2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS) | 979-8-3503-9737-6/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICACCS57279.2023.10112741

Web Security and Web Application Security: Attacks and Prevention

[1]Bhuvana Reddy Bhimireddy, [2]Alekhya Nimmagadda, [3]Harshith Kurapati, [4]Leelendra Reddy Gogula, [5]Radhika Rani Chintala, [6]Vijaya Chandra Jadala
Department of Computer Science and Engineering
Koneru Lakshmaiah Education Foundation
Guntur, Andhra Pradesh, India
[1]reddybhuvana24@gmail.com, [2]alekhyanimmagadda63@gmail.com, [3]harshithkurapati@gmail.com, [4]leelendrareddygogula08@gmail.com, [5]radhikarani_cse@kluniversity.in, [6]vijayachandra.phd@kluniversity.in

***Abstract*—The everyday life of a person goes on with the assistance of the internet at present. Without the internet, there is nothing that a person can do. As the days of the internet are evolving, the threats related to the internet are getting more rapid. Web applications are generally used over the internet which helps the users to provide their requested needs. As they are used over the internet, they are liable to many cyber-based attacks. Many security techniques have been developed over the years to build up the protection of web applications. Web application threats include both passive and active attacks. Prevention includes using various tools, applying security standards while building and measuring time-to-time risk factors, and acting based on them. In this article, we discussed some of the major threats to web applications and presented some better ways to ensure our web application is secure from the threats and vulnerabilities found on the internet.**

Keywords—Attack, Vulnerability, Threat, Security, Confidentiality, Integrity, Firewall

I. INTRODUCTION

Globally people living across the world are using the internet effectively. Few of them are using the internet for malicious and illegitimate activities. For many years there have been many attacks like Personal Computer (PC) hacking, data robbery, and tormenting/stalking. If the security of web applications is not taken seriously, there will be a lot of personal information shared/hacked into bad hands during cyber-attacks which are getting increased every year resulting in absolute chaos. Fig. 1 shows the number of attacks that an organization experiences in the years 2020 and 2021 for each quarter of the year. From the first quarter of 2020 to the fourth quarter of 2021, we can observe a sharp increase in cyberattacks. Security is the most pivotal aspect of any application, whether it's a hardware or software application. Here, we are going to deal with security related to web and web applications. As today's daily life goes on with the help of computers, most of the applications we use are related to the web and significant use was done in browsers. While using web applications, we always have doubts about whether our data is secure, am I entering my data on the right website, or are we secure enough to enter our data here in the application. The data we enter on the web is permanent. Even if we delete the data, there is always a chance that it might get stored someplace physically or virtually. Whenever we talk about web security, we always talk about threats, vulnerabilities, and confidentiality.

- Threats refer to the attacks that can happen to the web or web applications. In more simple terms, they are the most common means of malfunction of an application.
- Vulnerabilities refer to the loopholes of an application where an attacker can exploit the source and gain access to something which he/she doesn't have earlier [1].
- Confidentiality simply is the way how our data is getting secure or how our data is kept private from public access [2].

Website security indicates the security of both personal and organizational-facing websites from cyberattacks. Website security's main aim is to ensure that the website data is safe and secure, not easily disclosed to cyber criminals and to prevent the misuse of the website [3].

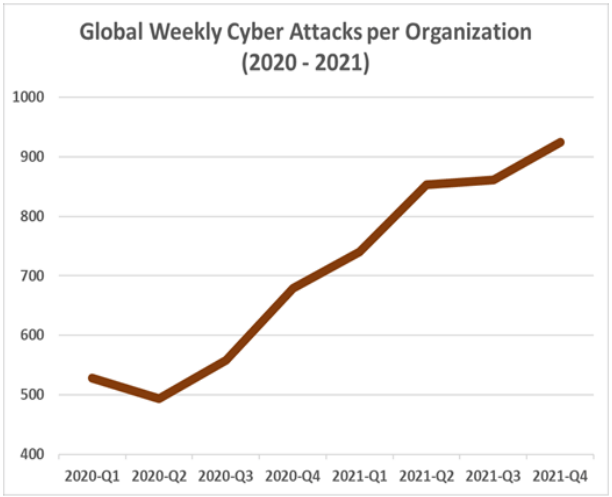

Fig. 1. Cyber Attacks comparison (2020 vs 2021)

