

**Securing web applications from
common hacking techniques.**

ebusinessmantra

P. O. Box 943

Norton, MA 02766

www.ebusinessmantra.com

Contents Introduction What is a web application? Why are web applications not secured? Top 10 vulnerabilities Find vulnerabilities before hackers find them. How can we help? More Information	Introduction More and more businesses are moving their normal processes to the web. Businesses derive benefits by realizing cost savings and improved workflow while offering ease and convenience to their customers. What is web application? Web application is what drives a web site and is at the foundation of every web based process. It is an entity that consists of layers of software code that executes business logic in conjunction with the database. It interacts with the data repository and then presents information to the user through a web browser (Internet Explorer, Firefox, Safari and the like). Web applications can vary from simple forms to complex ones such as online banking, stock or mutual fund trade.
--	--

Your web site is not safe just because you have SSL certificate or have good network protection.

Why are web applications not secured?

The title pre-supposes that web applications are not safe and to some degree, that is quite true.

It is a big misconception to think that your web site is safe because it has SSL , firewall, or other network protections provided by your web hosting company. Unfortunately, all network protections (firewall, SSL, and like) are not effective against attack on web applications. This is because the network has to keep access to the web site open and is the route exploited by hackers to attack web sites.

<p><i>Cross Site Scripting</i></p> <p><i>Injection Flaws</i></p> <p><i>Malicious File Execution</i></p> <p><i>Insecure Direct Object Reference</i></p> <p><i>Cross Site Request Forgery (CSRF)</i></p>	<p>Top 10 vulnerabilities</p> <p>For the year 2008, the security community has established that the top 10 web application vulnerabilities.</p> <p>Cross Site Scripting (XSS)</p> <p>XSS flaws occur whenever an application takes user-supplied data and sends it to a web browser without first validating or encoding the content. XSS allows attackers to execute script in the victim's browser which can hijack user sessions, deface web sites, and possibly introduce worms, etc.</p> <p>Injection Flaws</p> <p>Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data.</p> <p>Malicious File Execution</p> <p>Code vulnerable to remote file inclusion (RFI) allows attackers to include hostile code and data, resulting in devastating attacks, such as total server compromise. Malicious file execution attacks affect PHP, XML and any framework which accepts filenames or files from users.</p> <p>Insecure Direct Object Reference</p> <p>A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, database record, or key, as a URL or form parameter. Attackers can manipulate those references to access other objects without authorization.</p> <p>Cross Site Request Forgery (CSRF)</p> <p>A CSRF attack forces a logged-on victim's browser to send a pre-authenticated request to a vulnerable web application, which then forces the victim's browser to perform a hostile action to the benefit of the attacker. CSRF can be as powerful as the web application that it attacks.</p>
--	--

<p><i>Information Leakage and Improper Error Handling</i></p> <p><i>Broken Authentication and Session Management</i></p> <p><i>Insecure Cryptographic Storage</i></p> <p><i>Insecure Communications</i></p> <p><i>Failure to Restrict URL Access</i></p>	<p>Information Leakage and Improper Error Handling</p> <p>Applications can unintentionally leak information about their configuration, internal workings, or violate privacy through a variety of application problems. Attackers use this weakness to steal sensitive data or conduct more serious attacks.</p> <p>Broken Authentication and Session Management</p> <p>Account credentials and session tokens are often not properly protected. Attackers compromise passwords, keys, or authentication tokens to assume other users' identities.</p> <p>Insecure Cryptographic Storage</p> <p>Web applications rarely use cryptographic functions properly to protect data and credentials. Attackers use weakly protected data to conduct identity theft and other crimes such as credit card fraud.</p> <p>Insecure Communications</p> <p>Applications frequently fail to encrypt network traffic when it is necessary to protect sensitive communications.</p> <p>Failure to Restrict URL Access</p> <p>Frequently, an application only protects sensitive functionality by preventing the display of links or URLs to unauthorized users. Attackers can use this weakness to access and perform unauthorized operations by accessing those URLs directly.</p>
--	--

<p><i>Awareness of the security risks to web applications</i></p> <p><i>Develop secured code</i></p> <p><i>Automated testing of web applications in production.</i></p>	<p>Find vulnerabilities before hackers find them</p> <p>This list of top 10 attacks includes the most common hacking techniques but there are many more techniques that a hacker can employ. So what should organizations do?</p> <p>The foremost pre-requisite is to have awareness among all the stake holders. It is so necessary that web site owners and web application developers remain sensitive to the possibility that your web application will be hacked.</p> <p>Where do we start? This depends on the state of your web application.</p> <p>Web Application is being developed – This is the best time to nip it in the bud. Source code scan coupled with code review is the best option.</p> <p>Web application has been built and is in production - Start by conducting an automated scan of the web application. Automated scans are performed using software tools that emulate hack for several pre-configured parameters and known mode of attacks.</p> <p>Although automated scan report false positives and false negatives, it is more important in that they highlight potential path or mode of attack. Each website stake holder must then discern the validity of the results and the risk each identified vulnerability poses.</p>
---	--

Ebusinessmantra can help you secure your web applications.

How can we help?

Ebusinessmantra provides software and consulting services for web application security. With our experience in web application development, we bring unique perspective to web application security.

More Information

To learn about how our consulting services and how we can help you secure your applications and minimize potential for common hacks, please contact us or visit our web site.

Ebusinessmantra

www.ebusinessmantra.com

ebusinessmantra