Web Application Security Testing Methodology

LEAN SECURITY, SUITE 1A LEVEL 2, 802 PACIFIC HIGHWAY, GORDON NSW 2072, AUSTRALIA
+61 (0) 2 8231 6635 | WWW.LEANSECURITY.COM.AU | INFO@LEANSECURITY.COM.AU

CONTENTS

SECURITY TESTING METHODOLOGY

A security testing methodology of web application is necessary in order to evaluate the level of security of a certain web application. It is also a way of ensuring that its security measures are also effective and are working well. The testing process includes the discovery and analysis of weaknesses, flaws as well as vulnerabilities that are present in the application. With such procedures being done, the company or the creator of the application is given the chance to provide a technical solution for the problems found.

Just as what was mentioned above, such methods are used in determining vulnerabilities and threats present. Utilizing the right method is important, as it is the one to be used in determining whether there are things that might compromise the security of the web application. Apart from that, it aims to reduce the security risk for the end users. Ultimately, it aims to meet the security requirements of the one who would be using it.

OUR APPROACH

Our web applications approach involves entirely understanding the reason as to why the application has been created. After that, we then determine each function's purpose in relevance to the environment of the Client. By simply listing down the things that we expect from it, it has now become easier for the auditor of the Lean security to design the attacks that has a high success rate. These processes are then essential as they assure the detection of not only the web vulnerabilities that common occurs but also the specific attacks to the application itself. Moreover, by doing so, we are given the opportunity to craft as well as test its supported business process.

To further let you understand the concept, we have provided the following example below. It would show you how Lean Security is able to test certain types of vulnerability. OWASP Top Ten has become our basis for the said test. Moreover, it only indicates the approach that we are using and not the entire test that we have conducted.

THE OWASP

OWASP stands for Open Web Application Security Project. It is an internal organization that has been developed for a long time with the aim to enhance the security of web applications. It is consists of members who are considered as security experts all over the world whom have knowledge about attacks, threats, vulnerabilities as well as countermeasures. It is used in helping the people understand all the things involved in the web application testing. It involves a testing framework and not just a simple checklist of the things that are needed to be addressed. One of the most important aspects of it is evaluating security measurements.

As a part of the organization's mission, they have been sponsoring various projects that are of course, related with security. One of it is the Top 10 that we have used as a basis for the test conducted. It is a project that has provided a list of the top 10 security risk for web applications worldwide. The list includes the description of the vulnerabilities a well as suggestions on how one would be able to avoid it. The latest version of the list have been published in 2013. It is a list that is based on the data provided by 7 firms working on application security. Moreover, the top 10 has been prioritized based on their prevalence as well as relative impact, detectability and exploitability. The list would be further discussed in this book.

On the other hand, the OWASP approach is described as both collaborative and open. This is because it is free and every expert when it comes to security can actively participate in it. This also means that they are given the opportunity to share their knowledge and ideas. Apart from that, they have the chance to have a cooperative vision for the project as participation is promoted.

This approach commonly creates a testing methodology that is described as reproducible, rigorous and consistent while the quality is maintained under control. One thing that makes it great is that everything would be set out in detail. This includes the documentation as well as testing of the problems discovered. This approach has been popular due to the reason that it tests all vulnerabilities as well as activities that are related with the web application's security.

INJECTION

Injection has been at the top of the list. This is because a hacker or someone with an ill intention to gain access even to protected data can use it. Injection flaws occur when the interpreter has received an untrusted data as a part of a query or a command. This is where the hostile data can somewhat trick the interpreter to execute commands such as accessing data even without undergoing the authorization phase or other unintended command.

All of the candidate fields would be tested by Lean security for certain types of injection including:

- SQL Injection
- Xpath Injection
- LDAP Injection
- OS Commands
- Program Arguments

In the testing phase, we have utilized automated scanners. These scanners were programmed in order to search for error messages whenever special characters as well as commands are inserted. One should remember that there are certain injection types wherein the exploitation of special characters are not needed.

