Safeguarding Information Systems: An Analysis of Security Flaws, Attacks, and Techniques

Madhav Prabhu[1], Neha Nihana[1], Samiha Najah[1] and Samiha Najah[1#]

[1]Middle East College, Muscat, Oman
[#]Advisor

ABSTRACT

A crucial component of contemporary computing involves guaranteeing the security of information networks. This study paper provides a thorough examination of various security flaws, attacks, and techniques that can be employed to lessen the impact of such attacks. This report names three vulnerabilities discovered in the earlier stages by utilizing well-known Vulnerability Scoring Systems and Databases like Common Weakness Enumeration (CWE). The study of three security attacks that are capable of taking advantage of vulnerabilities is presented in the report's opening section, along with a thorough explanation of the risks involved. Threats like malware attacks, SQL injection, cross–scripting attacks, and man-in-the-middle attacks are included in this study. Along with the steps to perform footprinting of publicly accessible information and the scanning phase for finding vulnerabilities, the paper also offers a thorough discussion of three different methods. Three techniques for listing usernames, group details, and network shares of networked computers are also covered in the study. This study paper offers a thorough analysis of security attacks, Vulnerabilities, and solutions, making it a vital tool for people and organizations trying to protect their information systems.

Introduction

Cybersecurity is now a top stress among companies worldwide in the modern digital era. Detection of possible weaknesses and attack paths is essential for organizations for safeguarding their computer networks. Network reconnaissance is a critical procedure that helps companies to discover information regarding their target networks and identify potential security holes that hackers can attack. The three primary methods used in the reconnaissance of networks are footprinting, scanning, and enumeration.

Without communicating with the target system, footprinting involves collecting details about it, such as Whois search, DNS enumeration, and web server fingerprinting. Scanning, which includes scanning of ports and vulnerability scanning, is more invasive than footprinting and requires sending packets to the computer system in order to identify any potential vulnerabilities. Enumeration, including NetBIOS enumeration, is the method of learning details about the system being targeted by interacting with it. Due to its intuitive user interface and comprehensive feature collection, such as host identification and port scanning, Zenmap is a well-liked scanning application. user accounts, groups, and various other crucial data may be obtained through the widely used NetBIOS enumeration program.

Attackers employing network reconnaissance methods are exposed to a variety of vulnerabilities, such as Insecure Transportation Security Protocol Supported, missing X-Frame-Options headers, and source code leakage. various risks, such as cross-scripting attacks, man-in-the-middle attacks, and SQL injection attacks, can arise from these vulnerabilities. Organizations may take the necessary measures to secure their computer systems by recognizing these weaknesses and methods of attack. Organizations can take the required actions to defend their networks against potential attacks by recognizing these vulnerabilities and

attack strategies. assists network reconnaissance can assist find potential weaknesses and enhance network security.

Footprinting

The technique of "Footprinting" includes gathering information on a goal, such as a computer system, network, or website, to better comprehend it and possibly spot vulnerabilities. This could be done for several reasons, including security testing, cyber espionage, or just to use it to know the target better. Footprinting methods can comprise acquiring data from public sources like business websites and social networking profiles, in addition to more technical ones like network scanning and DNS record analysis.

Technique 1: Whois Lookup Using Domain Tool

Whois Footprinting includes information well about the target domain, along with its owner, registrar, name of the server, information regarding the registration, contacts, etc. With the use of this understanding, a network map of the company may well be made, the internal network data can be retrieved, and attacks like social engineering can be carried out.

Steps to Perform Whois Lookup Technique

Domain tool is used to conduct Whois Lookup to acquire the data.

- STEP 1: Open a web Browser of your choice. Enter the following address in the address bar: http://whois.domaintools.com.
- STEP 2: Type https://dvwa.co.uk/ into the search box marked as "Enter a domain or IP address..." and click on Search. (Figure 1)
- STEP 3: Review the information that will be presented regarding the domain's owner, registrar, name server, user profiles, contact details, etc. (Figure 1a to 1c)

Figure 1. Type https://dvwa.co.uk/ into the search box marked as "Enter a domain or IP address..." and click on Search.

