

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

Lecture – 60

(Refer Slide Time: 00:10)



How to Secure Web Applications

- ▣ Incorporate security into the lifecycle
 - ▣ Apply information security principles to all software development efforts
- ▣ Educate
 - ▣ Issue awareness, Training, etc...

Let us look at how to secure web application. Incorporate security in the life cycle; apply information security principles to all software development efforts. So right from module one onwards we have been talking incorporates security into the life cycle; do not retrofit security in your application or organization. Educate yourself, issue awareness, conduct trainings, now all of those things have to be done, use secure coding practices, so if we developer do not know train them on secure coding practices.

(Refer Slide Time: 00:57)

How to Secure Web Applications

- ▣ Incorporating security into lifecycle
 - ▣ Integrate security into application requirements
 - ▣ Including information security professionals in software architecture/design review
 - ▣ Security APIs & libraries (e.g. ESAPI, Validator, etc.) when possible
 - ▣ Threat modeling
 - ▣ Web application vulnerability assessment tools



When you talk about securing web application, incorporating security into the life cycle, integrate security into the application requirements, include information security professionals in this software architecture or design review, which is very important. Security APIs and libraries example ESAPI, validator etcetera when possible; then do a threat modeling that use a web application vulnerability assessment tools to test the application. Now if you see on the right hand side, the security is encompassed why four criteria, now where to begin so it should be begin right from the development to the QA, then to production and then to audit. So security should be a process which has to be followed in all stages of the development, quality analysis or quality assurance, productions and audit.

(Refer Slide Time: 02:00)



How to Secure Web Applications

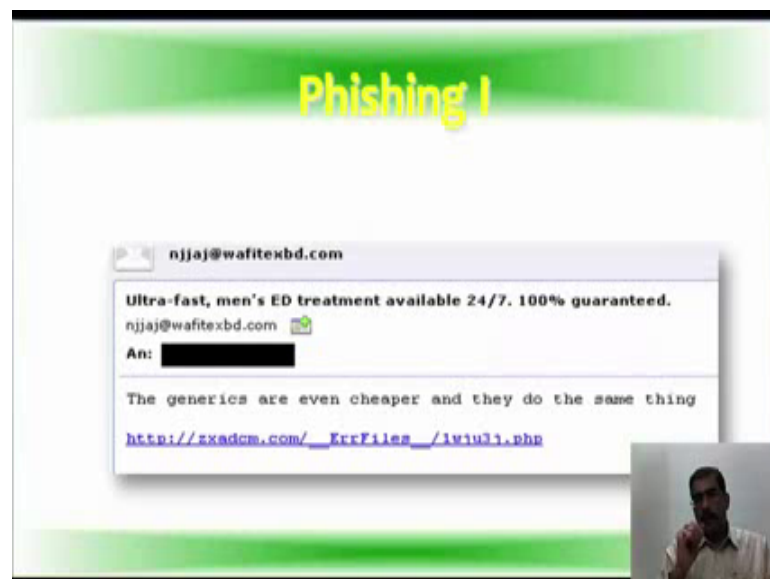
Educate

- Developers – Software security best practices
- Testers – Methods for identifying vulnerabilities
- Security Professionals – Software development, Software coding best practices
- Executives, System Owners, etc. – Understanding the risk and why they should be concerned

A small inset video shows a man speaking.

How to secure web applications? Again educate the developers on the software security best practices; educate the testers on methods for identifying the vulnerabilities. The security professionals on software development and software coding practices best practices so that they can actually go and audit whether the development team and the testing team had done the correct job; then executives, system owners and all others so understanding the perspectives of risk and why they should be concerned about it.

