Checklist

Category	Ref Number	Name	Objective	Notes	
AppDOS	OWASP-AD-001	Application Flooding	Ensure that the application functions correctly when presented with large volumes of requests, transactions and / or network traffic.	Use various fuzzing tools to perform this test (e.g. SPIKE)	✓
	OWASP-AD-002	Application Lockout	Ensure that the application does not allow an attacker to reset or lockout user's accounts.		✓

Category	Ref Number	Name	Objective	Notes	
AccessControl	OWASP-AC-001	Parameter Analysis	Ensure that the application enforces its access control model by ensuring that any parameters available to an attacker would not afford additional service.	Typically this includes manipulation of form fields, URL query strings, client-side script values and cookies.	✓
	OWASP-AC-002	Authorization	Ensure that resources that require authorization perform adequate authorization checks before being sent to a user.		✓
	OWASP-AC-003	Authorization Parameter Manipulation	Ensure that once valid user has logged in it is not possible to change the session ID’s parameter to reflect another user account	i.e. accountnumber, policynumber,usernr etc.	✓
	OWASP-AC-004	Authorized pages/functions	Check to see if its possible to access pages or functions which require logon but can be bypassed		✓
	OWASP-AC-005	Application Workflow	Ensure that where the application requires the user to perform actions in a specific sequence, the sequence is enforced.		✓

Category	Ref Number	Name	Objective	Notes	
Authentication	OWASP-AUTHN-001	Authentication endpoint request should be HTTPS	Ensure that users are only asked to submit authentication credentials on pages that are served with SSL.	This ensures that the user knows who is asking for his / her credentials as well as where they are being sent.	✓
	OWASP-AUTHN-002	Authentication bypass	Ensure that the authentication process can not be bypassed.	Typically this happens in conjunction with flaws like SQL Injection.	✓
Authentication. User	OWASP-AUTHN-003	Credentials transport over an encrypted channel	Ensure that usernames and passwords are sent over an encrypted channel.	Typically this should be SSL.	✓
	OWASP-AUTHN-004	Default Accounts	Check for default account names and passwords in use		
	OWASP-AUTHN-005	Username	Ensure that the username is not public (or “wallet”) information such as email or SSN.		✓
	OWASP-AUTHN-006	Password Quality	Ensure that the password complexity makes guessing passwords difficult.		✓
	OWASP-AUTHN-007	Password Reset	Ensure that user must respond to a secret answer / secret question or other predetermined information before passwords can be reset.	Ensure that passwords are not sent to users in email.	✓

Category	Ref Number	Name	Objective	Notes	
Configuration. Management	OWASP-CM-001	HTTP Methods	Ensure that the web server does not support the ability to manipulate resources from the Internet (e.g. PUT and DELETE)		✓
	OWASP-CM-002	Virtually Hosted Sites	Try and determine if site is virtually hosted.	If there are further sites, they could be vulnerable and lead to the compromise of the base server	✓
	OWASP-CM-003	Known Vulnerabilities / Security Patches	Ensure that known vulnerabilities which vendors have patched are not present.		✓
	OWASP-CM-004	Back-up Files	Ensure that no backup files of source code are accessible on the publicly accessible part of the application.		✓
	OWASP-CM-004	Web Server Configuration	Ensure that common configuration issues such as directory listings and sample files have been addressed		✓
	OWASP-CM-005	Web Server Components	Ensure that web server components like Front Page Server Extensions or Apache modules do not introduce any security vulnerabilities		✓
	OWASP-CM-006	Common Paths	Check for existence of common directories within the application root	/backup & /admin may contain information	✓

! OWASP-AUTHN-008

It’s not Possible for attackers to bruteforce users Password since we implemented a strict password creation requirements, in addition of protection against flood requests, which will block the attacker from accessing our resources for 24h if they are using some sort of attacking tools.

