OWASP Web Application Security Quick Reference Guide 0.3

Introduction

This checklist contains the basic security checks that should be implemented by all Web Applications.

The checklist contains following columns:

- Name – The name of the check.
- Check Question – The check is presented as a question
- Required Answer – This column contains the answer that is required for the check question.
- How to check – It contains a simple description of how this should be tested.
- Comments – Additional comments about the check containing best practice and references to OWASP documentation.

Web Application Security Checklist

Name	Check Question	RA	How to check	Comments
User management				
Simple passwords	Do the users have simple passwords?	No	Verify if the password meets the policy.	If there is no policy, check if the password meets OWASP recommendation: OWASP Reference - Password length & complexity
Simple password without verification	Does the application check the complexity of the password during the password change?	Yes	Verify if a password meets the policy during the password changing process.	If there is no policy, check if the password meets OWASP recommendation: OWASP Reference - Password length & complexity
Empty passwords	Can empty passwords be used?	No	Check if the user can change a password to a blank password.	OWASP Reference - Password length & complexity
Password case insensitive	When using a case-sensitive password (PaSsWorD134) is it possible to login using the case-	No	Check if the user can log in using only small or capital characters.	OWASP Reference - Password length & complexity

	insensitive version of it (password123/PASSWORD123)?			
Saving login and password	Does the browser ask users to store their login and password?	No	One needs to check, if the server's response contains proper parameter (AUTOCOMPLETE=OFF in IE, disableautocomplete in Firefox, etc.).	OWASP Testing for Vulnerable Remember Password
Lack of "Change Password" functionality	Can user change his password?	Yes	Check if the application allows user to change the password.	All applications should give the users opportunity to change password any time.
Lack of verification during password change	Is the old password required during the password change?	Yes	Verify if the old password is needed when using the password change functionality.	When an attacker steals the session, she/he will not be able to change the password if the old one is required.
Using old passwords	Can the user change a password to the previous one?	No	Check if user can change password to the previous one.	Using the previous password implies that the users are not willing to change to a new one. If the user is using the same password all the time, the password is more vulnerable to be guessed.
Password reset DoS	Is it possible to reset user password by providing known data, without confirmation through separate channels (e-mail, phone, SMS)?	No	- Check if the password reset tool forces the user to immediately change the password. - Check if the password reset only needs the user to answer the secret questions.	OWASP Testing for Vulnerable Pwd Reset
Locking account after few tries	Is the account blocked after few incorrect login attempts?	Yes	Check if account is locked after a few incorrect login attempts.	This protects against brute force attack. The account lockout can be temporary.
Automatic account creation	Is there any protection against automatic account creation (for example CAPTCHA)?	Yes	- Check Accessibility: CAPTCHA must be accessible by all. Audio CAPTCHA for the visually impaired. - Check if Images of text are distorted randomly. - Check if response is sent in cleartext or in encrypted/hashed form.	This check is only for the applications that allow creating new user accounts. CAPTCHA prevents against malicious software that creates accounts for the purpose of SPAMMING. Prevent Dictionary attacks in the password systems, Protect website registration by 'bots'. Encryption/hash algorithm should be sufficiently strong.

Locking (Disabling) non-existing accounts	Is the message for existing accounts the same as the message for non-existing accounts when one tries to lock this account?	Yes	Compare two responses from the login request: - Account exists and is locked and password is correct. - Account does not exist. Both responses should be the same.	If there is a different message an attacker is able to enumerate the existing accounts.
Information about wrong login and password	Are there any differences between the message when an account doesn't exist and the message when an account is correct but password is wrong during the login process?	No	Compare two responses from the login request: - Account is correct and password is incorrect. - Account does not exist and password is random. Both responses should be the same.	If there is a different message an attacker will be able to enumerate the existing accounts.
Public login and password	Are the login and password sent over clear text?	No	The login and password should always be sent via HTTPS instead of HTTP	If the login and password are not encrypted, there is a possibility that it can be hijacked by an attacker.
Log out user after a period of time	Is the user logged out after period of inactivity (usually 30 min)?	Yes	Wait required amount of time and see if the user session was terminated.	Each application should log out the user after a period of time. The time is reliant on the type of the application but it never should be infinite. This one should be implemented server side. OWASP Reference - Session Expiration
Session termination after closing application	Does the application terminate the session after the application is closed?	Yes	Check is the session id is deleted after the application is closed.	OWASP Reference - Client-Side Defenses for Session Management
Session management				
Random SessionID	Is SessionID random?	Yes	The Sequencer tab from Burp Suite can be used to check the session randomness.	OWASP Reference - Session Prediction OWASP Reference - Session ID Entropy
Simple SessionID	Is SessionID simple?	No	This check should be done through source code review. You need to check if the mechanism of SessionID generation is predictable –if an attacker	OWASP Reference - Session Management Implementations