(Refer Slide Time: 02:42)



Phishing I

A screenshot of an email from njjaj@wafitexbd.com. The email content is:

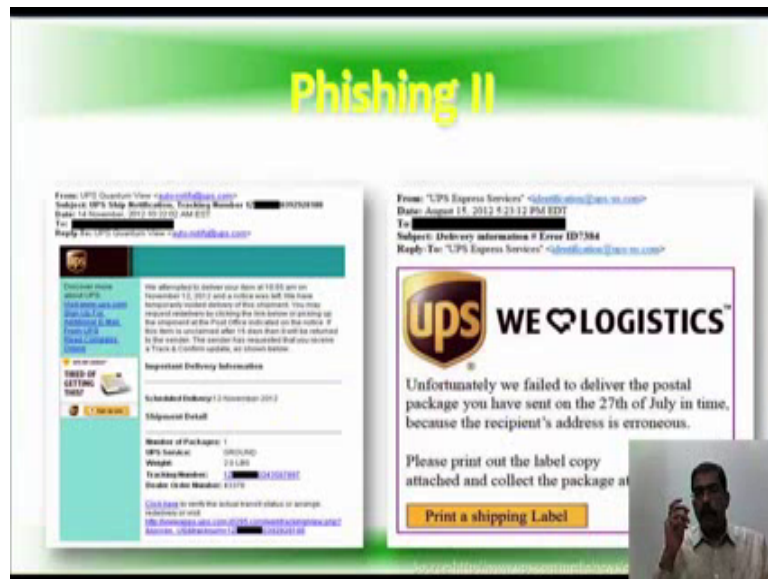
Ultra-fast, men's ED treatment available 24/7. 100% guaranteed.
njjaj@wafitexbd.com
An: [REDACTED]
The generics are even cheaper and they do the same thing
http://xxadcm.com/_ErrFiles_/1viu3i.php

A small inset video shows a man speaking.

This is an example of a phishing attack we had already spoke about phishing in domain four, but this is a actual, or this is how the phishing attack appears you would have seen from Nigeria also. Seeking or telling you that somebody wants to transfer 400 million

dollars to your account, then as to go they will ask keeping you to deposit some money and all those nonsensical things they will send, there are people who actually fall for it and go ahead and waste their money in such scheme and incidentally. This phishing itself started or became very prevalent from Nigeria, under the Nigerian penal code the section is the section 419; it is also called the Nigerian connection scam. So whenever you get these kind of mails reject it or just spam it put it into junk mail, do not use it.

(Refer Slide Time: 03:50)



It is very surprising to know that a lot of big companies have also been compromised. If you see on the left, it is appearing to come from UPS, so the page itself is has been UPS page itself has been created. In fact, two of them on the right hand also it is ups express services, and the left it is ups quantum view. Now this a typical phishing breach which has happened. Now if you go to ups site, which is www ups dot com slash media slash news, there is a link behind this bottom of this line. So if you go there you will know the entire background of how this phishing actually took place.

(Refer Slide Time: 04:36)



There is something called whaling; this is a Dilbert cartoon which comes in the news papers almost every day. Now phishing attacks on senior executives and other high profile targets within the business is called whaling. Now, if you look at the cartoon, the boss says I have new hobby, it is called phishing. I sent fake banking e mails to gullible executive then I find out their financial information and use it to steal the money that they do not deserve. So he is sending the mail dear customer, this is your bank we forgot your social security number and password, why do not you send them to us, so we can protect your money, sincerely The banker. So the guy who reading this mail thinks that it looks legit, it looks just like it came from the bank, so this kind of attack is called whaling.

(Refer Slide Time: 05:32)



In 2013, burger king twitter account was hacked, so the messaging twitter was we just got sold to the McDonalds; look for McDonalds in a hood near you. So this also actually happened this came as a news article in yahoo dot com.

