Robust Defenses for Cross-Site Request Forgery

A. BARTH, C. JACKSON, J. MITCHELL

IN

PROC. 15TH ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY (CCS '08)

Presented by:
Christopher Haden

Summary

- *"In this paper, we examine the scope and diversity of CSRF vulnerabilities, study existing defenses, and describe incremental and new defenses based on headers and web application firewall rules."*
- CSRF stands for Cross-Site Request Forgery.
- CSRF is an attack that interrupts a user's session by injecting malicious code to a user's browser.
- The paper focuses on login CSRF.

Example

- Login CSRF attacks go as follows:
  - First user visits attackers site.
  - Embedded into the attackers homepage is a form that makes the browser send off a request to a honest web site (e.g. PayPal) to log the user in with an account set up by the attacker.
  - Honest site logs user in and set cookie in browser.
  - User is now logged into honest site with attackers account, any activity done on the honest website is logged to the users account (e.g. Adds credit card to PayPal account).

Appreciations

- Good critique of existing solutions, highlighting their weaknesses.
  - Secret Validation Token
    - Difficult and complex to implement
  - Strict Referrer validation
    - Can cause many normal users to be denied access
  - Custom HTTP headers.
    - Relies on JavaScript, which could be disabled.

Criticisms

- All proposed defences require significant technical knowledge.
  - Even some specifically designed CSRF defence frameworks fail to correctly implement the solutions.
    - NoForge
    - CSRFx
    - CSRF Guard
  - Proposed origin header requires server and client changes to be effective.

Question

- Have you ever heard of or considered CSRF attacks when building a website?