Challenges and Security Prospect of Websites

Kamal, Rajita

Department of Computer Application

Chandigarh School of Business

Chandigarh Group of Colleges, Jhanjeri,Mohali,India

kamalkumaro1838@gmail.com, rajita.j2849@cgc.ac.in

Abstract

In this paper, we investigate the Challenges and Security prospect of websites. The ongoing competition between hacking techniques and preventive measures, maintaining website security in today's digital landscape is a difficult task. In order to strengthen websites' defenses, this paper explains the various issues that come with maintaining their security and suggests modern approaches. Hackers use loopholes to steal confidential information, and one of the biggest challenges is the constant barrage of cyber attacks. This risk is exacerbated by not updating out-of-date software since hackers can exploit known flaws in defenses. Weak password practices also make people more vulnerable, making it easier for hackers to access websites without authorization and jeopardizing user credentials. In order to tackle these obstacles, it is imperative that forthcoming approaches give precedence to preemptive software updates, strong encryption methods, and user training programs that foster a mindset of elevated security consciousness and adaptability to dynamic cyber hazards.

Keyword

Websites, Web Pages, Security, Challenges in Security, Artificial Intelligence, SQL, SQL Injection Attack, hacker, attacks, website security, threats in security.

I. INTRODUCTION

In the context of website security, navigating the complex terrain of obstacles and opportunities is essential for protecting digital assets in a world that is becoming more interconnected by the day. The numerous challenges in maintaining website security are examined in this introduction, along with the promising paths for improving security in the coming years. The issues are numerous and require thorough solutions, ranging from the dynamic strategies used by malevolent actors to the weaknesses present in out-of-date software and careless password usage. Notwithstanding the obstacles at hand, there are prospects for creativity and progress, as novel technology and preemptive tactics have potential in strengthening website defenses and safeguarding the authenticity of virtual environments. The framework for a more thorough examination of the possibilities and problems related to website security in the contemporary day is established by this introduction.

Artificial intelligence (AI) is expected to usher in a new age in cyber security, where it will be used not only as a defense against SQL injection assaults but also as a proactive deterrence against a wide range of cyber dangers. Artificial Intelligence (AI)-driven solutions, which make use of sophisticated algorithms and machine learning capabilities, guarantee to proactively detect and address vulnerabilities, strengthening websites against advancing cyber threats. Website managers can prevent possible breaches before they happen by using artificial intelligence (AI) to leverage anomaly detection and predictive analytics to keep one step ahead of hostile actors. AI systems are also capable of learning and evolving on a constant basis, which allows them to quickly and skillfully respond to new threats. Above and beyond protection, AI-powered cyber security projects have the power to revolutionize the field and bring in a new era of proactive risk management and robust resilience management and robust resilience.

Artificial Intelligence enhances human efforts by providing quick and effective action against cyber attacks through self-governing threat detection and response systems.AI integration also promises to optimize incident response processes, reduce downtime, and lessen the effect of cyber attacks. These benefits are inherent in the integration of AI with current security frameworks. The need for AI-driven cyber security solutions is becoming more and more obvious as enterprises struggle with the ever-present threat of cyber attacks. Safeguarding confidential information and maintaining the integrity of digital assets is a requirement

that cuts across all business sizes. Businesses may efficiently strengthen their digital fortresses, creating walls against attackers and maintaining the trust of their stakeholders by embracing AI as the cornerstone of their cyber security initiatives. In fact, as the digital world develops further, the mutually beneficial partnership between cyber security and AI becomes increasingly important for preserving the networked nature of the internet. As a whole, the paper not only highlights the dangers of SQL injection attacks but also signals the beginning of a new era in cyber security, one in which Artificial Intelligence is ready to act as a sentinel against cyber threats, protecting the integrity and robustness of websites in an increasingly hostile cyberspace.

A. Website: A website is an assemblage of online pages that may be viewed with any web browser. For example, if we connect the three web pages—home, contact, and services—we can refer to it as a website.

Search engine Google

YouTube- Platform for sharing videos.

