**A Secure E-Commerce WebSite with a payment Gateway**

Ali Zarafshani, Seemaparvez Shaik  
 CSCE Masters in Cybersecurity *University of the North Texas University of North Texas*

Denton

[seeemaparvezshaik@my.unt.edu](mailto:seeemaparvezshaik@my.unt.edu)

***Abstract*—**The main objective of this project titled “A Secure E-Commerce Website with a Payment Gateway” is to develop a secure e-commerce website with a payment gateway, then perform a few attacks on it to assess its vulnerability, and finally implement security measures to mitigate those attacks in the future.

**keywords: Cybersecurity Attacks, E-Commerce, Mitigation Techniques, Vulnerability, Vulnerability Assessment**

***Introduction:***

Security is an essential component of modern computing systems. It refers to the protection of computer systems, networks, and data from unauthorized access, theft, damage, or other malicious activities. Security measures are designed to ensure the confidentiality, integrity, and availability of information, as well as the privacy of users. When we talk about confidentiality in the context of security, we are referring to the protection of information from unauthorized disclosure. This means making sure that sensitive information is only accessible to those who need it and have permission to access it. Confidentiality can be ensured through access controls and encryption. Integrity, on the other hand, means the protection of information from unauthorized modification. It is crucial to ensure that data or information is not changed or tampered with in any way without authorization. This can be achieved through the use of data validation, user authentication, and access controls. Availability is another critical aspect of security. It means protecting information from unauthorized destruction or disruption. Availability ensures that information is always accessible when it is needed and that it is not lost or destroyed due to unauthorized access or malicious activities. Finally, privacy refers to the protection of personal information from unauthorized disclosure. Personal information includes sensitive data such as name, address, social security number, and other confidential information. This kind of information should be kept private and only accessible to authorized individuals. There are different ways to ensure strong security measures. Hardware security measures include firewalls, intrusion detection systems, and data encryption. Software security measures include antivirus software, firewalls, and intrusion detection systems. Procedural security measures include security policies, security training, and security audits. It is essential to ensure that security measures are in place and working correctly to prevent unauthorized access, data breaches, and other malicious activities that can cause significant harm to individuals and businesses. By implementing strong security measures, we can protect our sensitive information and maintain the confidentiality, integrity, and availability of our data.

***How Security is Crucial for an E-Commerce Website?***

Security is an incredibly vital aspect of any transaction that takes place in the e-commerce space. It involves the protection of sensitive data, such as personal information, banking details, and credit card numbers, from being accessed, stolen, or manipulated by unauthorized personnel. Therefore, it is essential to ensure that every transaction has several security measures in place to protect the data being exchanged.

To achieve this, there are six crucial security principles that must be implemented in any e-commerce transaction. These principles are:

1. Confidentiality: This principle requires that information is protected from unauthorized access, use, disclosure, disruption, modification, or destruction. Confidentiality ensures that only authorized personnel have access to sensitive data.
2. Integrity: The integrity principle ensures that the information being exchanged is accurate and complete, and must not be modified or destroyed in an unauthorized manner. It is important to maintain data integrity to ensure that the data is reliable and trustworthy.
3. Availability: This principle requires that information is accessible and usable when needed. Availability ensures that the information is readily available to authorized personnel whenever they need it.
4. Authenticity: Authenticity is the principle that ensures that information is genuine and not counterfeit. Authenticity is critical in ensuring that the data being exchanged is trustworthy and reliable.
5. Non-repudiation: Non-repudiation is the principle that ensures that the sender and recipient of the information can prove that they sent or received the information. This principle is essential in case of a dispute regarding the transaction.
6. Encryption: Encryption is the principle that ensures that information is protected using cryptographic techniques. Encryption plays a crucial role in ensuring the confidentiality and integrity of the data being exchanged.

these six security principles are essential to protect the privacy, integrity, and availability of information in the e-commerce space. Therefore, it is crucial to implement these security measures to safeguard sensitive data and ensure that e-commerce transactions are secure and reliable.