Threats not only come through the source of the internet but sometimes they can also be injected through unprotected hardware. For reference, if some unprotected

979-8-3503-9737-6/23/$31.00 ©2023 IEEE

external storage is mounted to the server system, in case there is no protection from these external devices, there is always a chance that some corrupted file or an intended file will cause havoc. It can be from any hardware not only from storage [4].

Web Applications generally store their data in storages called databases (DB) in either remote locations or server rooms. The data stored in the databases can be used in various ways by any person who has access to them. The terms in which how he uses will define whether the person is an authorized user or an intruder. These databases are the primary sources the attackers focus on since all the data is stored in this location and if this database can be infused, then all the information of the organization and information of users can get into a data breach.

The information kept in the databases of the web applications is used for many different things in addition to being kept in the databases themselves. Web applications and services need to be protected for this reason. Cyberattacks of all kinds, including Structured Query Language (SQL) injection, cross-site scripting, data leakage, code espionage, password guessing, botnet-based attacks, and application denial of service, are prevalent in the web security industry.

II. Literature Review

This section deals with the various attacks against web applications that cause major damage.

A. SQL Injection

As many web applications use SQL-related databases (MySQL, Oracle DB, Microsoft SQL Server, etc.,) for storing data about various fields in an application, an attacker tries to find vulnerabilities or get access to the database in order to modify the data about the fields or gather data from database and use it a distorted way for threatening users, or website owners [5].

B. Password Breach

Password breach is a common type of attack that happens on a web application where the attacker tries a brute-force method to crack the password and get access to the application or the attacker tries to login into the application by entering the credentials that an application user uses to login into another application [6].

C. Data Breach

In general, data breaches are the most effective way of finding vulnerabilities in a system. When a data breach happens, the attacker finds the data that is useful to outbreak the application [7].

D. Code Injection

Code Injection is a method where an attacker finds a weakness in the application and modifies the source code which helps the attacker control the system/software/hardware [8].

E. Remote File Inclusion

It is a method where a hacker/attacker simply includes external links/external files in the client-side code by finding some vulnerability in the application and trying to capture details like passwords or trying to implant malware in the user's system [9].

F. Malware Attacks

It is one of the most common attacks in the cyber security aspect. It is something that interrupts the network through a vulnerability. When a user clicks on an illegal link, a file with a virus will be downloaded automatically and corrupt the files from inside.

G. Phising Attacks

It is a cyber-attack where the attacker portrays himself as trustworthy and loyal but sends fake emails to his victims. While the victim is heedless and if he clicks on the link that was sent by the attacker then the attacker can get access to all the credentials and important files within split seconds [10].

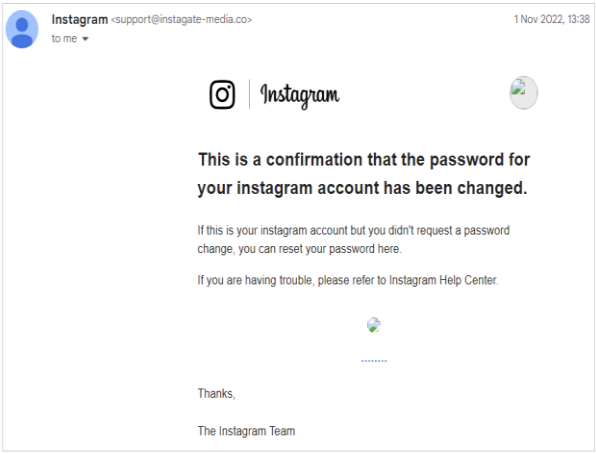

Fig. 2. Fake email with name of Instagram

We can see from Fig. 2 that the email was sent from support@instagate-media.co, which is not the actual email address that Instagram uses to send mails to its users. By clicking on the "reset your password" link, we will be redirected to a website that resembles like an original Instagram page. In case we type the password, the hacker will be able to record the user credentials and use it for illegal activities.

