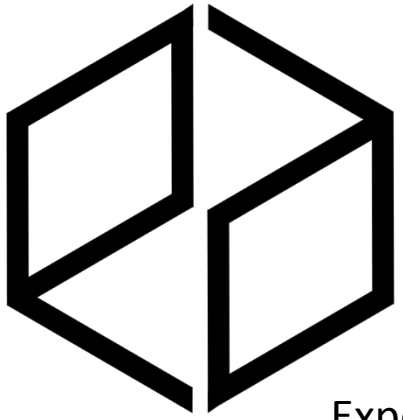

www.pandoralabs.net
PANDORA
SECURITY LABS
Expert advice. Experience advantage.
Proactive Security Solutions Through Cutting-Edge Research.



PANDORA
SECURITY LABS

Expert advice. Experience advantage.
Proactive Security Solutions Through Cutting-Edge Research.
www.pandoralabs.net

We are a Security-as-a-Service company

Providing businesses with on-demand IT security controls for them to meet their 24x7 security strategies & requirements.

We Make IT Secure

Developing Secure Applications

Quick Tips

Session Management

Session Authentication

- Session management is by its nature closely tied to authentication, but this does not mean users should be considered authenticated until the web application has taken positive action to tie a session with a trusted credential or other authentication token.

Session Authentication

- If possible, tie a session to a specific IP. Force re-authenticate if the IP changes. This is to prevent hijacking and replay attacks.

- Ensure that unauthenticated users does not have any or have minimal privileges only.

Session Authentication

- Ensure all unprotected pages use as few resources as possible.
- Ensure all uprotected pages should not leak information about the protected portion of the application.
- Enforce session timeouts.

Session Timeout

- Session tokens that do not expire on the HTTP server can allow an attacker unlimited time to guess or brute-force a valid authenticated session token.
- An example is the "Remember Me" option on many retail websites. If a user's cookie file is captured or brute-forced, then an attacker can use these static-session tokens to gain access to that user's web accounts. This problem is particularly severe in shared environment, where multiple users have access to one computer.
- Additionally, session tokens can be potentially logged and cached in proxy servers that, if broken into by an attacker, could be exploited if the particular session has not been expired on the HTTP server.

Homework:

- Enforce session timeout on your website


www.pandoralabs.net
PANDORA
SECURITY LABS
Expert advice. Experience advantage.
Proactive Security Solutions Through Cutting-Edge Research.