Abstract

Session hijacking is also called as cookie hijacking in which the attacker exploits a valid computer session sometimes also called a session key or session token to get an unauthorized access to user system or back-end server. So to prevent this type of attack, we are creating a protocol that will prevent the attacker from gaining access to the encrypted cookie and back-end server. We are developing a Reverse proxy server (RPS) with a One Time Cookie (OTC) and generating a browser fingerprinting, IP address of system, session ID such that Reverse Proxy server handles a request using One Time Cookie (OTC) protocol to prevent adversary from capturing and injecting the session credentials. Also, we are using Blowfish Algorithm for encryption purposes. If any of these parameters alter than we can be easily identified the attacker.


Index Terms

Computer Science Security

Keywords

Session Hijacking, One Time Cookie, Reverse proxy server, Browser fingerprinting, session ID, IP address, Blowfish Algorithm, HTTP.