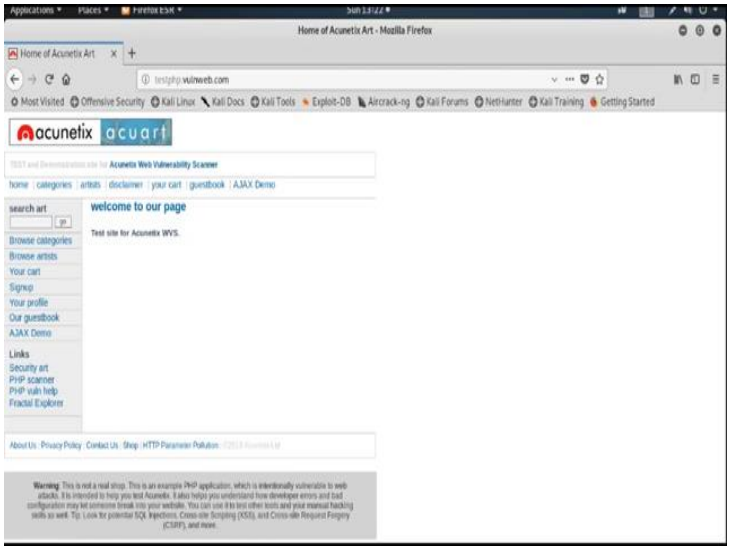
Ethical Hacking
Prof. Indranil Sengupta
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Lecture - 51
Web Application Vulnerability Scanning

In this week, we will discuss about how to hack Web Application. Web application penetration testing is the most commonly used security testing technique for web applications. Web application penetration testing is done by unauthorized attack internally or maybe externally to get access to the sensitive data or may sometimes change the data stored inside the web application. A web penetration testing helps end user find out the possible vulnerabilities for a hacker to access the data from the internet; find all the security of their servers and also get to know how secure the web hosting site and server are.

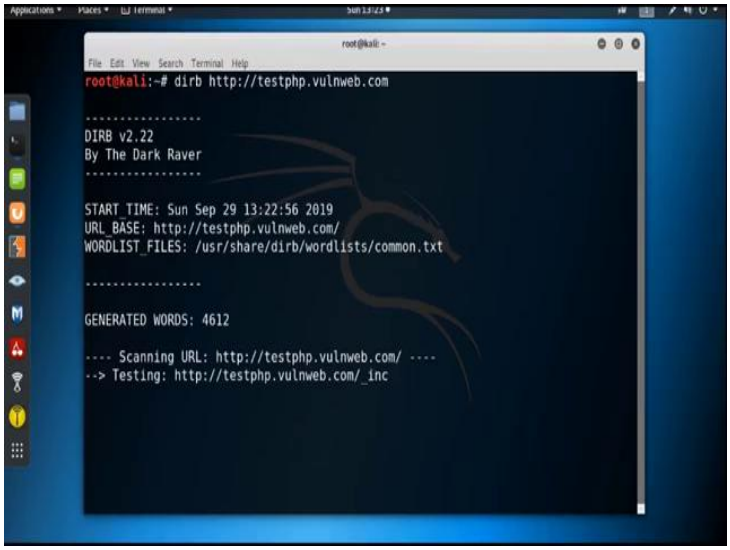
Like network for web application, our first step is also information gathering and scanning. We already discuss about the information gathering part previously; now we will discuss about the scanning. For web application for network scanning, we use the tool like nmap or nessus. For web application scanning we use the tool like dirb, uniscan, nikto, vega, acunetix, etc. Now, I will show you few tools.

