Cross Site Request Forgery is considered as one of the top vulnerabilities in today's web, where an untrusted website can force the user browser to send the unauthorized valid request to the trusted site. Cross Site Request Forgery will let the integrity of the legitimate user. So far many solutions have been proposed for the CSRF attacks such as the referrer HTTP Header, Custom HTTP header, Origin Header, client site proxy, Browser plug-in and Random Token Validation. But existing solutions are not so immune as to avoid this attack. All the solutions are partially protected only. This paper focuses on describing the implementation of various possible cross site request forgery methods and describing the pitfalls in the various preventive techniques of cross site request forgery and so we suggested some defense mechanism to prevent this vulnerability.

References

- A. Barth, C. Jackson, and J. C. Mitchell. "Robust defenses for cross site request
Cross Site Request Forgery: Preventive Measures

- Nenad Jovanovic, Engin Kirda, and Christopher Kruegel. &quot;Preventing cross site request forgery attacks&quot;; In IEEE International Conference on Security and Privacy in Communication Networks (SecureComm), 2006.
- Sooel Son, &quot;Prevent Cross site Request Forgery PCRF&quot;; userweb. cs. utexas. edu/~samuel/PCRF/Final_PCRF_paper. pdf.

Index Terms
Computer Science
Security
Keywords

Security threats  Security breaches  Browser security  Forgery prevention  Defense mechanisms

Open web application security