Instagram- A social media platform

B. Webpage: A webpage is an HTML page that has text, photos, audio, video, and other types of information on it.

C. Website security: Website security, to put it simply, is safeguarding our website against unauthorized users, hackers, and other cyber attacks.

II. CHALLENGES IN SECURITY OF WEBSITES

A. Staying Ahead of Evolving Threats: Because hackers are continuously coming up with new technology or ways to attack websites, website owners need to stay updated. Webmasters ought to understand how to defend their websites against assaults as well as the ways in which they can be launched.

1) The Mouse-and-Cat Game: Cybercriminals have a great deal of time to develop new technologies or methods in order to attack websites. They are highly skilled and financially motivated. They regularly monitor the website, and as soon as they discover a weakness, they take advantage of it to steal your information. If you now resolve the issue that caused the hack, then hackers will attack your website somewhere else, and if you resolve that location as well, then they will attack your website somewhere else. This cycle of life never ends.

2) Zero Day Attack: Based on their recent development and lack of knowledge about the website owner, these attacks are the most deadly since only hackers are aware of them. These are the attacks that are thought to be the most hazardous because of this. This attack cannot be stopped until a remedy is developed, but if the owner of the website is aware of it, he can certainly receive assistance.

3) Supply Chain Attacks: In this type of attack, hackers target third-party software that is utilized by all websites and that is required by all websites. As a result, hackers introduce viruses into these third-party programs, which then spread to all websites through the use of those third-party programs. Hackers can concurrently target and steal data from multiple websites with this approach.

4) The Evolving Threat Landscape: The new technology that is developing now like cloud computing and Internet of Things brings some new problems and security concerns. The website owner should be aware of these security problems and the website owner should also know how to solve the problem, otherwise it will become very easy to attack the website.

B. CONTINUOUS SOFTWARE MAINTENANCE AND UPDATES

Because it is simpler to hack websites and web apps belonging to users of outdated software than to those whose websites and applications are regularly updated, many hackers specifically target users of these platforms. As a result, hackers like to target outdated websites and steal their data; for this reason, we should constantly upgrade both our websites and online apps. The issues that may arise if we don't update our website and application are listed below.

1) Threats to Security: The main issue is that numerous aspects of outdated software are vulnerable to hacking attacks. Hackers have total

access over users' devices, making it incredibly simple to assault them with viruses. This is by far the largest issue ever. We expose the security of our websites to danger if we do not upgrade our web applications and software.

2) Compatibility issues: Using older software on websites and online apps made with newer software does not operate effectively since the older program does not have the same hardware as the newer software, which causes a gap between them. There are compatibility problems and websites created with new software won't function with previous versions.

3) Not Included New Features: We lose out on new features that improve user interaction and decrease workload if we don't upgrade our website and software.

C. HUMAN ERROR

No matter how skilled a person is, mistakes will inevitably happen. These errors are known as human error. For instance, leaving your account open on a public computer or clicking on a malicious email. All these errors are attainable by everyone. A list of some of the issues this has caused is provided below.

1) Unintentional Errors: Sometimes even the most careful individuals make mistakes. For example, they may open and download a malicious file on their laptop, click on a phishing email, or leave their private account open on a public computer. We refer to all of these errors as unintended errors.

2) Lack of Awareness: Many website visitors are unaware of the most recent cyber threats, particularly those without any technological experience. They either leave their accounts open on numerous websites and machines, or they leave their accounts open and use very simple passwords that are very easy t-o guess, which makes them easy targets for hackers.

3) Social engineering attacks: Phishing emails, phone conversations, and phony websites are just a few of the engineering approaches used by cybercriminals to trick consumers into believing they are dealing with real hackers and handing over their personal information. Hackers can then readily obtain personal info after that.

III. SQL INJECTION ATTACK

A. SQL: SQL stands for structured query language. This special method is used to retrieve data from the database and to store the database data.

B. SQL Injection Attack: SQL injection attacks can be done on any websites or web applications that use SQL. In this attack, hackers put some malicious code in the user name and password in the login page of the website and when this code is executed with the real query of the website, it reaches the database and after that with the help of this attack, the information about the database is deleted. Data can be accessed, deleted and modified.