H. Man-in-the-middle

This type of attack occurs when an attacker comes between two parties who are interacting as shown in Fig. 3, the attacker hijacks the session between a client and the host, allowing attackers to steal and manipulate data [11].

Fig. 3 shows an interaction going between the client and the server. A session is established for this communication to take place. Now, the attacker tries to expropriate the session and manipulates the data.

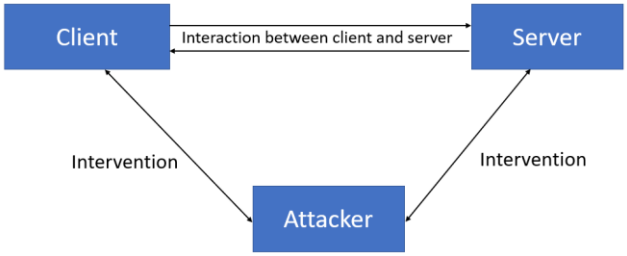

Fig. 3. Man in the Middle

I. Active Attacks

These attacks are the part of man in the middle attack. In active attacks, the attacker attempts to change or transform the content of messages or information. Active attacks are further divided into types. They are

1) Replay: Here, the attacker captures the data that is getting transmitted and then the attacker may resend it to the destination party

2) Denial of Service: When two people are communicating with one another, the attacker prevents the message being delivered to the another person.

3) Masquerade: When there are two parties and an attacker, the attacker sends the message in the name of the first person and the receiver gets the message in the name of first person.

4) Modification of Message: In this case, the attacker tries to modify the message sent by the sender.

Active attacks are easy to detect and hard to stop [12][13].

J. Passive Attacks

Man-in-the-middle attacks where the attacker doesn't modify any data, but looks over the whole conversation happening between the sender and receiver are known as passive attacks. Passive attacks are further divided into two types

1) Traffic Analysis: Here, the attacker analyses the messages that are communicated between the parties. Analysis include size, time, etc.,

2) Release of Message Content: In this case, the attacker will read the messages transferring between the communicating parties and tries to store them.

Passive attacks are hard to detect and easy to stop [13].

K. Cross-Site Scripting

Another typical web security vulnerability is called Cross-Site Scripting (XSS). Application attack technique involving the transmission of attacker-supplied code to a user's browser or other client sites that the target users viewed over the internet. The attackers here may host or inject malicious code in several static or dynamic languages such as HTML, Java, JavaScript, ActiveX, Flash, or any other technologies that a browser supports [14].

L. Denial-of-Service-Attacks

Denial-of-Service Attacks pose a serious threat to companies. By flooding systems, servers, or networks with traffic, attackers exhaust their resources and bandwidth. The servers become overwhelmed when this happens, resulting in the website it hosts either going down or slowing down. As a result, authorized service requests go unresolved. Attackers who launch this attack through multiple compromised systems are also known as DDoS (Distributed Denial-of-Service) attacks.

M. Crypto-Jacking

The time period Crypto jacking is closely associated with cryptocurrency. Crypto jacking occurs when intruders get access to a target's computer to mine cryptocurrency. By infecting a website or tricking the victim into clicking on a malicious link, the attacker gains access. For this, they also utilize web advertisements with JavaScript code. Sufferers are blind to this because the Crypto mining code works inside the heritage; a put-off inside the execution is the most effective signal they could witness.

III. Possible Solutions

There are numerous solutions for providing web security. In this section we have presented efficient.

A. Web Application Firewalls

It is basically a software that monitors the traffic between the application and the internet. Fig. 4 shows the working of a firewall. There exists a firewall at server side that analyses every incoming packet. Only packets that are safe are forwarded to server and all unsafe packets are discarded by the firewall. Even though a Firewall is said to be a good protection method, it can't protect the applications from all the attacks [15].

