

OWASP Web Application Security Quick Reference Guide 0.2

Copyright and License

Copyright © 2013 The OWASP Foundation.

This document is released under the Creative Commons Attribution ShareAlike 3.0 license. For any reuse or distribution, you must make clear to others the license terms of this work. http://creativecommons.org/licenses/by-sa/3.0/

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 Control of the Contr						
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.

whon account docenit aviet		Account is correct and passurerd is				
G		- Company of the Comp				
		•				
<u> </u>						
•		,	If the login and password are not encrypted, there is			
password sent as clear text?	No	sent via HTTPS instead of HTTP	possibility that can be hijacked by an attacker.			
Is the user logged out after		Wait required amount of time and see if	Each application should log out the user after a period			
period of inactivity (usually		the user session was terminated.	of time. The time is addicted to type of the application			
30 min)?	Yes		but it never should be infinite. This one should be			
			implemented on the server side.			
			OWASP Reference - Session Expiration			
Does the application log			OWASP Reference - Client-Side Defenses for Session			
out after it was closed?	Yes		<u>Management</u>			
Can two sessions of the	Na	Check on the different browsers if two	OWASP Reference - Simultaneous Session Logons			
same user be done?	INO	simultaneous sessions can be created.				
Can user change his			All applications should give the users opportunity to			
password?	Yes		change password any time.			
			,			
functionality Session management						
Is SessionID random?	Voc	The Sequencer tab from Burp Suite can be	OWASP Reference - Session Prediction			
	163	used to check the session randomness.	OWASP Reference - Session ID Entropy			
Is SessionID simple?		This check should be done from source	OWASP Reference - Session Management			
	No	code perspective. You need to check if the	<u>Implementations</u>			
		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				
a a ptl A ptels p3	s the user logged out after period of inactivity (usually 80 min)? Does the application log out after it was closed? Can two sessions of the ame user be done? Can user change his password?	and the message when account is correct but bassword is wrong during the login process? Are the login and bassword sent as clear ext? Is the user logged out after beriod of inactivity (usually 60 min)? Con two sessions of the ame user be done? Can user change his bassword? SessionID random? Yes SessionID simple?	wrong. Account does not exist and password is random. Both responses should be the same. The login process? Are the login and bassword sent as clear ext? So the user logged out after period of inactivity (usually 10 min)? Wait required amount of time and see if the user session was terminated. Wait required amount of time and see if the user session was terminated. Check on the different browsers if two simultaneous sessions can be created. So SessionID random? Yes SessionID random? Yes SessionID simple? The Sequencer tab from Burp Suite can be used to check the session randomness. 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 predictable.			

but if you know that this is MD5 from timestamp it is likely to predict next IDs. Changing SessionID after logout? Changing Does the SessionID change after logout? Changing Changing Changing Does the SessionID change after login? Changing Changing Changing Using old Using old SessionID Sessi					
Changing SessionID after logout? Yes Yes These checks can be performed by using a proxy tool and capturing the whole login event. Yes Proxy tool and capturing the whole login event. Yes Proxy tool and capturing the whole login event. OwASP Reference. Renew Session ID After Any Privilege Level Change OwASP Reference. Renew Session ID After Any Privilege Level Change OwASP Reference. Renew Session ID After Any Privilege Level Change OwASP Reference. Renew Session ID After Any Privilege Level Change OwASP Reference. Renew Session ID After Any Privilege Level Change OwASP Reference. Renew Session ID After Any Privilege Level Change OwASP Reference. Renew Session ID After Any Privilege Level Change OwASP Reference. Renew Session ID After Any Privilege Level Change OwASP Reference. Renew Session ID After Any Privilege Level Change OwASP Reference. Renew Session ID After Any Privilege Level Change OwASP Reference. Renew Session ID After Any Privilege Level Change OwASP Reference. Renew Session ID After Any Privilege Level Change OwASP Reference. Renew Session ID After Any Privilege Level Change OwASP Reference. Renew Session ID After Any Privilege Level Change OwASP Reference. Renew Session ID After Any Privilege Level Change OwASP Reference. Renew Session ID After Any Privilege Level Change OwASP Reference. Renew Session ID After Any Privilege Level Change OwASP Reference. Renew Session ID After Any Privilege Level Change OwASP Reference. Renew Session ID After Any Privilege Level Change OwASP Reference. Renew Session ID After Any Privilege Level Change OwASP Reference. Renew Session ID After Any Privilege Level Change OwASP Reference. Renew Session ID After Any Privilege Level Change OwASP Reference. Renew Session ID After Any Privilege Level Change OwASP Reference. Renew Session ID After Any Privilege Level Change OwASP Reference. Renew Session ID After Any Privilege Level Change OwASP Reference. Renew Session ID After Any Privilege Level Change				•	
SessionID after logout After logout? Yes After logout? Yes After logout? All after lo				timestamp it is likely to predict next IDs.	
