**ARACHNI WEB APPLICATION SECURITY FRAMEWORK**

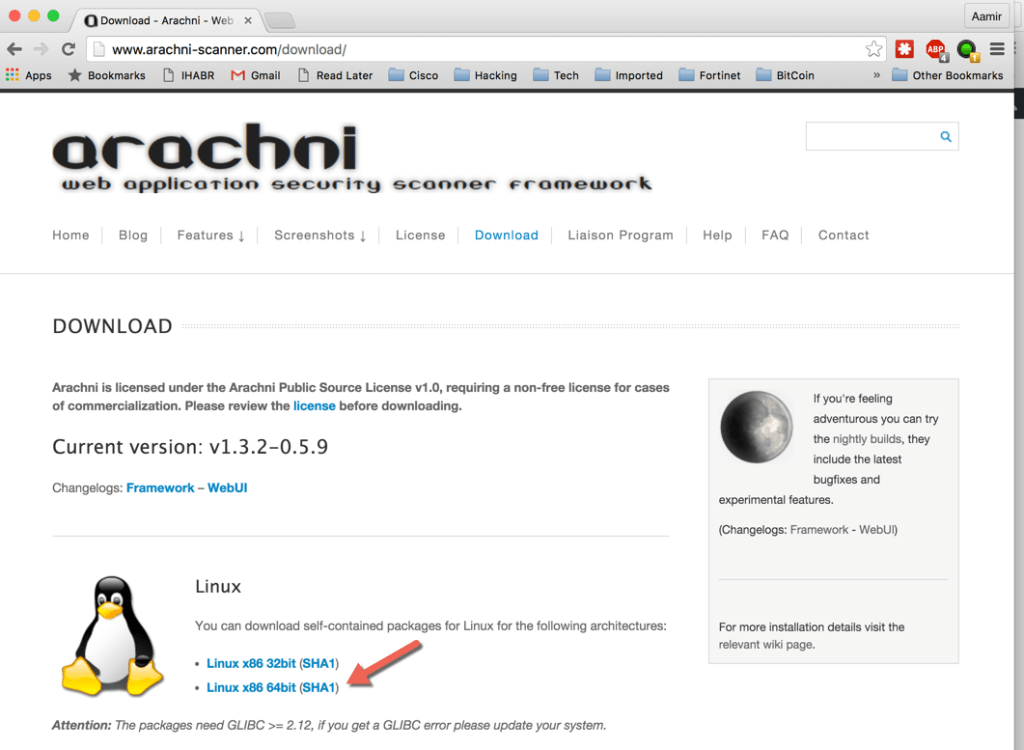
Arachni Web Application Security Framework is an open-source Web application scanner and vulnerability penetration testing tool. Unlike many other system scanners, Aracni specializes in finding Web application vulnerabilities.

**Steps for Installing Arachni on Kali Linux Systems**

First we will download the Arachni Web Application Security Framework. To do so we will go to:

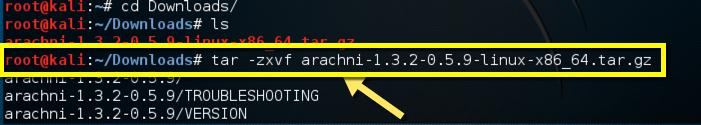
<http://www.arachni-scanner.com/download/>

Since I am using 64-bit version of Kali, I will get the software version specific for my system.