Not executed due to which the password is not validated and hackers get logged in using this query we retrieve data from the database.

C. HOW TO RETRIEVE DATA FROM DATABASE:

SELECT * FROM table name WHERE Username = 'username' AND Password = 'password'

In this 1=1 is always true and because in SQL query after the double dashed is not executed due to which the password is not validated and hackers get logged in.

D. MALICIOUS CODE

' OR 1=1- Hackers put malicious code in the username due to which they can login to the website even without the login password and this malicious code is executed with the real query and this makes the query SELECT * FROM table name WHERE Username = ' 'OR 1=1-- AND Password = 'password'

E. HOW ATTACKER ATTACK ON WEBSITE USING SQL INJECTION TECHNIQUE

1) In the first step he decides which website he wants to attack.

2) In the second step he goes to the login page of the website.

3) In this step he inserts this code in the username ' OR 1=1-- and puts anything in the password.

Step4. Now he enters the website as an administrator and after this he can do anything here like transferring money to someone or deleting or modifying the database.

Example:- We are going to demonstrate this attack in a demo website.

Step1. First of all we have to type testfire.net in Google

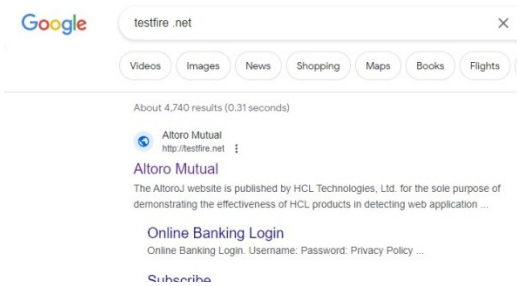

Fig.1 (testfire.net website)

Step2. After this you have to open this website

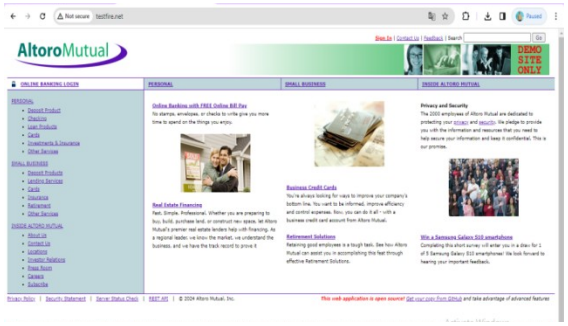

Fig.2 (open testfire.net website)

Step3. Then you go to its login page

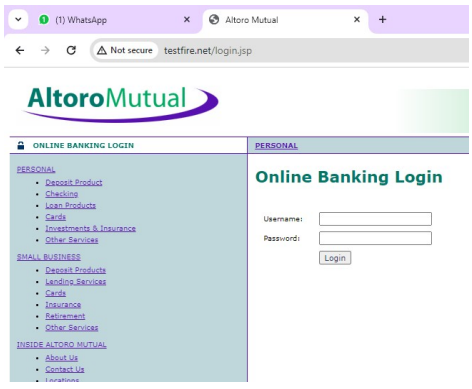

Fig.3 (Login page)

Step4. Now enters your username and password to see if you are logged in or not and it will deny you that there is no user with this name in our database.

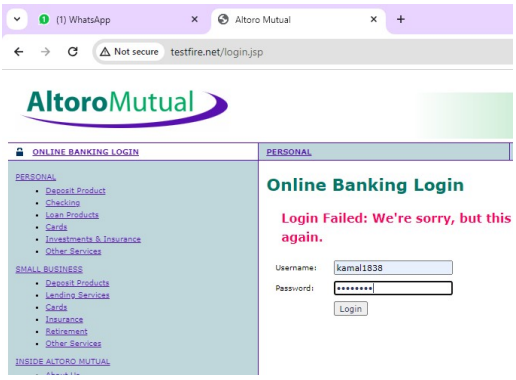

Fig.4 (Try Login In)

Step5. Now you have to write this code in the user name ' OR 1=1-- and you can write anything in the password.

