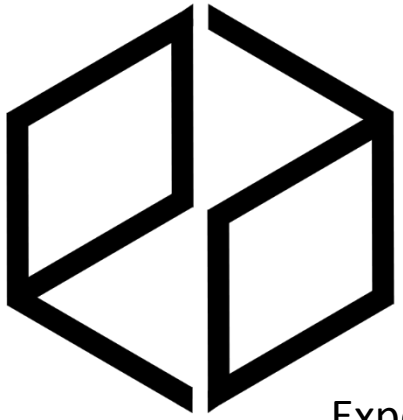

www.pandoralabs.net
PANDORA
SECURITY LABS
Expert advice. Experience advantage.
Proactive Security Solutions Through Cutting-Edge Research.



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

Error Handling, Auditing, and Logging

Log Relevant Data

- Auditable – all activities that affect user state or balances are formally tracked
- Traceable – it’s possible to determine where an activity occurs in all tiers of the application
- High integrity – logs cannot be overwritten or tampered by local or remote users
- Audit logs are legally protected – protect them

Log Relevant Data

- Data from logs can be used to monitor your application
- Never log confidential data!
- Consider hooking your system to a centralized logging server or other security solutions like a Security Information and Event Manager (SIEM)
- Logging may be a requirement if you are tying to comply to some security standards like PCI-DSS or HIPAA

Log Relevant Data

Use heuristics and other business logic to determine if users are likely to act on a certain sequence of events, such as:

- Clearing out their accounts
- Conducting many small transactions to get under your daily limits or other monitoring schemes
- If orders from multiple accounts are being delivered to the same shipping address.
- If the same transactions are being performed quickly from the same IP address

Never Disclose Information via Error Messages

- Stack traces show the inner workings of an application
- Do not give attackers clue about your application (ie. Invalid username / password)
- Use generic error messages


www.pandoralabs.net
PANDORA
SECURITY LABS
Expert advice. Experience advantage.
Proactive Security Solutions Through Cutting-Edge Research.
OWASP TOP 10: #1 Injection
By @isaacsabas