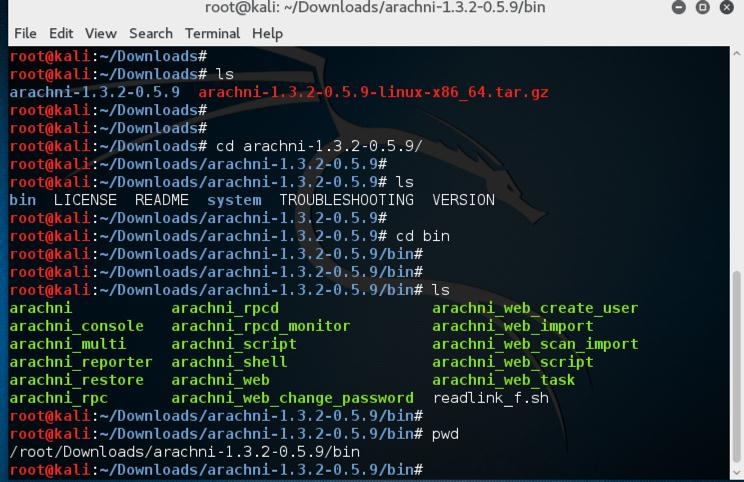


1. Next, we will untar the files with the following command:

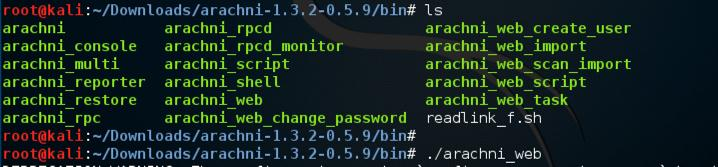
**tar –zxvf arachni-1.3.2-0.5.9-linux-x86\_64.tar.gz**



2. We then navigate to the arachni-1.3.2-0.5.9/bin directory:



3. The next thing we will do is launch arachni\_web:



4. This opens the Web Graphical User Interface for Arachni. Please note we are listening in on port 9292 by default. For now you will need to use the local machine and local host to browse to the scanner.



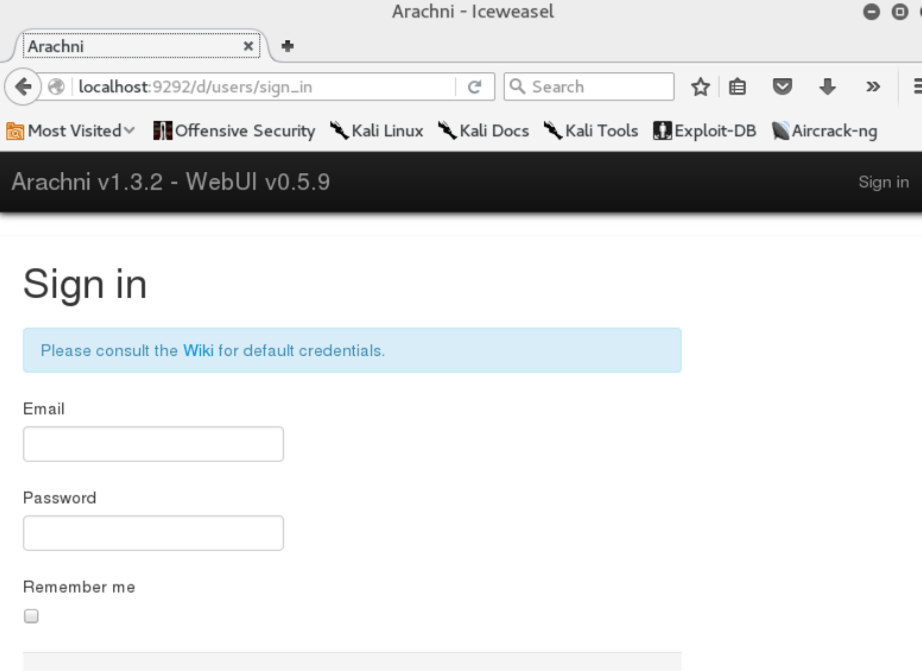
**Logging onto Arachni Web Interface**

1. The default login credentials are:

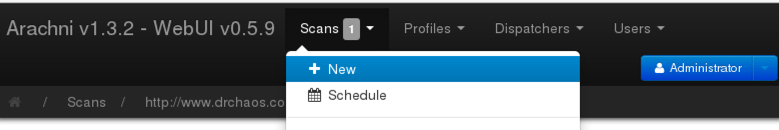
**Administrator account**

E-mail: [admin@admin.admin](mailto:admin@admin.admin)