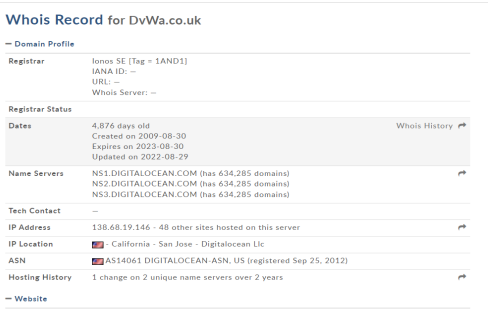

Figure (1a)

Figure (1b)

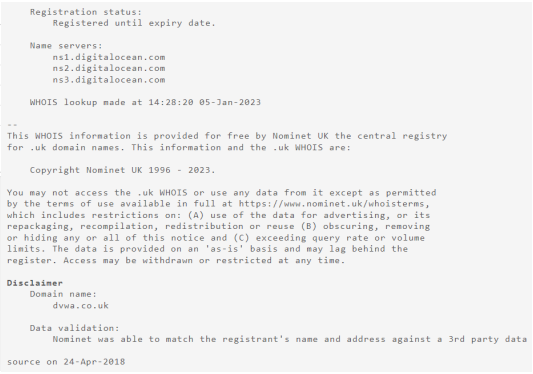

Figure (1c)

You can discover the identity of the holder of a domain name or IP address by executing a WHOIS lookup. Because it may educate you on details about the target and even perhaps reveal weaknesses, this data is beneficial for Footprinting. You will be able to access the following information via a WHOIS lookup:

- The domain name registrant's name and contact details
- The domain's technical and administrative contacts' names and phone numbers
- The domain name servers' name servers
- Both the domain's registration and expiration dates are included here.
- The domain's registrar

Scanning

Identification and recording of a target's qualities and characteristics is the process of scanning. In terms of cybersecurity, the technique of discovering and cataloging the properties and characteristics of a computer network, system, or website for better comprehending it and possibly spotting vulnerabilities is called scanning. When beginning a cyberattack, scanning can be a significant stage because it allows the attacker to discover details about the target and detect any potential vulnerabilities. Network scanning, port scanning, and vulnerability scanning are just a few of the numerous scanning techniques that can be deployed.

To perform scanning, two VMs are used which are EH-Client and EH-server. Both the client and server are connected to the same internal network. All the scanning tools are installed in the client machine.

Technique 1: Zenmap Also Known as The Nmap Scanning Tool

Attacks make use of Nmap to extract information like a network that has live hosts, Open ports, and services that are available along with the application name and its version, the type of packet filters available, and also about the type of operating system used and its version. Network administrators and cybersecurity specialists frequently use Nmap (short for "Network Mapper"), an open-source and free network scanning application, to identify and assess network resources as well as to identify vulnerabilities. To conduct a cyberattack, attackers might also utilize it to gather data about a victim's network or system.

Nmap is used by attackers in a variety of ways, including:

- A method for searching a network for active hosts and open ports that might be used by an attacker to locate targets or points of access.
- Version detection is the procedure of discovering the software and versions that are being utilized on the target system, which may also assist the hacker in locating known vulnerabilities they can exploit.

- Doing tasks like brute-force password cracking or vulnerability scanning with Nmap scripts.

Steps to Perform Nmap Scanning Tool

- STEP 1: Open the Nmap Scanning tool from EH-Client Machine.
- STEP 2: Enter the IP address 192.168.1.2 and profile as Intense Scan and Click Enter.
- All the Active ports, Open Ports, and Versions of the Operating System will be published after scanning is completed.

