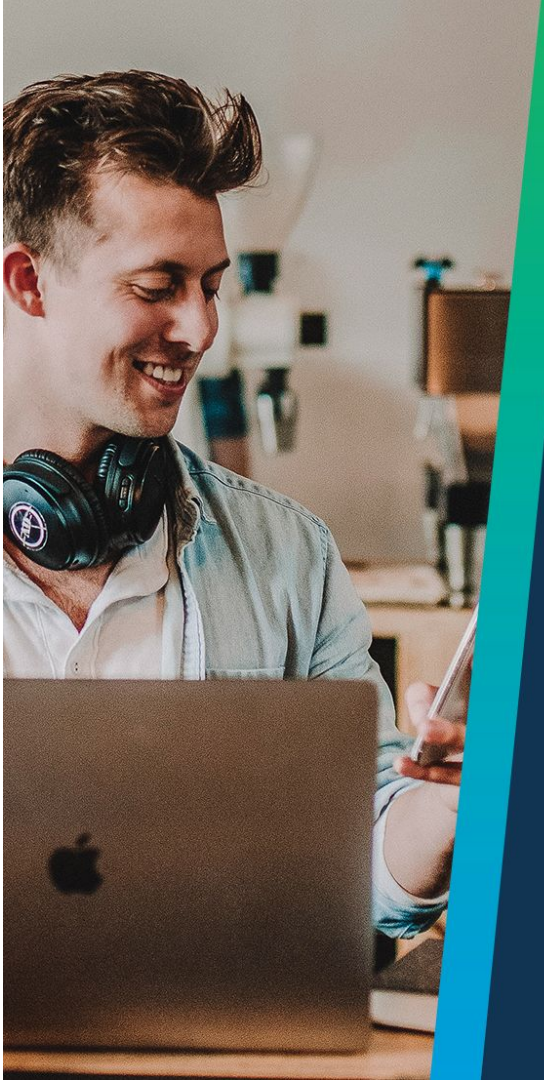


Cyber Security Bootcamp

Hyperiondev

MITM Attacks & XSS Vulnerabilities

Lecture - Housekeeping

- The use of disrespectful language is prohibited in the questions, this is a supportive, learning environment for all - please engage accordingly.
- No question is daft or silly - ask them!
- There are Q/A sessions at the end of the session, should you wish to ask any follow-up questions.
- For all non-academic questions, please submit a query: www.hyperiondev.com/support
- Report a safeguarding incident: http://hyperiondev.com/safeguardreporting

Objectives

1. Define key terms related to MITM attacks and XSS vulnerabilities.
2. Explain how MITM attacks and XSS vulnerabilities compromise security.
3. Explore the different types of of MITM attacks and measure to prevent XSS
4. Configure and secure a apache server running locally with a self-signed certificate.

Previously:

Covered how the web works and touched on the HTTP and SSH protocols.

We learned about HTML & CSS and created our very first static HTML and CSS webpage.

Poll

What is the primary method to prevent Man-in-the-Middle (MITM) attacks?

Poll

Which type of input handling is most effective in preventing XSS vulnerabilities?