Apart from what was said before, the test that we are conducting also has the aim of trying to bypass the validation process on the part of the Client. This includes cookies' values, JavaScript, drop down boxes and others that makes use of hidden fields and which seems to be passed back. This process is done through injecting various directly to the post or getting the command, depending on what is more appropriate for the situation.

CROSS SITE SCRIPTING (XSS)

The hackers who aim to send malicious codes to websites that are considered to be trusted and benign uses Cross-Site scripting and that is why it is also included in the top list. Usually, the malicious code comes in the form of browser side script. Such attacks often happen when a user input has been used by the web application within its generated output without even encoding nor validating it.

The XSS could even be used to send malicious code to an unsuspecting application user. What makes it more threatening is the fact that the browser that the end user is using has no way of knowing that it should be an untrusted source and so, it results to it executing the code. With the use of the code, it is possible for the hacker to access even the sensitive information that are used in the site.

As that is the case, the Lean Security would then be testing various user input. It may be headers, fields and even cookies. This procedure is done tin order to determine the vulnerabilities in cross site scripting including:

- Stored
- DOM Based XSS
- Reflected

In this process, the testing done by XSS would not only involve the web application but also in the module and the web server software as well. The testing would then be conducted through the process of returning the unique strings of all of the data that were back to the server. The HTML page that were then returned would be scanned to discover unique strings, not only by its visible content but also by source. If in case it has found the unique string, then it undergoes the process of HTML tags insertion in order to make sure that such strings would be retuned in a way where the special characters in the HTML would be considered as not safe. Apart from that, the browser would then execute its content.

After the approval of the cross site scripting, other types would then be tested in order to determine the limitations of the vulnerability discovered. It would also be done in order to know whether other malicious types exists, that might bring harm to the application. Such malicious types may include Flash XSS and JavaScript. All of these processes are essential in order to determine the things that these may bring to the experience of the end user and to the application itself.

SESSION MANAGEMENT AND BROKEN AUTHENTICATION

This is one of the most common vulnerabilities exploited since it is capable of allowing someone, even the attackers an access to web applications. Commonly, these are used in order to retrieve information such as user ID, passwords, account details and other information that should be kept private.

Such attacks would often starts when the attacker imitates the user through the use of the information that they have gathered from other users. With that, they are able to ask for valuable information of the user. In order to avoid it from happening, Lean Security would now inspect the management of sessions as well as the methods used for authentication for the problems given below:

- Session Timeouts
- Predictable generation of session
- Authentication Strength
- Session Stealing Session ID
- Password Hashing (In order to determine whether access could be gained or provided to the back end)
- Improper transmission of session

Typically, this process is done through the process of examining mechanisms involved in session management. Through it, it would be so much easier to determine what action should be taken. It includes the following:

- Log in repeatedly in order to check the fixation and prediction of the session;
- Examining the session identifier's location;
- Examining the flags found on the cookies and determining whether it is used for the maintenance of the session;
- Considering the possibility that cross site scripting vulnerabilities are present;
- Considering the chance of the cross site request being forged;
- Reading the password database with the use of other vulnerabilities, if possible.

These testing methods will be used to identify whether the application is vulnerable either to external compromise, or internal privilege escalation.

DIRECT OBJECT REFERENCES (INSECURE)

It is common to experience surfing through a website that would ask for values for the sake of determining the parameters of their application. However, such process might not be safe, especially if they are not properly examined.

This is because other people, especially the hackers could use it in order to pass malicious codes to the website. This only means that without proper protection and access control, it is possible for others to manipulate the references or values in order to access data that they have not been given the authorization to do so.

In order to fight it, the Lean Security would be ensuring that the objects that are found in the application's backend would not be directly executed and instead, they would be executed through the application. Such objects may include database queries, files and scripts. The process is done through the generation of the table that contains not only the available functionality but also the available resources as well. The contents of the table are available for all roles as well as its duplicate as long as it is possible for the escalation of the horizontal privilege to occur.

