LOGIN PAGE VALIDATION WITH PASSWORD ENCRYPTION

Aswani P,
M Tech Cyber security,
Nehru College of Engineering and Research Centre,
Thrissur, India
pookotaswani@gmail.com

Soumya T,
Assistant Professor CSE,
Nehru College of Engineering and Research Centre,
Thrissur, India
soumyanikshay@gmail.com

Abstract: Wireless communication technology's rapid evolution necessitates user authentication for security. Password validation is crucial to prevent attacks. Attackers can sniff passwords for illegal activities. Solutions include AES encryption for password security and validation methods in user fields to prevent backdoors during authentication. These measures aim to improve wireless technology security.

Keywords: Encryption, AES, Input validation

I. INTRODUCTION

Login authentication systems are crucial in web-based applications to secure privilege access. MD5 is often used, but it's vulnerable to dictionary attacks and rainbow tables. Hash functions like MD5, SHA1, and SHA256 can be used. Other alternatives include symmetric algorithms like DES, AES, IDEA, RC4, and asymmetric algorithms like RSA, DSA, DH, and ECC. These alternatives help manage content application access. In this paper using AES algorithm for the encryption of password. Server-side validation along with client-side validation also ensures more safety to login page authentication.

II. LITERATURE REVIEW

Authentication is a process used by both servers and clients to verify identity, requiring users or computers to prove their identity to the server or client. Data validation is crucial for web form submission, ensuring data integrity, protecting against security threats, and enhancing user experience, making it a critical aspect of any web development project.

Passwords should not be stored in clear text, as a website or service can easily retrieve forgotten or old passwords, which is concerning. Passwords are essential for accessing sensitive data and accounts, and users often keep similar passwords for multiple accounts. The AES algorithm is renowned for its robust security and efficiency, making it ideal for various applications such as data encryption, secure network communication, and device data protection. AES provides enhanced security by utilizing multiple encryption rounds, making it

harder for attackers to intercept or steal encrypted information through brute-force attacks.

Data validation is crucial for web form submission, ensuring data integrity, protecting against security threats, and enhancing user experience, making it a critical aspect of any web development project. Server-side input validation is crucial for valid data processing in dynamic application security tests, as tools can bypass client-side restrictions for injection attacks like Cross-Site Scripting and SQL injection.

Secure login pages are essential in web and application development, as they protect user data from unauthorized access, identity theft, fraud, and privacy violations. They require users to authenticate their identity before accessing sensitive information, reducing the risk of malicious actors compromising sensitive data.

Cyber threats like password cracking, phishing, and credential stuffing pose significant risks to individuals, organizations, and systems in the digital world. Password cracking involves unauthorized retrieval of passwords through brute force attacks, while phishing is a social engineering attack that trick users into disclosing sensitive information. Credential stuffing exploits reused usernames and passwords from data breaches to obtain unwanted access to user accounts across a number of platforms. Attackers automate the process of trying stolen credentials across multiple websites or applications, exploiting the practice of users using the same password for multiple accounts. These threats compromise the confidentiality, integrity, and availability of sensitive information and systems. Secure login pages and robust authentication mechanisms are essential defenses against these threats. Understanding these threats is essential for putting in place efficient security measures and protecting against potential vulnerabilities in login processes and authentication systems.

Robust validation and encryption techniques are crucial for mitigating cybersecurity risks, protecting user privacy, preventing unauthorized access, and ensuring regulatory compliance. These techniques ensure that only legitimate users with valid credentials can gain access to private data, lowering the danger of data breaches. Encryption encoding data in a secure format, only deciphered by authorized parties, reduces the risk of data manipulation and unauthorized modifications. It also safeguards user privacy by ensuring sensitive data remains confidential. Credential-based attacks can be mitigated through hashing and salting, while additional security measures like password complexity requirements and rate limiting can further protect user accounts.