(Refer Slide Time: 05:54)



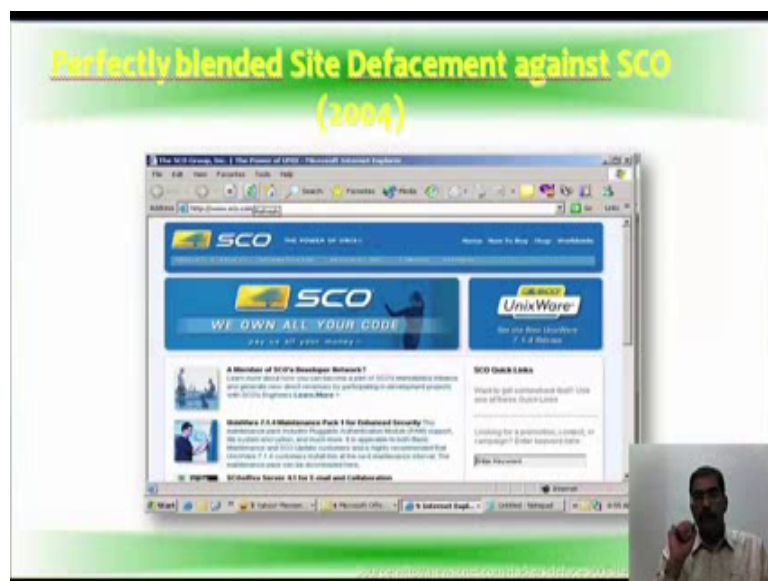
Similarly, twitter itself was defaced by Iranian cyber army; this was quite a while back in 2009. The site has been hacked by Iranian cyber army, so there are lots of incidences that have happened because of phishing, whaling, web application hacking.

(Refer Slide Time: 06:13)



There one more for you ESPN site decorated with cute unicorns, in 2009, it was hacked.

(Refer Slide Time: 06:21)



Way back in 2004 SCO - Santa Cruz Organization that they were hacked.

(Refer Slide Time: 06:29)



Probably, Sony get into the news for all the wrong reason. Again in 2011, Sony pictures data breach happened, where one millions passwords were exposed. If you see the highlighted in blue sentence, it say it was via a SQL injection attack. And the hacker group that did it were LulzSec, they released hundred and fifty thousand Sony picture records including usernames and password, so it was big setback for the consumer giant.

Now, what they had stated here is we had recently broke into Sony pictures dot com, and compromised over millions users personal information including passwords email address, home address, date of birth and all Sony opt-in data associated with their account. So, among other place we also compromised all admin details of Sony pictures including password along with seventy five thousand music, video and 3.5 million music coupons. So, it was a very big attack, and it was one of the top ten massive breaches that happened. Now, with so much information available for the hacker can we not do an identity tough this very possible, all you need is one picture with all these information date of birth is there, social security number is there, address is there, everything is there, so why cannot you do a identity which is very possible.

(Refer Slide Time: 08:12)



This is one of the newer one which is 2014 ebay, there was a data breach. In fact, ebay published that change your password, the site was hacked the company said the breached database house the customer or had the customer name, email addresses and physical addresses, phone number, date of birth and encrypted password no financial transaction was taken. I think they are missing the point here, because once you have customers detail, so much customer detail are available or was hacked, I think it is much more valuable than the data itself, because with this you can create havoc in the system and when I mean system not the computer system the entire society system.

(Refer Slide Time: 09:06)



After seeing those hacked, we ask ourselves why web application security is a high

priority; web application have become the number one target 75 percent of attacks target the application layer as stated or as researched by the Gartner. Most web application are vulnerable 95 percent of web application have some sort of vulnerability that is again a research done by Imperva. And 78 percent of easily exploitable weaknesses occur in web application that is again a research done by Symantec and again by Symantec. 67 percent of websites used to distribute malware are legitimate, but compromised websites.

(Refer Slide Time: 09:58)



Now, website attackers by country, it again by Incapsula in 2012. If you see the global distribution of the website attackers USA 48.8 percent; and India was 0.74 percent we should be ashamed of ourself. So then again if you see the proportions of website attackers, if you see distribution of attack site server takeover, the green one nothing has happened. The maximum that have happened the red one were the data theft, which was 10.9 percent somewhere in Alaska, somewhere in South America, somewhere in China, so the distribution of attack types is also given where. And surprisingly credential theft is 15.7 percent; the green one server takeover is actually 73 percent. So I think there is a mistake in the color coding released by Incapsula. The yellow ones should have been green; anyway the server takeover 73 percent is the open number; credential theft is also pretty high when you consider the statistics; data theft 10.9 percent, vulnerability scanning only 0.4 percent.

