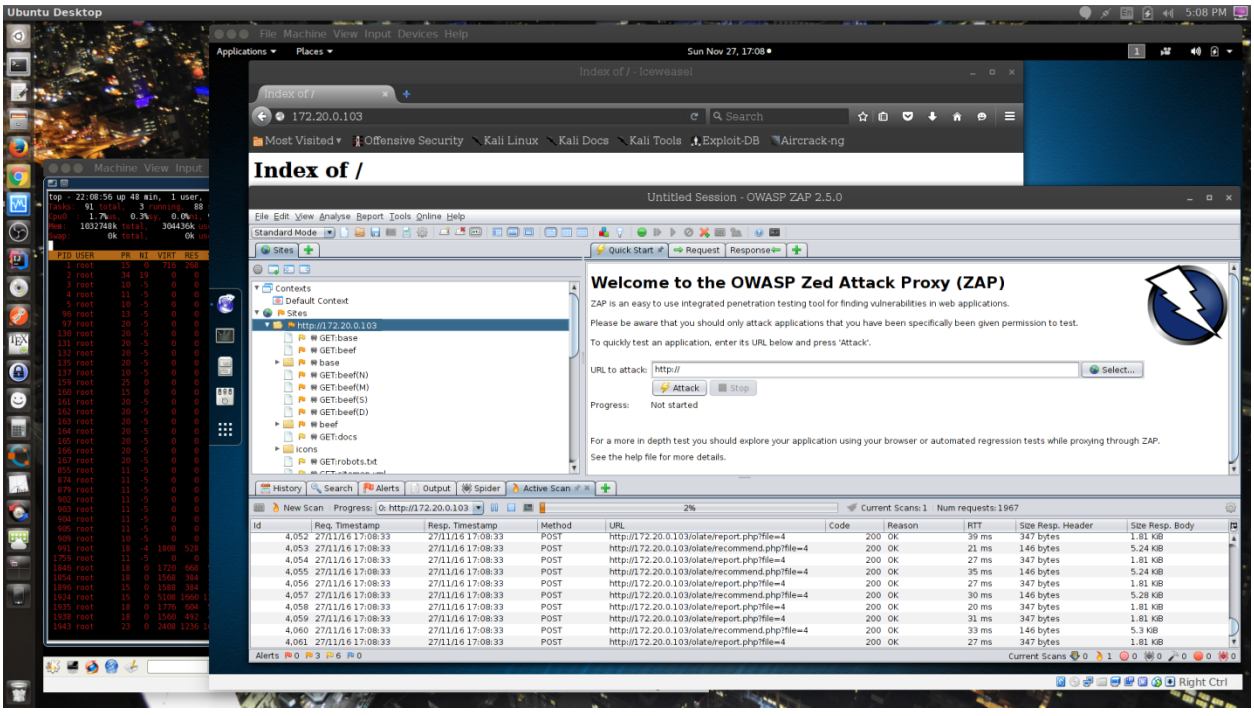
Check the box for Advanced Options.



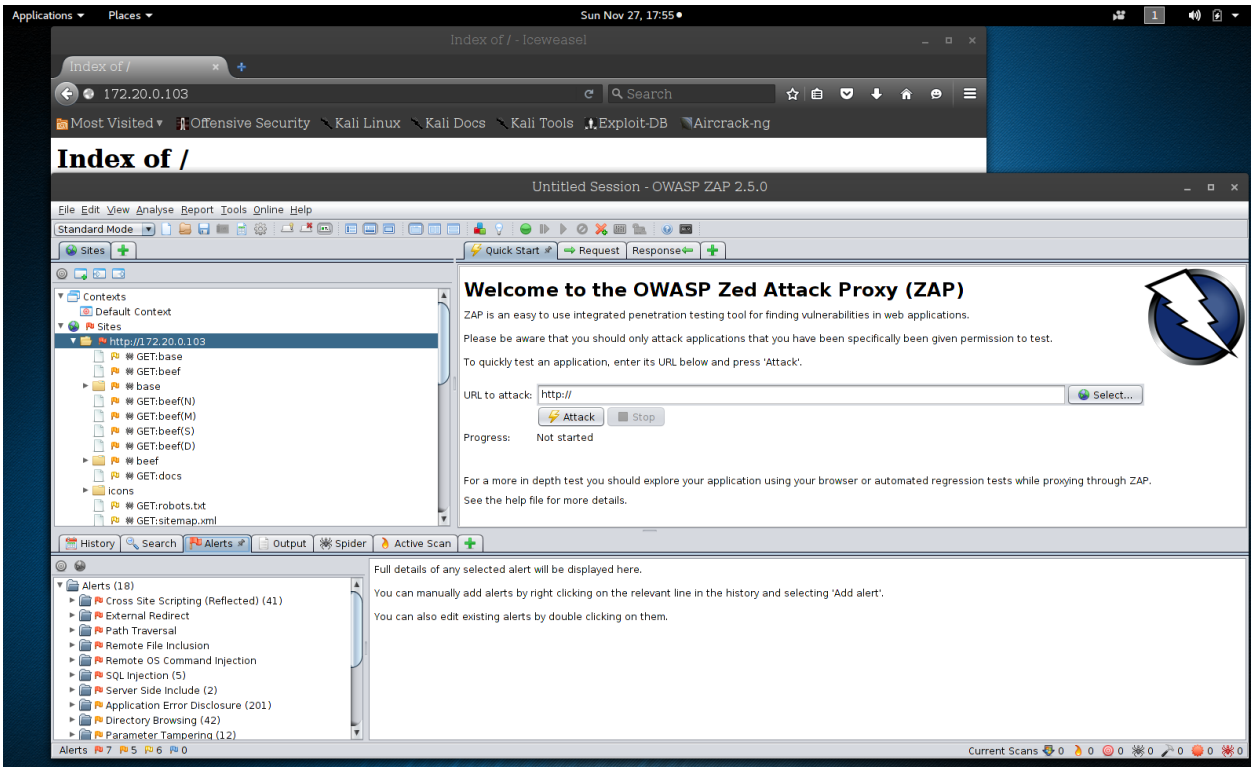
Click on the Policy tab, and set everything to Low. Then hit the Go buttons. Then Start Scan.