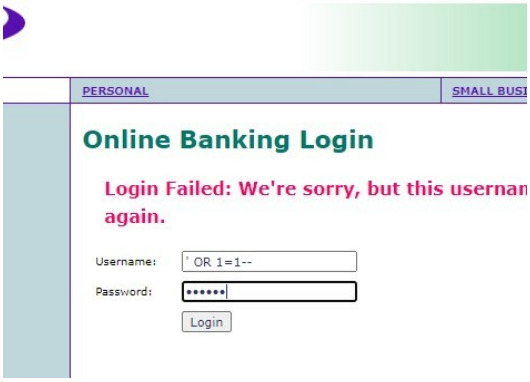

Fig.5 (Enter Malicious code)

Step6. We have become like administrators in the office website, now you can do anything in this website, make any modification in the database or even delete the database.

Fig.6 (Attack is successful)

IV. PREVENTION FOR SQL INJECTION ATTACK

A. Verify User Input: You need to make sure that the information a user enters on your website is correct and formatted correctly. In order to prevent the hacker from

writing the code correctly and from performing a SQL injection attack on your website, you can use this to restrict the user's input such that he is only allowed to use single quotes in his username.

B. Limited access: This indicates that only individuals who manage your database are permitted. You are the only person who can change or view your database; nobody else can, aside from them. You are granting access, update, and delete permissions to the database manager alone.

C. Website firewalls: Firewalls block all kinds of website visitors, much like a security guard in a building verifies each individual entering and only allows authorized people entry. Verifies the person and only permits authorized users and permitted data. A website's firewall functions as its website's security guard.

V. FUTURE SCOPE IN WEBSITE SECURITY

While hackers continue to develop new techniques to breach websites, new technologies aimed at enhancing website security are also being developed. However, in the future, certain technologies will be able to offer extremely high levels of website protection. The list below includes a few of them.

A. AI: Artificial Intelligence is the acronym for this concept. Due to its ability to provide information on website attacks even before they occur, this technology is expected to be the most widely employed in the future to secure websites. It will follow the established patterns and provide information even before it occurs; the user will receive comprehensive information about it from its administrator. This device will operate around the clock, recognizing patterns in hacker activity and providing the administrator with advance notice of any attempted attacks on the website.

B. Decentralized Security: The main component of a website, which we refer to as the server, stores user data and information. This primary component is highly vulnerable to hacking attacks since it gives any hacker access to all of our keys. As a result, decentralized security will be implemented going forward. He only had access to one compromised server, therefore all of the information was available. Each person will have access to their critical information, and none of the data will be maintained on a single server. The data on that particular computer will be the only thing that hackers can steal if they manage to breach someone else's PC.

VI. CONCLUSION

The paper provides an in-depth analysis of the complex issues related to website security while also providing an overview of emerging technologies that have the potential to strengthen website security. It covers the well-known SQL injection attack in detail and clarifies the malicious techniques hackers use to steal data from websites that are susceptible to attack. The study sheds light on the vulnerabilities present in online systems by providing a clear illustration of the attack's mechanics on a simulated platform. The study also describes in detail how to defend websites from these kinds of attacks, offering a roadmap for preventative defenses. Anticipating the future, artificial intelligence integration appears to be a critical answer that will transform preconceptions about website security.

REFERENCES

[1] Deepa, G., & Thilagam, P. S. (2016). Securing web applications from injection and logic vulnerabilities: Approaches and challenges. Information and Software Technology, 74, 160-180.

[2] Mitropoulos, D., Louridas, P., Polychronakis, M., & Keromytis, A. D. (2017). Defending against web application attacks: Approaches, challenges and implications. IEEE Transactions on Dependable and Secure Computing, 16(2), 188-203.

[3] Sardar, R., & Anees, T. (2021). Web of things: security challenges and mechanisms. Ieee Access, 9, 31695-31711.

[4] Gupta, S., & Gupta, B. B. (2017). Detection, avoidance, and attack pattern mechanisms in modern web application vulnerabilities: present and future challenges. International Journal of Cloud Applications and Computing (IJCAC), 7(3), 1-43.

