

ID	OWASP Reference*	OWASP Category*	Description*	Action Required	Assigned To	Priority	Open Date	Projected Resolve Date	Resolved Date	Status	Notes
001	OWASP-AT-001	Authentication Testing	Credentials transport over an encrypted channel	Only use secure channels such as HTTPS to transport authentication credentials	Vendor Name	Medium	06/23/09		08/28/09	Closed	
002	OWASP-IG-006	Information Gathering	Analysis of Error Code	Use universal server-wide error pages that do not disclose sensitive details	Vendor Name	Low	06/23/09	See notes	n/a	Closed	
003	OWASP-IG-006	Information Gathering	User controllable error message	Do not rely on user supplied input to control application output	Vendor Name	Low	06/23/09	See notes	n/a	Closed	
004	OWASP-CM-001	Configuration Management	HTTP running on secure site	HTTPS should be forced	Vendor Name	Medium	06/23/09	Not an issue-See notes	08/28/09	Closed	
005	OWASP-IG-006	Information Gathering	User controllable error message	Do not rely on user supplied input to control application output	Vendor Name	Medium	06/23/09	Not an issue-See notes	n/a	Closed	
006	OWASP-DV-001	Data Validation Testing	Reflexive Cross Site Scripting	Use a white-list to ensure that user supplied input is properly validated	Vendor Name	High	06/23/09	Resolved	08/28/09	Closed	
007	OWASP-AZ-001	Authorization Testing	Path Traversal	Use a white-list to ensure that user supplied input is properly validated	Vendor Name	High	06/23/09	Resolved	08/28/09	Closed	
008	OWASP-SM-002	Session Management	User names in cookies	do not store sensitive information in cookies	Vendor Name	High	06/23/09	Resolved	08/28/09	Closed	
009	OWASP-AT-001	Authentication Testing	Credentials transport over an encrypted channel	do not store sensitive information using encoding or hashing algorithms Instead use secure encryption protocols	Vendor Name	High	06/23/09	Not an issue-See notes	08/28/09	Closed	

\*Ref : OWASP Testing Guide v3

Low

Medium

High