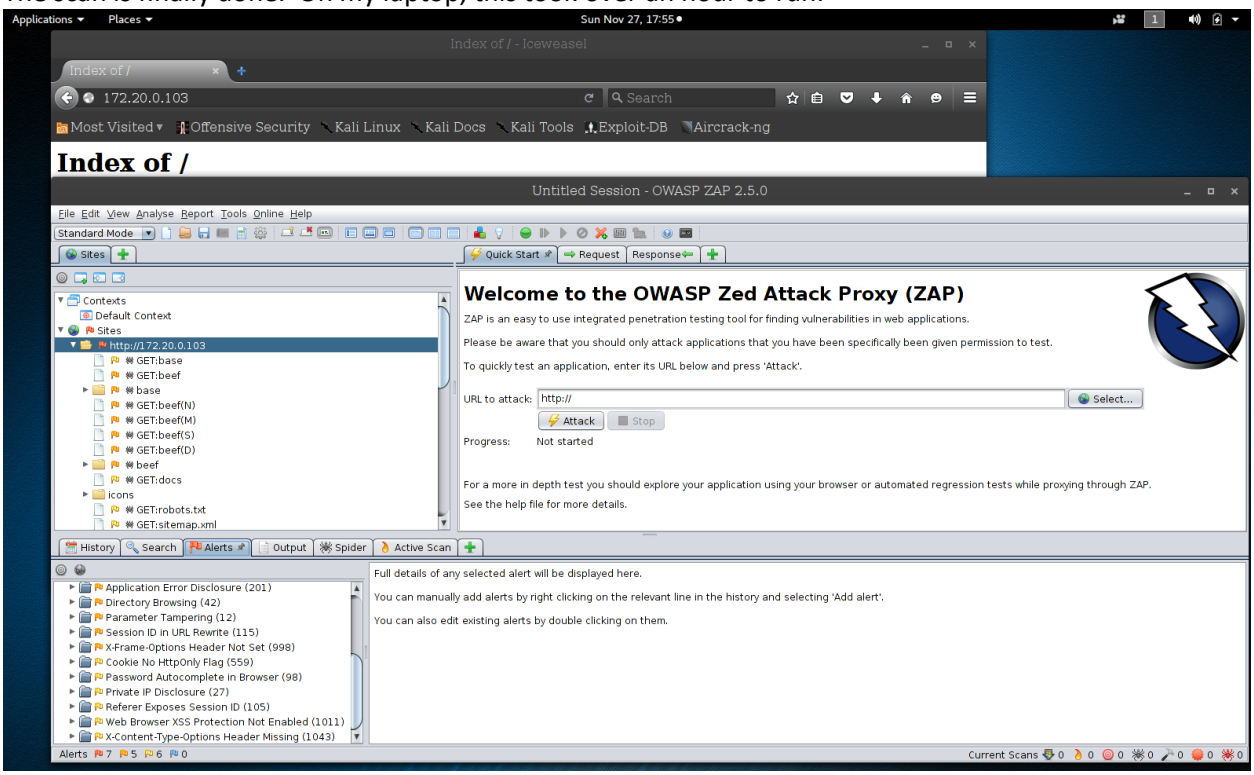
Attack in motion.



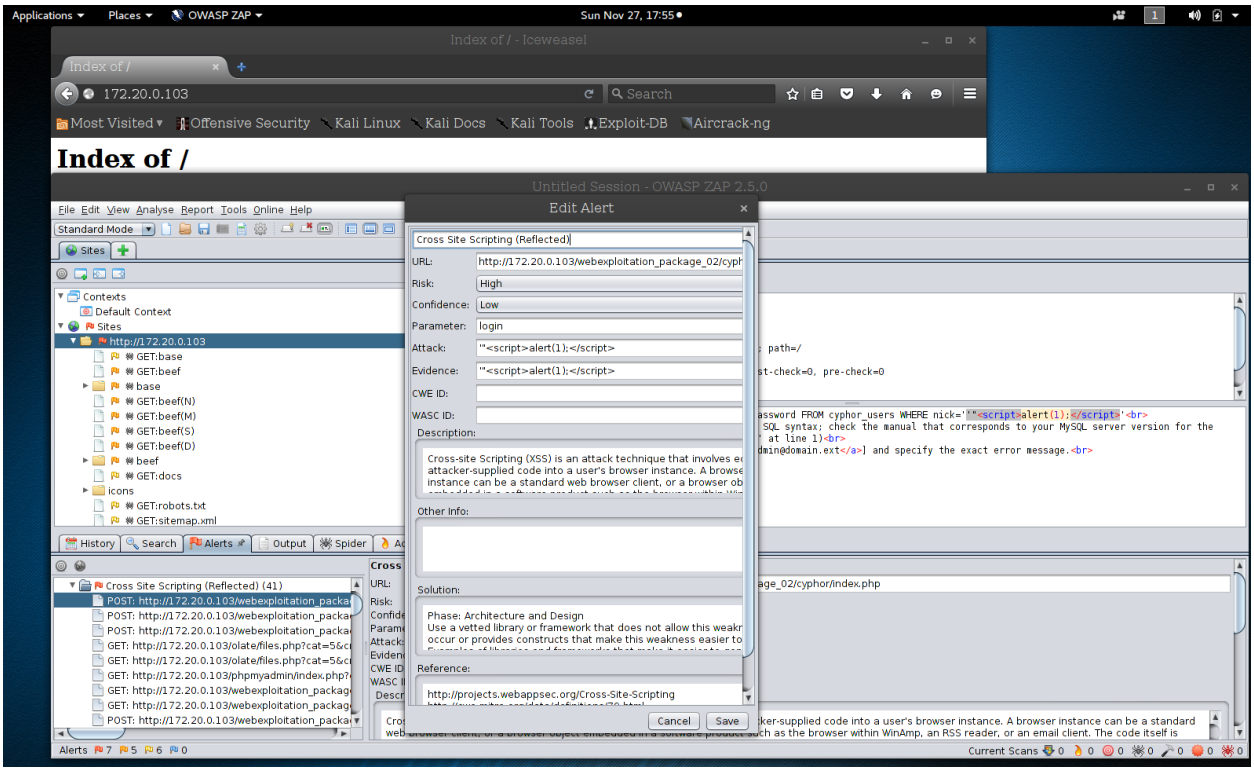
Starting to see some results. You can see I have DVL in the back ground with top open in a terminal watching the CPU utilization.



