



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.

✓	
<input type="radio"/>	Ask for password before modifying critical information <p>Even if user is remembered on a particular computer, or even if the user successfully logged in some time ago, the password should be always requested when accessing or modifying critical data like the password itself, email address, or a backup of the data.</p>
<input type="radio"/>	HTTP Strict Transport Security <p>When serving pages in HTTPS, serve only in HTTPS. Otherwise a middle-man can act as a HTTPS-HTTP transformer and interpret the data by letting the user make requests in HTTP.</p>
<input type="radio"/>	Use HTTPS throughout the application <p>HTTPS is a world-standard encryption; there's no overhead except after the initial connection hand-shake. All pages and resources should be transferred over HTTPS. Using HTTPS also reveals referral information when the source is also HTTPS; otherwise browsers won't display it.</p>
<input type="radio"/>	Validate session against browser and location <p>Session cookies can be hijacked. Browser headers and user's last IP address location can be validated against the original session's. For a more aggressive solution, match sessions against IP addresses; but this is problematic on dynamic IP addresses and on mobile devices.</p>

ABOUT THE AUTHOR



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

DZONE RESOURCES

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



DZone communities deliver over 6 million pages each month to more than 3.3 million software developers, architects and decision makers. DZone offers something for everyone, including news, tutorials, cheat sheets, research guides, feature articles, source code and more.

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

Copyright © 2014 DZone, 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.

DZone, Inc.
150 Preston Executive Dr.
Suite 201
Cary, NC 27513
888.678.0399
919.678.0300

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

ISBN-13: 978-1-936502-77-6
ISBN-10: 1-936502-77-1