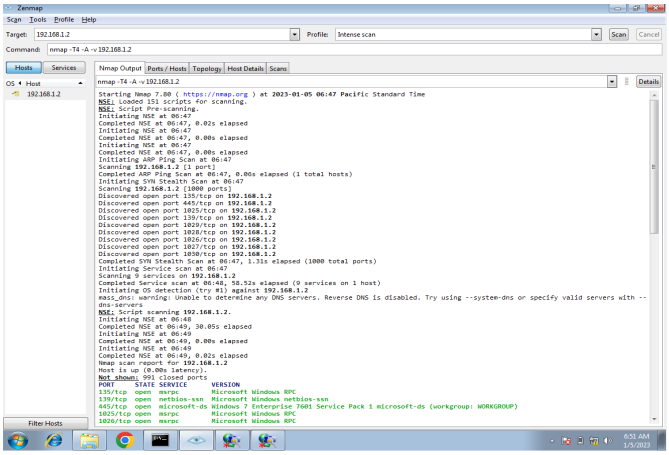

Figure 2. Showing All the open Ports.

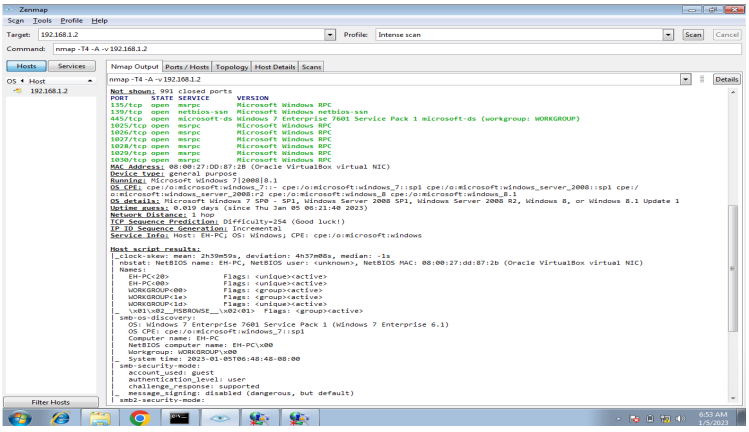

Figure (2 a)

Possible Vulnerabilities that are identified are listed Below:

- 7 different open ports are shown after the scanning. (By checking which open port is vulnerable, we can attack the system)
- The state of each Port is shown along with its version.
- After Scanning, the OS is revealed along with its version which is Windows 7.
- Through Which user we have logged in is provided as Guest User
- Traceroute is provided along with the HOP count.
- Mac Addresses are provided.

Enumeration

Enumeration is indeed the method of continuously gathering data about a specific system or network in the topic of networking and cybersecurity. Enumeration may be performed lawfully as a component of network management, security testing, or for any other legitimate reasons. It may also be a component of violent action, such as a cyberattack when the hacker attempts to learn as much, as they can about the victim to find weaknesses they can exploit. There are different kinds of enumeration like SNMP enumeration, DNS enumeration, etc. To perform enumeration, two VMs are used which are EH-Client and EH-server. Both the client and server are connected to the same internal network. All the tools for enumeration are installed in the client machine.

Technique 1: NetBIOS Enumeration Tool

NetBIOS enumeration tool helps to enumerate data for IP addresses within a range like usernames, groups, Domain Names, and also NetBIOS names.

STEP 1: The NetBIOS tool will appear on the screen when we click on the tool from EH- Client machine.

STEP 2: Provide the IP address range from 192.168.1.0 to 192.168.1.255 under “IP range to scan”.

STEP 3: The scanned results can be seen in the left pane.