Security measures are essential in enhancing the security posture and resilience of authentication processes. Common methods include password-based, multi-factor authentication (MFA), biometric authentication, token-based authentication, and single sign-on (SSO). Password-based authentication offers advantages like familiarity, low cost, and flexibility but is vulnerable to attacks like brute force, dictionary attacks, and phishing. Common vulnerabilities include weak passwords, plaintext storage, and insecure password reset mechanisms. To manage passwords effectively, enforce strong password policies, use strong cryptographic hashing algorithms, and require multiple authentication factors. Regular password rotation can reduce the risk of compromise due to password reuse or theft. Multi-factor authentication reduces unauthorized access but introduces complexity and inconvenience for users. Implementation challenges include user experience and integration complexity across different systems and platforms. Password complexity requirements are essential for enhancing security but can also negatively impact user experience by increasing the likelihood of forgotten passwords or password resets.

Balancing security and usability are crucial when establishing complexity requirements. To balance security and usability, login page design should adopt a

user-centric approach, simplify authentication, progressive disclosure, feedback and error handling, accessibility considerations, and user education. User-centric design prioritizes usability and ensures adequate security measures. Simplified authentication streamlines the process, while progressive disclosure introduces security measures and additional authentication factors. Feedback and error handling provide informative and actionable feedback to help users troubleshoot errors and understand security-related prompts. Accessibility considerations ensure login pages are accessible to users with disabilities, providing alternative authentication methods, assistive technologies, and customizable settings. User education empowers users to make informed decisions about their security settings and behaviors. Clear feedback during the login process improves user experience, with effective error handling minimizing frustration and personalized recommendations. Continuous improvement involves soliciting user feedback through surveys, testing sessions, and analytics.

The impact of security measures on user experience depends on a balance between security requirements and usability. Organizations should prioritize user-centric design principles, streamline authentication workflows, provide clear feedback, and empower users to make informed decisions about their security settings. By adopting strategies for balancing security and usability, organizations can enhance the overall login experience and mitigate risks associated with authentication vulnerabilities and user errors. A financial institution implemented several enhancements, including Multi-factor Authentication, Biometric authentication, revised password complexity requirements, and an awareness campaign to educate users about security best practices. Major e-commerce platforms face constant threats to user credentials due to high transaction volume and user data attractiveness. Lessons learned from security breaches include password reuse, inadequate password policies, insufficient monitoring and response, and lack of user education.

Lack of user education can increase vulnerability to credential theft. To protect sensitive financial information, comprehensive user education and awareness training should be provided. Password complexity requirements should be enforced to encourage strong passwords, including a minimum length and a combination of digits, capital and lowercase letters, and special characters. Multi-Factor Authentication (MFA) options should be offered to add an extra layer of security to the login process. HTTPS should be used for secure communication, and SSL/TLS certificates from trusted certificate authorities should be obtained to establish a secure connection. Recommendations for implementing secure login page validation with password encryption include using strong password hashing algorithms. Regular updates and patching systems are essential to address vulnerabilities and prevent exploitation by attackers.

III. SYSTEM REQUIREMENTS

Programming Environment: Windows 11(2021)

Features: Login page creation in bootstrap framework with sever side validation and password encryption using AES algorithm in java.

Tool required and requirements:

- Eclipse

Eclipse is a popular Java development environment (IDE) with a foundational workspace and an expandable plug-in framework for customization. It is the second-most popular IDE for Java development and can be used for developing Java applications in various programming languages. The Eclipse software development kit (SDK) is designed for Java developers and allows them to extend

its capabilities by installing and managing plugins. Since Eclipse 3.0, plug-ins are installed and managed using Equinox, an OSGi implementation. The SDK is free and open-source, released under the Eclipse Public License.

- Bootstrap

Bootstrap is a popular HTML, CSS, and JavaScript framework for creating responsive websites and web applications. It solves cross-browser compatibility issues and offers Design templates for HTML and CSS, in addition to optional JavaScript plugins.

- MySQL Workbench

MySQL Workbench is an open-source, cross-platform tool that simplifies MySQL and SQL development work by offering data modeling, SQL development, and configuration administration tools.

IV. PROPOSED SYSTEM

Login page validation is necessary to avoid backdoor entry to a web page application. In that case client-side validation is easily hackable by a hacker through inspect element. To avoid that use server-side validation using JavaScript, so that an intruder unable to hack the authentication details. Bootstrap framework is used to provide a responsive web page to a user. Along with that while storing password to a database, it is encrypted using AES algorithm in java. By using AES algorithm while storing password, it ensures more safety.