Category	Ref Number	Name	Objective	Notes	
	OWASP-AUTHN-008	Password Lockout	Ensure that the users account is locked out for a period of time when the incorrect password is entered more that a specific number of times (usually 5).		!
	OWASP-AUTHN-009	Password Structure	Ensure that special meta characters cannot be used within the password	Can be useful when performing SQL injection	✓
	OWASP-AUTHN-010	Blank Passwords	Ensure that passwords are not blank		✓
Authentication. SessionManagement	OWASP-AUTHSM-001	Session Token Length	Ensure that the session token is of adequate length to provide protection from guessing during an authenticated session.		✓
	OWASP-AUTHSM-002	Session Timeout	Ensure that the session tokens are only valid for a predetermined period after the last request by the user.		✓
	OWASP-AUTHSM-003	Session Reuse	Ensure that session tokens are changed when the user moves from an SSL protected resource to a non-SSL protected resource.		✓
	OWASP-AUTHSM-004	Session Deletion	Ensure that the session token is invalidated when the user logs out.		✓
	OWASP-AUTHSM-005	Session Token Format	Ensure that the session token is non-persistent and is never written to the browsers history or cache.		✓

Category	Ref Number	Name	Objective	Notes	
	OWASP-CM-007	Language/Application defaults	I.e. J2EE environmental quirks e.g Availability of snoop.jsp /*Spy.jsp and loaded modules		✓
Configuration. Management Infrastructure	OWASP-CM-008	Infrastructure Admin Interfaces	Ensure that administrative interfaces to infrastructure such as web servers and application servers are not accessible to the Internet.		✓
Configuration. Management. Application	OWASP-CM-009	Application Admin Interfaces	Ensure that administrative interfaces to the applications are not accessible to the Internet.		✓

Category	Ref Number	Name	Objective	Notes	
Error Handling	OWASP-EH-001	Application Error Messages	Ensure that the application does not present application error messages to an attacker that could be used in an attack.	This typically occurs when applications return verbose error messages such as stack traces or database errors.	✓
	OWASP-EH-002	User Error Messages	Ensure that the application does not present user error messages to an attacker that could be used in an attack.	This typically occurs when applications return error messages such as “User does not exist” or “User Correct, Password Incorrect”	!

Category	Ref Number	Name	Objective	Notes	
DataProtection	OWASP-DP-001	Sensitive Data in HTML	Ensure that there is no sensitive data in the HTML (cached in the browser history) that could lead an attacker to mount a focused attack.	This typically occurs when developers leave information in html comment or the application renders names and addresses in HTML.	✓
	OWASP-DP-002	Data Storage	Ensure where required, data is protected to protect its confidentiality and integrity.		✓
DataProtection. Transport	OWASP-DP-003	SSL Version	Ensure that SSL versions supported do not have cryptographic weaknesses.	Typically this means supporting SSL 3 and TLS 1.0 only.	✓
	OWASP-DP-004	SSL Key Exchange Methods	Ensure that the web server does not allow anonymous key exchange methods.	Typically ADH Anonymous Diffie-Hellman.	✓
	OWASP-DP-005	SSL Algorithms	Ensure that weak algorithms are not available.	Typically algorithms such as RC2 and DES.	✓
	OWASP-DP-006	SSL Key Lengths	Ensure the web site uses an appropriate length key.	Most web sites should enforce 128 bit encryption.	✓
	OWASP-DP-007	Digital Certificate Validity	Ensure the application uses valid digital certificates.	Ensure that the digital certificate is valid, that is to say its signature, host, date etc are all valid.	✓

Category	Ref Number	Name	Objective	Notes	
InputValidation	OWASP-IV-001	Script Injection	Ensure that any part of the application that allows input does not process scripts as part of the input.	Classic case of Cross Site Scripting but includes other scripting as well.	✓
InputValidation.SQL	OWASP-IV-002	SQL Injection	Ensure the application will not process SQL commands from the user.		✓
InputValidation.OS	OWASP-IV-003	OS Command Injection	Ensure the applications will not process operating system commands from the user.	This typically includes issues such as path traversal, spawning command shells and OS functions.	✓
InputValidation.LDAP	OWASP-IV-004	LDAP Injection	Ensure the application will not process LDAP commands form the user.		✓
InputValidation.XSS	OWASP-IV-005	Cross Site Scripting	Ensure that the application will not store or reflect malicious script code.		✓

Category	Ref Number	Name	Objective	Notes	
BufferOverflow	OWASP-BO-001	Overflows	Ensure that the application is not susceptible to any buffer overflows.	Fuzzing tools help with testing all components of an application for this issue.	✓
	OWASP-BO-002	Heap Overflows	Ensure that the application is not susceptible to any heap overflows.		✓
	OWASP-BO-003	Stack Overflows	Ensure that the application is not susceptible to any stack overflows.		✓
	OWASP-BO-004	Format Strings	Ensure that the application is not susceptible to any format string overflows.		✓