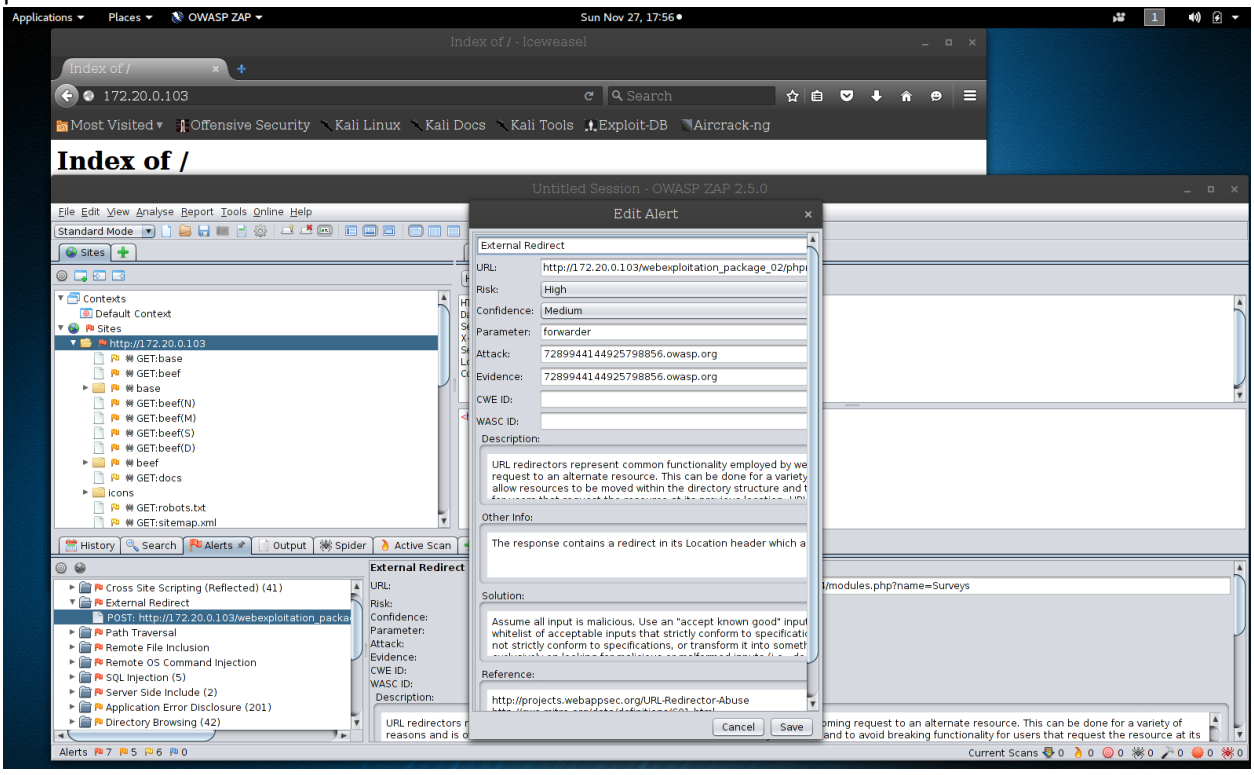
The scan is finally done. On my laptop, this took over an hour to run.