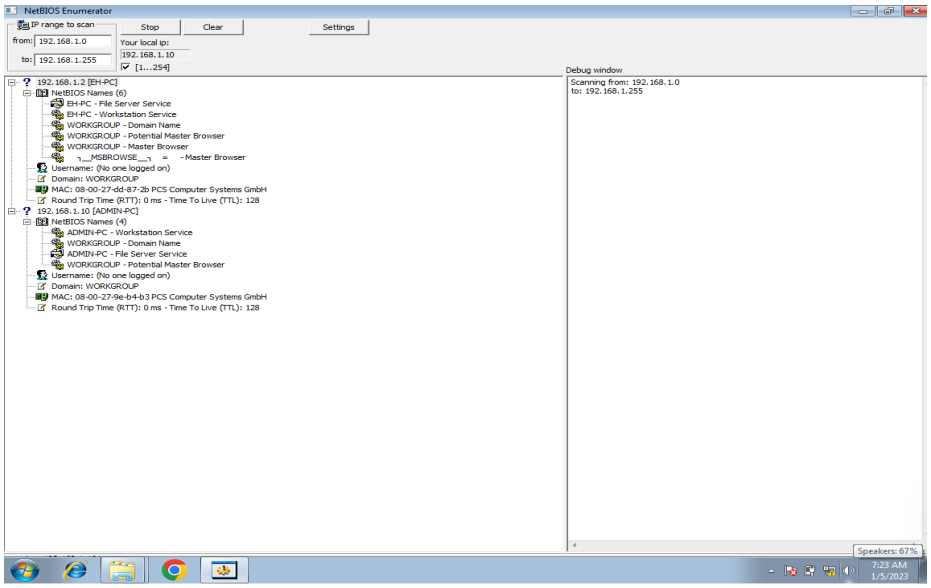

Figure 3. Providing all the information about the usernames, the workgroup is mentioned, and the Mac address is provided.

Common Vulnerabilities

Vulnerability Found: Missing X-Frame-Options Header

Risk: Low

Description:

The X-Frame-Options HTTP header field represents a policy that determines if the sent content must be rendered by the user in an iframe or a frame. To prevent clickjacking attacks and guarantee that the information is not injected into other sites or frames, servers should express this strategy in the header of their HTTP responses. Your software pages can be integrated without restrictions in any other website whenever the X-Frame-Options Header is not set, for example, to generate a harmful website with your original programming enhanced with risky elements like adverts, clickjacking code, and phishing efforts. Threats involving clickjacking are prevented by using the "X-Frame-Options" HTTP header. A clickjacking attack normally occurs whenever a client is misled into clicking an icon or link on a page which is not what they believe it is. This could be accomplished by placing an invisible page over the site that the client is actively communicating with, or through integrating the page in a manner that prevents the client from seeing what they're interacting on using the HTML elements <frame>, <iframe>, or <object>. (Saleem,2021)

Attacks like Clickjacking attack exploit these kinds of vulnerabilities:

ClickjackingAattack

A clickjacking attack misleads an individual into clicking a component of a webpage that's also hidden or portrayed like another component. Because of this, clients may inadvertently download malware, access fraudulent websites, offer confidential material or login credentials, transfer cash, or interact with the internet. The most popular method of clickjacking is to overlay the page the user can view with an opaque page or HTML element that would be presented within an iframe. In actuality, the client is clicking an unseen element on the supplementary page that is inverted on top of the apparent page when they think they are accessing the visible page. (Imperva, 2019)

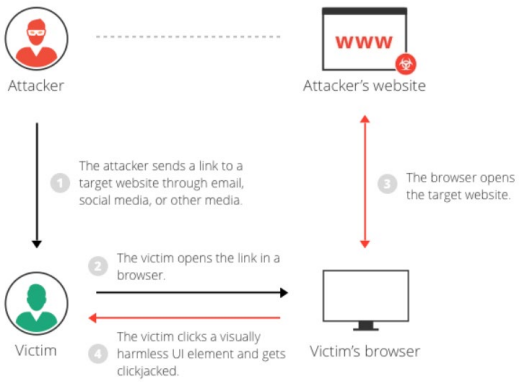

Figure 3. How Clickjacking Attack works. (Imperva, 2019)

The above figure shows that the malicious activity was performed by the user when the user was accessing their account. (Imperva, 2019)

The Risk Associated with Cross-Site Scripting (XSS) Attack Includes

Attacks such as "clickjacking" disguise a harmful application link inside an unnoticeable frame, thereby making them difficult for frequent users to recognize. Effective clickjacking attacks pose the threat of revealing a customer's details, like credit card information or login information. Since the fraudulent page or feature

must be engaged physically by the user, the clickjacking vulnerability is regarded as a medium risk; nevertheless, the seriousness of an attack varies based on the application environment, the user accesses exposed, and the type of data gathered.