Systematic testing of the table would then be done. This is to ensure that each role would attempt to gain access to the resources as well as attempt to execute the functions in which should only be available for another user or role. It is expected that we should be logged out from the application after failure in every attempt or if not, at least, a message stating that the access is denied should be presented. There is a need to take note of the resources that should not be available but were successfully used by another role or user who was not supposed to be given access to it.

CROSS SITE REQUEST FORGERY (CSRF)

The CSRF has been included in the list due to the fact that it is capable of allowing the attacker to perform certain actions without them being able to even know about it. Thus, they are somewhat forced to do something unknowingly as they remain logged in in a web application. This is often used to target sites that are related with social media, online shopping and banking since these are the sites that often involves information from the user as well as actions that are available for them. This forces the browser of the victim to execute request as it thinks that the request came from the user itself.

In this one, the verification done by Lean Security in order to ensure that it is impossible for 3rd parties to inject the commands for the application in the stead of the user through the execution of the predictable URLs.

The process would be done through the following:

- Checking the way URLs are constructed and formatted;
- Determining the process involved in maintaining the state of the session.

SECURITY MISCONFIGURATIONS

Having a good, security means that a good configuration was also done. However, when a web application has been misconfigured, then attackers can abuse them in no time. Thus, to ensure security, there is a need for the secure settings to be defined, implemented as well as maintained. This is because the defaults are likely to be unsecured. In addition, there is also a need for the software to be updated as often as possible. Moreover, a web examination is also needed. It would also include Lean security doing the following:

- Ensuring that the default account passwords have been disabled or changed;
- Checking useless services pages, ports and accounts;
- Ensuring that the operating systems, supporting databases, modules content management systems or applications that are non-custom as well as web servers have proper levels of patching;
- Ensuring that the external viewing does not contain default administrative pages anymore;
- Ensuring that the listing of the directory has been disabled;
- Externally checking whether the filter as well as firewalls have been configured properly.

INSECURE CRYPTOGRAPHIC STORAGE

This happens whenever secure storage of data, specially the sensitive ones is not achieved. It involves vulnerabilities that something to do with ensuring that all important data are encrypted. Moreover, there is also a need to ensure that the right data were the ones that have been encrypted. Aside from that, proper management is also necessary.

When exploited, these flaws tend to have a high impact. This is because usually, the important information and data are the ones encrypted. Many people think that the attack is done through the cryptography itself.

Although that may be somewhat true, the attackers nowadays go after how the cryptography is being used. There are various ways to detect it and one of it is through the help of Lean Security and through the use of the right security testing methodology. As much as possible, it would examine the cryptography of the storage. This is because it is one of the main concerns for the hashes of password. However, in case it has identified other requirements, then these would also be examined. It would then ensure the following:

- Any encrypted data has been encrypted with ciphers having sufficient strength;
- That cryptographic keys are secured and managed properly.
- Passwords have been hashed;

FAILURE TO RESTRICT URL ACCESS

It is known that failure to restrict URL access is one of the most common weaknesses, which is listed right on the Open Web Application Security Project or also called as the OWASP Top 10. Its details are truly imperative vulnerability when it comes on web application. Its main objective here is to boost up the awareness of various developers. Thus, the application security measures were specifically designed in order to make the development process better.

What's the real deal about it?

As soon as your application have fail to restrict properly URL access, there's a high tendency that the security will be then compromised by means of a certain technique known as forced browsing. You should know that forced browsing is not just a mere minor problem. It is a serious matter, most especially when the intruders tries to collect confidential data on your web browser through requesting particular pages or even data files.

Through this technique, your attacker does have now the ability to bypass the security of your website with accessing directly files rather than following any links. It will then allow that particular attacker on accessing source data files instead of utilizing a web application. Attacker could now guess specific names of the backup files you have, which possess sensitive information as well as location and even identify source code. This goes along with other information you left right on the server and be able to further bypass web pages "order".