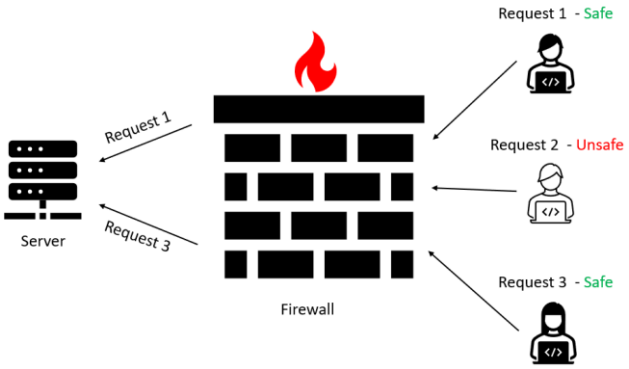

Fig. 4. Working of a Firewall

B. Vulnerability Scanners

A vulnerability Scanner is again a software in which a developer/admin of a particular application can scan for vulnerabilities. Once the scan is completed, the developer can check the details and work on fixing these vulnerabilities [16].

C. Fuzzing Tools

These are generally used by the developers where it helps in pointing out the programming errors that may

lead to a vulnerability. Once the tool points out the error, the developer takes action to correct it.

D. Testing Tools

Some of the major testing tools are:

1) Black Box Testing Tools: This is the case where the testing concentrates only on the input and expected output of a particular functionality. If any deviation is found in the expected output and actual output the developer concentrates on fixing it. Black Box testing is also done to find the behaviour of the function when an unexpected input is given by users.

2) White Box Testing Tools: In this, the testing is done with complete access to all the resources such as business logic, Syntax, Fields, etc. White box testing is done by the ones who already know how the application works.

E. Signature Based Virus Detection

Signature of a virus is a hash value that is generated when a virus attacks the system. All the known signatures of the viruses are stored in a database. With this, if an intrusion is detected by the server, then the signature of the intrusion or malware was verified with all the signatures that are stored in the database in a particular order of how fast they can start attacking. Table I shows the signatures of popularly known viruses.

TABLE I. SIGNATURES OF POPULARLY KNOWN VIRUSES

Table Head	Table Column Head
Accom. 1280	89C3 B440 8A2E 2004 8AOE 2104 BAOO 05CD 21E8 0500 BF50 04CD
Die.448	B440 B9E8 0133 D2CD 2172 1126 8955 15B4 40B9 BA5A 01CD
Xany.979	8B96 0906 B000 E85C FF8B D5B9 D303 E864 FFC6 8602 F8C3

F. Penetration Testing

Penetration testing is a method of finding vulnerabilities and it is an offensive way of dealing with security. Penetration testers act as real attackers while going through the testing phase and find the possibilities that help viruses to attack our systems. The purpose of doing this is to find the flaws that may lead to the theft of sensitive data to control the system/application. Penetration Testing is used as one of the security assessment processes to determine the effectiveness of the web. The process of penetration testing goes through the following phases [17].

1) Information Gathering: This is the first step in the process of penetration testing, where the tester explores as much as possible to find the system architecture in detail.

2) Enumeration: In this step, the tester gathers the information on vulnerabilities that help in exploitation from the information gathered either manually or by using any external tools.

3) Exploitation and Reporting: Here, from all the known vulnerabilities, the tester exploits the system to find the severity of the vulnerability and exploits whether these vulnerabilities help other vulnerabilities to attack the system and report all of these to the organization [18].

G. Cloud Computing

Security is given the utmost priority when major cloud providers like Amazon Web Services (AWS), Microsoft Azure, and Google are involved [19]. Switching to cloud will increase the overall security. Fig. 5 shows the working of a cloud environment. It contains the elements such as the hardware, software, network, storage, and security components. The architecture also specifies the way elements work together to provide services to users. There are various categories of cloud architecture, including public, private, hybrid, and community cloud. The architecture that an organization chooses will rely on its goals and requirements including security, data sovereignty, cost, and performance.