- Unintentional download of malware
- Unknowingly visiting malicious web pages.
- Share all the sensitive information.
- Location Exposure.
- Activation of Microphone or Webcam (Sengupta,2022)

Vulnerability Found: [Possible] Disclosure of Source Code

Risk: Medium

Description:

A significant source code disclosure was discovered by Netsparker (Generic).

A hacker has access to the server-side source code of the online application, which may contain both business and technical functionality as well as confidential material like database connection strings, usernames, and passwords. Critical information is highly prevalent in source code. It may include information surrounding the web application's operation or configuration-related data, like database access. If source code sources are released publicly, an attacker might utilize this information to find logical flaws. Without exposure to the user's source code, this might become out of control and culminate in a series of attacks. Attacks like SQL injection exploit these kinds of vulnerabilities. (Birgjaj,2019)

SQL Injection

An injection attack known as SQL Injection (SQL) facilitates the execution of malignant SQL commands. These commands handle a database server that sits on top of a web application. SQL Injection flaws enable an attacker to work around application security safeguards. The full information of a SQL database can indeed be downloaded by getting around the identification and authorization of a web page or online application. They could also add, alter, and remove data in the database using SQL Injection (Birgjaj,2019). Another occurrence is when confidentiality, like API secret keys or login information, is defined in the public code. Hackers can easily undermine these systems or make these unreachable to legitimate people by using this information. Internal IP addresses are a whole other source of data that is commonly given after information disclosure, providing hackers the opportunity to recognize and understand the internal network topology. The internal structure and application logic of an application may be found relying on the source code, database connection strings, usernames, and passwords.

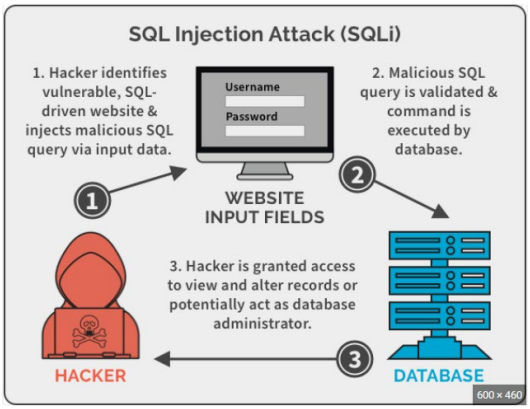

Figure 4. SQL Injection Altering the Source Code (Oza,2020)

Whenever the source code is disclosed, the attacker gets access to the database of the application, and hence, by using the SQL injection, it will inject malicious SQL query through input data. The Malicious SQL is then executed into the database as valid. Now, the attacker will take over as a database administrator to get access to every confidential data. Attackers could become administrators of the database server, spoof attributes, alter already-existing data, start causing complete rejection problems like canceling transfers or shifting balances, permit complete transparency of all data on the system, corrupt information, or otherwise, make it inaccessible, and cause condemnation issues. (Kingthorin, n.d)

The Risk Associated with SQL Injection Include

- Sensitive data gets exposed.
- Data Integrity will be compromised as it can alter the data from the system.
- Privacy of the user is compromised. Depending on the data available, attackers can expose sensitive information that includes passwords, and credit cards.
- Giving Access to the attacker (Kaspersky,2022)

Vulnerability Found: Insecure Transportation Security Protocol Supported

Risk: Low

Description:

Insecure Transportation Security Protocol (TLS 1.0) that supports the web server was detected by the Netsparker. The protocol's initial launch, TLS version 1.0, came out in 1999. Subsequent iterations of the protocol had already overtaken TLS 1.0. (TLS 1.1, TLS 1.2, and TLS 1.3). Due to a variety of weaknesses that have been found in the protocol, TLS 1.0 is recognized as being extremely unsafe. In contrast, TLS 1.0's lower message authentication method (MD5) increases its susceptibility to cyberattacks. Connection Failures can be caused by the attack and hence can trigger the use of TLS 1.0. TLS 1.0 has a weak hash function, No Perfect Forward Secrecy which means that the private key of the server can be compromised, No Support for AES-GCM, and No Certificate Transparency. TLS 1.0 is more prone to Man in middle attacks in which they can monitor the encryption traffic that is passed through your website of yours and its visitors.