***Importance of Security Protocols and SSL(Secure Socket Layer Protocol)***

The Secure Sockets Layer (SSL) protocol is a security protocol that's commonly used to ensure secure communications over a network. It's used in a wide range of applications such as web browsing, email, and file transfers. The way SSL works is by providing a secure channel of communication between two parties. This secure channel is created using a combination of authentication, encryption, integrity, and non-repudiation. Authentication is the process of verifying the identity of the parties involved in the communication. This is important because it ensures that the parties communicating are who they say they are. Authentication can be done using a variety of methods, such as passwords, digital certificates, or biometric authentication. Encryption is the process of converting data into a form that can't be read by anyone who doesn't have the key to unlock it. This is important because it keeps the data private while it's being sent. SSL uses encryption algorithms such as AES, DES, and RC4 to encrypt data. Integrity is the process of ensuring that data hasn't been tampered with while it's being sent. This is important because it ensures that the data hasn't been modified or corrupted during transmission. SSL uses hash functions such as SHA-1, SHA-256, and SHA-384 to create a message digest that's sent along with the data. The receiver can use this message digest to verify the integrity of the data. Non-repudiation is the process of ensuring that the person who sent the data can't deny that they sent it. This is important because it provides a way to prove that the data was sent by a particular person. SSL uses digital signatures to provide non-repudiation. A digital signature is a mathematical technique used to verify the authenticity of a message.

Overall, SSL is an important protocol that helps ensure secure communication over a network. By using a combination of authentication, encryption, integrity, and non-repudiation, SSL provides a secure channel of communication between two parties.

***Threats and Points of Vulnerability in an E-Commerce Website***

There are several points of vulnerability that can be found in an e-commerce website's client-server communication channel. One potential vulnerability is a lack of encryption for the data being transmitted. This means that sensitive information, such as credit card numbers, could be intercepted by attackers. Another point of vulnerability is the use of outdated software or protocols. If the website is using an old version of TLS, for example, it may be susceptible to attacks that have since been patched in newer versions. Additionally, if the website is not regularly updated with security patches, it may be vulnerable to known exploits that could be used to compromise the server or steal user data. To mitigate these vulnerabilities, it is important for e-commerce websites to implement strong encryption methods, such as the use of HTTPS and SSL/TLS protocols. Regular updates and maintenance should also be performed to ensure the website is protected against the latest threats. By taking these steps, e-commerce websites can help ensure the security and privacy of their users' data.