logout Changing Changing Does the SessionID change SessionID after login Using old SessionID Odd SessionID? Sending SessionID Odd SessionID SessionID Through GET Check if the server can be forced to use the old session cookie. SessionID in the GET parameters? Check if the server can be forced to use the old session cookie. SessionID No Check if the server can be forced to use the old session cookie. Check if the server can be forced to use the old session ID After Any Privilege Level Change OWASP Reference - Renew Session ID After Any Privilege Level Change OWASP Reference - Renew Session ID After Any Privilege Level Change Sending SessionID Is the SessionID sent in GET parameters? Check if there is any request that send SessionID in the GET parameter. SessionID when the channel is changed SessionID when channel? Changing SessionID when the channel is changed SessionID when channel? Changing SessionID when the channel is changed Secure cookies Is the secure attribute set to the cookies? Ves 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. Cookie's domain Is the cookie's domain set to parent? Option HTTPOnly Is the HTTPOnly option added to cookies? Ves Capture the cookie using a proxy like burp or the same can be checked by using extensions of Firefox. Server HTTP TRACE method Can the TRACE method be Check if the response from the login OWASP Reference - Renew Session ID After Any Privilege Level Change OWASP Reference - Renew Session ID After Any Privilege Level Change OWASP Reference - Renew Session ID After Any Privilege Level Change OWASP Reference - Renew Session ID After Any Privilege Level Change OWASP Reference - Renew Session ID After Any Privilege Level Change OWASP Reference - Renew Session ID After Any Privilege Level Change OWASP Reference - Renew Session ID After Any Privilege Level Change OWASP Reference - Secure Attribute OWASP Reference - Domain an	Changing	Does the SessionID change		These checks can be performed by using a	It is good practice to delete the SessionID from the
Changing Does the SessionID change SessionID after Any Privilege Level Change OWASP Reference - Renew Session ID After Any Privilege Level Change OWASP Reference - Renew Session ID After Any Privilege Level Change OWASP Reference - Renew Session ID After Any Privilege Level Change OWASP Reference - Renew Session ID After Any Privilege Level Change OWASP Reference - Renew Session ID After Any Privilege Level Change OWASP Reference - Renew Session ID After Any Privilege Level Change OWASP Reference - Renew Session ID After Any Privilege Level Change OWASP Reference - Renew Session ID After Any Privilege Level Change OWASP Reference - Renew Session ID After Any Privilege Level Change OWASP Reference - Renew Session ID After Any Privilege Level Change OWASP Reference - Renew Session ID After Any Privilege Level Change OWASP Reference - Renew Session ID After Any Privilege Level Change OWASP Reference - Renew Session ID After Any Privilege Level Change OWASP Reference - Renew Session ID After Any Privilege Level Change OWASP Reference - Renew Session ID After Any Privilege Level Change OWASP Reference - Renew Session ID After Any Privilege Level Change OWASP Reference - Renew Session ID After Any Privilege Level Change OWASP Reference - Renew Session ID After Any Privilege Level Change OWASP Reference - Renew Session ID After Any Privilege Level Change OWASP Reference - Renew Session ID After Any Privilege Level Change OWASP Reference - Renew Session ID After Any Privilege Level Change OWASP Reference - Renew Session ID After Any Privilege Level Change OWASP Reference - Renew Session ID After Any Privilege Level Change OWASP Reference - Renew Session ID After Any Privilege Level Change OWASP Reference - Renew Session ID After Any Privilege Level Change OWASP Reference - Renew Session ID After Any Privilege Level Change OWASP Reference - Renew Session ID After Any Privilege Level Change OWASP Refere	SessionID after	after logout?	\ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \	proxy tool and capturing the whole login	browser that is not used any more.
