PCIDSS Compliance Report

Compliance Check Results

Check	*Description*	*Result*	*Remedy (if failed)*
SSH connection	Ensure that the SSH connection to the server is secure.	**Passed**	N/A
MySQL connection	Ensure that the system can connect to the MySQL database.	**Failed**	Check the database credentials and ensure the MySQL server is running.
Firewall configuration	Ensure that firewalls are implemented to protect cardholder data.	**Failed**	Configure firewalls to restrict inbound and outbound traffic to only what is necessary.
Encryption of cardholder data	Ensure that encryption is used to protect cardholder data in transit.	**Passed**	N/A
User access control	Ensure proper access controls are in place to protect cardholder data.	**Failed**	Implement role-based access control (RBAC) for restricting access to cardholder data.
Logging for cardholder data access	Ensure logging mechanisms are in place to track access to cardholder data.	**Failed**	Implement logging for access to cardholder data and regularly review these logs.
Vulnerability management	Ensure that a vulnerability management program is in place.	**Passed**	N/A
Security Systems Test	Verify that security systems are active.	**Failed**	IDS/IPS (snort) is not running or not active.