Session Management Attacks

Session Hijacking

Session Hijacking

- Research about Session Hijacking prevention methods in Web Applications
- What kind of policy can be used to protect users against Session Hijacking?

Session Hijacking - Solution

- A good countermeasure is destroying the session after a certain amount of time (for example an hour) or renewing it after validating the client browser
- Also, traffic must be encrypted using SSL/TLS to protect against eavesdropping
- The session itself must be encrypted and securely randomized. I.e. don't make these mistakes:
  - SESSID={"user": "manager"} , SESSID={"user": "john"}
  - SESSID=sess2564 , SESSID=sess2565
  - SESSID=rand()
- Also in the session validation phase, ensure the requests using a session are from the same client who initially established the session

ZDResearch Advanced Web Hacking

ZDResearch

www.zdresearch.com