Failure to Restrict URL Access, to make it more simple, do happens once an error right on the access and control settings lead user on accessing hidden or restricted pages. With that, it results to security problems since these pages are less being protected than other usual public access pages. That also means that people who have no authority to access that page could easily obtain it anonymously. Most of the time, restricted or hidden pages only protection here is through not linking into the pages or at some point not showing links publicly.

How could attackers could Exploit its Vulnerabilities?

With simple methods, attackers could easily interact as well as access along with your unlinked or hidden pages within a website. And basically that what forced browsing is doing. In general sense, forced browsing attack could happens whenever the intruder could guess correctly your URL or even employ brute force on accessing the page. Take note that it is much easier when there's a flaw, which exist on the access-control policy of the page. Such flaw usually includes pages which are hidden along with their easy-to-guess URL, outdated access-control policy code, applications that could allow access on that pages which means to be restricted or hidden and lastly, lack on the server side access-control policy.

Verification of the Security

The main objective here is to be able to verify access control that is being consistently enforced on the presentation layer as well as the business logic no matter what URLs within the application.

Manual Approach

It is the most effective and even efficient approach for you to use. It utilize code review as well as security testing combination in verifying the access control mechanism. Once the mechanism is being centralized, its verification could be quite magnificent. On the other hand, when the mechanism is being distributed on the whole codebase, this verification process could be too time consuming. Likewise, provided that mechanism is externally enforced, then configuration then must be tested and examined.

Automated Approach

Static analysis and even vulnerability scanner tools do have that difficulty on the verification of the URL access control however, for various reasons. It is known that vulnerability scanners are having hard time to guess hidden pages as well as identifying pages that must enable every user.

Meanwhile, these so-called static analysis engines do struggle a lot on determining custom access control on the link and code of the presentation layer along with the logic of the business.

INSUFFICIENT TRANSPORT LAYER PROTECTION

Through the help of insufficient layer protection, it enables communication be exposed on unreliable 3rd parties while giving attack vector in order to compromise various web application or even grab sensitive information. Typically, website utilizes SSL/TLS or known as Secure Socket Layer/ Transport Layer Security on providing encryption right on the transport layer. But unless the site is being configured in order to employ SSL/TLS, such site could be vulnerable on the modification and interception of the traffic.

Furthermore, once the transport layer is not being encrypted, all possible communication between the client and the website is now being sent right with clear text that leaves this open into injection, interception as well as redirection.

UNVALIDATED REDIRECTS AND FORWARDS

Most web applications oftentimes redirect and then forwards their users into other sites and pages as well as utilize unreliable data to identify the right destination pages. The absence of proper validation, attackers could take redirect these victims on malware or even on phishing sites or even employ forwards in order to access different unauthorized pages.

How could you avoid unvalidated redirects and forwards?

You can perform safe redirects and forwards in different ways:

- Prevent yourself from utilizing redirect and forward
- When being used, never involve with user parameters in computing destination. It is typically could be done.
- When the destination can't be kept away with, make sure that the supplied value is right as well as authorized for the sake of the user. Also, it is advisable that these destination parameters will serve as a mapping value instead of being the actual URL or even part of the URL. In connection with this, application may be used ESAPI in order to override sendRedirect() procedure in order to ensure every redirect destination are all secured.

Prevent in these flaws is really necessary since they are the favorite target of various phishers who are trying to acquire the trust of users.

SECURITY ARCHITECTURE AND DESIGN

In order to be successful in building web applications, you have to make sure that you right architecture as well as design. The effort and cost of the retrofitting security right after the development of the security were too high. Through reviewing the architecture and design, it will greatly help you on the validation of security-related features of that particular application prior on the beginning of the development phase. It lets you identify as well as repair possible vulnerabilities prior on the exploitation as well as prior on the need to repair, which needs substantial engineering effort.