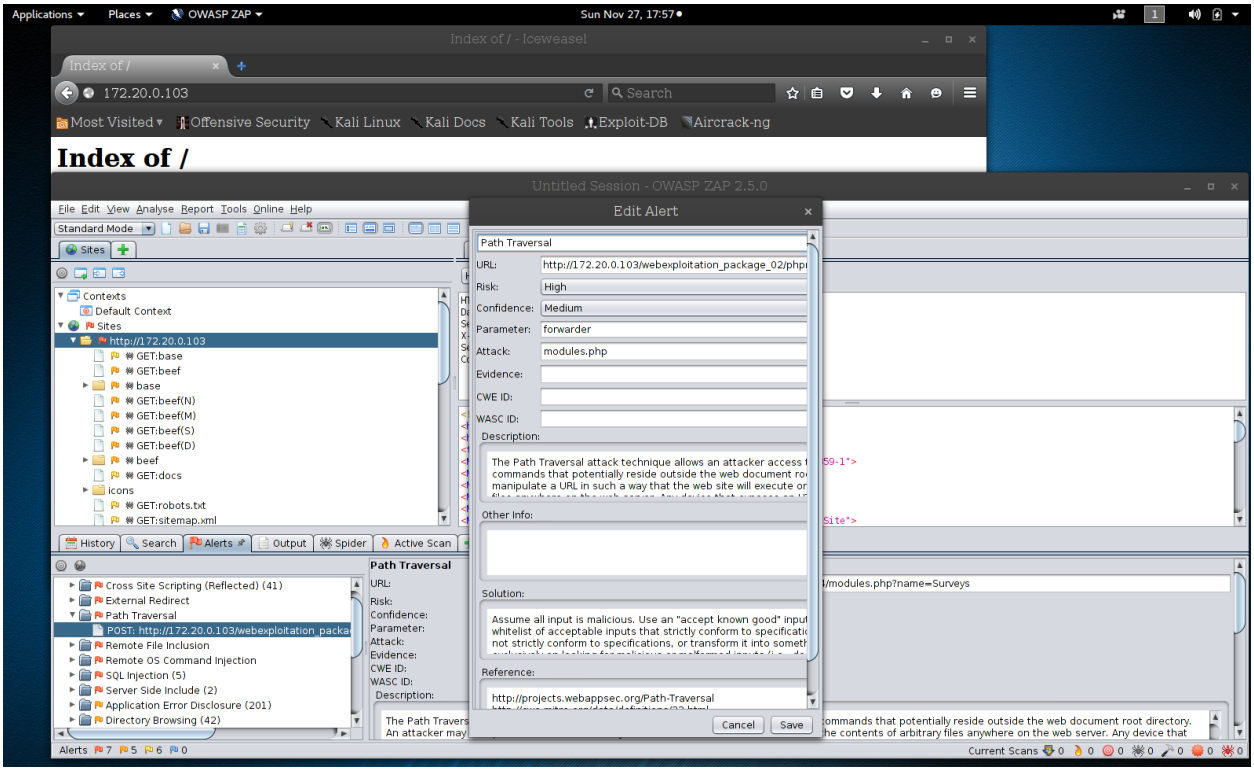
Click on the Alerts tab.



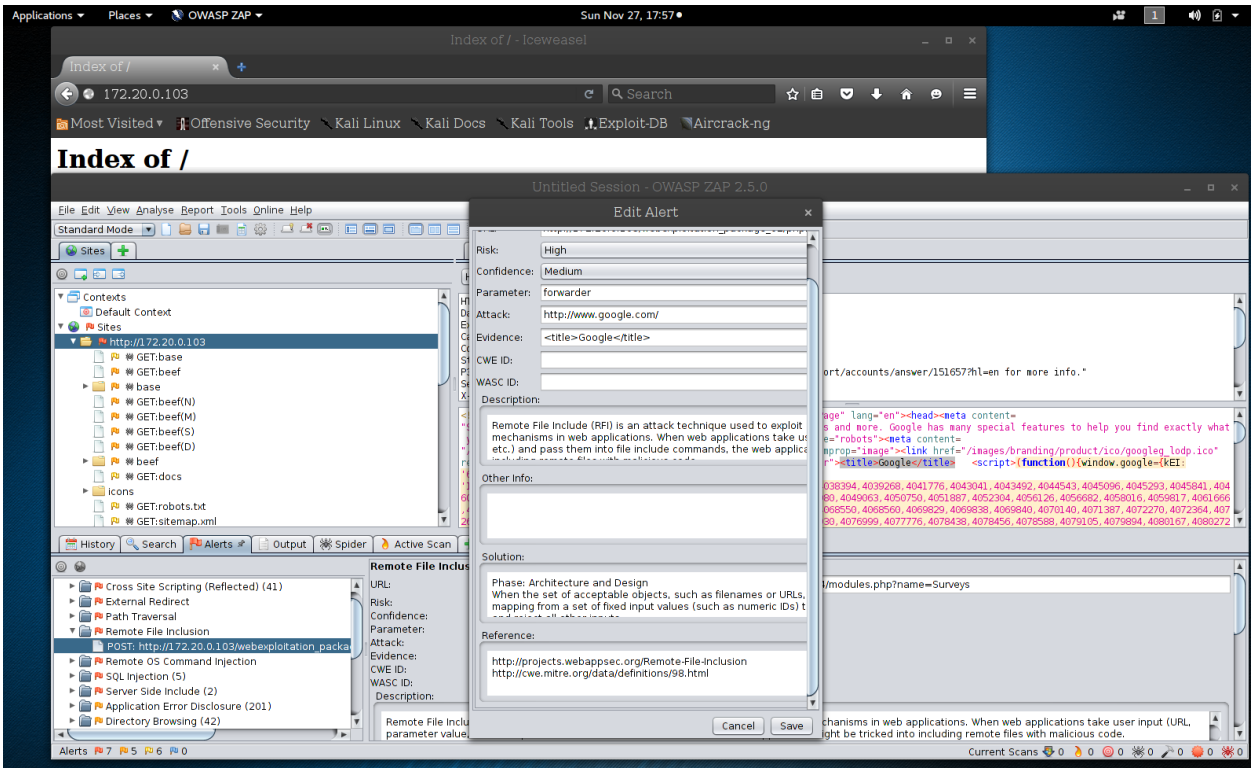
Expand on the first vulnerability. Dig through the details. This information is great for ruling out false positives.