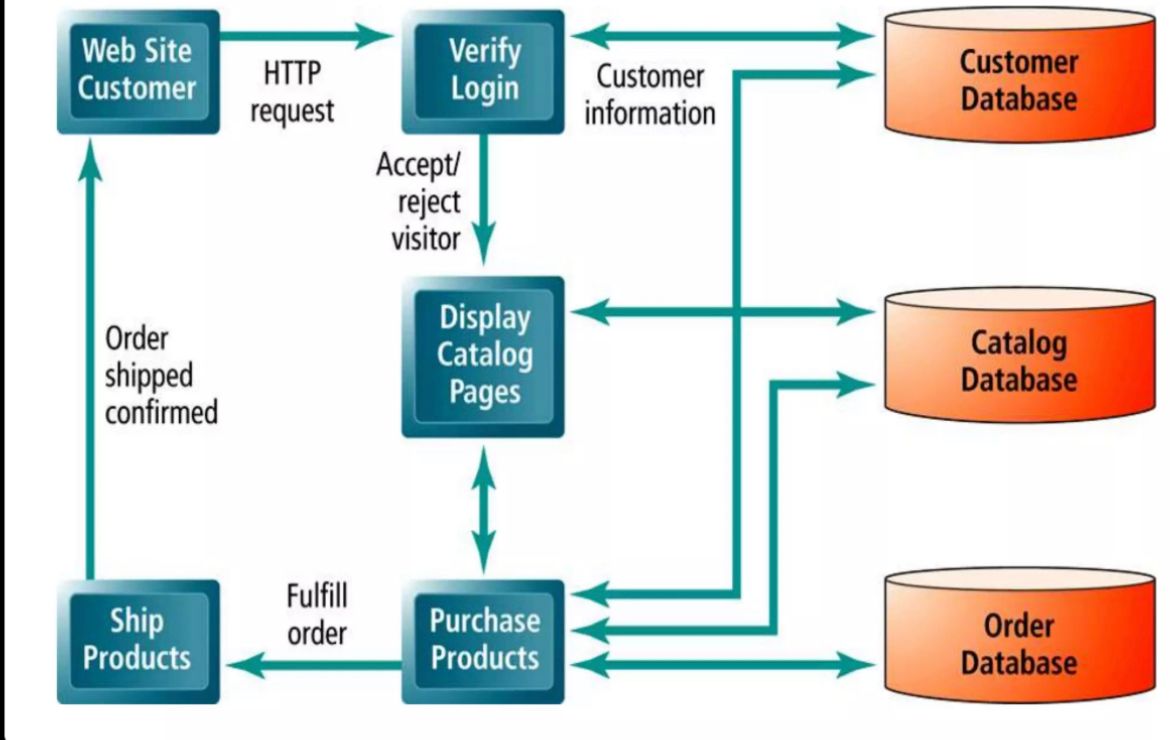
***Threats–***

E-commerce websites are often targeted by cybercriminals due to the sensitive data they possess, such as credit card information and personal details. Therefore, it is crucial to be aware of the common threats that these websites face. One such threat is malicious code, which refers to any code that is designed to harm a website or its users. This can take the form of viruses, Trojans, or other types of malware. Hacking is also a significant threat to e-commerce websites. Cybercriminals may attempt to gain unauthorized access to a website's database or payment system to steal sensitive data or install malware. Credit card fraud is another common threat. This occurs when a criminal obtains a victim's credit card information and uses it to make unauthorized purchases. Spoofing is a type of cyber attack in which a criminal impersonates a legitimate website to trick users into revealing their sensitive information. Sniffing is another type of attack where an attacker intercepts and reads data that is being transmitted between a user's device and a website. Lastly, DDoS (Distributed Denial of Service) attacks, where multiple systems overwhelm a website's server with traffic, can also cause significant damage to an e-commerce website.

To protect an e-commerce website from these threats, it is essential to implement robust security measures such as firewalls, encryption, and regular vulnerability assessments.

