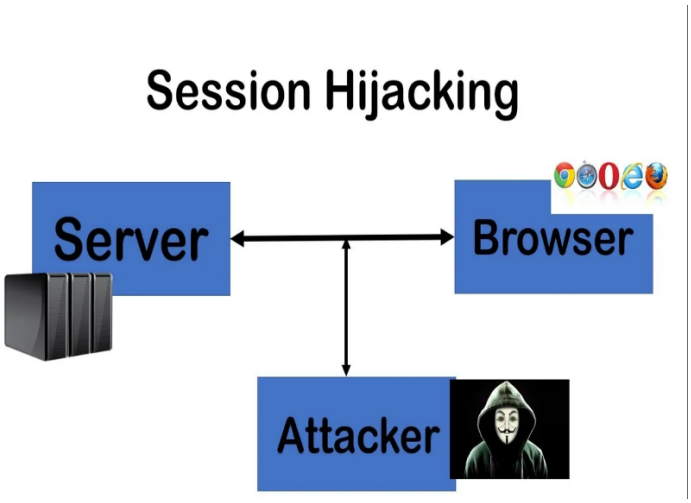
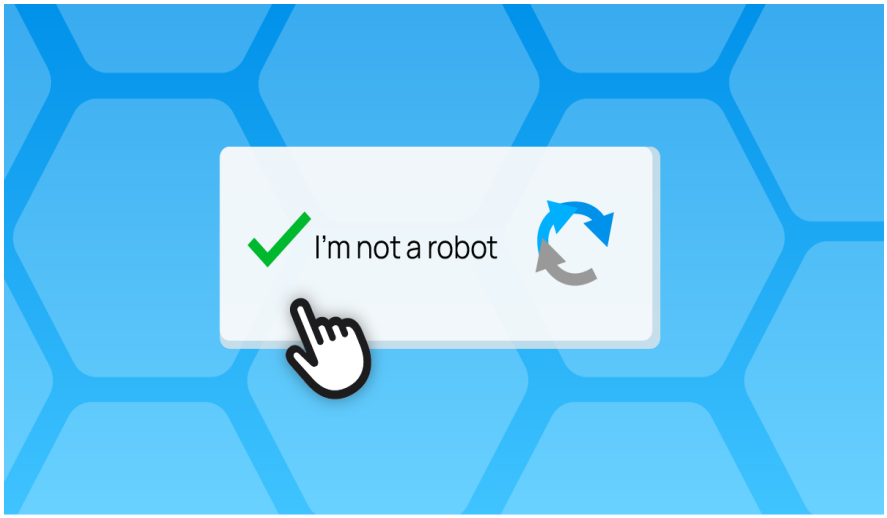
Session Fixation; Session Hijacking