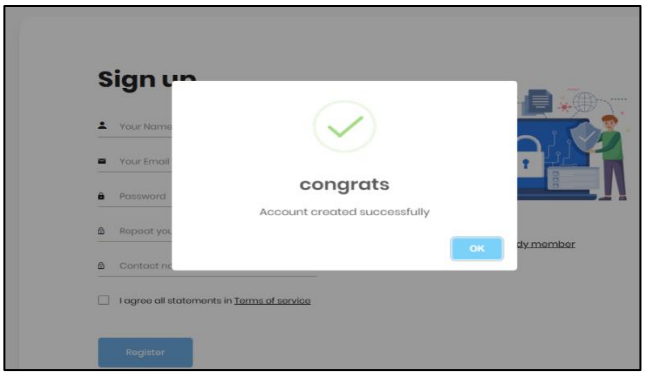

Fig. 1 sign up form with validation

15	sanju	vTTMANO1cJtL2fgNvWkLZA==	sanju@gmail.com	8904567832
16	ani	HEmxd95KyYnhXVCgoTkf8Q==	ani@gmail.com	9876789098
17	rithanya	HEmxd95KyYnhXVCgoTkf8Q==	rithanya@gmail....	8790789076
18	gowri	HEmxd95KyYnhXVCgoTkf8Q==	gowri@gmail.com	9807689098
19	ani	HEmxd95KyYnhXVCgoTkf8Q==	ani@gmail.com	9087656789
20	lali	HEmxd95KyYnhXVCgoTkf8Q==	lalis@gmail.com	9808798098
NULL	NULL	NULL	NULL	NULL

Fig. 2 Encrypted password in database

while sign up each and every field has unique input validation along with server-side validation in order to ensure the authenticity of signed up user. Once

the user signed in, the password is encrypted and stored in database. Even if the hacker attacks the database server, it's difficult to find the password of the user. In Fig. 1, while sign up each and every field has unique input validation along with server-side validation in order to ensure the authenticity of signed up user. Once the user signed in, the password is encrypted and stored in database. Even if the hacker attacks the database server, it's difficult to find the password of the user. In Fig. 2 the encrypted password is stored in database.

V. CONCLUSION

Using Bootstrap framework, developed a user-friendly login page with client-side and server-side validation. Along with that to ensure the safety to the user, encrypted the user password using AES algorithm in java and stored it in a database. Only authenticated users can login by matching the entered password with the password in the database. Once the password mismatches the user cannot enter into web page.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: "The authors certify that they have no competing interests with regard to this research."

REFERENCES

[1]. Javier Andres Bargas-Avila, Online Form Validation: Don't Show Errors Right Away. Conference: Human-Computer Interaction INTERACT '03: IFIP TC13 International Conference on Human-Computer Interaction, 1st-5th September 2003, Zurich, Switzerland.

[2]. Ako Muhammad Abdullah, Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data, Article · June 2017.

[3]. Katha Chanda, Password Security: An Analysis of Password Strengths and Vulnerabilities, July 2016International Journal of Computer Network and Information Security 8(7):23-30.

[4]. Flevina Jonese D'souza,Dakshata Panchal, Advanced encryption standard (AES) security enhancement using hybrid approach.

[5]. Herley, Cormac, Paul C. van Oorschot, and Andrew S. Patrick. "Passwords: If we're so smart, why are we still using them?" Financial Cryptography and Data Security. Springer Berlin Heidelberg, 2009. 230-237.

[6]. Halderman, J. Alex, Brent Waters, and Edward W. Felten. "A convenient method for securely managing passwords." Proceedings of the 14th international conference on World Wide Web. ACM, 2005.

[7]. Manber, Udi. "A simple scheme to make passwords based on one-way functions much harder to crack." Computers & Security 15.2 (1996): 171-176.

[8]. Duggan, Geoffrey B., Hilary Johnson, and Beate Grawemeyer. "Rational security: Modelling everyday password use." International journal of human-computer studies 70.6 (2012): 415-431.