			knows the code on how SessionID's are generated, is the next SessionID predictable. For example: SessionID is MD5 from time stamp. For outsider this ID is very random but if you know that this is MD5 from timestamp it is likely to predict next IDs.	
Changing SessionID after logout	Does the SessionID change after logout?	Yes	Using a proxy tool and capturing the whole login event can perform these checks.	It is good practice to delete the SessionID from the browser that is not used any more. OWASP Reference - Renew Session ID After Any Privilege Level Change
Changing SessionID after login	Does the SessionID change after login?	Yes	Check if the response from the login request sets a new cookie.	OWASP Reference - Renew Session ID After Any Privilege Level Change
Using old SessionID	Does the server use the old SessionID?	No	Check if the server can be forced to use the old session cookie.	OWASP Reference - Renew Session ID After Any Privilege Level Change
Sending SessionID through GET	Is the SessionID sent in GET parameters?	No	Check if there is any request that send SessionID in GET parameters.	Sensitive information within URLs may be logged in various locations, including the user's browser, the web server, and any forward or reverse proxy servers between two endpoints.
Changing SessionID when the channel is changed	Is the SessionID changed after switching to the open channel?	Yes	If the application change the channel from HTTP to HTTPS check if the session cookie has also be changed.	OWASP Reference - Transport Layer Security
Secure cookies	Is the secure attribute set for the cookies?	Yes	Capture the set of cookies that are getting generated by the Web Application and check for the secure attribute in the cookie, which contains important information.	OWASP Reference - Secure Attribute
Cookie's domain	Is the cookie's domain set to parent?	Yes	Cookie Analysis can fetch can be used to check this.	OWASP Reference - Domain and Path Attributes

Option HTTPOnly	Is the HTTPOnly option set for cookies?	Yes	Capture the cookie using a proxy like burp or using extensions of Firefox can check the same.	OWASP Reference - HttpOnly Attribute
Concurrent user session allowed	Is it possible to have 2 or more active sessions with one account at the same time?	No	Use two separate browsers to login with the same account and see if two active sessions are allowed at the same time.	OWASP Reference - Simultaneous Session Logons
Server HTTP				
Access to .htpasswd	Is it possible to access to the .htpasswd file?	No		
PUT method	Can the PUT method be used?	No	Check for the different verbs that are enabled in the server.	Enables an attacker to upload malicious content.
Server version	Does the server send its version number in the header?	No	Check HTTP response if there is any information about the server.	If an attacker knows the server version, she/he can create more adjusted types of attacks. This information also helps in automated attacks on particular server version.
Contents of robots.txt	Is the robots.txt accessible? Are there any directories inside?	No		
Communication channel				
Using SSL	Is the channel encrypted?	Yes	If the application is using HTTPS check if it possible to send request using HTTP, in particular if user can log in to the application.	OWASP Reference - Transport Layer Security
SSL Cipher Strength	Can weak ciphers be used?	No	This can be check by SSLDigger, which is free tool.	
SSL v2	Is the SSL version 2 used?	No	This can be check by SSLDigger, which is free tool.	
SSL v3	Is SSL version 3 used?	No	This can be check by SSLDigger, which is free tool.	
SSL – Client initiated renegotiation/Secure renegotiation	Is client initiated renegotiation allowed?	No	This can be check by openssl.	OWASP Reference - Client Initiated Renegotiation and Secure Renegotiation

