INSY7314

ICE TASK 3

Kayla Ferreira
VARSITY COLLEGE | ST10259527

Table of Contents

How do you protect against brute-force attacks on a login page?

To protect against brute-force attacks on a login page, you can limit the number of times someone can try to log in before their account is locked for a short time. Adding delays between failed login attempts, using CAPTCHAs, and monitoring unusual login activity also helps. The best protection is to use multi-factor authentication so that even if a password is guessed, the attacker still cannot log in (Fortinet, 2025).

What is the principle of least privilege in application security?

The principle of least privilege means giving users or systems only the access they absolutely need to do their job, and nothing more. For example, if an application only needs to read from a database, it should not be given permission to delete or change everything in that database. This keeps the system safer because if someone's account is hacked, the damage they can do is limited (Paloalto, 2025).

How do you handle secrets management in a web application?

Secrets management in a web application is about keeping things like passwords, API keys, and database connections safe. These should never be written directly in the code. Instead, they should be stored in secure places like AWS Secrets Manager, Azure Key Vault, or environment variables. That way, they are encrypted, harder to steal, and easier to manage safely (Fortinet, 2025).

Discuss the importance of input validation and output encoding?

Input validation and output encoding are important to keep a web application safe. Input validation means checking the data that users type in to make sure it is in the right format, such as making sure an email looks like an email. Output encoding means making sure that when this data is shown on a web page, it cannot run harmful code. For example, it can stop hackers from sneaking in malicious scripts through forms. These two practices prevent common attacks like SQL injection and cross-site scripting (XSS) (Irwin, 2023).

References

Fortinet, 2025. *What Is A Brute Force Attack?*. [Online]
Available at: https://www.fortinet.com/resources/cyberglossary/brute-force-attack
[Accessed 8 September 2025].

Fortinet, 2025. *What Is Secret Management?*. [Online]
Available at: https://www.fortinet.com/uk/resources/cyberglossary/secret-management
[Accessed 8 September 2025].

Irwin, A., 2023. *Validation and Output Encoding in API Security Testing*. [Online]
Available at: https://www.aptori.com/blog/input-validation-output-encoding-api-security-testing
[Accessed 8 September 2025].

Paloalto, 2025. *What Is the Principle of Least Privilege?*. [Online]
Available at: https://www.paloaltonetworks.com/cyberpedia/what-is-the-principle-of-least-privilege
[Accessed 8 September 2025].