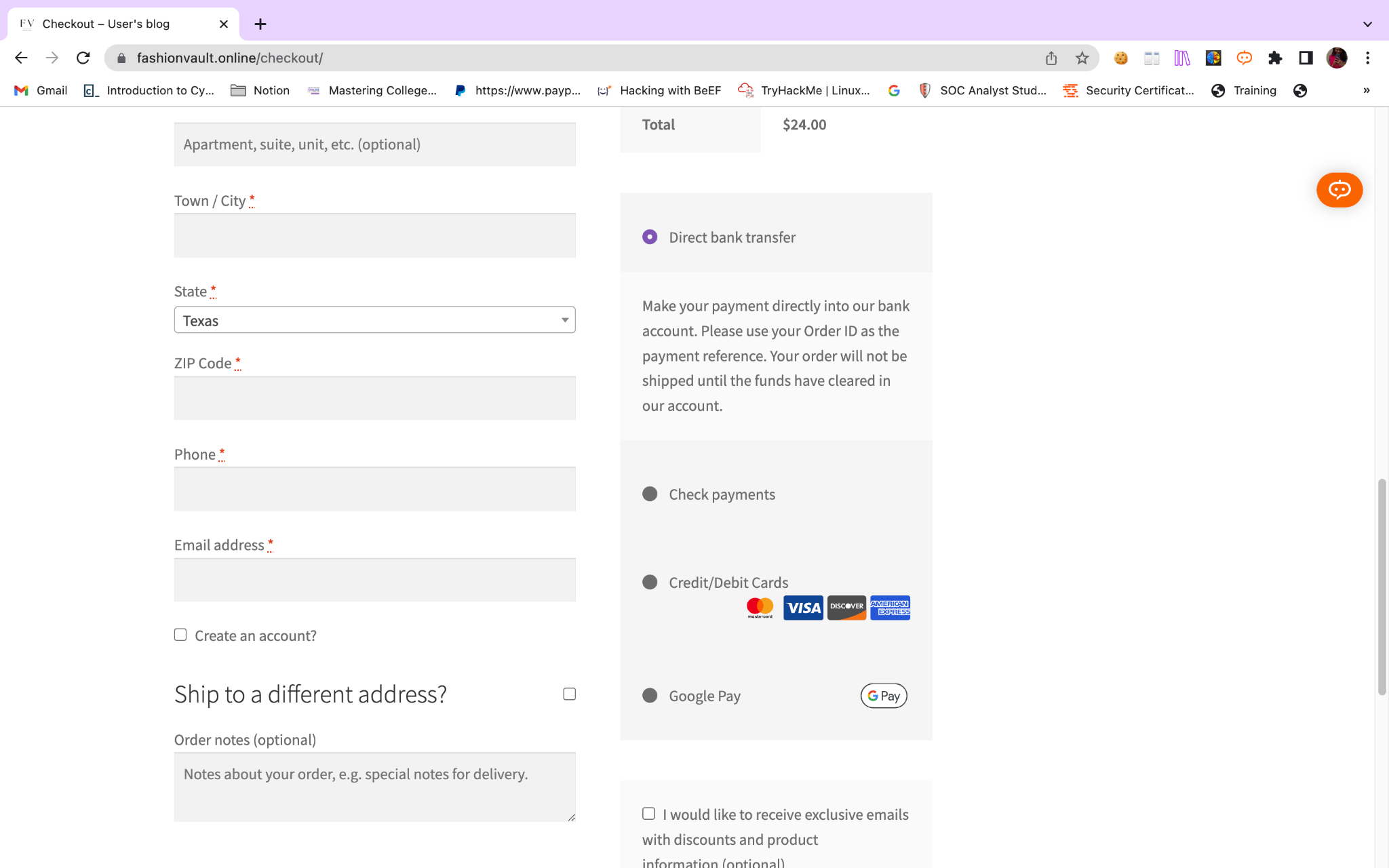
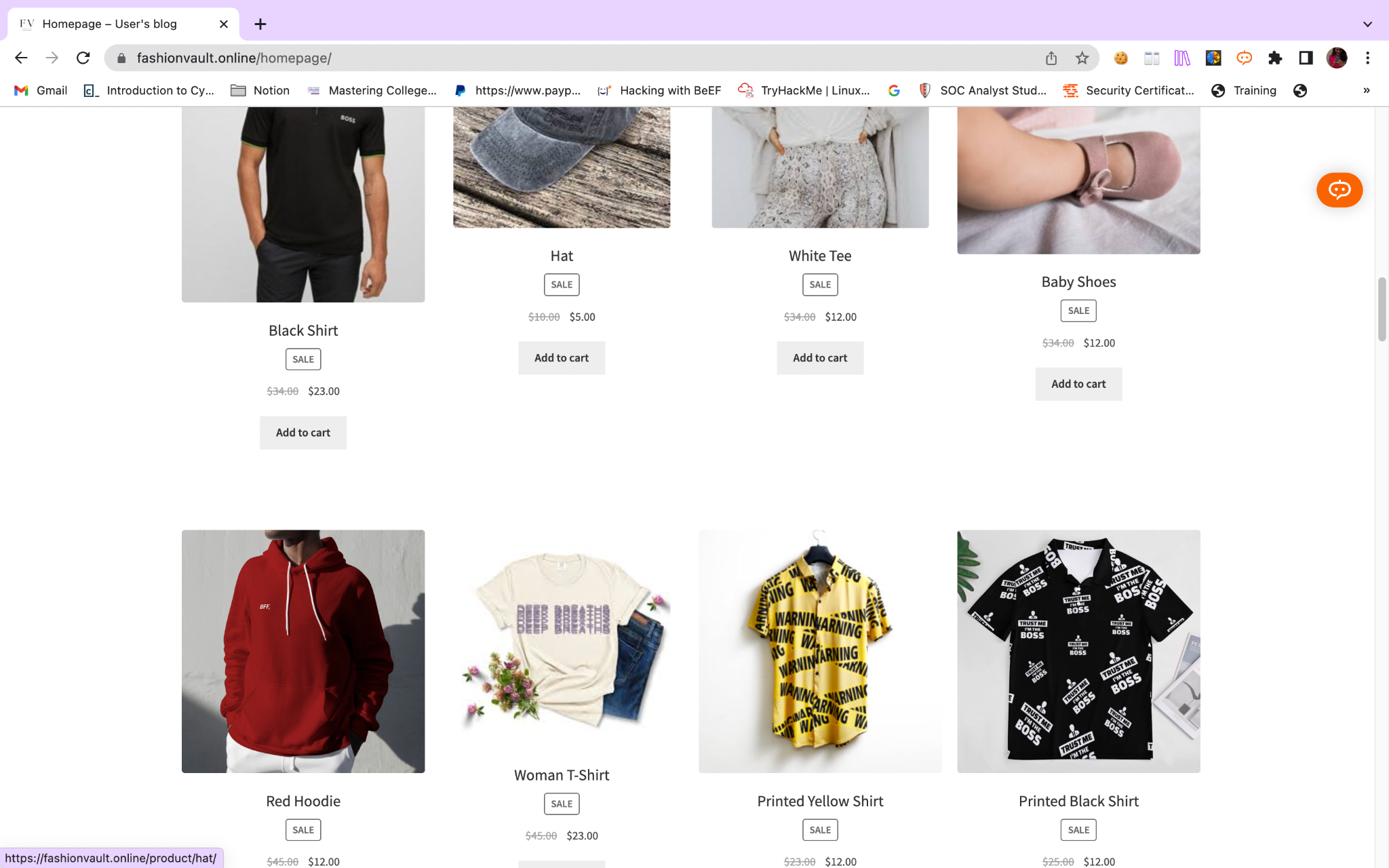