&

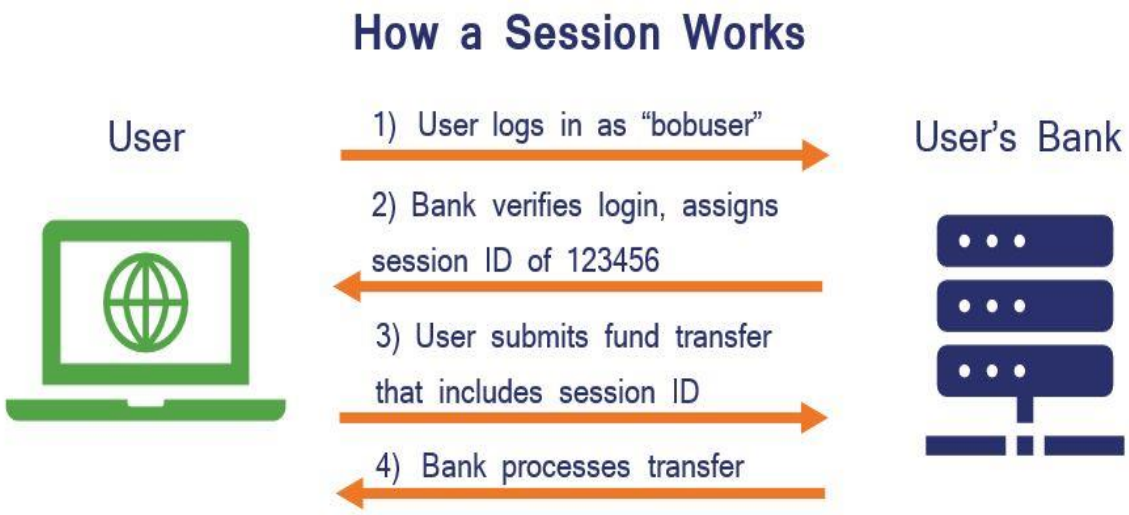
Captcha Bypass





Session

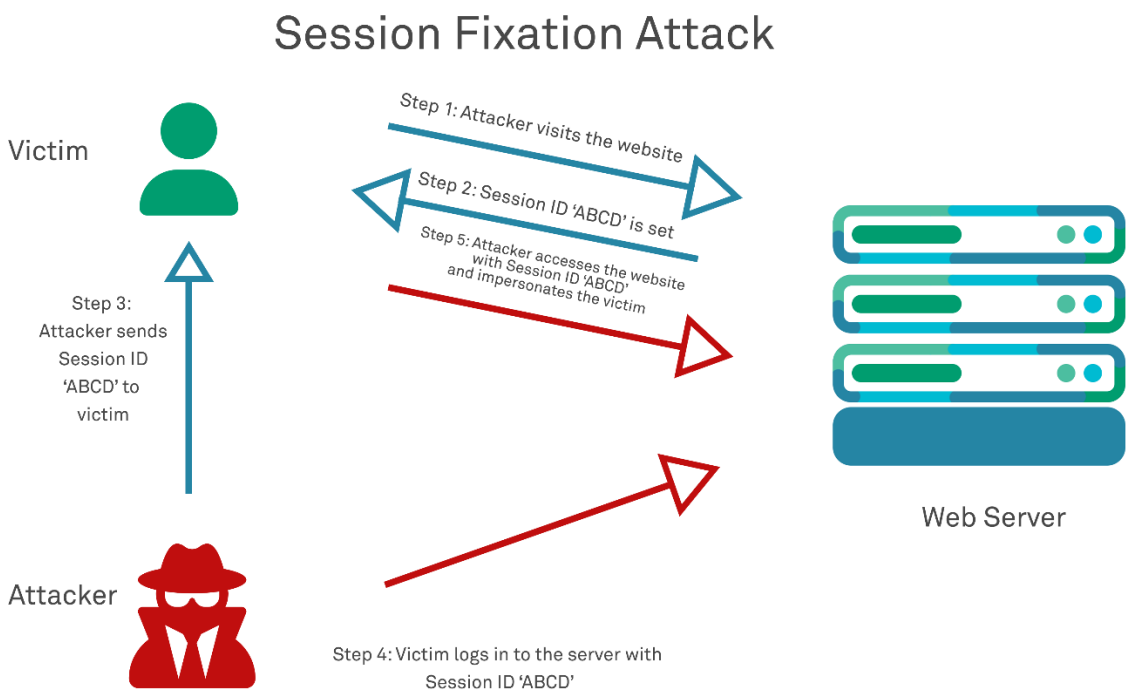
- A session is a sequence of interactions between a user and a system, typically a website, that occurs over a specified period.
- It allows websites to identify and remember users as they navigate through the site without requiring them to re-authenticate or re-enter information repeatedly.
- It is used to maintain stateful information about the user's activities on the website



