Unit 4: Web Attack

4

Unit Structure

4.1 LEARNING OBJECTIVE

After studying this unit student should be able to:

- Study various kinds of web attack.
- Identify browser attack, phishing.
- Get the details of user from website.

4.2 INTRODUCTION

This block is focus to securing web applications has become incredibly importantas the information processed by web applications has becomecritical to corporations, customers, organizations, andcountries. Web applications manage a wide array of informationincluding financial data, medical records, social securitynumbers, intellectual property and national security data.The purpose of a web based attack is significantly differentthan other attacks; in most traditional penetration testingexercises a network or host is the target of attack. Web basedattacks focus on an application itself.

4.3WEB ATTACK

Technology growth on the Web has changed the way businesses and consumers communicate and interact with each other.The Web has become a staple for information sharing and commercial transactions. At the same time it has also becomecomplex, without boundaries and immediate in its nature.

Web application provides an interface between the web server and the client to communicate. Web pages are generated at the server, and browsers present them at the client side. The data is passed between client and server in the form of HTML pages through HTTP protocol.

A single Web page today can be comprised of information from manysimultaneous sources from around the world. It only takes one of these sources to be compromised in order for a new Web attackto be quickly propagated and delivered

to many unsuspecting Web users. The ubiquity and complexity, compounded with holesin the infrastructure, have made the Web vulnerable to attack.

4.3.1 BROWSER ATTACKS

Of all the software in use, browsers are the most exposed. They are constantly connecting to the outside world, and frequently interacting with websites and applications that cybercriminals have infected with malware.

Browsers are powerful, data-rich tools that if compromised, can provide an attacker with a vast amount of information about you, including your personal address, phone number, credit card data, emails, IDs, passwords, browsing history, bookmarks etc.

Browsers are also perfect instruments for cybercriminals to establish a foothold on your device, your personal network, and your business systems. Browsers rely on a number of third-party plug-ins like JavaScript, Flash, and ActiveX to perform various tasks. However, these plug-ins often come with security flaws that cybercriminals exploit to get access to your systems. These vulnerabilities allow attackers to wreak havoc by, for example, installing ransomware, exfiltrating data, and stealing intellectual property.

During the past year or so, we've seen a sharp increase in web threats that are specifically designed to leverage browser-based vulnerabilities. This increase in popularity is not only because browsers are strategically desirable as hacking targets, but because browser-based web threats are difficult to detect.

Most malware detection and prevention technologies work by examining files such as downloads or attachments. However, browser-based threats don't necessarily use files, so conventional security controls have nothing to analyse. Unless organizations implement advanced tools that don't rely on analysing files, browser-based attacks will likely go undetected.

How Browser Based Cyber-threats operate

As an example of how a browser-based attack works, consider a scenario where a Windows user visits a seemingly benign but now malicious website, possibly one he

or she has visited before, or as the result of an enticing email. As soon as a connection occurs, the user's browser begins interacting with the site.

Assuming the system is using JavaScript, which according to research firms like Web Technology Surveys, 94% of all websites do and over 90% of browsers have it enabled, the browser will immediately download and start executing JavaScript files from the malicious website.

The JavaScript can harbour malicious code that's capable of capturing the victim's data, altering it, and injecting new or different data into their web applications—all in the background and invisible to the user.

For instance, one method malware authors use to accomplish this is by embedding an obfuscated Adobe Flash file within the JavaScript. Flash is frequently used due to its seemingly never-ending set of vulnerabilities. The following is representative of what typically occurs:

- The Flash code invokes PowerShell, a powerful OS tool that can perform administrative operations and exists on every Windows machine.
- Flash feeds instructions to PowerShell through its command line interface.
- PowerShell connects to a stealth command and control server owned by the attackers.
- The command and control server downloads a malicious PowerShell script to the victim's device that captures or finds sensitive data and sends it back to the attacker.
- After the attacker has met his objectives, the JavaScript, Flash, and PowerShell scripts are wiped from memory, leaving essentially no trace of the breach.

The MarioNet attack is a browser-based attack; it opens the door for assembling giant botnets from users' browsers. These botnets can be used for in-browser crypto-mining (cryptojacking), DDoS attacks, malicious files hosting/sharing, distributed password cracking, creating proxy networks, advertising click-fraud, and traffic stats boosting, researchers said.

Moreover, MarioNet can survive after users close the browser tab or move away from the website hosting the malicious code.

4.3.2 WEB ATTACKS TARGETING USERS

Cyber criminals often go after your enterprise data by preying on your end users. Here are some of the most current exploits to watch for.

Every day, criminals devise new malware and social engineering attacks that target what has become an organization's weakest link: end users and their Web-connected devices. Here are the most common attack methods and social engineering techniques, and ideas on how to stop these attacks before they infect end user devices and work their way into your corporate data.

Drive-By Downloads

Drive-by downloads are a central part of many of the most sophisticated Web attacks that criminals perpetrate against online users. They are so dangerous because they require no user action to download malicious content onto an endpoint. What's more, these attacks are often unleashed from legitimate sites.

