What is CSRF?

CSRF (Cross-Site Request Forgery) is a web security vulnerability that tricks a user into performing an unwanted action on a website they are currently authenticated to.

How it works:

1. **Malicious Website:** A malicious website (e.g., a phishing site or an ad) contains a hidden link or form that targets the victim's legitimate website.
2. **User Action:** The user is tricked into visiting the malicious website or clicking on a link/button.
3. **Unauthorized Request:** The malicious website sends a request (e.g., transferring funds, changing passwords) to the victim's website in the background, using their active session.
4. **Action Performed:** Since the victim is already logged in, the website authenticates the request and performs the action, without the victim's knowledge or consent.

Example:
Imagine you're logged into your bank's website. A malicious website might contain a hidden form that attempts to transfer money from your account to the attacker's account. If you visit the malicious website, the form is submitted in the background, and your bank might unknowingly process the transaction.

Prevention Techniques:

- **Same-Site Cookies:** Browsers now support the "SameSite" attribute for cookies, which restricts cookies to only be sent with requests from the same origin as the one that set the cookie.
- **CSRF Tokens:** Implementing CSRF tokens adds a unique, unpredictable value to every request. The server checks this token to ensure the request originated from the expected source.
- **HTTP Strict Transport Security (HSTS):** Enforces HTTPS connections, making it harder for attackers to intercept and modify requests.

Key Takeaways:

- CSRF is a serious security threat that can have significant financial and data loss implications.
- Implementing robust security measures like Same-Site cookies and CSRF tokens is essential for protecting web applications from this vulnerability.

- By default spring security will implement CSRF for POST, PUT & DELETE request types but not for GET because, it not perform any changes.