(Refer Slide Time: 01:54)



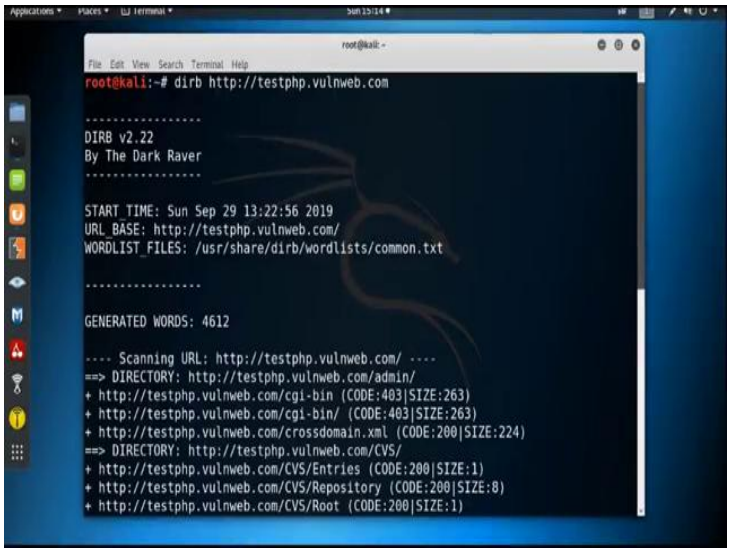
Now, suppose consider a web site **testphp.vulnweb.com** as our target web site or web application, **testphp.vulnweb.com**. So, now our first step is to find out the vulnerabilities by scanning this particular web application. So now, first we will use the tool dirb to find out all possible directories of these particular web application. So, open terminal.

(Refer Slide Time: 03:05)



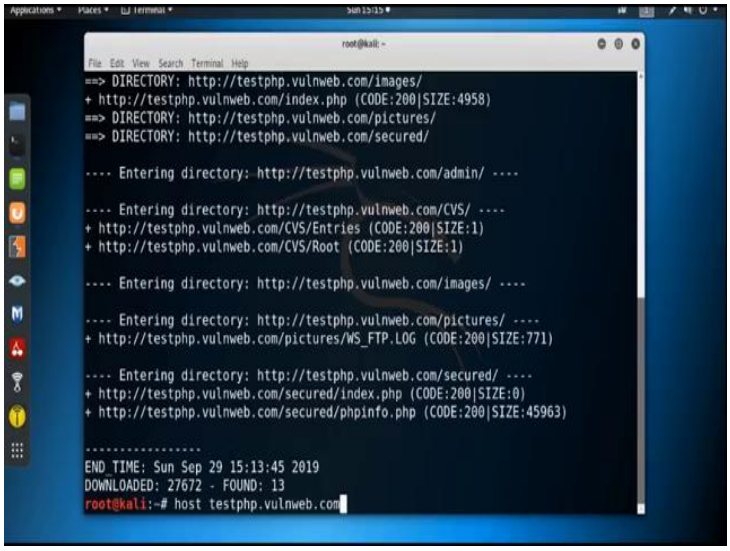
And use the command dirb followed by the url **http://testphp.vulnweb.com**, hit enter and it will search for the possible directories for this particular web application; we got the result.

(Refer Slide Time: 03:43)



And see, we got all the directories inside this particular web application. We got common dot txt file and admin directory, CVS directory and images, picture, secured. We got all the directories which is inside this particular web application.

(Refer Slide Time: 04:09)

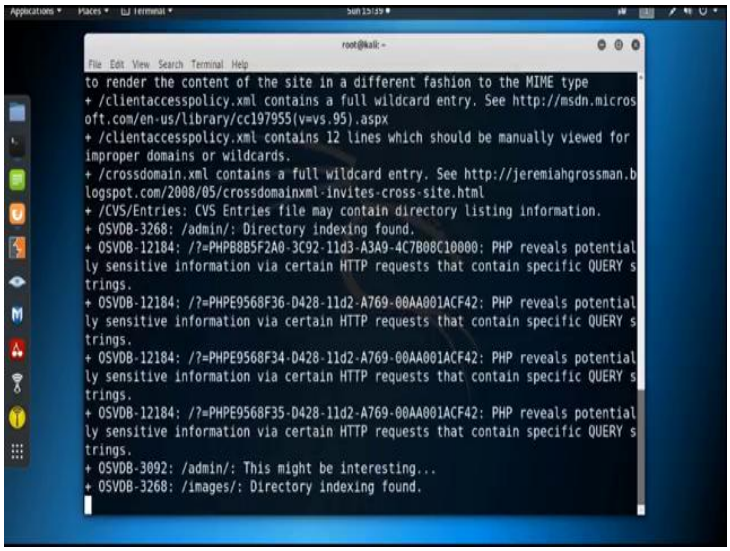


Next we will use the tool nikto to find out the vulnerabilities in this web application. So, to use the tool nikto, first we need the IP address of this particular web application. So, by using the command host, we can find out the IP address, host testphp.vulnweb.com.