Changing SessionID after login? Using old SessionID Does the Server use the old SessionID? Sending SessionID Sending	logout		162	event.	OWASP Reference - Renew Session ID After Any
SessionID after login? Using old SessionID old SessionID? SessionID old SessionID? Sending SessionID Is the SessionID sent in through GET Changing SessionID when the channel is changed Secure cookies Secure cookies Is the secure attribute set to the cookies? Cookie's domain Is the cookie's domain to parent? Option HTTPOnly Is the HTTPOnly TRACE method Check if the server can be forced to use the old session ID After Any Privilege Level Change 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. OWASP Reference - Renew Session ID After Any Privilege Level Change 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. OWASP Reference - Transport Layer Security OWASP Reference - Transport Layer Security OWASP Reference - Secure Attribute 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. Cookie's domain Is the cookie's domain set to parent? Option HTTPOnly Is the HTTPOnly option added to cookies? Server HTTP TRACE method Can the TRACE method be No Check for the different verbs that are					Privilege Level Change
Iogin Using old Does the server use the SessionID Does the session ID Does the session that send Does the session ID Does the session that send Does the session	Changing	Does the SessionID change		Check if the response from the login	OWASP Reference - Renew Session ID After Any
Using old SessionID Does the server use the old SessionID? Sending SessionID Is the SessionID sent in GET parameters? No SessionID in the GET parameter. Changing SessionID when the channel is changed Secure cookies Secure cookies Is the secure attribute set to the cookies? Cookie's domain Is the cookie's domain Is the cookie's domain Is the Cookie's domain Is the Cookie's domain Is the Cookies? Cookie Analysis can fetch us this check. Option HTTPOnly Is the HTTPOnly option added to cookies? Server HTTP TRACE method Cookie Analysis can fetch different verbs that are SessionID the server can be forced to use the old session ID After Any Privilege Level Change Option HTRACE method be SessionID sension in After say request that send SessionID in the GET parameter. Check if the server can be forced to use the old session ID After Any Privilege Level Change 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. OWASP Reference - Transport Layer Security OWASP Reference - Secure Attribute OWASP Reference - Secure Attribute OWASP Reference - Domain and Path Attributes OWASP Reference - Domain and Path Attributes OWASP Reference - HttpOnly Attribute	SessionID after	after login?	Yes	request set new cookie.	Privilege Level Change
SessionID old SessionID? Sending SessionID Is the SessionID sent in GET parameters? Changing SessionID when the channel is changed Secure cookies Secure cookies Is the secure attribute set to the cookies? Option HTTPOnly Is the HTTPOnly option added to cookies? SessionID is the SessionID cookie. No Old session cookie. Privilege Level Change 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. OWASP Reference - Transport Layer Security OWASP Reference - Secure Attribute OWASP Reference - Secure Attribute OWASP Reference - Domain and Path Attributes Capture the cookie using a proxy like burp or the same can be checked by using extensions of Firefox. Server HTTP TRACE method Can the TRACE method be No Old session cookie. Privilege Level Change 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. OWASP Reference - Transport Layer Security OWASP Reference - Secure Attribute OWASP Reference - Domain and Path Attributes OWASP Reference - Domain and Path Attributes OWASP Reference - HittpOnly Attribute OWASP Reference - HittpOnly Attribute OWASP Reference - HittpOnly Attribute	login	_			
SessionID old SessionID? Sending SessionID old Session Cookie. Sending SessionID Is the SessionID sent in GET parameters? Check if there is any request that send SessionID in the GET parameter. Changing SessionID when after switching to the open channel? Secure cookies Is the secure attribute set to the cookies? Cookie's domain Is the cookie's domain set to parent? Option HTTPOnly Is the HTTPOnly option added to cookies? Server HTTP TRACE method Can the TRACE method be No Cookie SessionID sessionID in the GET parameter. Check if there is any request that send SessionID canged check if there is any request that send SessionID warious locations, including the user's browser, the web server, and any forward or reverse proxy servers between the two endpoints. OWASP Reference - Transport Layer Security OWASP Reference - Secure Attribute 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. OWASP Reference - Transport Layer Security OWASP Reference - Secure Attribute OWASP Reference - Secure Attribute OWASP Reference - Domain and Path Attributes OWASP Reference - Domain and Path Attributes OWASP Reference - HittpOnly Attribute	Using old	Does the server use the	NI-	Check if the server can be forced to use the	OWASP Reference - Renew Session ID After Any