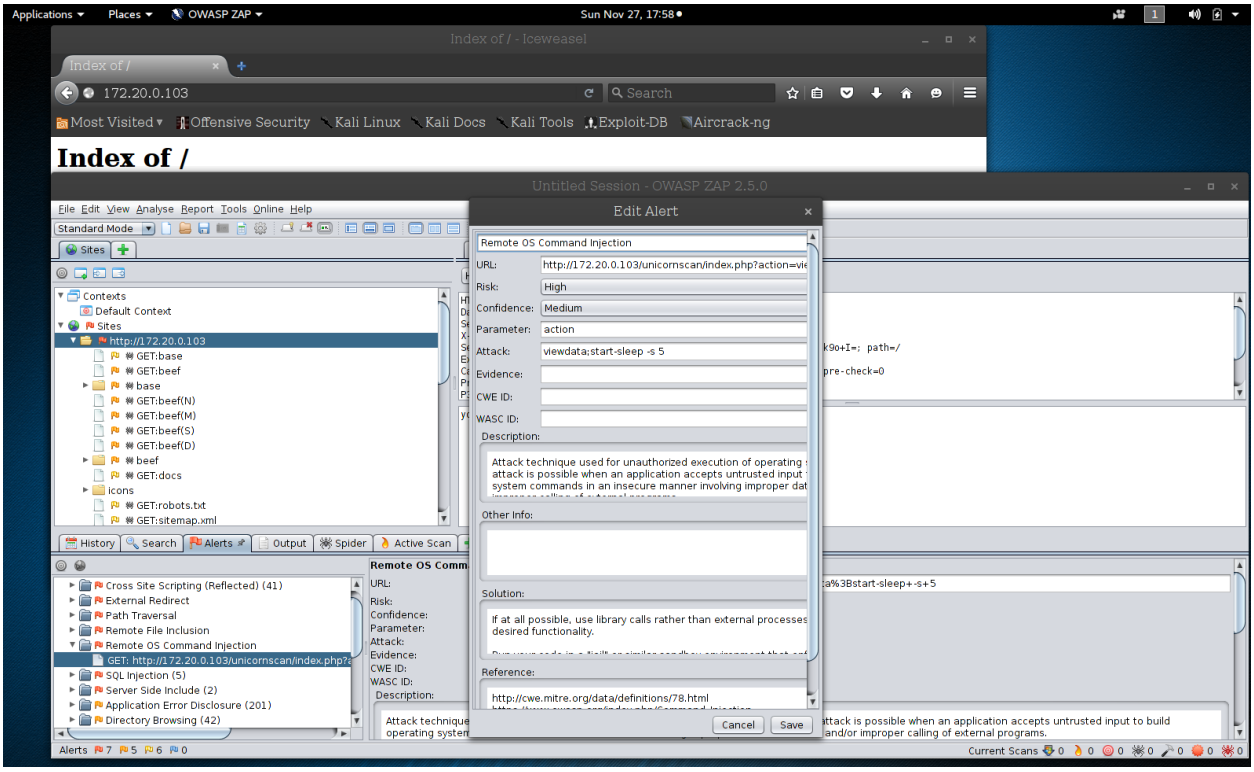
Continue exploring the vulnerabilities.



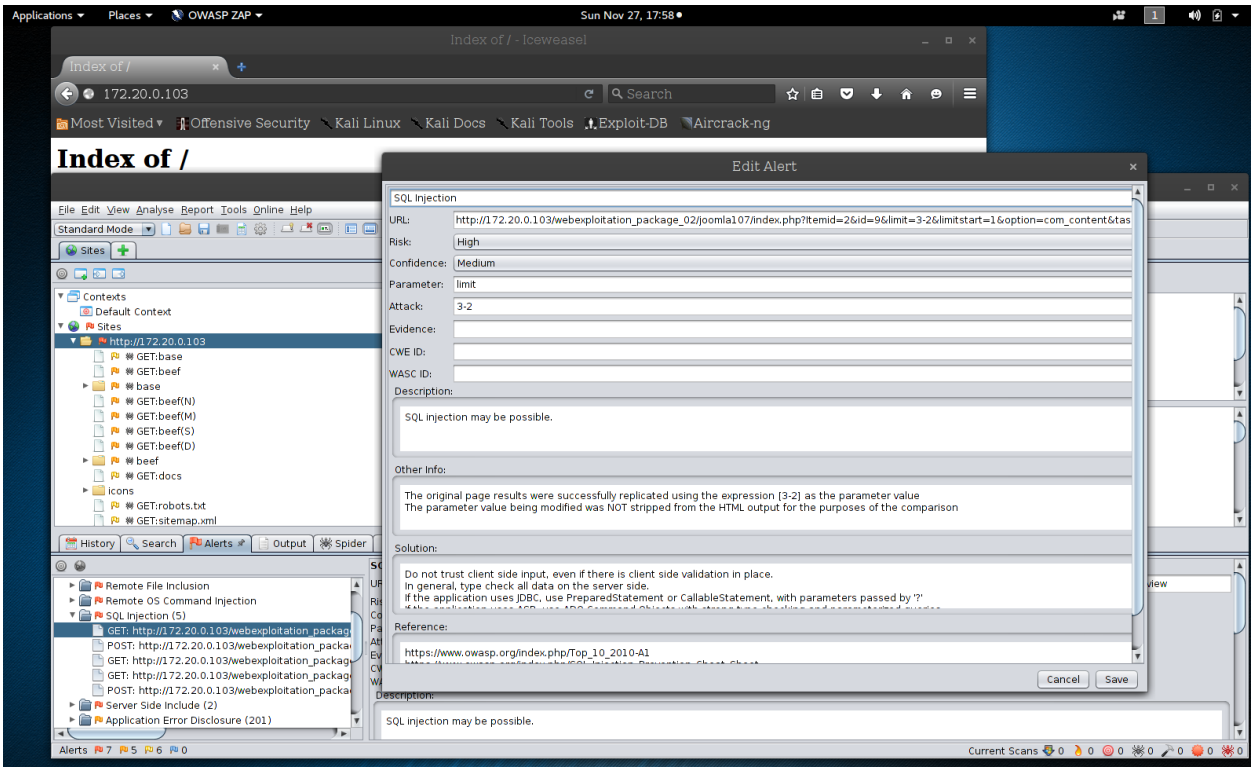
More on Path Traversal.