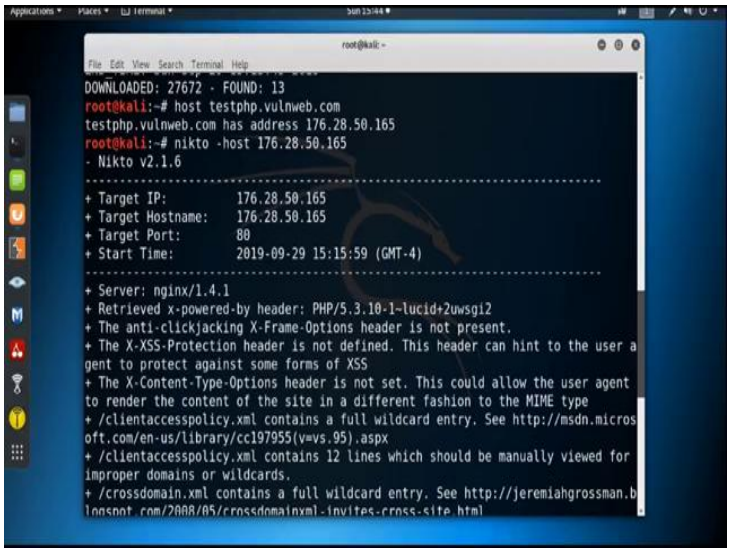
(Refer Slide Time: 04:55)

So, you got the IP address. So, use this IP address in the tool nikto; nikto, then this host specify the IP address, then the IP address of this particular web application.

(Refer Slide Time: 5:28)

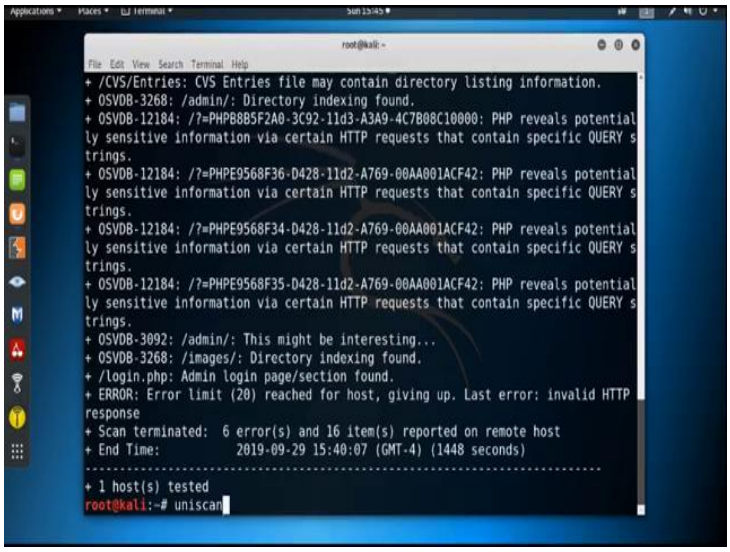


(Refer Slide Time: 05:39)



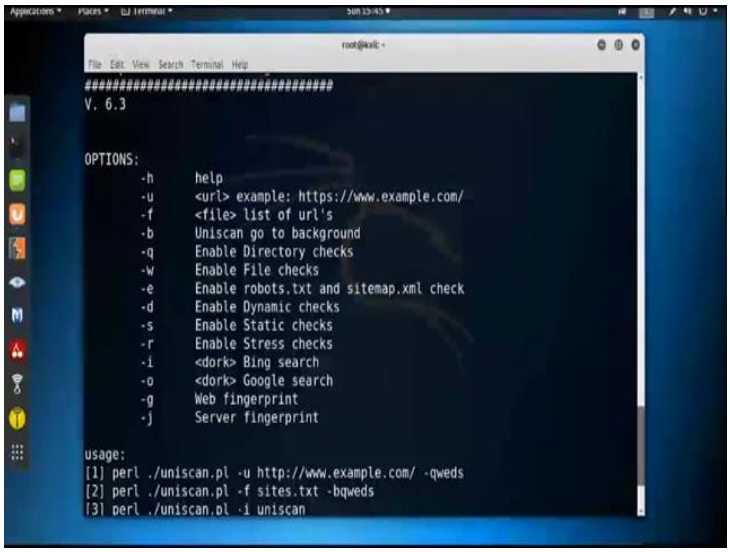
We got the result and see some vulnerabilities listed, target IP, this target hostname, target port is 80 and server is nginx retrieved x powered by header this; the x-xss protection header is not defined; this header can hint to the user agent to protect against some form of xss. Shows all the vulnerabilities which are available in that particular web application are listed here.

