

CHECKLIST

WEB APPLICATION CHECKLIST NUMBER 3 OF 5

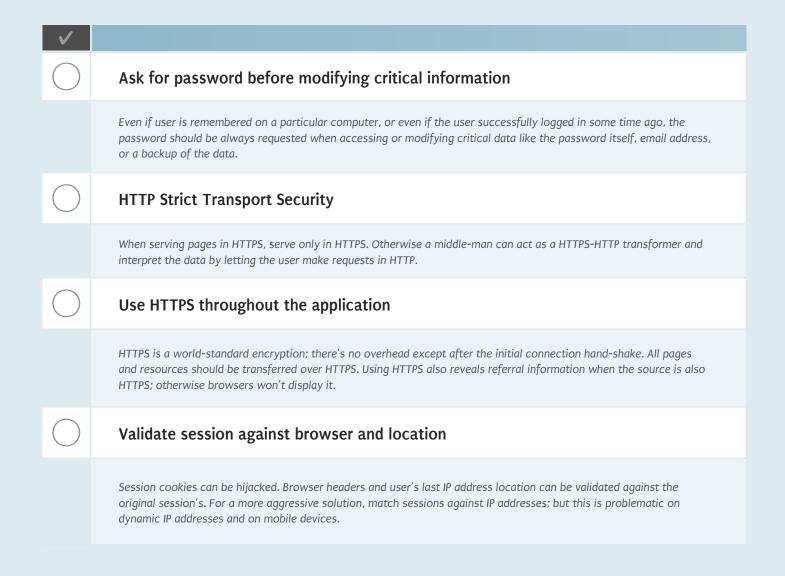
Web Application Security

BY ATA SASMAZ

✓	
	Isolate critical information in the DB
	Database users should be restricted from accessing critical information, like retrieving user passwords even if they are hashed, or retrieving all of the user email addresses. Stored Procedures or Views should be used for validation purposes and for customized data.
	Protect from Remote Code Execution
	Remote Code execution allows attackers to execute code when the application relies on weak code inclusions.
	Flood and spam protection
	Flood and spam attacks are possible even from authenticated users. Always track the last X operations of users with their times to prevent users from making too many requests.
	Hash passwords with unique salts
	All user passwords should be hashed with a salt and salts should be unique for each user. People tend to use same passwords in different services and it's the application's responsibility to protect users' passwords.
	Global XSS protection
	XSS (Cross Site Scripting) lets users execute a malicious URL.
	Protect from SQL injection vulnerability
	SQL Injection is a common vulnerability wherein SQL commands are manipulated as strings by the attacker, which allows harmful SQL commands to be executed. Using an ORM is one good way to be protected.
	Protect from CSRF
	Cross-Site Request Forgery is a common web vulnerability which allows attackers to place an iframe in their websites and request pages from the application while the user is not in the application. To avoid, this do not allow any modification with GET requests; protect POST requests outside of application's domain; but the best solution is to

provide a token in each form and validate against it.





ABOUT THE AUTHOR



ATA SASMAZ is a software engineer specializing in web application architectures. He blogs regularly at **www.ata.io**.

DZONE RESOURCES

DZone, Inc.

Suite 201 Cary, NC 27513

888.678.0399

919.678.0300

BROWSE OUR COLLECTION OF 250+ FREE RESOURCES, INCLUDING:

RESEARCH GUIDES: Unbiased insight from leading tech experts REFCARDZ: Library of 200+ reference cards covering the latest tech topics **COMMUNITIES:** Share links, author articles, & engage with other tech experts

JOIN NOW



 $DZ one \, communities \, deliver \, over \, 6 \, million \, pages \, each \, month \, to \, more \, than \, 3.3 \, million \, software \, and \, communities \, deliver \, over \, 6 \, million \, pages \, each \, month \, to \, more \, than \, 3.3 \, million \, software \, communities \, deliver \, over \, 6 \, million \, pages \, each \, month \, to \, more \, than \, 3.3 \, million \, software \, communities \, deliver \, over \, 6 \, million \, pages \, each \, month \, to \, more \, than \, 3.3 \, million \, software \, communities \, deliver \, over \, 6 \, million \, pages \, each \, month \, to \, more \, than \, 3.3 \, million \, software \, communities \, deliver \, over \, 6 \, million \, pages \, each \, month \, to \, more \, than \, 3.3 \, million \, software \, communities \, deliver \, over \, 6 \, million \, software \, communities \, deliver \, over \, 6 \, million \, software \, communities \, c$ $developers, architects \, and \, decision \, makers. \, DZ one \, of fers \, something \, for \, everyone, \, including \, developers \, and \, decision \, makers \, decision \, makers \, decision \, de$ $news, tutorials, cheat sheets, research guides, feature \, articles, source \, code \, and \, more.$

"DZone is a developer's dream," says PC Magazine.

Refcardz Feedback Welcome refcardz@dzone.com **Sponsorship Opportunities** sales@dzone.com

150 Preston Executive Dr.



 $Copyright @\ zo 14\ DZ one, Inc.\ All\ rights\ reserved.\ No\ part\ of this\ publication\ may\ be\ reproduced,\ stored\ in\ a\ retrieval\ system,\ or\ transmitted,\ in\ any\ form\ or\ by\ means\ electronic,\ mechanical,\ photocopying,\ or\ otherwise,\ without\ prior\ written\ permission\ of\ the\ publisher.$