(Refer Slide Time: 11:31)

Top 5 Internet Security Threats
(RSA, 2012)

- ❑ **Idealistic young Hacktivists** will continue to attack
- ❑ **Big Data Companies** are taking control of users while profiting from user information
- ❑ **Attackers** will make more use of **Mobile Exploits** for hacking into corporate networks
- ❑ **Insiders** (Employees, Consultants, Business Partners) can always pose security risks
- ❑ **Foreign Governments** will start to target clouds and more types of businesses with APTs

Again there was a top five internet security threat, a research done by RSA in 2012 which says idealistic young Hacktivists will continue to attack big data companies are taking control of users while profiting from user information. Attackers will make more use of mobile exploits for hacking into corporate networks. Insiders that are employees, consultants, business partners always or can always pose security risks. Foreign governments will start to target clouds and more types of business with APTs. Now here what we have to again consider is BYOD - bring your own device is gaining popularity in many companies. So use of more mobile exploits or hacking into corporate network is possible. You take for an example an android phone, you sign in with your Google account, so you get access to your Gmail, you get access to YouTube, you get access to the other services of Google so many of these services are there. and your username and password is also stored in the android phone. Imagine the situation that your mobile is lost, and you actually use some kind of credential to connect your corporate network or some other software is put, a malware is put on your mobile phone. Now you have seen that the way that the mobile phone we have seen in the domain 5 about window c embedded system and all that, just because you have a embedded system or phone does not mean that you can be attacked by a virus or malware.

Now, most of the phones, there are antivirus software available, so it is recommended to install that antivirus internet security etcetera on that because at home or office when you connect through a WIFI, you still are prone to vulnerability that happen to your desktop. So you have to be careful on how you protect your mobile phones; at the same time,

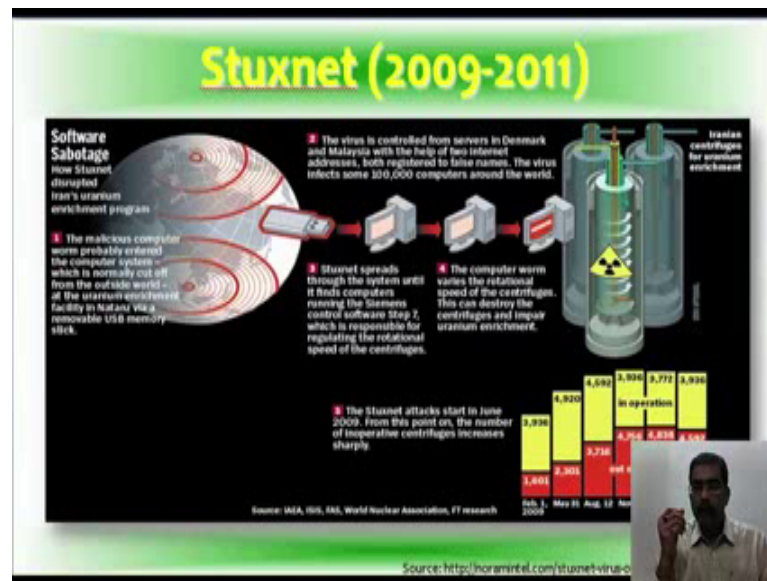
attackers make more use of mobile exploits for hacking into corporate network. Suppose I bring a basic phone, do my hack, throw away the phone, somewhere into a river, now tracing also become little difficult, so mobile exploits may be easier to do where the same time difficult to detect.

