Web Application Security

Dr. Digvijaysinh Rathod
Associate Professor
School of Cyber Security and Digital Forensics
National Forensic Sciences University

digvijay.rathod@nfsu.ac.in

HTTP Cookie

HTTP Cookie

- ✓ HTTP cookies are text-based files created by web servers and stored locally on a user's device.
- ✓ They consist of key-value pairs and are primarily used to store information about the user's browsing activity and preferences.
- ✓ When a user visits a website, the server sends one or more cookies along with the HTTP response, which are then stored by the browser.

HTTP Cookie

- ✓ Subsequent requests to the same website include these cookies, allowing the server to recognize the user and retrieve relevant information.

Uses of HTTP Cookies:

- ✓ **Session Management:** Cookies are commonly employed to maintain session state between the client and server. A session cookie, containing a unique identifier, allows the server to associate multiple requests from the same user as part of a session.
- ✓ **Personalization:** Websites use cookies to remember user preferences, such as language settings, theme choices, or personalized content recommendations.

Uses of HTTP Cookies:

- ✓ **Tracking and Analytics:** Cookies are utilized by advertisers and website owners to track user behavior, monitor site performance, and gather analytics data for targeted advertising and website optimization.
- ✓ **Authentication:** Cookies play a vital role in user authentication by storing authentication tokens or session identifiers, allowing users to remain logged in across multiple visits to a website.

Security Considerations:

- ✓ While HTTP cookies offer valuable functionality, they also present security and privacy concerns:

1. Cross-Site Scripting (XSS): Malicious scripts injected into web pages can access and manipulate cookies, potentially leading to session hijacking or data theft.

2. Cross-Site Request Forgery (CSRF): Attackers may exploit cookies to perform unauthorized actions on behalf of the user by tricking them into making unintended requests.

3. Session Hijacking: Insecure transmission of cookies over unencrypted connections (HTTP) can expose them to interception, allowing attackers to hijack user sessions.

4. Privacy Concerns: Cookies can be used to track users across websites, raising privacy concerns. Regulations like GDPR and CCPA impose restrictions on cookie usage and require transparent consent mechanisms.

Mobile Phone Security

Dr. Digvijaysinh Rathod
Associate Professor
School of Cyber Security and Digital Forensics
National Forensic Sciences University

digvijay.rathod@nfsu.ac.in