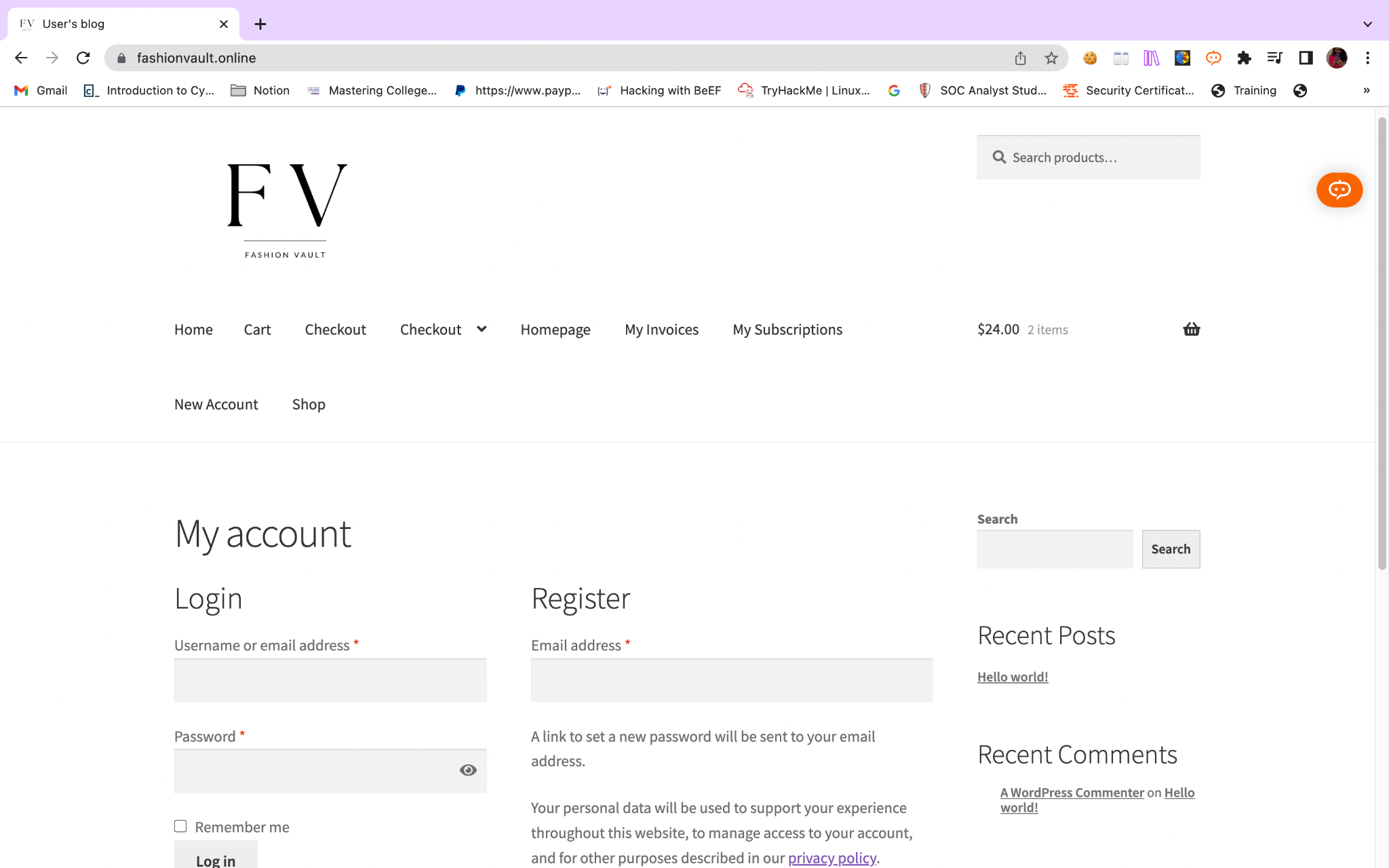
***How Does An E-Commerce Website Work?***