MitM Attack

MitM Attack

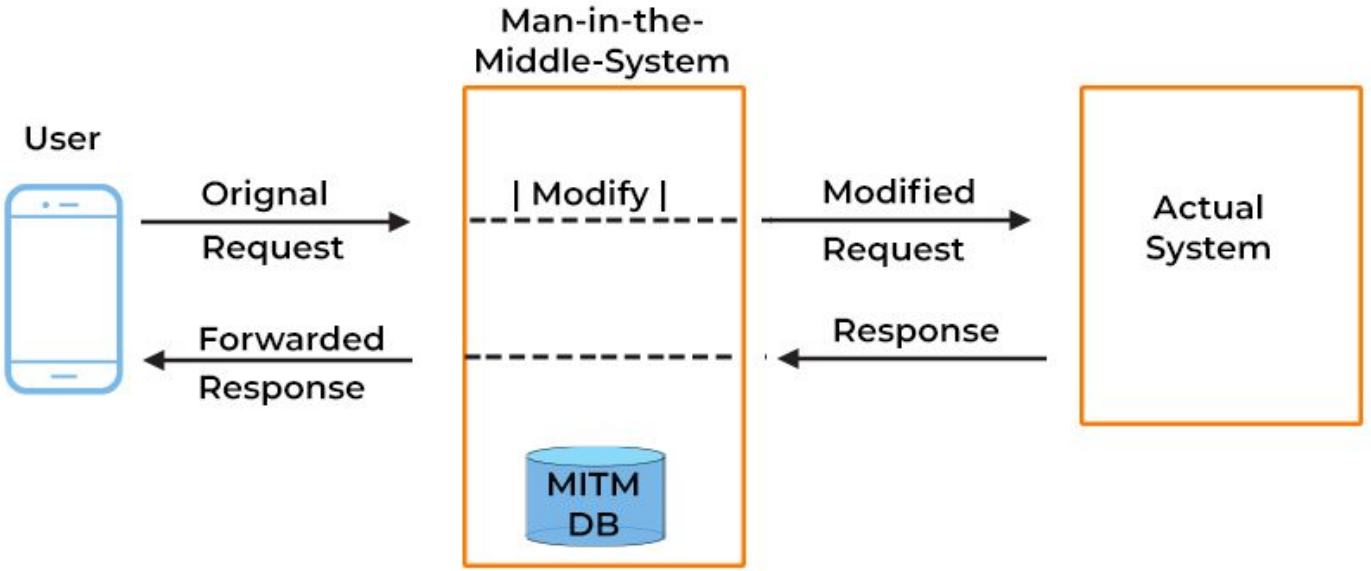
- A cyberattack known as a "man-in-the-middle" (MitM) occurs when an attacker surreptitiously intercepts and relays messages between two parties that seem to be speaking with each other directly. The attack is a form of eavesdropping in which the perpetrator records the entire conversation/transmission and takes complete control of it.

- MitM cyberattacks are a severe threat to online security because they allow the attacker to instantly obtain and alter sensitive personal data, including credit card numbers, account information, and login credentials.

