Introduction to Information Security
Prof. Dilip H. Ayyar
Department of Computer Science and Engineering
Indian Institute of Technology, Madras

Lecture – 65

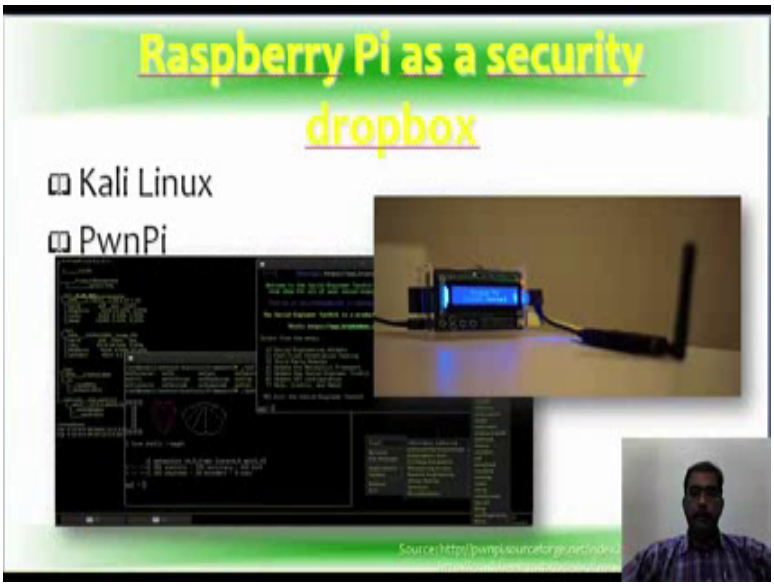
(Refer Slide Time: 00:10)

We come to the end of module six; here we have seen what is OWASP, what is SAN Top twenty five, and what are the ten domains of OWASP, as little bit of what each vulnerability is. Now these are some very good books if you are interested in web applications security. The web application hacker's handbook is really interesting on the right hand side, it is available, it is not very expensive you can probably buy it. All kinds of attacks and methods are given in that book.

(Refer Slide Time: 00:50)

Then there are live CDs and DVDs available. Kali which was earlier called backtrack, Samurai web testing frame framework, OWASP play CD is available.

(Refer Slide Time: 01:03)



Then Raspberry Pi one on the right can be used as a security a dropbox. I have installed Kali Linux in Raspberry pi.

(Refer Slide Time: 01:17)

Then some OWASP links you can learn about ZAP, zet attack proxy, then enterprise security API, open zap it is similarity or cmf, it is not exactly, but the framework is similar.

(Refer Slide Time: 01:37)

Then other useful links are about top twenty five, you can get detail from that site. There is a vulnerable web application also put code dot Google dot com bod g e i t then kali dot Kali Linux PwnPi, Juice-shop. So we come to the end of module six. So, I thank you for your attention, and what I would like to add here is whenever you doing a web application testing, whether it is live or whether you are using VM to test your skills or the learn the skills, always try to do it in a manual method possible or with minimalistic

set of tools. Some of the good tools that I have used at least from the open source site or free side is some of the Mozilla add-ons like web developer toolbar then you have the tamper data for cookie manipulation, you have cookie manager plus. The same things are available for Chrome also; fiddler is a good one for Microsoft internet explorer; web developer tool bar is available for chrome as well then you can try out with the tools available in OWSAP itself like your zet attack proxy, your web scarab is there, wapiti there, W3AF that is web application attack frame work, the best place to start I think is install Kali on a VM and play around with the tools with the vulnerable application downloaded and installed, or on the online site you will gain a lot of experience and a lot of inside on how security assessment are done. One of the major things that you see which you use commercial scanners, no doubt you will get a good result, but there are a lot things as I have said in the beginning of this module that you have to test it manually.

For example, unsuccessful attempt to log off log in, then existence of a captcha of captcha bypass itself has to be tested then you have existence of an audit trail in an application. So there are several manual methods or skills that are require to see that the application secure. There may be other areas also, but if you take the password itself as an example, you can probably list out at least six seven points of the for example, a password length, the password content in the sense alphanumeric, special character, whether it is validating, unsuccessful attempts to log in, whether password history is being maintained that is password reused, then whether your password is maintaining or if you say that I need a minimum of eight characters when I do a change password does it accept only five. So these are several things that you will have to work it out, and do the assessment. This is only a small area of password that I said.

Then the log in is very, very important in web applications. If you have a WAP then review of or frequent analysis of the WAP logs also will give you a lot of information on what exactly is happening in the applications server then the exploits that are related to your frame work itself dot Net, your internet explorer, client side validations all these also have to be check. So it takes time, it takes efforts; it takes a lot of practice also. Now different people have different difficulty levels and areas personally when I started doing a web application audits, I found SQL to be quite difficult, then once I started working on SQL itself then it became relatively easy. So if you have a problem in any of the particular area, I suggest that you if you have problem with SQL install SQL on Linux server and work around play around with it see how it behaves, so you will get a basic

understanding of how the database works. Similarly for XSS, use the cheat sheet in the beginning so that you get familiarize with what kinds of scripts are being accepted and how the scripts are being formed.

So, in due courses start learning to make your own scripts; same name from your CSRF then cookie hijacking or cookie manipulation or session hijacking, so you play around with the cookie manager or the burp suite. See how the cookies are behaving, whether you can copy that cookie, make a new cookie on other computer with the same cookie value, and see if the page is opening in a logged in state in the other computer. Try to sniff password so then it through wireshark or again use burp so that you track the request and see what how the password is exactly traversing in the network, before it goes into the SSL, so these are things that you will gain experience over time.

Since this course is an introductory course, and theoretical course; I myself find it a little uninteresting, but it is a necessary evil that we know the theoretical part of how each of these work or how each of these are exploited, so that when you actually perform the practical assessment, it becomes easier for you. So conceptually your base will be strong, your foundation will be strong wherein you can try out even variations of these vulnerabilities or use a combination of vulnerabilities to exploit a particular feature, so you will get better and better with time. With this we end this module six, and our sincere thanks to all the participants who have registered for this course. And we hope to see you soon in course two, the contents of which will be announced in due course of time and we hope you enjoyed the course and we are always there to help and assist in case you have a problem, so please feel free.

Thank you.