through GET GET parameters? No SessionID in the GET parameter. 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 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. Cookie's domain Is the cookie's domain set to parent? Option HTTPOnly Is the HTTPOnly option added to 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. Cookie's domain Is the cookie's domain set to parent? Yes Cookie Analysis can fetch us this check. 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. Server HTTP TRACE method Can the TRACE method be Check for the different verbs that are	SessionID	old SessionID?	INO	old session cookie.	Privilege Level Change
Changing SessionID when the channel is changed Secure cookies Is the secure attribute set to the cookies? Cookie's domain Cookie's domain Option HTTPOnly Is the HTTPOnly option added to cookies? Server HTTP TRACE method Can the TRACE method Is the SessionID changed after switching to the open channel? 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. Cookie's domain 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. Cookie's domain Capture the cookie using a proxy like burp or the same can be checked by using extensions of Firefox. Server HTTP TRACE method Can the TRACE method be Capture the 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 OWASP Reference - Domain and Path Attributes OWASP Reference - HttpOnly Attribute	Sending SessionID	Is the SessionID sent in		Check if there is any request that send	Sensitive information within URLs may be logged in
Changing SessionID when the channel is changed Secure cookies Is the secure attribute set to the cookies? Cookie's domain Cookie's domain Cookie's domain Is the cookie's domain added to cookies? Option HTTPONIy Is the HTTPONIy option added to cookies? Server HTTP TRACE method Can the TRACE method Is the SessionID changed after switching to the open changed after switching to the open changed 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. Cookie's domain OWASP Reference - Secure Attribute OWASP Reference - Domain and Path Attributes OWASP Reference - Domain and Path Attributes OWASP Reference - Domain and Path Attributes OWASP Reference - HttpOnly Attribute Capture the cookie using a proxy like burp or the same can be checked by using extensions of Firefox. Server HTTP TRACE method Can the TRACE method be	through GET	GET parameters?	No	SessionID in the GET parameter.	various locations, including the user's browser, the
Changing SessionID when the channel is changed Secure cookies Is the secure attribute set to the cookies? Cookie's domain Option HTTPOnly Is the HTTPOnly option added to cookies? Is the SessionID changed 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. Cookie's domain Cookie's domain Cookie's domain Is the cookie's domain set to parent? Option HTTPOnly Is the HTTPOnly option added to 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. Cookie Analysis can fetch us this check. Owasp Reference - Domain and Path Attributes Owasp Reference - HttpOnly Attribute Owasp Reference - HttpOnly Attribute Capture the cookie using a proxy like burp or the same can be checked by using extensions of Firefox. Server HTTP TRACE method Can the TRACE method be No. Check for the different verbs that are			INO		web server, and any forward or reverse proxy servers
SessionID when the channel is channel? Secure cookies Is the secure attribute set to the cookies? Cookie's domain Cookie's domain Is the cookie's domain set to parent? Option HTTPOnly Is the HTTPOnly option added to cookies? TRACE method 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. 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. Cookie's domain Is the cookie's domain set to parent? Capture the cookie using a proxy like burp or the same can be checked by using extensions of Firefox. Server HTTP TRACE method Can the TRACE method be Capture the cookies that are getting generated by the Web Application and check for the secure attribute in the cookie which contains important information. Cookie's domain Yes Capture the cookie using a proxy like burp or the same can be checked by using extensions of Firefox. Server HTTP TRACE method Can the TRACE method be					between the two endpoints.