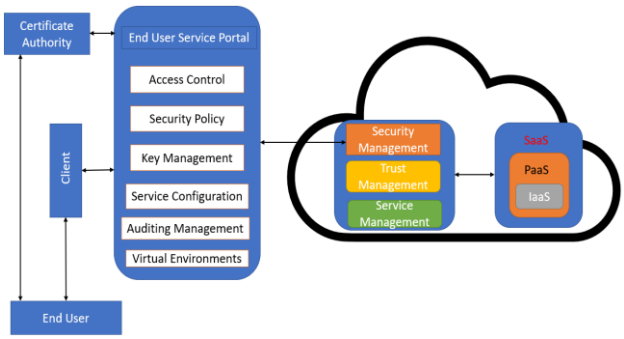

Fig. 5. Architecture of Cloud

In order to reduce the likelihood of security risks, data loss, data breaches, etc., cloud computing service providers typically store numerous copies of the data [20].

IV. CONCLUSION AND FUTURE SCOPE

Cyber Security is the paramount aspect when it comes to developing or utilizing web applications. Data security has emerged as one of the biggest challenges in the modern era. With each year that goes by, digital crime keeps going in new directions, and data security is no exception. While there is no perfect solution to digital wrongdoings, we should do everything in our power to prevent them in order to have a safe and secure future online. In this paper, we discussed major vulnerabilities such as Phishing, Distributed Denial-of-Service (DDoS), cross-site scripting (XSS), SQL injection assaults which are most frequent threats to web security. We also presented some of the prevention techniques such as web application firewalls, vulnerability scanners, fuzzing tools, testing tools, penetration testing, and cloud computing by exploring various domains.

The web application security is likely to evolve and become more complex as technology and cyber threats continue to advance. Some significant ideas for future work include applying Artificial Intelligence and Machine Learning Algorithms to find vulnerabilities and analyse how intrusions are taking place. Then building an intrusion detection system to discard these vulnerabilities using various algorithms and tools.

REFERENCES

[1] Humayun, M., Niazi, M., Jhanjhi, N., Alshayeb, M., and Mahmood, S., 2020, 'Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study', *Arabian Journal for Science and Engineering*, vol. 45, pp. 3171–3189, doi: 10.1007/s13369-019-04319-2.

[2] Domingo-Ferrer, J., Muralidhar, K., and Bras-Amoros, M., 2021, 'General Confidentiality and Utility Metrics for Privacy-Preserving Data Publishing Based on the Permutation Model', *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 5, pp. 2506-2517, doi: 10.1109/TDSC.2020.2968027.

[3] Efendi, A. I. M., Ibrahim, Z., Zawawi, M. N. A., Abdul Rahim, F., Pahri, N. A. M., and Ismail, A., 2019, 'A Survey on Deception Techniques for Securing Web Application', *2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)*, pp. 328-331, doi: 10.1109/BigDataSecurity-HPSC-IDS.

[4] Hu, W., Chang, C.-H., Sengupta, A., Bhunia, S., Kastner, R., and Li, H., 2021, 'An Overview of Hardware Security and Trust: Threats, Countermeasures, and Design Tools', *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 40, no. 6, pp. 1010–1038, doi: 10.1109/TCAD.2020.3047976.

[5] Priyanka, A. K., and Sai Smruthi, S., 2020, 'Web Application Vulnerabilities: Exploitation and Prevention', *2020 International Conference on Electrotechnical Complexes and Systems (ICOECS)*, pp. 1-5, doi: 10.1109/ICOECS50468.2020.9278437.

[6] Vinny Troia 2020, 'Passwords, Dumps, and Data Viper in Hunting Cyber Criminals', *A Hacker's Guide to Online Intelligence Gathering Tools and Techniques, Wiley*, pp. 407-431, doi: 10.1002/9781119541004.ch18.

[7] Kamurthi, R. T., Chopra, S. R., and Sharma, R., 2021, 'Confrontation-Wi-Fi Risks and Data Breach' ,*2021 International Conference on Emerging Smart Computing and Informatics (ESCI)*, pp. 633-638, doi: 10.1109/ESCI50559.2021.9397047.

