Session hijacking attack

Method

1. Inspect the page
2. Check if there is cookies in `/Applications/cookies`

   `I_am_admin : 68934a3e9455fa72420237eb05902327`
3. Decrypt the cookie value (md5)

   `68934a3e9455fa72420237eb05902327 : false`
4. Encrypt the value `true` (md5)

   `true : b326b5062b2f0e69046810717534cb09`
5. Replace the actual cookie value by the new one

   `I_am_admin : b326b5062b2f0e69046810717534cb09`
6. Refresh the page

Risks

The Session Hijacking attack consists of the exploitation of the web session control mechanism, which is normally managed for a session token. This attack compromises the session token by stealing or predicting a valid session token to gain unauthorized access to the Web Server.

Prevention

- **Use HTTPS**

Make sure that web servers and applications, require the use of HTTPS everywhere. In addition, all internet communications should be encrypted to ensure sessions are secured at every stage. Every interaction, including sharing session keys, should be encrypted with TLS/SSL. Security teams should also use robust client-side defenses to protect client browsers and session cookies from XXS attacks.

- **Use web session cookie**

Web frameworks simplify session management since they can generate more prolonged and random session cookies. This makes session tokens, cookies, and IDs harder to predict and exploit.

- **Always rotate session keys after authentication**

Changing the session key after a successful login makes it hard for a session hijacker to follow the user session even if they know the original key. Even if an attacker sends a phishing link that the user clicks on, attackers can’t hijack sessions with self-generated keys in such setups.

Flag

`df2eb4ba34ed059a1e3e89ff4dfc13445f104a1a52295214def1c4fb1693a5c3`

Resources

- https://owasp.org/www-community/attacks/Session_hijacking_attack
- https://md5decrypt.net/
- https://crashtest-security.com/session-hijacking-prevention/
- https://stackoverflow.com/questions/22880/what-is-the-best-way-to-prevent-session-hijacking