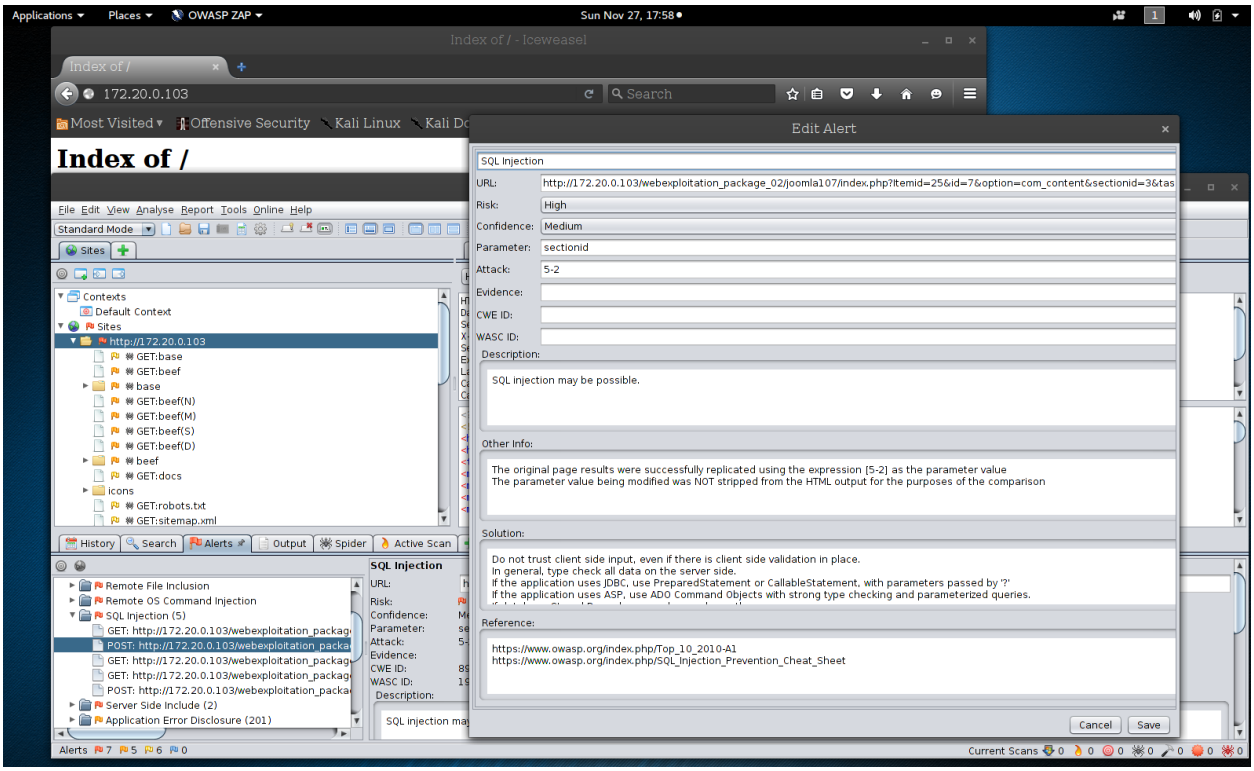
More on Remote File Inclusion.



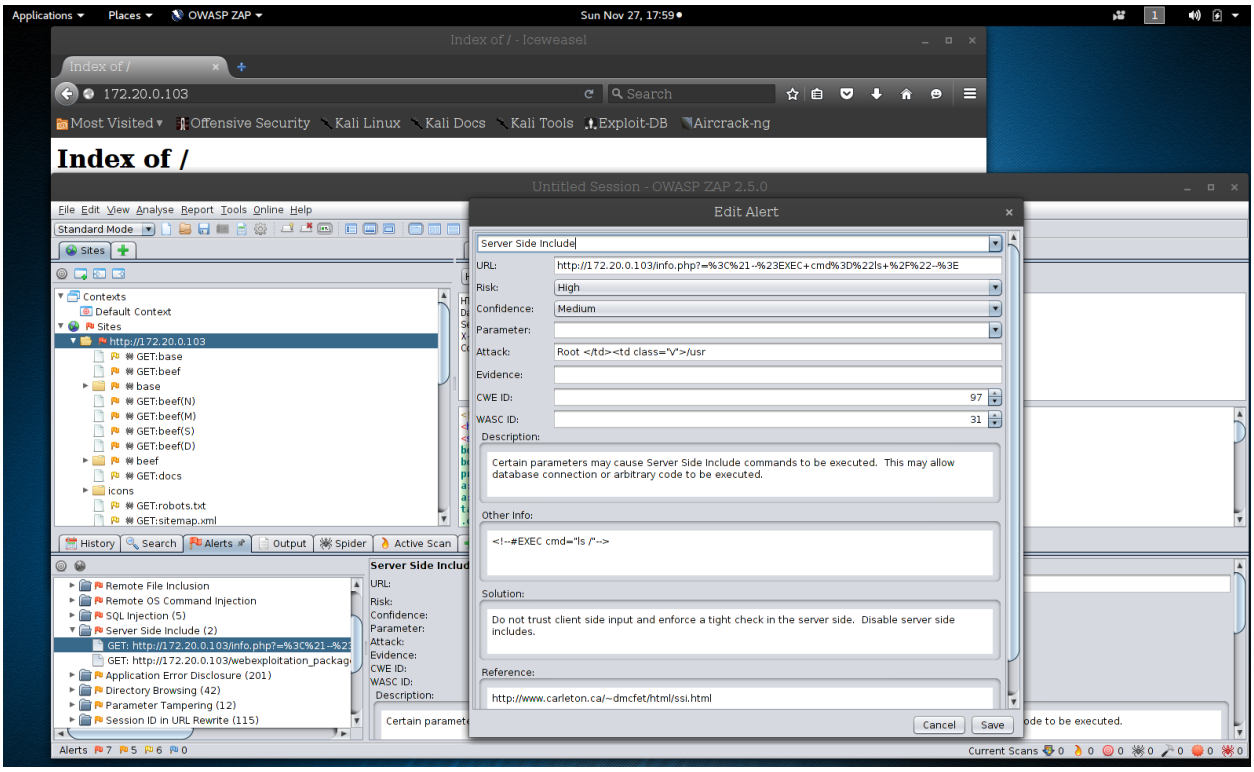
More on Remote OS Command Injection.