Once you've finished the whole design of a certain application, then design document can easily help you along with this process. No matter how comprehensive it is, you should be able to decompose the application as well as determine the key items which includes data flow, trust boundaries, entry points, data flow and even privileged code. In addition to this, you must be aware about the physical deployment configuration of the application itself. Since the network keep son growing and evolving along with security technologies, you have to give more time in reviewing security architecture.

Likewise, network architecture is being bounded by the organizational policy as well as specifically built right upon the requirements. It will then help your business operations. On that note, network security architecture does give you the assurance of reliable and continuous performance of organizational operation. Therefore, an effective solution should be able to give the right means of correlation, monitoring and even detection of any security-related network behaviour thru real-time as well as acting upon on internal and external threats. It could affect the organizational assets which includes data, services, network elements and applications.

Its Processes includes:

- Application Security Requirement Analysis
- Information verification
- Network Infrastructure and Deployment Analysis
- Application Component Analysis
- Communication and Reporting
- Deliverables

WEB INFRASTRUCTURE SECURITY TESTING

INFORMATION GATHERING

Moreover, tester will be the one responsible in determining various information as much as they could, which could help on the compromised internet which faces infrastructure. Thus, information would be accumulated right from the different sources as well utilized on various methods:

DNS INFORMATION GATHERING

This needs the right utilization of several DNS attacks in order to gather information regarding with domain you've provided. Such information is being used in order to:

- Distinguish hosts and networks needed to attack
- Be able to look for various virtual host names for the web servers in order to boost up attack surface area
- Give insights on the types of services which must be running in a certain IP address

SEARCH ENGINE INFORMATION GATHERING

You must be aware that public search engines are being employed in order to collect information regarding with the environment of the client. These information may simply include the following:

- Confidential technical information like configuration snippets or even diagrams being uploaded on the support forums
- Googlehack information, which determine possible vulnerable services
- Software or hardware descriptions being used right from press release or forum post

SERVICE DETECTION

When every helpful information regarding with the specific target scope is been accumulated, a reliable company would thoroughly scan IP address, which range within scope in order to diagnose all accessible services from the location. These scans basically includes:

- Selection of the most common UDP ports
- Wide range of TCP ports
- Any ICMP types

If these are being considered properly by tester, scans could be customised on the environment, which includes TCP half-open scans, full TCO handshakes as well as where there is the need to evade intrusion and firewall prevention, fragmented packets and even high tech odd flags.

With that, finalize services xlists could be define the type of attack surface of a particular environment in behalf of every opportunities in order to put into compromise the system so it could gain enough access on the sensitive information.

As website owners, you have to get the best possible solution during any security-related incidents. Make sure you've acquire in-depth defense. It must be a layered approach for reactive and proactive website security.

With it, you can avoid any breaches . Thus, it is really necessary to harden your web application against any current as well as merging threats. Look vulnerabilities along with WAS and there you can then mitigate this with WAF.

VULNERABILITY DETECTION

The vulnerability in the computer system, most especially in a software application, which is considered a malicious thing that can affect and damage the information provided in a website or in a computer system. It is very important to make sure that the computer systems of those software applications have enough security provided, in order to make sure that there will be no one that can hack the information provided in the website.

Lean Security is making use of the scanner of Qualys Vulnerability in order to scan those common issues with regards to misconfigurations and security. Qualys will be configured with the help of the latest updates.

Qualys is iterating with the other services in the infrastructure and then run on a database in checking and in configuring those security issues. Some of the security issues that it can detect include the vulnerabilities in privilege escalation, vulnerabilities in remote code execution, vulnerabilities in information disclosure, misconfigurations, insecure services, roque and backdoor services as well as insufficient security protections.

The scanners for web application are going to run on those available web interfaces. With the help of the scanner, it is going to identify the common vulnerabilities and issues which includes cross site scripting, injection attacks, forgery of cross site request as well as the attacks of those directory traversals.