(Refer Slide Time: 06:25)



Now, I can also use the tool uniscan.

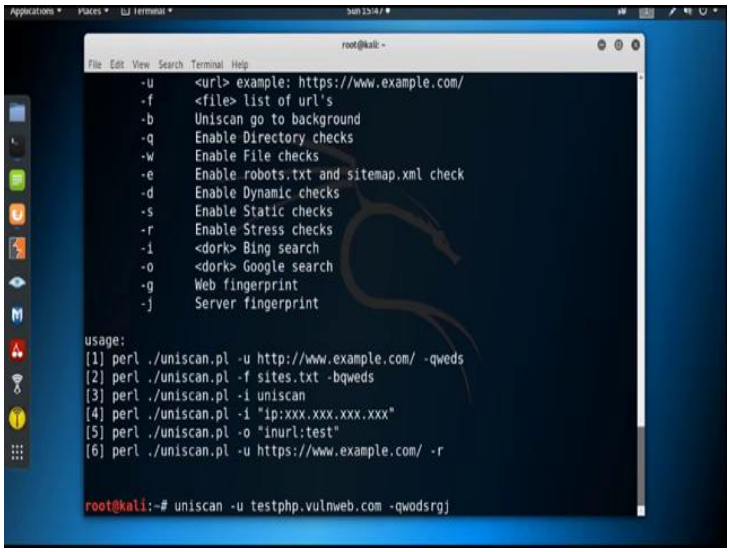
(Refer Slide Time: 06:36)



Now, just by typing uniscan, we can get the help of uniscan and see all these options are available; h for help, then -u specify the url and -f list of urls, -b uniscan to go to background, -q enable directory checks, -w check file, -e enable robots.txt file and sitemap.xml file check, -t enable dynamic check, -s enable static check, -r enable stress check, -i it search in Bing, -o search in Google, -g find out the web fingerprint, -j server fingerprint.

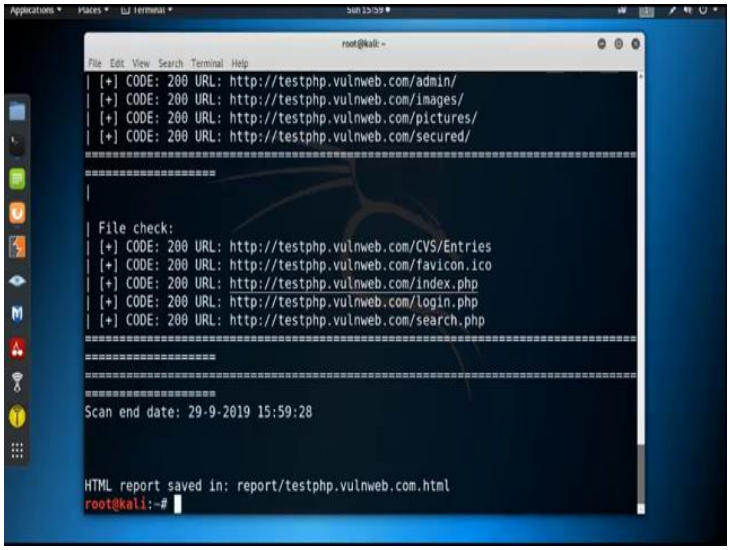
So, now suppose I am going to scan the same web application testphp.vulnweb.com using the tool uniscan with some specified options.