[8] Alnabulsi, H., Islam, R., and Talukder, M., 2018, 'GMSA: Gathering Multiple Signatures Approach to Defend Against Code Injection Attacks', *IEEE Access*, vol. 6, pp. 77829–77840, doi: 10.1109/ACCESS.2018.2884201

[9] Shahriar, H., Talukder, M. A. I., Rahman, M., Chi, H., Ahamed, S., and Wu, F., 2019, 'Hands-on File Inclusion Vulnerablity and Proactive Control for Secure Software Development', *2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)*, pp. 604-609, doi: 10.1109/COMPSAC.2019.10274.

[10] A.A., A., and K., P., 2020, 'Towards the Detection of Phishing Attacks', *2020 4th International Conference on Trends in Electronics and Informatics (ICOEI) (48184)*, pp. 337-343, doi: 10.1109/ICOEI48184.2020.9142967.

[11] Mallik, A., Ahsan, A., Shahadat, M. Md. Z., and Tsou, J.-C., 2019, 'Man-in-the-middle-attack: Understanding in simple words', *International Journal of Data and Network Science*, vol. 3, pp. 77–92, doi: 10.5267/j.ijdns.2019.1.001.

[12] Cai, N., and Hayashi, M., 2020, 'Secure Network Code for Adaptive and Active Attacks With No-Randomness in Intermediate Nodes', *IEEE Transactions on Information Theory*, vol. 66, no. 3, pp. 1428–1448, doi: 10.1109/TIT.2019.2957078.

[13] Eian, I. C., Lim, K. Y., Yeap, M. X. L., Yeo, H. Q., and Z, F., 2020, 'Wireless Networks: Active and Passive Attack Vulnerabilities and Privacy Challenges', doi: 10.20944/preprints202010.0018.v1.

[14] Bukhari, S. N., Ahmad Dar, M., and Iqbal, U., 2018, 'Reducing attack surface corresponding to Type 1 cross-site scripting attacks using secure development life cycle practices', *2018 Fourth International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB)*, pp. 1-4, doi: 10.1109/AEEICB.2018.8480945.

[15] Manaseer, S., and Al Hwaitat, A. K., 2018, 'Centralized Web Application Firewall Security System: Modern Applied Science', vol. 12, pp. 164, doi: 10.5539/mas.v12n10p164.

[16] Bairwa, S., Mewara, B., and Gajrani, J., 2014, 'Vulnerability Scanners: A Proactive Approach to Assess Web Application Security', *International Journal on Computational Science & Applications*, vol. 4, pp. 113–124, doi: 10.5121/ijcsa.2014.4111.

[17] Al-Ahmad, A. S., Kahtan, H., Hujainah, F., and Jalab, H. A., 2019, 'Systematic Literature Review on Penetration Testing for Mobile Cloud Computing Applications', *IEEE Access*, vol. 7, pp. 173524–173540, doi: 10.1109/ACCESS.2019.2956770.

[18] Auricchio, N., Cappuccio, A., Caturano, F., Perrone, G., and Romano, S. P., 2022, 'An automated approach to Web Offensive Security', *Computer Communications*, vol. 195, pp. 248–261, doi: 10.1016/j.comcom.2022.08.018.

[19] Muhammed, A. S., and Ucuz, D., 2020, 'Comparison of the IoT Platform Vendors, Microsoft Azure, Amazon Web Services, and Google Cloud, from Users' Perspectives', *2020 8th International Symposium on Digital Forensics and Security (ISDFS)*, pp. 1-4, doi: 10.1109/ISDFS49300.2020.9116254.

[20] Nowrin, I., and Khanam, F., 2019, 'Importance of Cloud Deployment Model and Security Issues of Software as a Service (SaaS) for Cloud Computing', *2019 International Conference on Applied Machine Learning (ICAML)*, pp. 183-186, doi: 10.1109/ICAML48257.2019.00042.