SSL certificate expiry	Did the SSL certificate expire?	No	This can be done using a browser.	
SSL certificate validation	Is the SSL certificate valid for the domain?	Yes	This can be done using a browser.	
HSTS header	Is the HSTS header used	Yes	Check the HTTPS response if this header is set.	OWASP Reference - HTTP Strict Transport Security
Online Banking Application Checks				
Negative amounts	Are negative amount transactions possible?	No		
Very small amount	Are there any transactions where the amount is very small (for example 0,001)?	No		
Transfer on itself	Can one make the transfer on the same account (src=dest)?	No		
Currency conversion	Is the currency conversion done correctly during the transfer?	Yes		
Credit card numbers revealed	Are the credit cards numbers visible?	No		
History of account	Can one see the history of other user's accounts?	No		
Account balance	Can one see other user's account balance?	No		
Incorrect deposit	Can one make an investment on the lowest value that is required?	No		
Incorrect period	Can a different period be than what is required by form?	No		
Others				
Software version	Is the technology used by the application revealed? For example PHP or ASP version?	No	Check if in the HTTP response if any information about the framework, platform is displayed.	If an attacker knows the technology/version being used, she/he can create more adjusted types of attacks. This information can also help in automated attacks on particular technology.

POST sent by GET	Can the parameters from the POST request be sent using the GET parameters?	Yes	Check if requests made by POST can be done using a GET method especially login request.	
X-Frame-Options	Does application use X-Frame-Option HTTP header with DENY or SAMEORIGIN value?	Yes	Check for main page, login page, user settings page.	OWASP Clickjacking OWASP Clickjacking Defense Cheat Sheet
X-XSS-Protection	Does application use X-XSS-Protection HTTP header with 1 value and mode with block value?	Yes	Check for main page, login page, user settings page.	
X-Content-Type-Options	Does the application use X-Content-Type-Options HTTP header with nosniff value?	Yes	Check for main page, login page, user settings page.	
Silverlight Cross-Domain Policy	Is the wildcard used in the policy file?	No		OWASP Reference - Client-Side Cross-Domain Requests
Flash Cross-Domain Policy	Is the wildcard used in the policy file?	No		There are only a small number of legitimate use cases for full wildcard (*) permissions. If granting full permission is absolutely necessary, then the best practice is to create a sub-domain on your site whose explicit purpose is to serve cross-domain data. Another option is to leverage Flash Player's support of per-directory cross-domain permissions and place the data and the full wildcard cross-domain policy within a sub-directory of the site dedicated for that purpose. Full wildcards on internal networks can also be dangerous since they can result in external content being granted access to internal resources. A full wildcard should also never applied to the headers attribute of the allow-http-request-headers-from element or the to-

				ports attribute of the allow-access-from element in production. Once, a wildcard permission has been deployed, it can be very challenging to restrict permissions at a later date because there is no easy way to identify what content depends on that permission. OWASP Reference - Client-Side Cross-Domain Requests
External scripts on login page	Are there any script tags with src from external domain on login page?	No		
Cacheable entries	Is the browser caching the pages with confidential info?	No		OWASP Reference - Testing for Logout and Browser Cache Management
Sensitive information set in cookies	Is any sensitive information sent unencrypted using cookies?	No		Some applications would use cookies to send sensitive information such as storing the user's username/userID unencrypted as a cookie value.
Sensitive POST returns 200 OK	When logging into and application/changing user's password does the application respond with 200 OK on a successful request?	No	Check when using a sensitive POST such as logging in or changing the user's password if the application responds with 200 OK.	

Contributors

Monika Chakraborty monikac@itsecurit.com
Piotr Duszyński piotr@duszynski.eu
Łukasz Pilorz lukasz.pilorz@owasp.org
Amit Kumar Sharma (aKs) amitsharma2009@gmail.com
Paweł Wyleciał pawel.wylecial@gmail.com
Marek Zmysłowski marek.zmyslowski@owasp.org
Christiaan Esterhuizen cesterhuizen@gmail.com