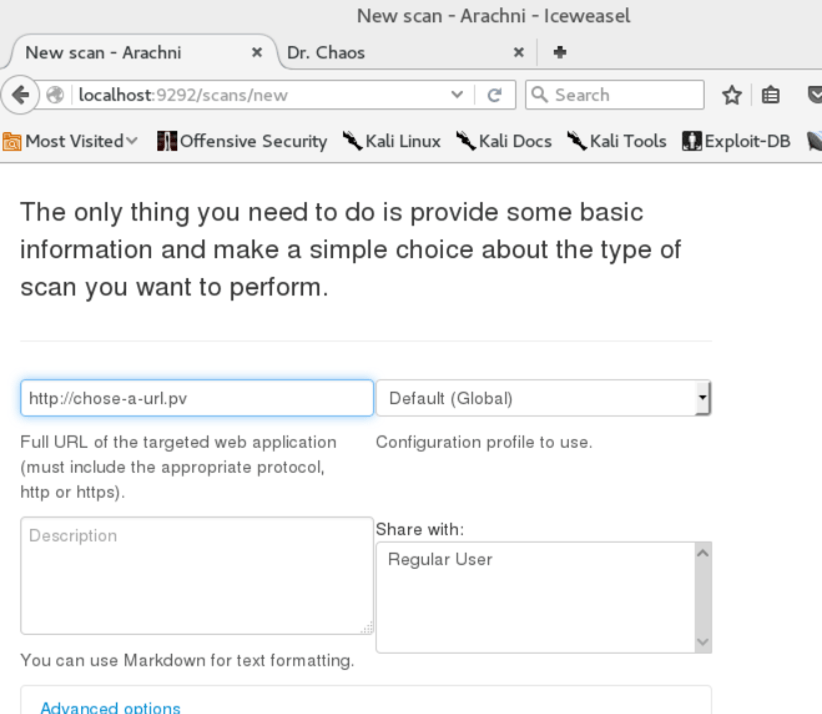
Password: administrator



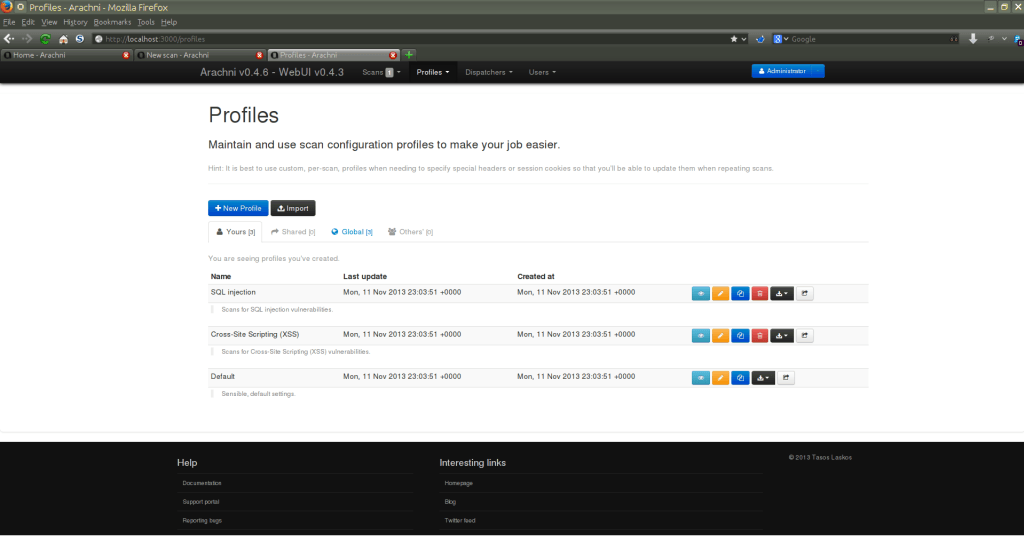
2. You can start a new scan by going to the scan drop-down menu on the top menu bar.