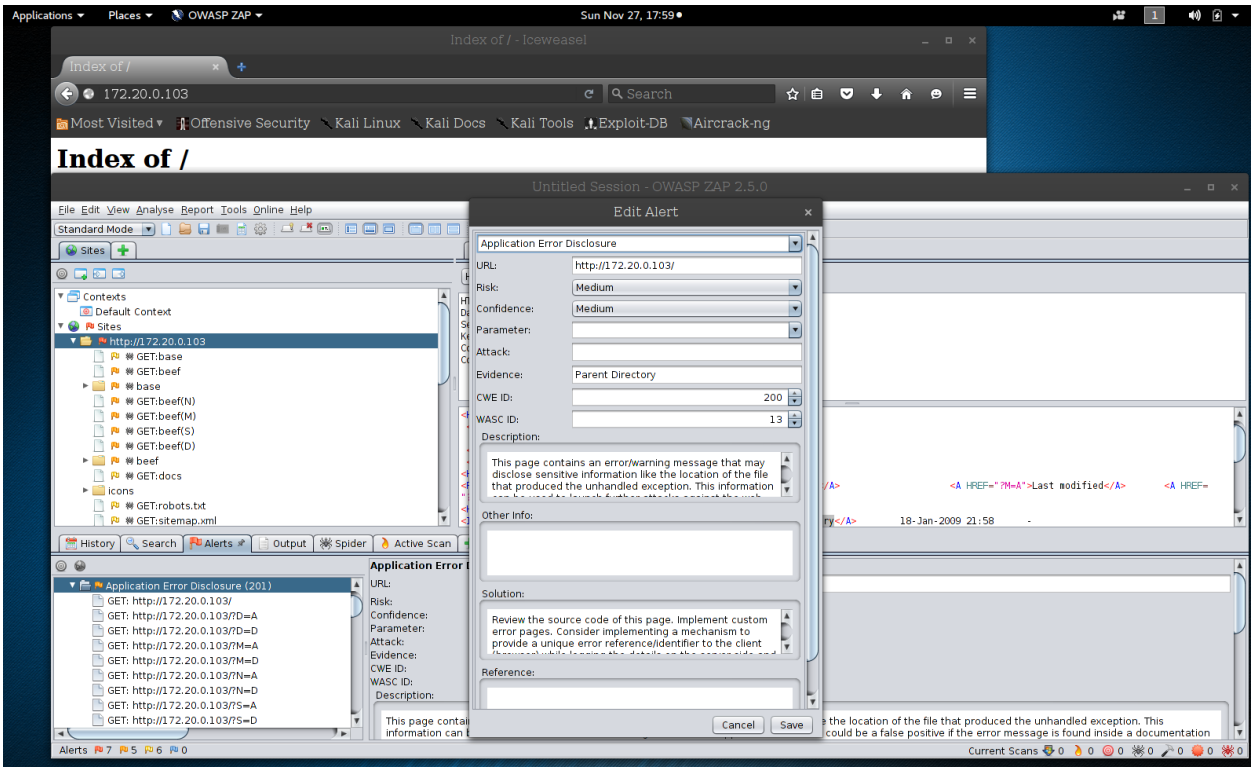
More on SQL Injection.



