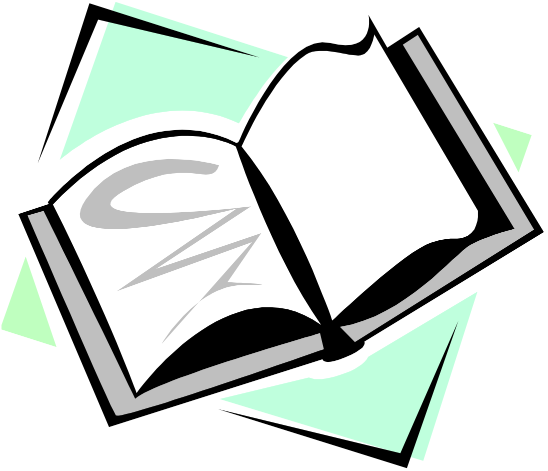
Information Security
CS 526
Topic 9

Web Security Part 2

Readings for This Lecture

- **Optional Reading**
  - Bandhakavi et al.: CANDID : Preventing SQL Injection Attacks Using Dynamic Candidate Evaluations
  - Chen et al.: Side-Channel Leaks in Web Applications: a Reality Today, a Challenge Tomorrow



Other Web Threats

- SQL Injection
  - See slides by Venkat
- Side channel leakages
  - See slides from MSR
- Web browsing privacy: third-party cookies and browser fingerprinting

OWASP Top 10 Application T10 Security Risks – 2013

- **A1 – Injection:** Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
- **A2 – Broken Authentication and Session Management :** Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities.

OWASP Top 10 Application T10 Security Risks – 2013

- **A3 – Cross-Site Scripting (XSS):** XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.
- **A4 – Insecure Direct Object References:** A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data.

OWASP Top 10 Application T10 Security Risks – 2013

- **A5 – Security Misconfiguration:** Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. Secure settings should be defined, implemented, and maintained, as defaults are often insecure. Additionally, software should be kept up to date.
- **A6 – Sensitive Data Exposure:** Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data deserves extra protection such as encryption at rest or in transit, as well as special precautions when exchanged with the browser.

OWASP Top 10 Application T10 Security Risks – 2013

- **A7 – Missing Function Level Access Control:** Most web applications verify function level access rights before making that functionality visible in the UI. However, applications need to perform the same access control checks on the server when each function is accessed. If requests are not verified, attackers will be able to forge requests in order to access functionality without proper authorization.
- **A8 - Cross-Site Request Forgery (CSRF):** A CSRF attack forces a logged-on victim’s browser to send a forged HTTP request, including the victim’s session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim’s browser to generate requests the vulnerable application thinks are legitimate requests from the victim.

OWASP Top 10 Application T10 Security Risks – 2013

- **A9 - Using Components with Known Vulnerabilities:** Components, such as libraries, frameworks, and other software modules, almost always run with full privileges. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications using components with known vulnerabilities may undermine application defenses and enable a range of possible attacks and impacts.
- **A10 – Unvalidated Redirects and Forwards**: Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination pages. Without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages.

Browser Cookie Management

- Cookie Same-origin ownership
  - Once a cookie is saved on your computer, only the Web site that created the cookie can read it.
- Variations
  - Temporary cookies
    - Stored until you quit your browser
  - Persistent cookies
    - Remain until deleted or expire
  - Third-party cookies
    - Originates on or sent to a web site other than the one that provided the current page

Third-party cookies

- Get a page from merchant.com
  - Contains <img src=http://doubleclick.com/advt.gif>
  - Image fetched from DoubleClick.com
    - DoubleClick knows IP address and page you were looking at
- DoubleClick sends back a suitable advertisement
  - Stores a cookie that identifies "you" at DoubleClick
- Next time you get page with a doubleclick.com image
  - Your DoubleClick cookie is sent back to DoubleClick
  - DoubleClick could maintain the set of sites you viewed
  - Send back targeted advertising (and a new cookie)
- Cooperating sites
  - Can pass information to DoubleClick in URL, …

Cookie issues

- Cookies maintain record of your browsing habits
  - Cookie stores information as set of name/value pairs
  - May include *any* information a web site knows about you
  - Sites track your activity from multiple visits to site
- Sites can share this information (e.g., DoubleClick)
- Browser attacks could invade your "privacy"

Browser Fingerprinting

- Browser sends HTTP head information, which includes
  - User agent: e.g., “Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/38.0.2125.111 Safari/537.36”
  - HTTP header: e.g., “text/html, */* gzip,deflate en-US,en;q=0.8”
  - Javascript can collect font information, installed browser-plugin information
  - Using canvas, e.g., how to render emoji
  - Can achieve high entropy.
  - Can be used to track users/browsers.

- https://panopticlick.eff.org/

Coming Attractions …

- Malware defenses