MitM Attack

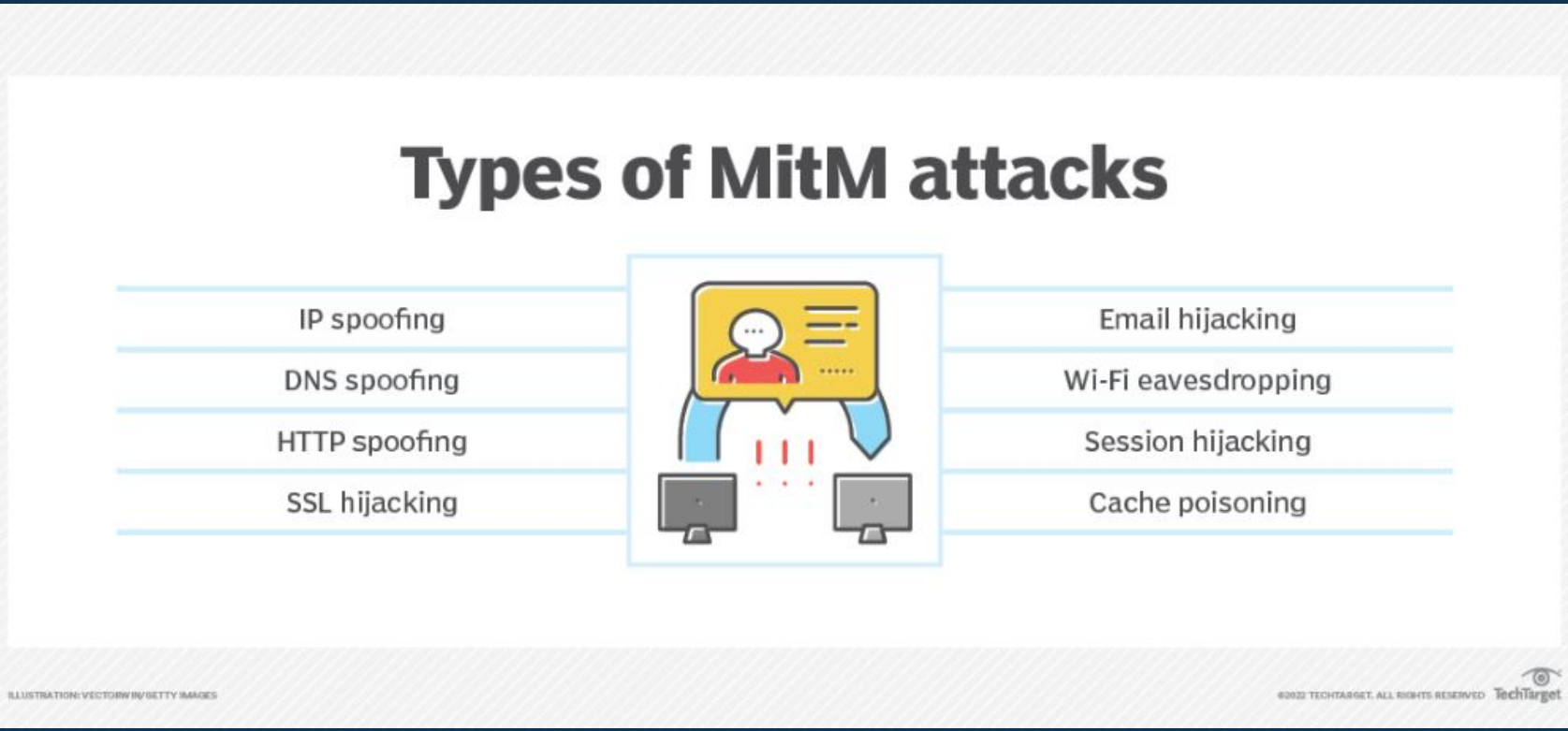
TOOLBOX™

HOW DOES A MAN-IN-THE-MIDDLE ATTACK WORK?



https://www.spiceworks.com/it-security/data-security/articles/man-in-the-middle-attack/