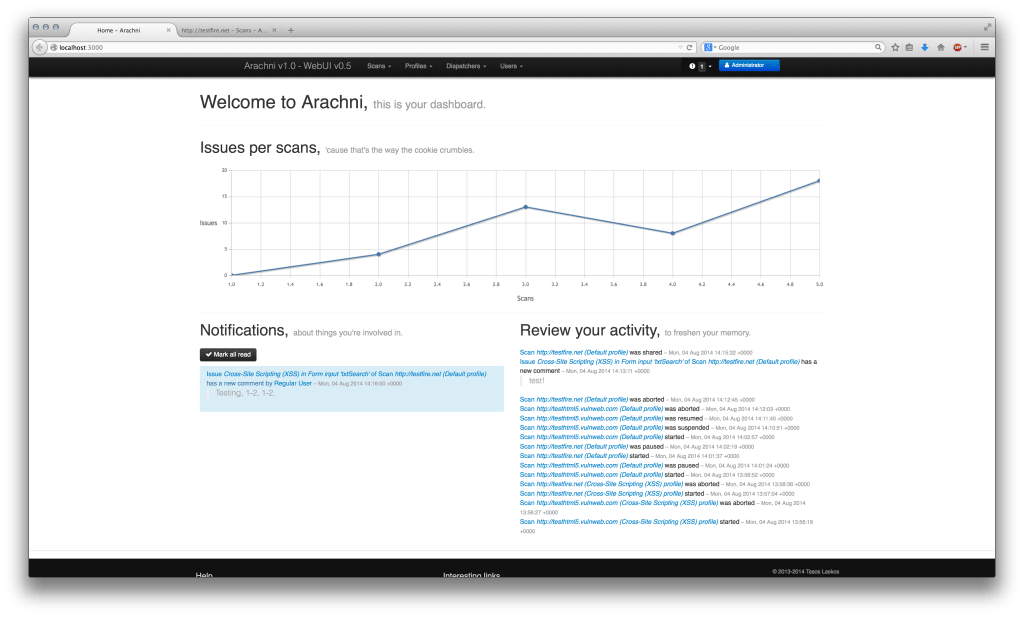
3. At this point in the process you can select some predefined profiles. Make sure you use the full URL (including the http://) when you select your target.



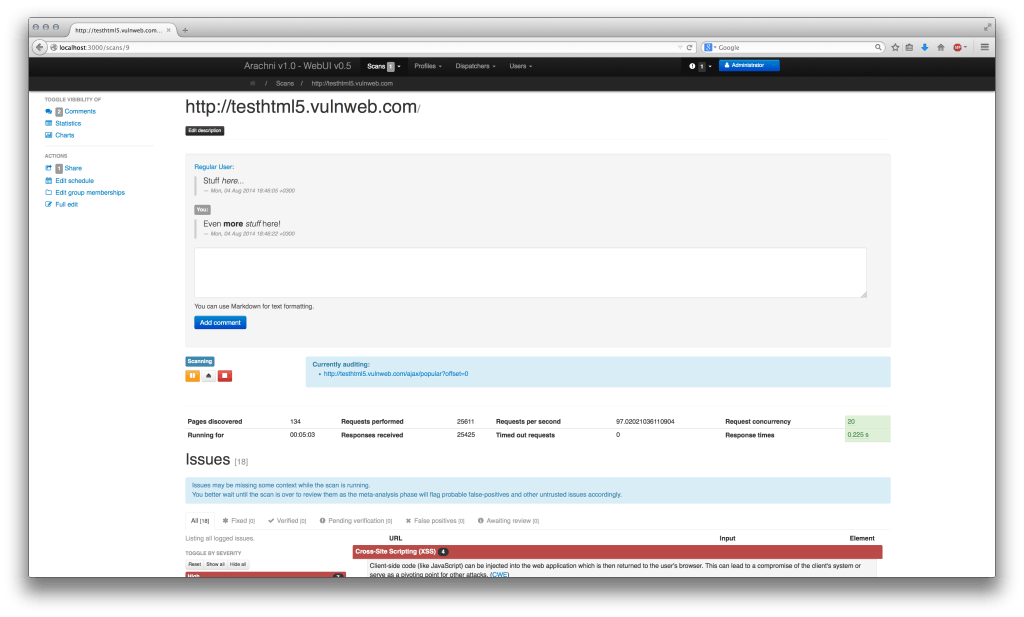
4. When you have a little more experience with the scanner, you will be able to create and save multiple scan profiles.