A typical e-commerce website works by providing customers with a user-friendly interface that allows them to browse through various products, add them to their shopping cart, and complete their purchases through a secure checkout process.Behind the scenes, e-commerce websites rely on a complex system of databases, payment gateways, and shipping integrations to ensure that orders are processed accurately and efficiently. These systems also help businesses manage their inventory, track sales, and analyze customer behavior to make data-driven decisions that can improve their overall performance



***My E-Commerce Website***

The success of an e-commerce website depends on a number of factors, including its design, user experience, and security. For my latest project, I created a website that addresses all of these factors. The website, Fashionvault. online, is an e-commerce platform that specializes in fashion apparel. It features a user-friendly interface that is easy to navigate and aesthetically pleasing. The website also offers a secure payment gateway, which ensures that customers can feel safe and secure when making purchases. I built Fashionvault.online using Microsoft Azure and WordPress packaged by Bitnami VM. These technologies allowed me to create a website that is both functional and secure. I also utilized various security and payment-related plugins to further enhance the security of the website.



I have utilized the Stripe payment gateway for my website, which is a plugin that can be found in WordPress. Not only does it act as a secure payment gateway, but it also offers various modes of payment, making it very convenient for my customers. In addition to these benefits, the Stripe payment gateway also allows me to manage and track my transactions more efficiently. This feature is especially helpful in ensuring that all of my payments are processed accurately and in a timely manner

***Major Attacks that Happen on an E-Commerce Website***

Hackers are constantly looking for vulnerabilities to exploit, and e-commerce websites are a prime target due to the sensitive information they store, such as customer details and payment information. One of the most common types of attacks is SQL injection. This type of attack involves injecting malicious code into the website's database, which can then be used to access sensitive information such as customer data or login credentials. Cross-site scripting is another major concern for e-commerce websites. This attack involves inserting malicious code into a website's HTML code, which can then be used to steal user data or perform other nefarious activities.DDoS attacks are also a significant threat to e-commerce websites. These attacks involve overwhelming a website with traffic, making it unusable, and causing significant financial harm. This type of attack can be particularly damaging to businesses that rely on e-commerce to generate revenu**e.**

***SQL Injection:***

This weakness in web security can be a big danger to keeping data confidential during e-commerce. It enables someone to change the questions an application asks its database. This lets them see data they shouldn't be able to, like private information or financial records from other users. This vulnerability can also harm the e-commerce business itself. The attacker could get hold of proprietary information, trade secrets, or other sensitive data from the application. This could lead to losing money, damaging reputation, and losing trust from customers and partners. To stop this weakness, businesses need to do a lot of things. They need to check security regularly, use secure coding, and have strong control over access. E-commerce businesses must make security a big priority for their applications and databases. By taking these steps, businesses can avoid huge problems and keep people's trust.

One of the ways in which SQL injection attacks can occur is through retrieving hidden data. Attackers can modify an SQL query to obtain additional information, such as private information or financial records from other users. This can be particularly damaging to e-commerce businesses that store sensitive data, as it can lead to a loss of trust from customers and partners. Another way in which SQL injection attacks can occur is through subverting application logic. Attackers can modify a query to interfere with the application's logic, potentially leading to unauthorized access or data loss. Union attacks are another type of SQL injection attack that involves retrieving data from different database tables. Attackers can use this method to obtain sensitive information, such as trade secrets or proprietary information.

Finally, examining the database can also be a way for attackers to obtain information about the structure and version of the database. This can help them plan their attacks more effectively and potentially gain access to sensitive information.

***Cross-Site Scripting***

Cross-site scripting (XSS) is a type of web vulnerability that can have serious consequences for websites. It happens when a website has a weakness that allows malicious JavaScript to be returned to users. When this code runs in the user's browser, the attacker can take control of their interaction with the website. They can take sensitive information from the user, change the website's content, or even control the user's browser. There are different ways that XSS attacks can happen.

They can occur through input fields that are not properly checked, or through external scripts that are included in the website's code. One common type of XSS attack is called reflected XSS, where the malicious code is shown to the user through a search query or other input field.

Another type is called stored XSS, where the malicious code is saved on the website's server and runs whenever a user accesses the affected page. To avoid XSS attacks, website owners can take important security measures such as regular vulnerability scanning, input validation, and output encoding. They should also teach their development team and website users about the risks and best practices for preventing XSS attacks. By doing these things, website owners can help protect their users' sensitive information and keep the trust of their customers and partners.

***DDoS Attacks***

A DDoS attack is when an attacker sends a lot of internet traffic to a server, making it hard for people to use connected online services and sites. The aim of a DDoS attack is to make the target's devices, services, and network unusable by sending lots of fake internet traffic.

***Application Layer DDoS Attack***

In this type of attack, the attacker targets HTTP traffic. They often use an attack called HTTP flood, where they send lots of HTTP requests at once. It's like hitting your browser's refresh button many times, but with many other people doing the same thing.