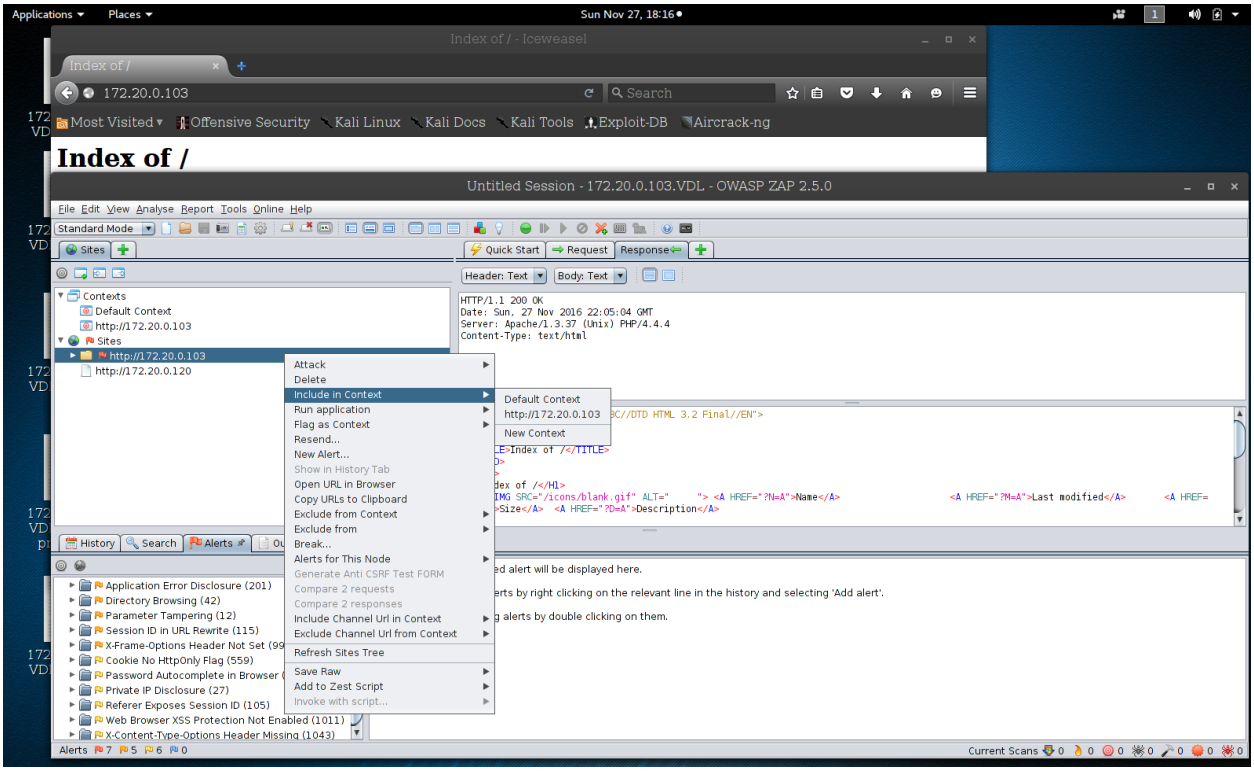
A POST action for SQL Injection.



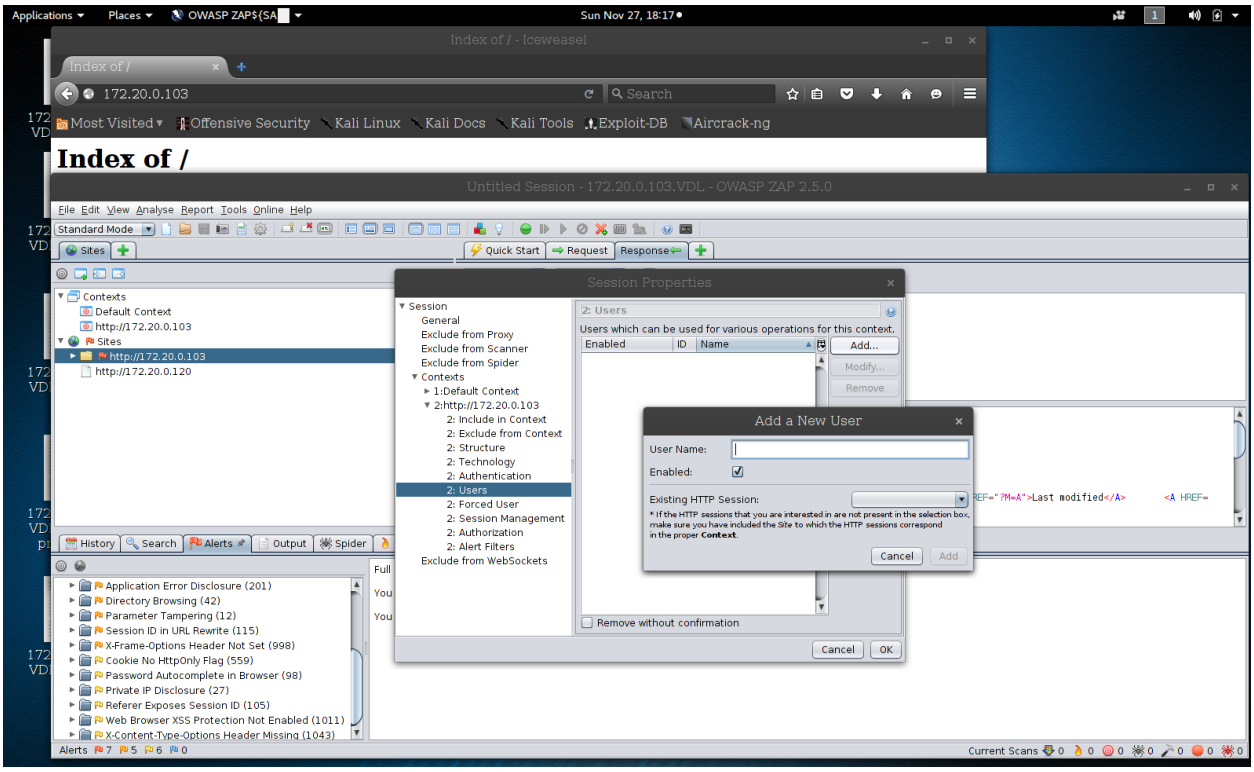
More on Server Side Include.



Medium findings, Application Error Disclosure.



If you have an https sites that requires authentication, right-click on the IP address, Include in Context, and New Context.



Add your credentials here and hit the button Add.

Conclusion

By following this narrative, you've successfully run a web scan against a very vulnerable server with a lot of findings to explore and take to the next level with actively exploiting, and if you are wise, understanding how to close on the web servers side. There is more to do here. I recommend if you have 2 network interfaces on your Kali Linux virtual machine, i.e. one for NAT and one for Host-only, to disable the NAT interface when you are not updating the server. This takes discipline. But, this action will make sure you don't have stray packets going out to web sites that might press legal charges against you when they discover them and turn those over to law enforcement. The choice is yours; I prefer to error on the side of caution.