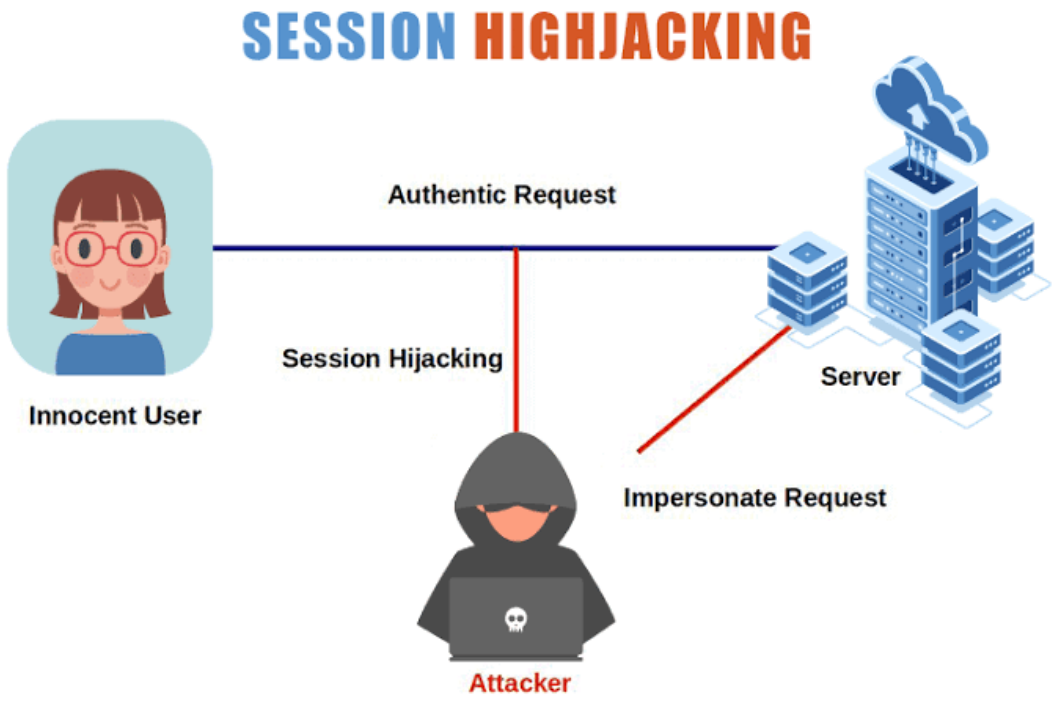
Session Fixation

- Session fixation is a type of web security vulnerability where an attacker sets or "fixates" a user's session identifier (typically stored in a cookie) to a known value.
- This can be done by tricking the victim into using a specific session ID, which the attacker can predict or has control over.
- Once the victim logs in or initiates a session with the manipulated session ID, the attacker can gain unauthorized access to the user's account.

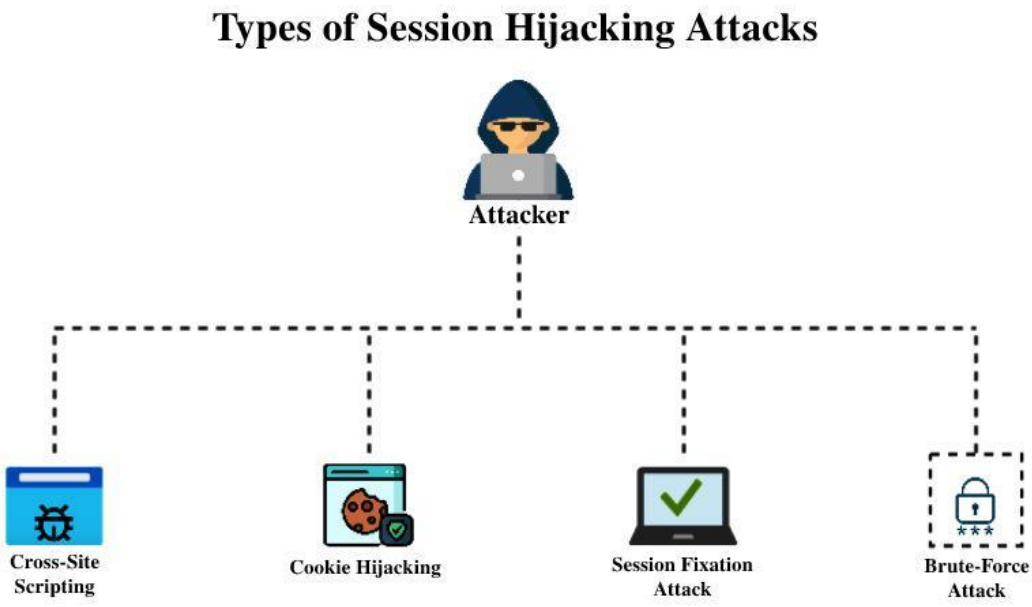
- To prevent session fixation, web applications should regenerate session identifiers after authentication and validate the session ID on each request to ensure it matches the one originally issued.



