Best Practices of Web Application Fundamentals and Secure Development

[Author Name(s), First M. Last, Omit Titles and Degrees]

[Institutional Affiliation(s)]

Author Note

[Include any grant/funding information and a complete correspondence address.]

# Introduction

In this age of modern science and technology, software and web applications are an important part of the digital and technical industry. Almost all the engineering and non- engineering processes are shifting towards virtualization and the trend is increasing day by day. A web-application is very alluring for business and enterprise. Using these applications and software tools, services can be utilized with user-friendly interface to get the task done. Almost all the famous services used world wide have their own web applications and dedicated software applications for their customers and users including Amazon, Ali Express, Uber, and many others. To achieve success and accomplishment in business it is very important to adapt best web development approaches and techniques in order to make sure the reliable operation of the services and also determining the security. In fact, web application security is very important in almost every step of the development of web applications. It is important because every year there are considerable number of security breaches and data thefts all around the globe causing serious financial harm to the businesses and enterprises. Hackers industry has emerged and evolved into a multi-million dollars industry and penetration testers now-a-days are using state of the art tools and techniques to breach and infiltrate the web applications and popular websites too. Security testing of the web applications make sure the capability of the information system to maintain the functionality and the protection of the data. So, it is important to adapt best techniques and practices to build secure web applications to minimize the threat of security breaches and data thefts. In this paper we will cover some of the best approaches that should be adopted by the web developers to ensure safe and secure web application operations.

# Discussion and Recommendations

The most important thing which should be kept in consideration to build a secure web application is to work upon a specific framework of security development lifecycle. The framework or the process should encompass analyzing the web application for its weaknesses, vulnerabilities and flaws from the development and design phase. Managing the security of your web application, the primary objective or motive should be to indicate and identify the possible risks and then fix those before launching final product for commercial use. For security management of the web applications, six concepts of cyber security should be considered. These are confidentiality, authentication, integrity, Authorization, availability and non-repudiation . For confidentiality, it is expected that only authorized users are liable to access the important data of the web application. Authentication suggests determining the identity of the user and integrity means determining the correctness of the data on the receiver size my adopting adequate security measures. Authorization is associated with permission to any user to perform any task or utilize or receive any service. Availability means to make sure that the information and communication between client and the server are well-established and are readily available according to the requirement. The concept of non-repudiations means to assist in preventing later denials of any action that has happened.

## Perform a risk assessment

For creation of effective protocols, one of the key factors is identification of security requirements. The factors which may impact the security of web application must be focused and evaluated. These factors include the security level of data handled, traceability, accessibility, types of users and legal responsibilities. When these factors are identified, they should be listed according to their priority and impact so that most appropriate an effective strategy are built (M., Haddad, & A., 2009).

### Establish strategies against harmful user input

It is very important to create strategies which can prevent the expected harms form the user input. When the user entries are assumed to be safe and no precaution is taken for security, the malicious users are able to send damaging information easily to the application. For protection against such users, firstly the unfiltered user entries must not be played and Before the display of untrustworthy information, HTML should be encoded to change the possible harmful script into display strings. It is advised to not store the unfiltered user entries directly into the database. In case, HITML has to be accepted from a user, it should be first filtered manually. The filter will define the elements which can to cannot be accepted according to the security measures. Any confidential information like a cookie or a hidden file, should not be stored in location which can be accessed from the browser.

**Protect sensitive data**

One of the stronger strategies for the securing applications which handle sensitive data is implementation of SSL encryption. Moreover, configuring the webserver to automatically redirect every HTTP request towards the encrypted pages. In this way, the passwords and session IDs will not be transmitted visibly**.**

Developing a secure and intricate password reset system is one of the strategies as a security measure. The password reset is generally termed to the question set and answered by the user. The question must be of such difficulty level that they cannot be answered by anyone in vicinity. The validity of an account must not be revealed through the rest procedure as it prevents the listing of usernames**.**

The manual procedure happens to be extensive and tiring and also the breaches can be missed by humans. So, the automation of detection of liabilities of web applications through a security tool is recommended. One of such tools is Tenable.io as it lets a webpage to have complete visibility over the properties which constitute the infrastructure of a web application. For the access to complete map of web application as well as protection of further resources which include containers and assets in the cloud.

Numerous tools for the improved testing of software security are available in SDLC like penetration testing, DAST (dynamic application security testing), SAST (static application security testing), IAST (interactive application security testing) and RASP (runtime application self-protection). This software may not provide a 100% security for the applications, but they make them secure enough that malicious users are not able to attack the application (Curphey & Arawo, 2006).

For people who base the company around the web application, it is important to have deep knowledge of code ad techniques involved in the application. It is also important to the how an application will be used by the users and what significant outcomes will rise. It is very critical for the technical team to apprehend the usage, and deployment of application and from this information the team can integrate theta information into the threat prevention models.The development team should be provided incentives or lack of incentives according to situation, so that the priority of application is focused. For any application, the security is a significant part of software development. It is important at every step from evolving standards to modeling threats to testing for security errors. Throughout the procedure the developers are informed. The technical team must develop the foundation for application security according to formal threat modeling, standards and policies legally involved, and continuing omission in terms of exposures and hazards.(“Defending against Web Application Vulnerabilities,” 2012)

One important way is to use bounty programs which can be used in getting community feedback related to the possible web application security. Because many a times, even the presence of many employed security professionals can not identify any bug, error or a problem related to UI/UX design but the users may feel and indicate those issues. So many companies offer monetary awards to the members of community when if they identify any vulnerability in the web application.