Types of MitM attacks

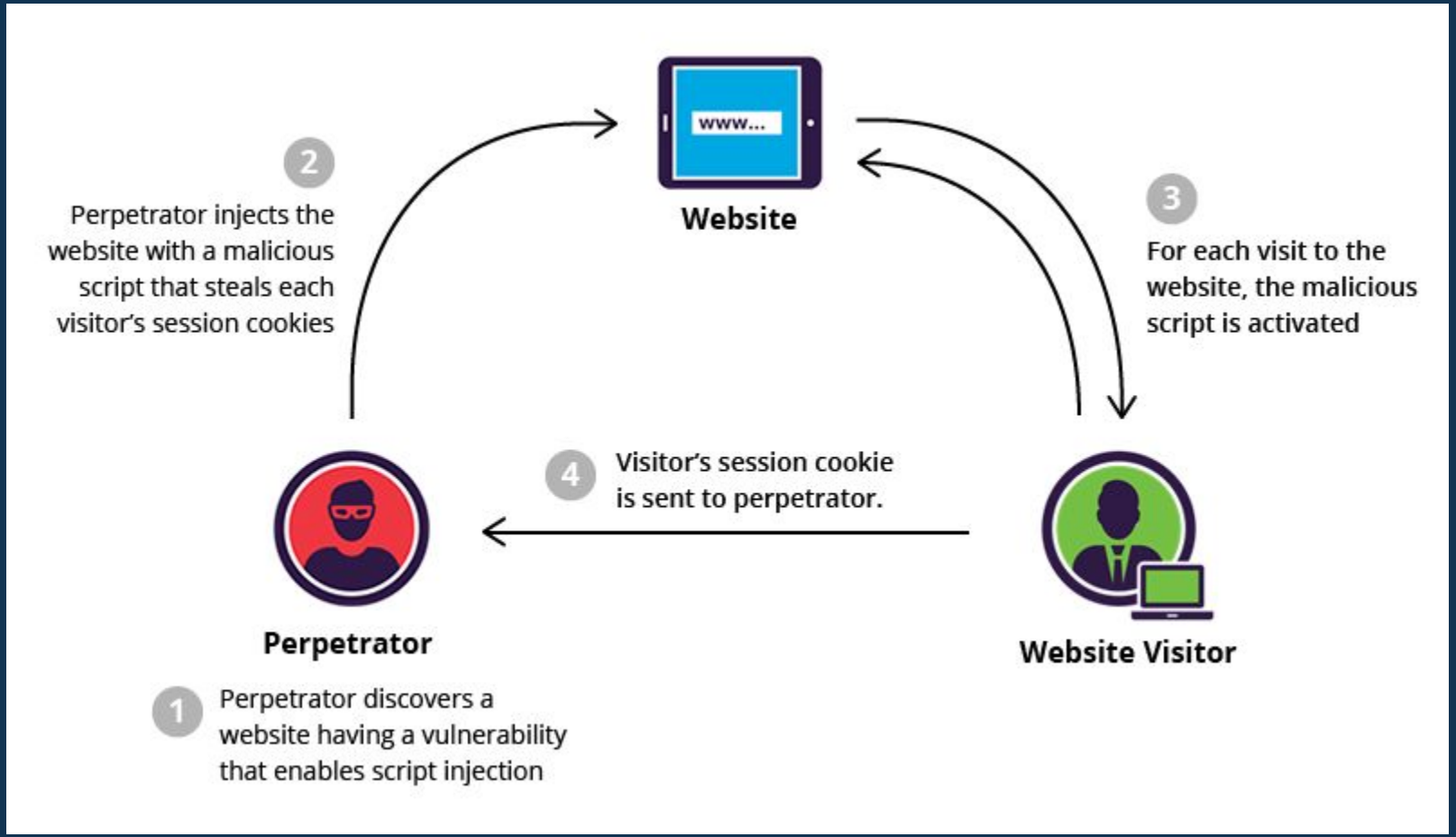


https://cdn.ttgtmedia.com/rms/onlineimages/types_of_mitm_attacks-f.png

XSS

XSS Attacks

A type of web security flaw called cross-site scripting (XSS) enables an attacker to insert malicious code into a web page that is being viewed by other users. By doing this, the attacker may be able to obtain sensitive data from unwitting victims, such as login credentials, session cookies, or personal information. Hackers frequently use this method to compromise websites and web applications.


www...
Website
2
Perpetrator injects the website with a malicious script that steals each visitor's session cookies
3
For each visit to the website, the malicious script is activated
4
Visitor's session cookie is sent to perpetrator.
Perpetrator
Website Visitor
1
Perpetrator discovers a website having a vulnerability that enables script injection

XSS Prevention

Avoiding HTML in inputs - if at all possible Preventing users from entering HTML into form inputs is a very effective way to avoid persistent cross-site scripting attacks. Other options, like markdown and WYSIWYG editors, enable users to create rich content without using HTML.

Validating inputs - Validation is the process of putting in place rules that stop users from entering data into forms that don't meet specific requirements. For instance, the validation rules for an input that requests the user's "Last Name" should restrict user input to alphanumeric characters only. The "script>" tags and other symbols frequently used in cross-site scripting can be rejected by validation rules.

Data sanitization - Data sanitization is similar to data validation in that it takes place after the data has been posted to the web server but before it is shown to another user. A variety of online tools are available to clean HTML and remove any malicious code injections.

XSS Prevention cont...

Using special rules for their cookie handling, Web applications can reduce cookie theft caused by cross-site scripting attacks. This is another method for implementing cookie security measures. Cross-site scripting attackers cannot access cookies if they are tied to specific IP addresses. Additionally, rules can be made to completely prevent JavaScript from accessing cookies.

Securing a server

Lesson Conclusion

XSS Attacks

Definition:

- XSS allows attackers to inject malicious scripts into websites, which are executed in users' browsers.
- Common Scenarios:

Phishing attacks using fake websites to steal credentials.

- Exploiting the default behavior of browsers that run scripts like JavaScript.

Types of XSS:

- Reflected XSS: Injected scripts are reflected off the server to the user's browser via manipulated URLs.
- Stored XSS: Malicious scripts are stored on the server and run whenever a user accesses the compromised page.

Prevention Methods:

- Input filtering and output encoding.
- Use of response headers like Content Security Policy (CSP).

MitM Attacks

Definition:

- An attacker intercepts communication between two parties, posing as one of them to gain access to sensitive information.

Causes:

- Lack of proper authentication and encryption.

Prevention Methods:

- **Robust Authentication:** Use of multi-factor authentication (MFA) and public-key authentication.
- **Encryption:** Encrypt communication channels to protect data integrity and confidentiality.
- **Digital Certificates:** Use certificates issued by trusted Certificate Authorities (CAs) to verify identities.
- **Network Security Measures:** Firewalls and intrusion detection systems to monitor and secure networks.

Hyperiondev

Q & A Section

Please use this time to ask any questions relating to the topic explained, should you have any

Hyperiondev

Thank you for joining us

Take regular breaks.
Stay hydrated.
Avoid prolonged screen time.
Remember to have fun :)