Compliance Report

Standard: OWASP-ASVS-Level-3

User Accounts

Report generated by:	Administrator admin
Unique ID:	user-accounts
Workflow State:	

Index

Summary

Countermeasure Compliance Status
- Verified countermeasures
  - Component: Generic Service
- Implemented countermeasures
  - Component: MySQL
- Required countermeasures
  - Component: Generic Service
  - Component: MySQL
- Non-Compliance
  - Component: Generic Service
  - Component: MySQL

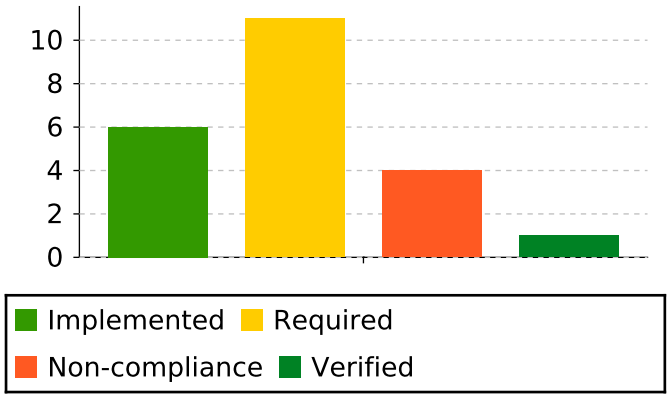
Summary

Shown below is a brief description of the product and summary analysis of the risks.

Product name:	User Accounts
Unique ID:	user-accounts
Product description:	
Business unit:	bu_user_admin
Owner:	Administrator admin

Compliance Summary

Below are the current countermeasure status' for the selected standard.



Countermeasure Compliance Status

Below are the current countermeasure status' for the selected standard per component.

Verified

Verified countermeasures are those with passed test results.

Component: Generic Service

- Escape meta-characters from un-trusted data

Implemented

Implemented countermeasures are those with implemented countermeasure status.

Component: Generic Service

- Escape meta-characters from un-trusted data
- Do not write secrets to the log files
- Develop a log retention policy
- Restrict actions of users that follow unusual patterns.

Component: MySQL

- Require authentication before presenting restricted data
- Access the data store from an account with the least privileges necessary

Required

Below are the “required” countermeasures per component.

Component: Generic Service

- Log details of user actions within the system
- Log and reject all data validation failures
- Encrypt data between the client and server/service
- Use a synchronised time source
- Validate all data received from the client side
- Log the backend TLS connection failures
- Ensure the integrity of the logging system
- Limit the number of accounts with privileges allowing modification and/or deletion of audit logs files
- Ensure that the client-side and the server-side are using the same encoding style

Component: MySQL

- Use prepared statements for all database queries
- Apply required security patches to the service

Non-Compliant

Below are the non-compliant countermeasures per component. “Non-compliant” are those countermeasures that are marked as recommended or rejected in the model, but required by the standard.

Component: Generic Service

Unique ID	Countermeasure name	Countermeasure description
RESTRICT-NUMBER-ACCOUNT-TO-LOGS	Limit the number of accounts with privileges allowing modification and/or deletion of audit logs files	Limit the number of account with privileges to modify and/or delete audit logs files.

Component: MySQL

Unique ID	Countermeasure name	Countermeasure description
CWE-306-SERVICE	Require authentication before presenting restricted data	The application should ensure users have undergone an Identification and Verification (ID&V) process before allowing access to secret, sensitive or otherwise restricted data. For less sensitive but still restricted data, simple verification of the location of the user may suffice (e.g. IP restrictions). • For non-sensitive but non-public data, access could be restricted by IP address, for example limiting access to internal networks, workstations, or gateways • For more sensitive data, TLS client-side certificates may be appropriate • Where secret or other sensitive data is handled, a full authentication process to identify and validate users with single or multi-factor authentication may be required