Drive-by downloads are typically deployed by hackers who have taken advantage of Web vulnerabilities such as SQL injection that can be exploited to "allow attackers to change the content of a website," says Chris Wysopal, CTO at the app security testing company Veracode.

Once implanted on a site, drive-by downloads typically take advantage of browser vulnerabilities to automatically download anything from full-fledged viruses to less detectable downloader apps that will trick the user into eventually loading malware onto the machine via a button press or click.

Clickjacking

If the attacker requires extra interaction from the user to load malware, this will be accomplished through an attack called "clickjacking."

The purpose of this attack is to open the target website in an invisible frame and get the user to click somewhere in the frame when they don't even know they're clicking in that website," says Ari Elias-Bachrach, application security consultant and trainer for security consultancy Defensium. "In this way, you can trick the user into making a mouse click that does something [malicious] on the website.

A common example is offering a bogus pop-up window made to look like a legitimate plug-in update or antivirus alert, such as a Microsoft Security Essentials window that says you have a few viruses and should push a button to clean them. "The pop-up itself is not harmful, but if you click the button, you open the gate to infect your machine," says Rick Doten, chief information security officer for DMI, an enterprise mobility company.

Plug-In And Script-Enabled Attacks

Not only do attackers look for vulnerabilities within the browser itself, they also frequently ferret out bugs in browser plug-ins and scripting programming to help them carry out drive-by downloads and clickjacking attacks.

Since these attacks rely on known vulnerabilities, "make sure users keep browsers and browser plug-ins updated to the latest versions by enabling auto-update functions," says Wolfgang Kandek, CTO of vulnerability management firm Qualys.

In some cases, it may also make sense to turn off scripting within the browser and other susceptible programs, such as Adobe Reader. Similarly, uninstalling certain problematic plug-ins can reduce the attack surface within susceptible user bases. But you'll still need to put controls in place and train users not to undo the work.

Advanced Phishing Attacks

While phishing attacks are typically associated with email, most are perpetrated via links to malicious content on the Web, whether a simple password capture form used in traditional phish attempts or a malicious drive-by download in more advanced targeted attacks.

Phishing attacks are designed to trick users into thinking they are a link from an organization or person they know, making people feel safe enough to click or divulge information they otherwise wouldn't. Many corporate security training programs have helped users spot the most obvious first-generation phishing attempts, which were designed to steal credentials such as banking passwords. But attackers are getting more crafty.

Social (Engineering) Networks

Millions of people sharing information on social networking sites such as Facebook, Twitter, LinkedIn and Google+ creates "an ideal attack bed for someone who wants to socially engineer a target individual, group of individuals or an organization as a whole," says Joe DeSantis, manager of incident response at security consultancy SecureState.

If people don't configure their privacy settings very stringently, attackers can simply troll their pages to dig up information about the target and then hone a particularly effective spear-phishing email. Or attackers can pose as friends or family to "friend" a target -- or a friend of the target -- to gain that intelligence. They can also use a social networking connection to directly send targets malicious links on their walls or Twitter feeds.

4.3.3 OBTAINING USER OR WEBSITE DATA

The value of web data is increasing in every industry from retail competitive price monitoring to alternative data for investment research. Getting that data from a website is vital to the success of your business.

Web scrapers automatically collect information and data that’s usually only accessible by visiting a website in a browser. By doing this autonomously, web scraping scripts open up a world of possibilities in data mining, data analysis, statistical analysis, and much more.

Why Web Scraping Is Useful

We live in a day and age where information is more readily available than any other time. The infrastructure in place used to deliver these very words you are reading is a conduit to more knowledge, opinion, and news than has ever been accessible to people in the history of people.

So much so, in fact, that the smartest person’s brain, enhanced to 100% efficiency (someone should make a movie about that), would still not be able to hold 1/1000th of the data stored on the internet in the United States alone.

As our eyes and brains can't really handle all of this information, web scraping has emerged as a useful method for gathering data programmatically from the internet. Web scraping is the abstract term to define the act of extracting data from websites in order to save it locally.

Think of a type of data and you can probably collect it by scraping the web. Real estate listings, sports data, email addresses of businesses in your area, and even the lyrics from your favourite artist can all be sought out and saved by writing a small script.