Session Hijacking



- Session hijacking, also known as session theft or session stealing, occurs when an attacker takes over an established user's session without their consent.
- There are several methods to achieve this, such as:
    a. **Session Fixation:** As mentioned earlier, an attacker may fixate a session ID and then hijack the user's session.
    b. **Session Sniffing:** Attackers can intercept network traffic to capture session cookies or tokens, especially if the communication is not encrypted (e.g., using HTTP instead of HTTPS).
    c. **Cross-Site Scripting (XSS):** In an XSS attack, malicious scripts injected into a website can steal session information when executed by unsuspecting users.



- To prevent session hijacking, web applications should use secure communication protocols (HTTPS), implement proper access controls, and employ mechanisms like HTTP-only cookies to make it more difficult for attackers to steal session information.

Difference Between Session Fixation and Session Hijacking

- The main difference between session fixation and session hijacking lies in how an attacker gains access to a user's session.
- In session fixation, the attacker sets a known session identifier in advance, while in session hijacking, the attacker steals or guesses the session identifier
- Session Fixation is a specific technique used in session hijacking.
- It involves setting a session ID to a known or controlled value before the victim logs in.
- Once the victim logs in using this session ID, the attacker can hijack the session. Session hijacking, on the other hand, encompasses a broader range of methods for taking over an active user's session, including session fixation, session sniffing, and XSS attacks.

Captcha Bypass

- Captcha (Completely Automated Public Turing test to tell Computers and Humans Apart) is a security mechanism used on websites to distinguish between automated bots and human users.
- A captcha typically presents a challenge, such as deciphering distorted text, selecting certain images, or solving puzzles, that a human can easily solve but is challenging for automated scripts.
- Captcha Bypass refers to techniques or methods used by attackers to circumvent or defeat captcha challenges, allowing automated bots or malicious actors to gain unauthorized access to websites or perform other malicious activities.
- Some common captcha bypass methods include:

a. **Captcha Solving Services:** Attackers can use third-party services or human workers to solve captchas automatically. These services employ humans who manually solve captchas in real-time.
b. **Machine Learning:** Sophisticated bots can use machine learning algorithms to recognize and solve captcha challenges, as they become more adept at pattern recognition.
c. **OCR (Optical Character Recognition):** Optical character recognition technology can be used to decipher text-based captchas programmatically.

- To mitigate captcha bypass, website administrators should regularly update and improve captcha mechanisms, deploy additional security layers, and monitor traffic for suspicious activity to detect and block automated bots.
- Additionally, rate limiting, IP blocking, and account verification measures can help prevent abuse of website services.

References

1. https://stackoverflow.com/questions/43752890/session-replay-vs-session-fixation-vs-session-hijacking
2. https://www.zenrows.com/blog/bypass-captcha-web-scraping
3. https://www.contrastsecurity.com/glossary/session-fixation-attack
4. https://captchas.io/