OWASP Web Application Security Quick Reference Guide 0.2

Introduction

This checklist contains the basic security checks that should be implemented in any Web Application.

The checklist contains following columns:

- Name – It is the name of the check.
- Check Question – It contains a check in the form of a question.
- Required Answer – This column contains the answer that is required for the check question.
- How to check – It contains simple description 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	Have users got simple password?	No	Check if a 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 complexity of the password during the password change?	Yes	Check if a password meets the policy during the 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
Saving login and password	Does the browser ask users to store their login and password?	No	One needs check, if server's response contain proper parameter (AUTOCOMPLETE=OFF in IE, disableautocomplete in Firefox, etc.).	OWASP Testing for Vulnerable Remember Password

Lack of verification during password change	Is the old password required during the password change?	Yes	Check if during the process of changing password, old password is required.	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 the new one. If the user is using the same password all 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 channel (e-mail, phone, SMS)?	No	- Check if the password reset tool forces the user to immediately change password. - Check if password is reset only by answering secret questions.	OWASP Testing for Vulnerable Pwd Reset
Locking account after few tries	Is the account blocked after few tries?	Yes	Check if account is locked after few tries of login.	This protects against brute force attack. The lock 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 visually impaired. - Check if Images of text are distorted randomly. - Check if response is sent in cleartext or encrypted/hashed form.	This check is only for the applications that allow creating the new user accounts. CAPTCHA prevents against malicious software that creates account for SPAM purpose. Prevent Dictionary attack in password systems, Protect website registration by 'bots'. Encryption/hash algorithm should be sufficiently strong.
Locking(Disabling) non-existing account	Is the message for existing account the same as the message for non-existing account 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	Are there any differences between the message	No	Compare two responses from the login request:	If there is a different message an attacker is able to enumerate the existing accounts.

login and password	when account doesn't exist and the message when account is correct but password is wrong during the login process?		- Account is correct and password is wrong. - Account does not exist and password is random. Both responses should be the same.	
Public login and password	Are the login and password sent as 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 possibility that 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 addicted to type of the application but it never should be infinite. This one should be implemented on the server side. OWASP Reference - Session Expiration
Log out user after closing application	Does the application log out after it was closed?	Yes		OWASP Reference - Client-Side Defenses for Session Management
Login twice on the same user	Can two sessions of the same user be done?	No	Check on the different browsers if two simultaneous sessions can be created.	OWASP Reference - Simultaneous Session Logons
Lack of "Change Password" functionality	Can user change his password?	Yes		All applications should give the users opportunity to change password any time.
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 from source code perspective. You need to check if the mechanism of SessionID generation is predictable –if an attacker 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	OWASP Reference - Session Management Implementations

			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	These checks can be performed by using a proxy tool and capturing the whole login event.	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 set 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 the GET parameter.	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 the two endpoints.
Changing SessionID when the channel is changed	Is the SessionID changed after switching to the open channel?	Yes		OWASP Reference - Transport Layer Security
Secure cookies	Is the secure attribute set to 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 us this check.	OWASP Reference - Domain and Path Attributes
Option HTTPOnly	Is the HTTPOnly option added to cookies?	Yes	Capture the cookie using a proxy like burp or the same can be checked by using extensions of Firefox.	OWASP Reference - HttpOnly Attribute
Server HTTP				
TRACE method	Can the TRACE method be used?	No	Check for the different verbs that are enabled in the server.	

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 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 sensitive directories inside?	No		
Access to .htpasswd	Is it possible to access to the .htpasswd file?	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 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.	
Online Banking Application Checks				
Negative amounts	Are the negative 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 made properly during the transfer?	Yes		
Credit card numbers revealed	Are the credit cards numbers visible?	No		
History of account	Can one see the other user history of the account?	No		
Account balance	Can one see the other account balance?	No		
Incorrect deposit	Can one make investment on the lower value that is required?	No		
Incorrect period	Can other period be provided than required by form?	No		
Others				
Software version	It the technology name used in application revealed - for example PHP or ASP version?	No	Check if in the HTTP response any information about framework, platform is stored.	If an attacker knows the technology version, she/he can create more adjusted types of attacks. This information also helps 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 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

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	Are the pages with confidential info being cached by the browser?	No		OWASP Reference - Testing for Logout and Browser Cache Management

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