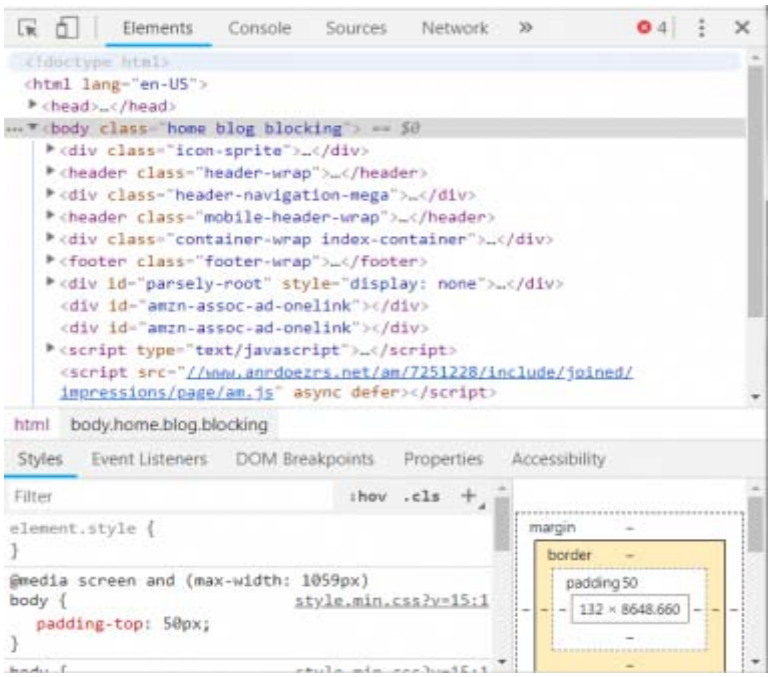
How Does a Browser Get Web Data?

First, your browser will take the URL you entered or clicked on and form a "request" to send to a server. The server will then process the request and send a response back.

The server's response contains the HTML, JavaScript, CSS, JSON, and other data needed to allow your web browser to form a web page for your viewing pleasure.

Inspecting Web Elements

Modern browsers allow us some details regarding this process. In Google Chrome on Windows you can press Ctrl + Shift + I or right click and select Inspect. The window will then present a screen that looks like the following.



Other Types of Responses

Additionally, servers can return data objects as a response to a GET request, instead of just HTML for the web page to render. A website's Application Programming Interface (or API) typically utilizes this type of exchange.

Scraping frameworks are available in Python, JavaScript, Node, and other languages. One of the easiest ways to begin scraping is by using Python and Beautiful Soup.

4.3.4 EMAIL ATTACKS

Malicious email remains one of the most significant and ongoing computer security threats that we face. Cybercriminals use a variety of email-based attacks to deliver malware, lure victims to malicious websites, and steal logon credentials, and organizations everywhere need to understand these threats and how to implement effective safeguards.

Many people rely on the Internet for many of their professional, social and personal activities. But there are also people, who attempt to damage our Internet-connected computers, violate our privacy and render inoperable the Internet services.

Email is a universal service used by over a billion people worldwide. As one of the most popular services, email has become a major vulnerability to users and organizations.

Malicious email authors are clever and relentless, and they are constantly developing new or at least different ways to deceive and attack us. Although the malicious payloads found in email-based attacks frequently change, the vast majority of cybercriminals use basic strategies:

Malicious attachments: Emails often include dangerous attachments that install keyloggers, ransomware, and other malware when opened by the victim.

Links to malicious web pages: Contained in either an attachment or in the body of the email, links to dangerous web pages also account for a significant number of data breaches.

Below are some of the most common types of Attacks:

Phishing: Phishing is a form of fraud. Cyber criminals use email, instant messaging, or other social media to try to gather information such as login credentials by masquerading as a reputable person. Phishing occurs when a malicious party sends a fraudulent email disguised as being from an authorized, trusted source. The message intent is to trick the recipient into installing malware on his or her device or into sharing personal or financial information.

Spear phishing is a highly targeted phishing attack. While phishing and spear phishing both use emails to reach the victims, spear phishing sends customized emails to a specific person. The criminal researches the target's interests before sending the email.

Whaling: Whaling is a phishing attack that targets high profile targets within an organization such as senior executives. Additional targets include politicians or celebrities.

Pharming: Pharming is the impersonation of an authorized website in an effort to deceive users into entering their credentials. Pharming misdirects users to a fake website that appears to be official. Victims then enter their personal information thinking that they connected to a legitimate site.

Adware: Adware typically displays annoying pop-ups to generate revenue for its authors. The malware may analyse user interests by tracking the websites visited. It can then send pop-up advertising relevant to those sites. Some versions of software automatically install Adware.

Spam: Spam (also known as junk mail) is unsolicited email. In most cases, spam is a method of advertising. However, spam can send harmful links, malware or deceptive content. The end goal is to obtain sensitive information such as a social security number or bank account information. Most spam comes from multiple computers on networks infected by a virus or worm. These compromised computers send out as much bulk email as possible.

Check Your Progress 1:

1. What is Phishing?
2. How Email attacks happen?

4.4LET US SUM UP

This block covers the various web attacks like phishing, pharming, etc.

4.5CHECK YOUR PROGRESS: POSSIBLE ANSWERS

Check Your Progress 1:

1. Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details by disguising oneself as a trustworthy entity in an electronic communication.
2. Malicious email remains one of the most significant and ongoing computer security threats that we face. Cybercriminals use a variety of email-based attacks by sending malicious attachment as well as links to malicious web pages.

4.6 FURTHER READING

For more focus on cyber security domain use CEH (Certified Ethical Hacking) books. Also you can refer https://www.sans.org/reading-room/whitepapers/application/web-based-attacks-2053.

4.7ASSIGNMENTS

- Describe various email attacks.

4.8ACTIVITIES

- Retrieve website data using web scrapper.