the channel is channel? 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. Cookie's domain Is the cookie's domain set to parent? Option HTTPOnly Is the HTTPOnly option added to 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. Cookie Analysis can fetch us this check. Yes Capture the cookie using a proxy like burp or the same can be checked by using extensions of Firefox. Server HTTP TRACE method Can the TRACE method be 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 - Domain and Path Attributes OWASP Reference - HttpOnly Attribute	Changing	Is the SessionID changed			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. Cookie's domain Is the cookie's domain set to parent? Option HTTPOnly Is the HTTPOnly option added to 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. Cookie Analysis can fetch us this check. Capture the cookie using a proxy like burp or the same can be checked by using extensions of Firefox. Server HTTP TRACE method Capture the set of cookies that are getting generated by the Web Application and OWASP Reference - Domain and Path Attributes OWASP Reference - HttpOnly Attribute OWASP Reference - HttpOnly Attribute Capture the cookie using a proxy like burp or the same can be checked by using extensions of Firefox. Server HTTP TRACE method Capture the set of cookies that are getting owaspetting and check for the different verbs that are	SessionID when	after switching to the open	Voc		
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. Cookie's domain Is the cookie's domain set to parent? Option HTTPOnly Is the HTTPOnly option added to 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. Cookie Analysis can fetch us this check. Capture the cookie using a proxy like burp or the same can be checked by using extensions of Firefox. Server HTTP TRACE method Can the TRACE method be Check for the different verbs that are	the channel is	channel?	res		
to the cookies? Yes generated by the Web Application and check for the secure attribute in the cookie which contains important information. Cookie's domain Is the cookie's domain set to parent? Option HTTPOnly Is the HTTPOnly option added to cookies? Yes Cookie Analysis can fetch us this check. OWASP Reference - Domain and Path Attributes Capture the cookie using a proxy like burp or the same can be checked by using extensions of Firefox. Server HTTP TRACE method Can the TRACE method be No Check for the different verbs that are	changed				
Cookie's domain Is the cookie's domain set to parent? Option HTTPOnly Is the HTTPOnly option added to cookies? Yes Cookie Analysis can fetch us this check. Capture the cookie using a proxy like burp or the same can be checked by using extensions of Firefox. Server HTTP TRACE method Can the TRACE method be Check for the different verbs that are	Secure cookies	Is the secure attribute set		Capture the set of cookies that are getting	OWASP Reference - Secure Attribute
Cookie's domain Is the cookie's domain set to parent? 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. Server HTTP TRACE method Check for the secure attribute in the cookie which contains important information. OWASP Reference - Domain and Path Attributes OWASP Reference - HttpOnly Attribute OWASP Reference - HttpOnly Attribute Capture the cookie using a proxy like burp or the same can be checked by using extensions of Firefox. Server HTTP TRACE method Can the TRACE method be No Check for the different verbs that are		to the cookies?	Vac	generated by the Web Application and	
Cookie's domain Is the cookie's domain set to parent? Option HTTPOnly Is the HTTPOnly option added to cookies? Yes Cookie Analysis can fetch us this check. Capture the cookie using a proxy like burp or the same can be checked by using extensions of Firefox. Server HTTP TRACE method Can the TRACE method be Cookie Analysis can fetch us this check. OWASP Reference - Domain and Path Attributes OWASP Reference - HttpOnly Attribute OWASP Reference - HttpOnly Attribute OWASP Reference - HttpOnly Attribute OFFICE O			res	check for the secure attribute in the cookie	
to parent? 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. Server HTTP TRACE method Can the TRACE method be No Check for the different verbs that are				which contains important information.	
Option HTTPOnly Is the HTTPOnly option added to cookies? Yes or the same can be checked by using extensions of Firefox. Server HTTP TRACE method Can the TRACE method be No Capture the cookie using a proxy like burp or the same can be checked by using extensions of Firefox. Capture the cookie using a proxy like burp or the same can be checked by using extensions of Firefox. Check for the different verbs that are	Cookie's domain	Is the cookie's domain set	Voc	Cookie Analysis can fetch us this check.	OWASP Reference - Domain and Path Attributes
added to cookies? Yes or the same can be checked by using extensions of Firefox. Server HTTP TRACE method Can the TRACE method be No Check for the different verbs that are		to parent?	162		
extensions of Firefox. Server HTTP TRACE method Can the TRACE method be No Check for the different verbs that are	Option HTTPOnly	Is the HTTPOnly option		Capture the cookie using a proxy like burp	OWASP Reference - HttpOnly Attribute
TRACE method Can the TRACE method be No Check for the different verbs that are		added to cookies?	Yes	, ,	
TRACE method Can the TRACE method be No Check for the different verbs that are				extensions of Firefox.	
$ \hspace{.1cm} \hspace{.1cm} \hspace{.1cm} \hspace{.1cm} \hspace{.1cm} \hspace{.1cm} $					
used? enabled in the server.	TRACE method	Can the TRACE method be	No	Check for the different verbs that are	
		used?	INU	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