5. When the scan is complete, you will be able to export your findings in a variety of different formats.



6. You can then look at the discovered issues per scan on each host:

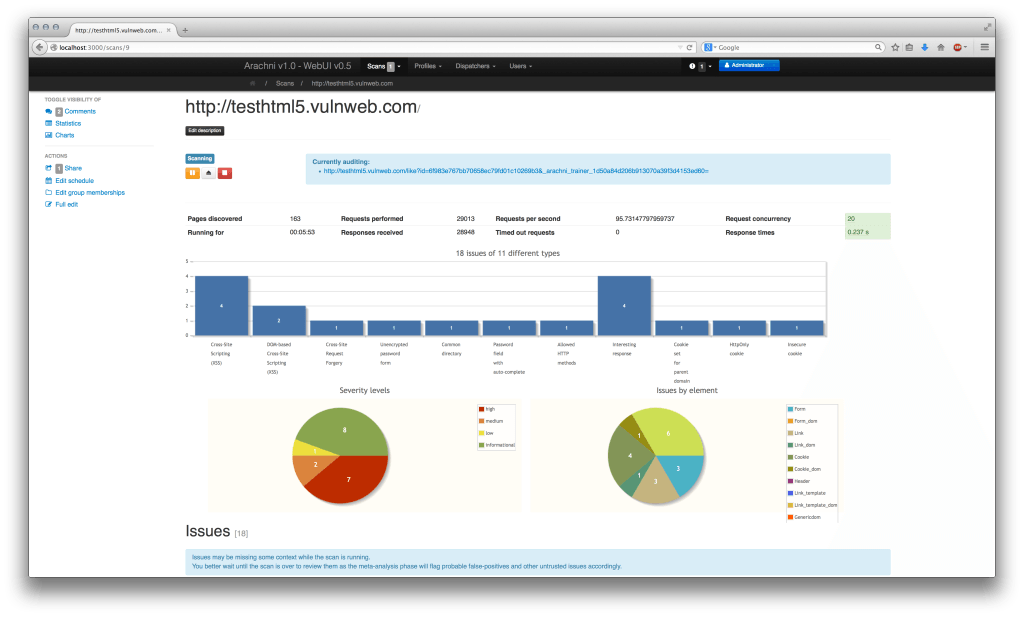


**My Analysis of the Tool**

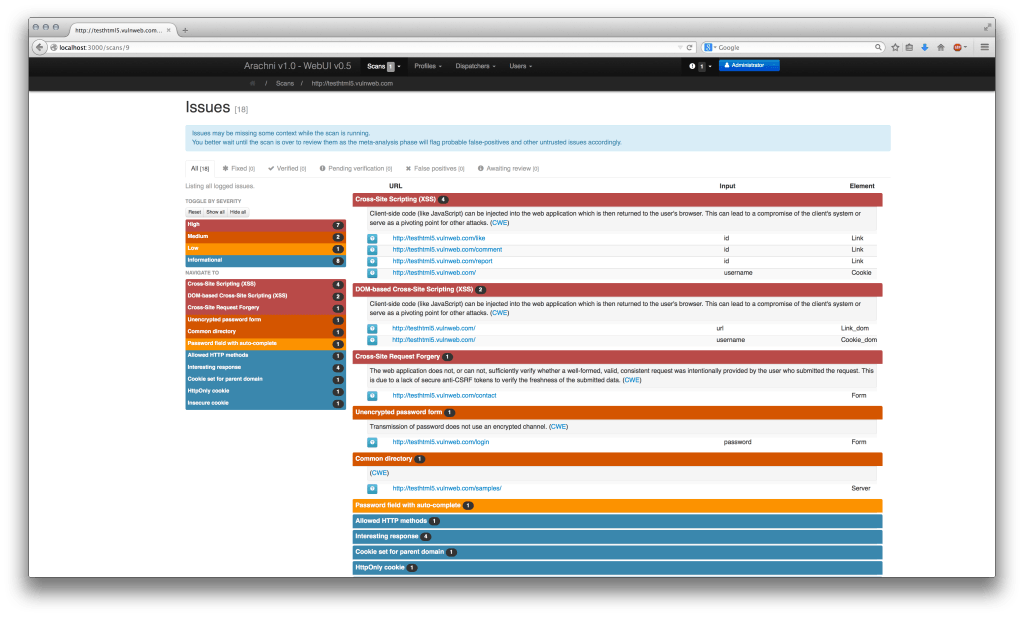
In my opinion, Arachni Web Application Security Framework is an enterprise-ready Web application scanning