(Refer Slide Time: 07:50)

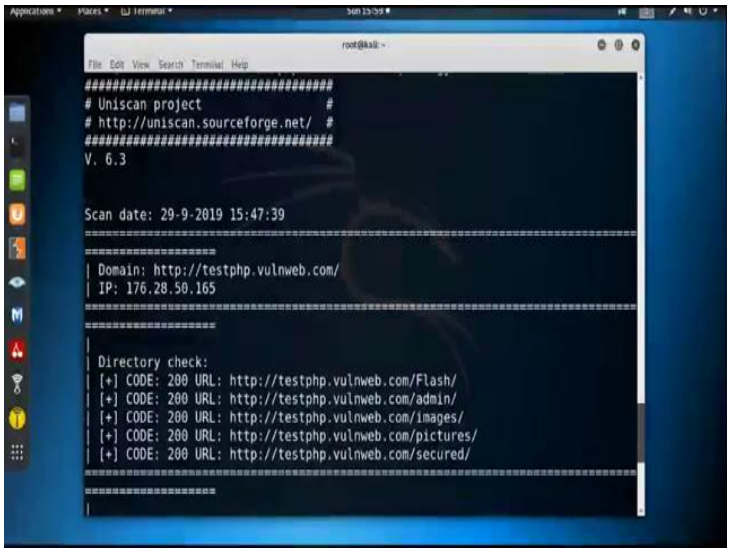


unican then -u specify the url testphp.vulnweb.com, then specify the option -qwodsrgj.

(Refer Slide Time: 08:32)

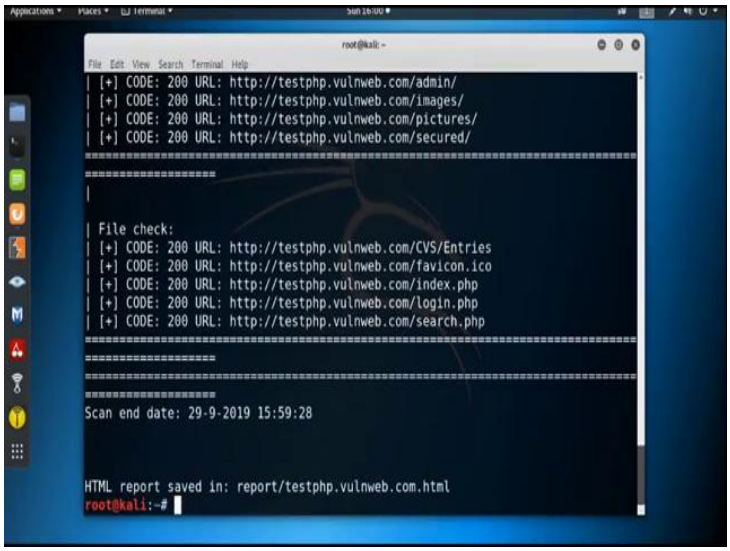


(Refer Slide Time: 08:39)



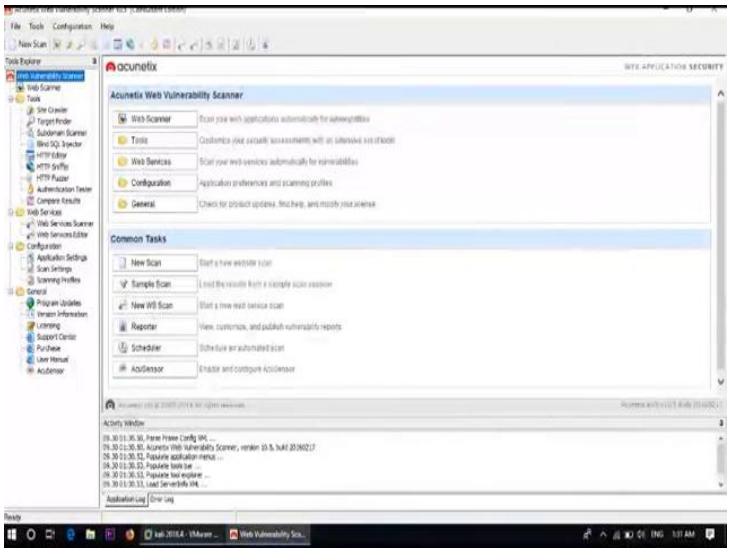
We got the result. It find out all the directory, flash, admin, images, pictures, secured and it also check all the file.