***Protocol DDoS Attack***

An example of this type of attack is the SYN flood attack. When making an internet request, three things happen a request for data (SYN), a response to the data request (ACK), and a confirmation that the data has arrived (SYN-ACK). The SYN flood attack sends many fake SYN packets from fake IP addresses, causing a denial of service.

***DNS Amplification Attack***

These attacks exploit open DNS servers' vulnerability to send a lot of traffic to the target server. The result is that the server gets overwhelmed and cannot respond to legitimate requests. Once the attacker successfully weakens the target server, they can launch more attacks and gain access to sensitive data.

As the Fashionvault.online website was built using Microsoft Azure it has a strong firewall prebuilt and a DDOS prevention mechanism the attacks were not successful hence making my website a secure website how I did a Vulnerability Assessment using OpenVAS, OWASP ZAP, and NMAP

***OPENVAS SCAN:***

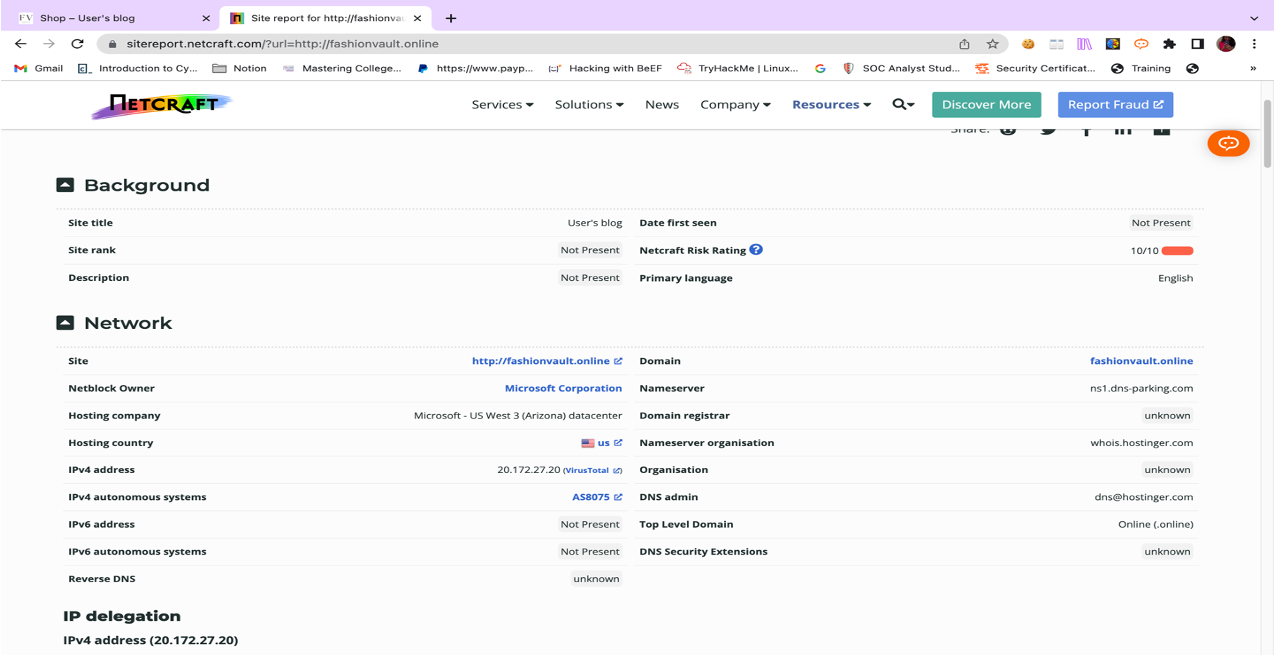
OpenVAS is a comprehensive vulnerability scanning system that is designed to identify and report security problems in various types of servers and network equipment. It is an open-source tool that can detect security vulnerabilities in network infrastructure, operating systems, and applications. The tool uses a variety of checks to evaluate the security posture of the target system, and it provides a detailed report of the vulnerabilities that it has detected.