tool. It has some eye candy charts and graphics that provide great visualization of scan results. I think it

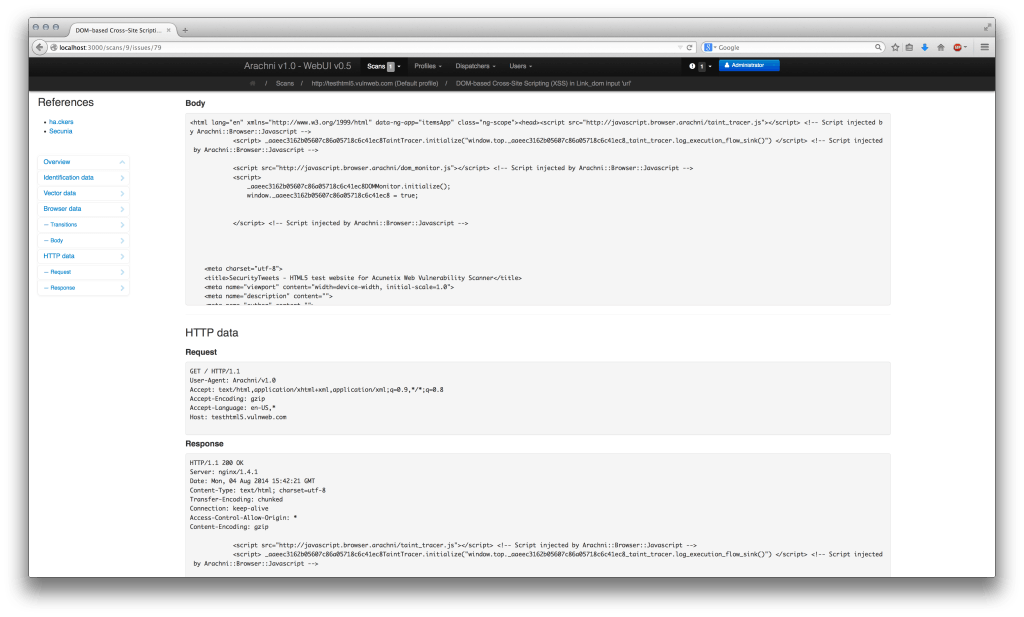
handily articulates the status of my Web applications.



The scanner will also give you a wealth information that is valuable for further analysis.



That wealth of information includes a full view into browser and HTTP traffic:



**To Summarize**

Arachni Web Application Security Framework is quickly becoming my go-to weapon of choice for testing Web applications. It has some really great features and the user interface is relatively intuitive and easy to use. If you prefer to go old school, the entire framework can be run using command lines, providing the ability to

script and automate your scans.

Play with it and give me some feedback and thoughts about it. If you have any tips or ideas please share them with me. I would also highly recommend joining discussions on their support forum at:

[http://support.arachni-scanner.com/discussions.](http://support.arachni-scanner.com/discussions)