[5] Sadique, K. M., Rahmani, R., & Johannesson, P. (2018). Towards security on internet of things: applications and challenges in technology. Procedia Computer Science, 141, 199-206.

[6] Daeef, A. Y., Ahmad, R. B., Yacob, Y., & Phing, N. Y. (2016, August). Wide scope and fast websites phishing detection using URLs lexical features. In 2016 3rd International Conference on Electronic Design (ICED) (pp. 410-415). IEEE.

[7] Appiah, V., Asante, M., Nti, I. K., & Nyarko-Boateng, O. (2018). Survey of websites and web application security threats using vulnerability assessment. Journal of Computer Science, 15(10), 1341-1354.

[8] Jain, A. K., & Gupta, B. B. (2017). Phishing detection: analysis of visual similarity based approaches. Security and Communication Networks, 2017.

[9] bt Mohd, N. A., & Zaaba, Z. F. (2019). A review of usability and security evaluation model of ecommerce website. Procedia Computer Science, 161, 1199-1205.

[10] Kaushik, D., Gupta, A., & Gupta, S. (2020, May). E-commerce security challenges: A review. In Proceedings of the international conference on innovative computing & communications (ICICC).

[11] Singh, J. (2014). Review of e-commerce security challenges. International Journal of Innovative Research in Computer and Communication Engineering, 2(2), 2850-2858.

[12] Dadkhah, M., Borchardt, G., & Lagzian, M. (2017). Do you ignore information security in your journal website?. Science and Engineering Ethics, 23, 1227-1231.

[13] Appiah, V., Asante, M., Nti, I. K., & Nyarko-Boateng, O. (2018). Survey of websites and web application security threats using vulnerability assessment. Journal of Computer Science, 15(10), 1341-1354.

[14] Purkait, S. (2012). Phishing counter measures and their effectiveness–literature review. Information Management & Computer Security, 20(5), 382-420.

[15] Halfond, W. G., Viegas, J., & Orso, A. (2006, March). A classification of SQL-injection attacks and countermeasures. In Proceedings of the IEEE international symposium on secure software engineering (Vol. 1, pp. 13-15). Piscataway, NJ: IEEE.

[16] Lawal, M. A., Sultan, A. B. M., & Shakiru, A. O. (2016). Systematic literature review on SQL injection attack. International Journal of Soft Computing, 11(1), 26-35.

[17] Sadeghian, A., Zamani, M., & Abdullah, S. M. (2013, September). A taxonomy of SQL injection attacks. In 2013 International Conference on Informatics and Creative Multimedia (pp. 269-273). IEEE.

[18] Boyd, S. W., & Keromytis, A. D. (2004). SQLrand: Preventing SQL injection attacks. In Applied Cryptography and Network Security: Second International Conference, ACNS 2004, Yellow Mountain, China, June 8-11, 2004. Proceedings 2 (pp. 292-302). Springer Berlin Heidelberg.

[19] Wei, K., Muthuprasanna, M., & Kothari, S. (2006, April). Preventing SQL injection attacks in stored procedures. In Australian Software Engineering Conference (ASWEC'06) (pp. 8-pp). IEEE.

[20] Alwan, Z. S., & Younis, M. F. (2017). Detection and prevention of SQL injection attack: a survey. International Journal of Computer Science and Mobile Computing, 6(8), 5-17.

[21] Clarke-Salt, J. (2009). SQL injection attacks and defense. Elsevier.

[22] Rawat, R., & Shrivastav, S. K. (2012). SQL injection attack Detection using SVM. International Journal of Computer Applications, 42(13), 1-4.

[23] Nasereddin, M., ALKhamaiseh, A., Qasaimeh, M., & Al-Qassas, R. (2023). A systematic review of detection and prevention techniques of SQL injection attacks. Information Security Journal: A Global Perspective, 32(4), 252-265.

[24] Bandhakavi, S., Bisht, P., Madhusudan, P., & Venkatakrishnan, V. N. (2007, October). CANDID: preventing SQL injection attacks using dynamic candidate evaluations. In Proceedings of the 14th ACM conference on Computer and communications security (pp. 12-24).