***OWASP ZAP:***

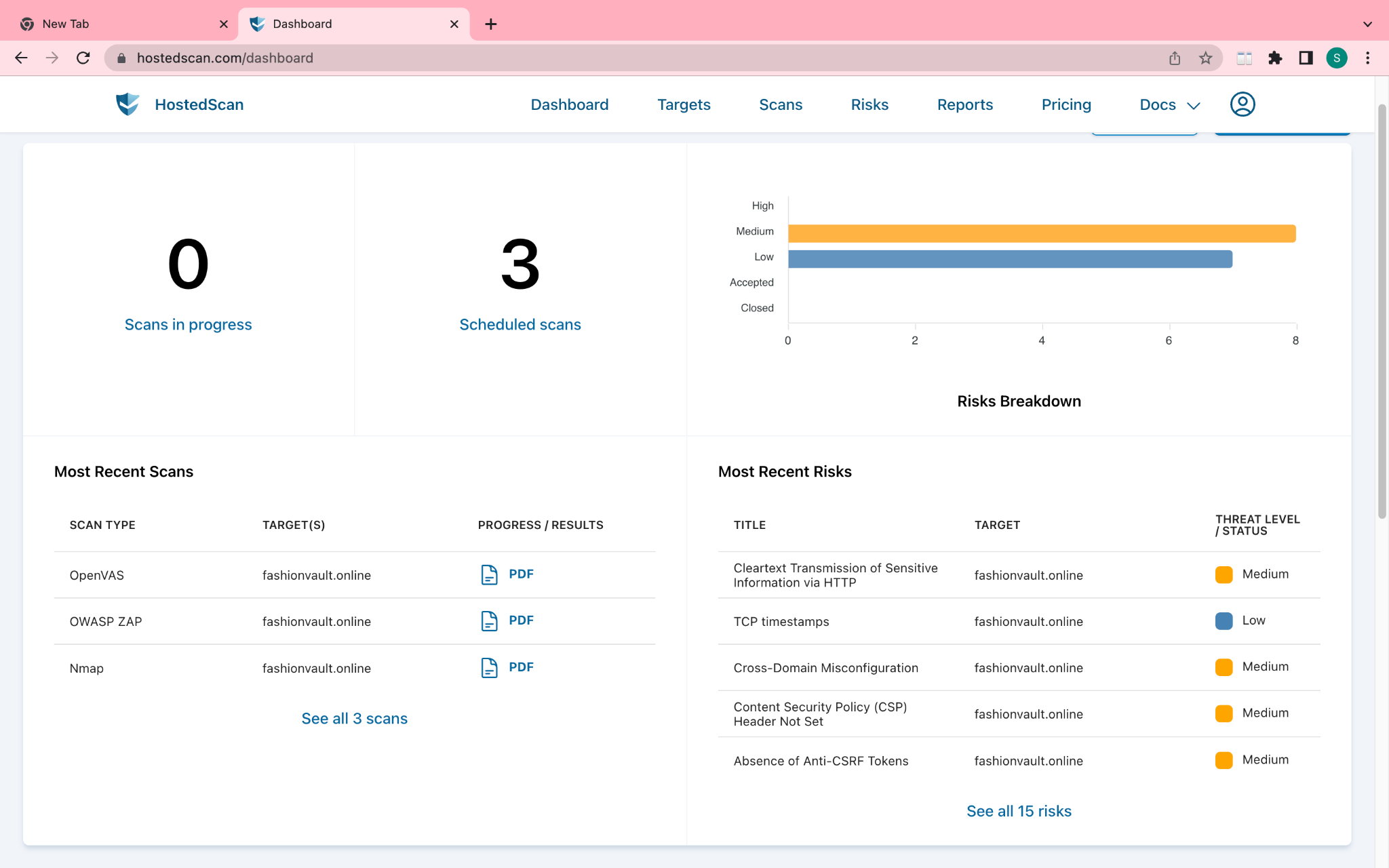
OWASP ZAP is an open-source web application security testing tool that is used to identify and fix security vulnerabilities in web applications during the development and testing stages. It provides an intuitive and user-friendly interface that allows developers and security professionals to assess the security of their web applications. OWASP ZAP has a wide range of scanning capabilities that can detect a variety of vulnerabilities in web applications, including SQL injection, cross-site scripting, and other common web application vulnerabilities.

***NMAP:***

Nmap is a powerful network exploration and security auditing tool that can be used in vulnerability assessments. It is not a dedicated vulnerability scanner, but it can identify open ports, services running on those ports, operating systems, and network topology. Nmap is a versatile tool that can be used for a wide range of tasks, including network inventory, monitoring, and troubleshooting. It is an open-source tool that is widely used in the security community, and it is supported by a large and active user community that contributes to its development and maintenance.



Shows all the details nd the risk rating of the website



Altogether 15 Risks were found all of them being medium and low.So in order to mitigate those I have added the following:

SECURITY PLUGINS

WP SECURITY PLUGIN

SSL CERTIFICATE

LIMITED LOGIN ATTEMPTS

2FA- 2 Factor Authentication

References:[www.fashionvault.](http://www.fashionvault.io)online

Hostedscan.com

Netcraft.com