(Refer Slide Time: 08:49)



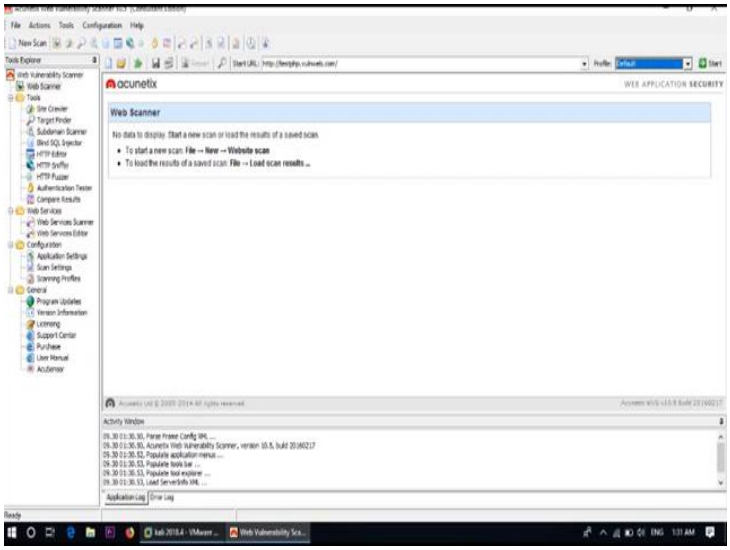
And also set the html report into the folder report testphp.vulnweb.com.html. Now finally, we will use the best tool acunetix to find out the vulnerabilities to that particular web application; open the tool acunetix.

(Refer Slide Time: 09:21)



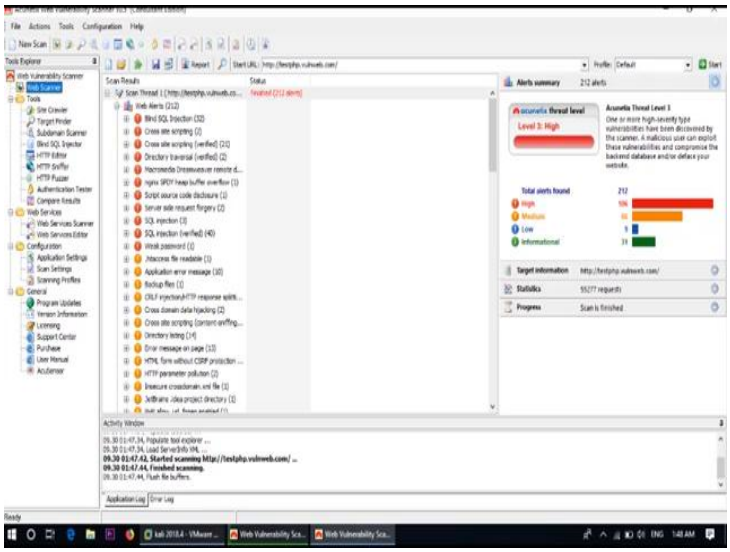
Here is my tool acunetix; go to web scanner.

(Refer Slide Time: 09:28)



And put the web application url, http://testphp.vulnweb.com which is our target web application. Now, we can select your profile; for blind SQL injection, you can use this option csrf, dictionary and file check, file upload, all these option are available. For the time being, I am using default option; then click on start.

(Refer Slide Time: 10:13)



It will take some time to complete the scan. Once it complete the scan, we will get all the vulnerabilities which is available in this particular web application. Here is the result; scan is completed; its total sent 55277 request and got some vulnerabilities and it basically divided all the vulnerabilities in three categories; one is high, then medium and low.

So, it got some high vulnerabilities; 106 high vulnerabilities are there and blind SQL injection, cross site scripting, cross site scripting verified, macromedia dreamoever remote, SQL injection with password, all these high vulnerabilities are present; then 66 medium vulnerabilities are there and 9 low vulnerabilities are there and 31 information are also there. So, this way by using different web applications scanning tool, we can find out the vulnerabilities present inside a particular web application.

Thank you.