Attacks like Man-In-The-Middle attacks exploit these kinds of vulnerabilities.

Man-in-The-Middle Attack

An attack known as a "man-in-the-middle" (MITM) allows the attacker to eavesdrop on confidential messages exchanged between two or maybe more endpoints and ultimately change the content of these interactions. (Invicti,2022) a man-in-the-middle mechanism to retrieve the shared key by inserting chunks of plain text transmitted by the user's website into the encrypted request channel. JavaScript connected to a fraudulent advertisement sent via a Web ad service, an IFRAME in a link-hacked website, an ad, or even other programmed elements on a website are 2 methods that by the code can be delivered into the user's browser. The victim's AES-encrypted requests, comprising encrypted cookies, will then be decrypted by using known text blocks by BEAST, who will then utilize the information obtained to take over the no longer secure network.

However, BEAST typically requires sessions of at least 30 minutes to decode cookies with keys greater than 1,000 characters. (Schneier,2011)

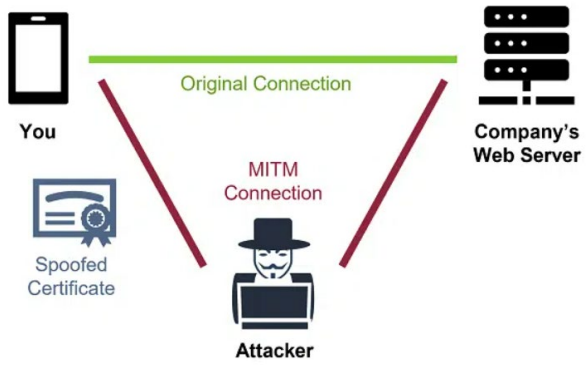

Figure 5. Man in the Middle Attack (Comodo, n.d)

An instance of a "guy in the middle" attack is the "coffee shop" attack (MITM). Therefore, in case, a coffee shop-based hacker could put up a laptop to transmit a Wi-Fi connection that looks exactly like the Wi-Fi in the coffee house. Ultimately, the target accidentally accesses the assailant's Wi-Fi rather than the Wi-Fi of the coffee shop. All of the suspect's internet traffic has become susceptible to being monitored and recorded by the hacker if they are using TLS 1.0 or earlier. If indeed the communication was encrypted, this kind of attempt would often be avoided. But potentially, it would be feasible to monitor the data and/or spoof one's communications owing to the vulnerabilities in TLS 1.0. (Comodo, n.d)

The Risk Associated with Man-in-The-Middle Attack Includes

Hackers have access to sensitive material including.

- Usernames
- Passwords
- Credit card numbers, and bank account information via man-in-the-middle attacks. It is indeed risky since this user is uninformed about the existence of a third-party interfering with their engagement with the application but rather that their data is just being forwarded to a dangerous party.
- Once each thief obtains exposure to this data, they may modify account credentials, commit fraud, or carry out unlawful transactions. Due to their breadth, MITM attacks generally target clients of SaaS platforms, online shops, and banks. (Magnusson,2022)

Recommendation

Security awareness training is a good method to stop employees from falling prey to these kinds of scams by periodically instructing them on how to spot and fend against social engineering attempts. Policies and Processes can minimize the danger of cyber security attacks by implementing clear guidelines and procedures for protecting critical data and reacting to information requests. Two-factor authentication is a good method because even if an intruder obtains the user's login credentials, using 2FA can assist avoid accidental access to accounts. Encryption: Protecting sensitive information and messages from becoming captured and viewed

by unauthorized individuals can be accomplished by encrypting them. Regular updating and servicing can help stop vulnerabilities from becoming attacked by ensuring that all equipment and software are upgraded with the most recent security patches.