(Refer Slide Time: 14:15)



We spoke about APTs in the previous slide, it is advance persistent threat. It is group with both the capability and the intent to persistently and effectively target a specific entity. An example is the Stuxnet creators can be considered an APT to the Iranian government. Now what actually happened to define a target, find and organize accomplices, build or acquire tools, research target infrastructure and employees, you test for detection, then you deploy, then the initial intrusion happens, then a outbound connection is initiated from within that network. Then expand access and obtain credentials, strengthen the foothold exfiltrate data infiltrate is going in exfiltrate taking out. Then cover tracks and remains undetected, so advance persistent threat covers this cycle.

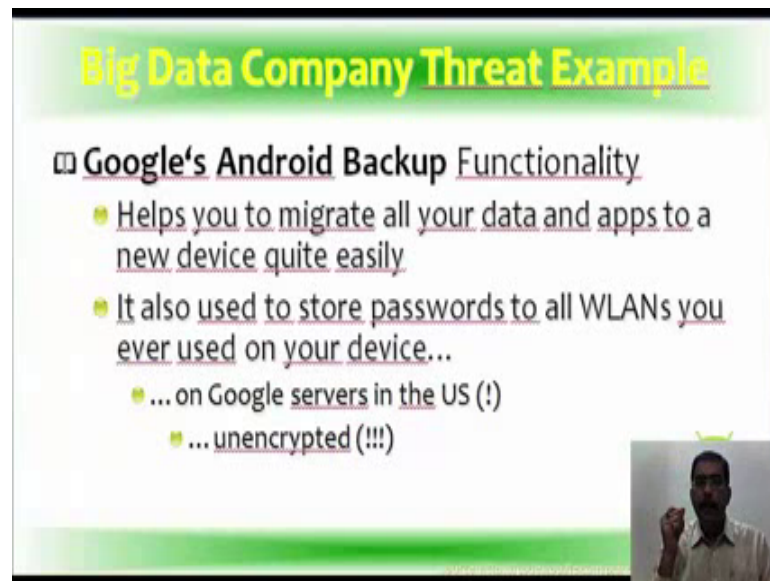
(Refer Slide Time: 15:28)



Now, take a look at this stuxnet 2009 to 2011 software sabotage how Stuxnet disrupted Iran's uranium enrichment program. The first is the malicious computer worm probably entered the computer system which is normally cut off from the outside world at the uranium enrichment facility at Natanz via a removable USB removable memory stick. Two, the virus is controlled from servers in Denmark and Malaysia with the help of two internet addresses. Both registered to false net, the virus infects some hundred thousand computers around the world. Then the third one is stuxnet spreads through the system until it finds computer running the Siemens control software step 7, which is responsible for regulating the rotational speed of the centrifuges.

Then there is the computer worm varies the rotational speed of the centrifuge this can destroy the centrifuges and impair uranium enrichment. then this the Stuxnet attack starts attack in June 2009. From this point on the number of inoperative centrifuges increases dramatically, so more on this particular attack you can read the url is given below. Now, similar to this, if you can see it has been made into a movie; one is independence oh sorry independence day is for your module three; diehard - diehard 4 was again a hacker, a disgruntled employee who left the government and hijacked all the computers of the government and disrupted the power he had the ability to control the aircraft so many of the diehard movie, it is something similar to that.

(Refer Slide Time: 17:41)



Big Data Company Threat Example

- ☐ **Google's Android Backup Functionality**
 - Helps you to migrate all your data and apps to a new device quite easily
 - It also used to store passwords to all WLANs you ever used on your device...
 - ... on Google servers in the US (!)
 - ... unencrypted (!!!)

Now we come to big data company threat example. Now Google's android backup functionality; it helps you to migrate all your data and application to a new device quite easily. The same is the case with IOS also, it also used to store passwords to all WLAN you ever used on your device. So when you configure it, it stream stored it. And everything is stored on the Google servers in the US and the encrypted. Imagine the situation where somebody get hold of this data, the same is possible with apple devices also. Now with icloud being integrated where you can work from your mac, store it on the i cloud, go home and work from your iphone or ipad, so as we technology also increases, the threat also increases substantially. So we discuss the fact bit of background on web application and some of the hacks data that have happened.