# Summary

As provided above, if you are part of a software company or organization, maintaining security of the web applications is a complete team work. It is observed that Web applications are integrally insecure, according to the exemplified by a number of recent events. The modern web application platform provides a ton of powerful and effective security tools which can help prevent the unfortunate events. Security management is not just confined to applying best practices rather it is a mindset within the organization where every employee is equally concerned and conscious of the possible threats. There is a possibility that an external offender can make use of company’s human resources to get sensitive information and data and later utilize this information for cyber-attack. So, it is important to take care of this aspect too and maintain an efficient security management process to avoid such possibilities. There are many immediate steps that can be taken to improve web application security. As applications grow in size or number, it becomes very cumbersome to manage the security requirements. However, applying the above-mentioned practices of security management of web application will ensure safe use of your application for everyone.

References

Curphey, M., & Arawo, R. (2006). Web application security assessment tools. *IEEE Security Privacy*, *4*(4), 32–41. https://doi.org/10.1109/MSP.2006.108

Defending against Web Application Vulnerabilities [Text]. (2012, February 1). https://doi.org/10.1109/MC.2011.259

M., B. D. R., Haddad, H. M., & A., J. E. M. (2009). A Methodological Tool for Asset Identification in Web Applications: Security Risk Assessment. *2009 Fourth International Conference on Software Engineering Advances*, 413–418. https://doi.org/10.1109/ICSEA.2009.66

[The abstract should be one paragraph of between 150 and 250 words. It is not indented. Section titles, such as the word Abstract above, are not considered headings so they don’t use bold heading format. Instead, use the Section Title style. This style automatically starts your section on a new page, so you don’t have to add page breaks. Note that all of the styles for this template are available on the Home tab of the ribbon, in the Styles gallery.]

Keywords: [Click here to add keywords.]

Best Practices of Web Application Fundamentals and Secure Development

[The body of your paper uses a half-inch first line indent and is double-spaced. APA style provides for up to five heading levels, shown in the paragraphs that follow. Note that the word Introduction should not be used as an initial heading, as it’s assumed that your paper begins with an introduction.]

# [Heading 1]

[The first two heading levels get their own paragraph, as shown here. Headings 3, 4, and 5 are run-in headings used at the beginning of the paragraph.]

## [Heading 2]1

[To add a table of contents (TOC), apply the appropriate heading style to just the heading text at the start of a paragraph and it will show up in your TOC. To do this, select the text for your heading. Then, on the Home tab, in the Styles gallery, click the style you need.]

### [Heading 3].

[Include a period at the end of a run-in heading. Note that you can include consecutive paragraphs with their own headings, where appropriate.]

#### [Heading 4].

[When using headings, don’t skip levels. If you need a heading 3, 4, or 5 with no text following it before the next heading, just add a period at the end of the heading and then start a new paragraph for the subheading and its text.] (Last Name, Year)

##### [Heading 5].

[Like all sections of your paper, references start on their own page. The references page that follows is created using the Citations & Bibliography feature, available on the References tab. This feature includes a style option that formats your references for APA 6th Edition. You can also use this feature to add in-text citations that are linked to your source, such as those shown at the end of this paragraph and the preceding paragraph. To customize a citation, right-click it and then click Edit Citation.] (Last Name, Year)

References

Last Name, F. M. (Year). Article Title. *Journal Title*, Pages From - To.

Last Name, F. M. (Year). *Book Title.* City Name: Publisher Name.

Footnotes

1[Add footnotes, if any, on their own page following references. For APA formatting requirements, it’s easy to just type your own footnote references and notes. To format a footnote reference, select the number and then, on the Home tab, in the Styles gallery, click Footnote Reference. The body of a footnote, such as this example, uses the Normal text style. (Note: If you delete this sample footnote, don’t forget to delete its in-text reference as well. That’s at the end of the sample Heading 2 paragraph on the first page of body content in this template.)]

Tables

Table 1

[Table Title]

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Column Head | Column Head | Column Head | Column Head | Column Head |
| Row Head | 123 | 123 | 123 | 123 |
| Row Head | 456 | 456 | 456 | 456 |
| Row Head | 789 | 789 | 789 | 789 |
| Row Head | 123 | 123 | 123 | 123 |
| Row Head | 456 | 456 | 456 | 456 |
| Row Head | 789 | 789 | 789 | 789 |

Note: [Place all tables for your paper in a tables section, following references (and, if applicable, footnotes). Start a new page for each table, include a table number and table title for each, as shown on this page. All explanatory text appears in a table note that follows the table, such as this one. Use the Table/Figure style, available on the Home tab, in the Styles gallery, to get the spacing between table and note. Tables in APA format can use single or 1.5 line spacing. Include a heading for every row and column, even if the content seems obvious. A default table style has been setup for this template that fits APA guidelines. To insert a table, on the Insert tab, click Table.]

Figures title:

Figure 1. [Include all figures in their own section, following references (and footnotes and tables, if applicable). Include a numbered caption for each figure. Use the Table/Figure style for easy spacing between figure and caption.]

For more information about all elements of APA formatting, please consult the APA Style Manual, 6th Edition.