PCI COMPLIANCE AND OWASP TOP 10

#	PCI DSS Security Controls	OWASP Top 10 - Mapping	STATUS
1	**USE AND MAINTAIN FIREWALLS**	The maintenance of firewalling is addressed by OWASP, officially OWASP has mentioned tool name "WAF" for managing firewall. Also, providing protection against common attacks like cross-site scripting (XSS) and SQL Injection where both comes under the rules of OWASP.	✓
2	**PROPER PASSWORD PROTECTIONS**	To protect passwords, OWASP has password protection set of rule which is authentication, mentioning all the possible solutions for password protection. To dig more information they have online page with reference to all the possible solutions i.e. https://owasp.org/www-pdf-archive/OWASP_Application_Security_Verification_Standard_4.0-en.pdf.	✓
3	**PROTECT CARDHOLDER DATA**	OWASP has many ways to provide proper set of security controls on protection of card holder data. According to PCI, encryption should be done to protect the information of the client and OWASP also guides for testing of weak encryption standards. Moreover, they also has solution to cover sensitive data exposure, insecure deserialization and broken authentication for protecting the cardholder data in many ways.	✓
4	**ENCRYPT TRANSMITTED DATA**	The testing of this part is also provided by OWASP. To protect the data OWASP tests for the weak ciphers, SSL/TLS, insufficient transport layer protection and moreover the sensitive/unencrypted channels through which traffic is sent.	✓
5	**USE AND MAINTAIN ANTI-VIRUS**	There is no specifically mentioned use of anti-virus, however, the security configuration principle of OWASP in which patches need to be updated and maintained may serve the purpose.	~
6	**PROPERLY UPDATED SOFTWARE**	The OWASP guides to keep the security patches up to date to maintain all the libraries and frameworks securely configured.	✓
7	**RESTRICT DATA ACCESS**	The access control principle provides complete guidelines how to manage access controls on data, moreover, session management is also provided by the OWASP where to keep the session protected in order to protect data leakage.	✓
8	**UNIQUE IDS FOR ACCESS**	The OTG has a complete set of rules for creating id and providing access controls. To provide security everything is available in the checklist along with different sets of testing.	✓
9	**RESTRICT PHYSICAL ACCESS**	The physical access is mentioned to some extent under components with known vulnerabilities. To keep secure access to everything it is needed to avoid use of components with known vulnerabilities.	✓
10	**CREATE AND MAINTAIN ACCESS LOGS**	Logging and monitoring is one of the principle of OWASP to keep the data secure otherwise attack could be possible in form of tampering, extracting or destruction of data etc.	✓
11	**SCAN AND TEST FOR VULNERABILITIES**	OWASP itself is methodology to find vulnerabilities in the infrastructure. The top 10 principles is well known to do all scanning and testing with tools as officially mentioned online.	✓

12	**DOCUMENT POLICIES**	The cheat sheets for tasks are available but no such documentation for policy is mentioned by OWASP.	✖