Conclusion

In conclusion, network reconnaissance is a significant technique for discovering potential vulnerabilities and attack pathways in computer networks. The three basic methods for network reconnaissance are footprinting, scanning, and enumeration. The most common techniques used for scanning and enumeration, respectively, are Zenmap and NetBIOS enumeration tools.

In addition, a variety of weaknesses such as the Insecure Transportation Security Protocol Supported, the missing X-Frame-Options header, and the source code disclosure, can be taken advantage of by attackers via network reconnaissance techniques. Cross-scripting attacks, man-in-the-middle attacks, and SQL injection attacks are only some of the dangers that could arise from these vulnerabilities. It is of the utmost importance that one puts into effect the necessary safety measures, such as routine software updates, safe coding techniques, and secure transport protocols, with the goal to mitigate these risks. Organizations ought to perform routine network reconnaissance to find any possible vulnerabilities and promptly repair them.

Overall, protecting computer networks versus prospective threats involves a vital method called network reconnaissance. Organizations may enhance their computer system security and resist possible attacks by taking appropriate safety measures after knowing various strategies and weaknesses.

References

Saleem, F. (2021, August 23). *How can I prevent ClickJacking attacks using X-frame-Options headers*? Stack Overflow. https://stackoverflow.com/questions/68895913/how-can-i-prevent-clickjacking-attacks-using-x-frame-options-headers

Imperva. (2019, December 29). *Clickjacking*. Learning Center. https://www.imperva.com/learn/application-security/clickjacking/

Schneier. (2011, September 23). *The man-in-the-Middle attack against SSL 3.0/TLS 1.0.* Schneier on Security. https://www.schneier.com/blog/archives/2011/09/man-in-the-midd_4.html

Sengupta, S. (2022, September 12). *【Clickjacking prevention 】What is this attack and what examples*? Crashtest Security. https://crashtest-security.com/clickjacking-attack/#:~:text=typical%20clickjacking%20attack.-,Risk%20and%20impacts%20of%20clickjacking%20attacks,card%20numbers%20or%20login%20credentials

Synospys. (n.d.). *How does cross-site scripting work?* https://www.synopsys.com/glossary/what-is-cross-site-scripting.html#:~:text=Cross%20site%20scripting%20(XSS)%20is,the%20user%20to%20click%20it

Sengupta, S. (2022, September 12). *【Clickjacking prevention 】What is this attack and what examples*? Crashtest Security. https://crashtest-security.com/clickjacking-attack/#:~:text=typical%20clickjacking%20attack.-

,Risk%20and%20impacts%20of%20clickjacking%20attacks,card%20numbers%20or%20login%20credentials

Birgjaj, J. D. (2019, May 9). *Why is source code disclosure dangerous?* Acunetix. https://www.acunetix.com/blog/articles/source-code-disclosure-dangerous/

Oza, S. (2020, February 4). *SQL injection attacks — web-based app security, Part 4*. Spanning. https://spanning.com/blog/sql-injection-attacks-web-based-application-security-part-4/

Kingthorin. (n.d.). *SQL injection.* OWASP Foundation, the Open Source Foundation for Application Security |OWASP Foundation. https://owasp.org/www-community/attacks/SQL_Injection#:~:text=SQL%20injection%20attacks%20allow%20attackers,administrators%20of%20the%20database%20server

Kaspersky. (2022, September 30). *What is SQL injection? Definition and explanation*. www.kaspersky.com. https://www.kaspersky.com/resource-center/definitions/sql-injection

Comodo. (n.d.). *TLS 1.0 is no longer used to secure communications | PCI compliance*. comodo.com. https://www.comodo.com/e-commerce/ssl-certificates/tls-1-deprecation.php

Mangusson, A. (2022, December 20). *Man-in-the-Middle (MITM) attack: Definition, examples & more*. StrongDM | Connect Your Team to Anything. https://www.strongdm.com/blog/man-in-the-middle-attack#:~:text=The%20Danger%20of%20Man%2Din%2Dthe%2DMiddle%20Attacks&text=Once%20a%20criminal%20has%20this,service%20(SaaS)%20platform%20customers