Aside from scanners, there are also additional tools that can be run on to provide specific service which has been considered appropriate by the tester.

MANUAL SERVICES INVESTIGATION

The services provided for each host are going to be tested by making use of those manual techniques. The manual techniques involve using certain tool for the services in order to find further all the vulnerabilities located in the security. Some of these manual investigation techniques include the following:

- The SNMP services will go under investigation in order to determine if it can be accessed by not having any authentication as well as default community strings.
- There will be attempts to do be done in order to login on the SMB services and FTP servers by making use of an anonymous and a guest account.
- SSH and Telnet services are go to be accessed in order to see the if the information is being exposed as well as if the default credentials are allowed to use in order to gain access
- there will be other manual techniques as well as specific services that will be done

The applications in the web will be visited in order to see if the functionality and the information are being exposed to the network. If ever the web application comes with a login interface, then a default credential is needed to be entered. The attacks on the common web will be attempted which includes those common web applications coming from the OWASP top ten.

The OWASP top 10 serves as a powerful awareness document specially designed for the security of web applications. It represents a wide consensus with regards on the most critical flaws that can happen on the web applications. There will be project member that are going to include a wide variety of experts when it comes security from all over the world who were able to share their expertise in the production of this list.

OWASP top 10 urge all the companies in adopting this kind of awareness document in the organization and then start immediately in the process in order to make sure that the web application they have does not contain any flaws.

By adopting the OWASP top ten, it serves as the most effective first step in changing the development of the software's culture in the organization into something that has a secure code.

The OWASP top 10 was able to be translated in so many languages with the help of numerous volunteers. Some of the available translations include all the versions of the OWASP top 10 in the year 2013, all the versions of OWASP top 10 in the year 2010 as well as all the information with regards on all the various terms of translations.

The usage of OWASP top 10 is free. It is a licensed program that falls under the Creative Commons Attribution-Share A Like 3.0 license which means that you can copy it, distribute it an then transmit the work, adapt it and make use of it for commercial purposes. However, it is very important to provide attribution on the work and if you alter, build upon and transform this work, you will be able to distribute its resulting work but only on a similar or the same license it has with this one.

To sum up, OWASP top 10 offers the most accurate list of all the 10 most critical security risks on a web application. For each risk, it offers a description, an example of the vulnerabilities, an example of an attack, a guide with regards on the way on how it will be avoided as well as a reference on OWASP and from those other sources that are related.

The tester is not going to do a comprehensive test in those authenticated areas of the web application. It will continue even though the access gained has gone through certain vulnerability in the web application.

Manual techniques are proven effective when it comes on detecting those vulnerabilities and other malicious acts that take place in a computer software application. With the help of OWASP top 10, it offers an accurate way of detecting those vulnerabilities that enter a software and see the things that can possible be done in order to retrieve all the important information as well as to provide security on the software application so that it will not be infected by other malicious acts and vulnerabilities that can possible take place in the computer system as well as software application.

THE EXPLOITATION

If there will be vulnerability detected, it will be immediately exploited if possible. It will be done by the tester by making use of an automated or a manual technique.

The phase of exploitation provides two important purposes. The first one is to make sure that none of those detected misconfigurations and vulnerabilities are considered false alarm. Secondly, it order to give the important information with regards on the depth of information and vulnerability in order to help in assessing the risk in the business that can possibly results from the suspicious vulnerabilities.

If ever the exploitation of the vulnerabilities has been proven to have a potential risk on the system's availability, the Lean security is going to contact the client with regards on the exploitation of the vulnerabilities. The possible risks as well as the benefits brought by the exploitation are going to be given. On the other hand, the exploitation will not just be done an explicit permission coming from the client.

THE ESCALATION OF PRIVILEGES

After the exploitation of those detected vulnerabilities in the web application, the tester is going to make use of the privileges as well as information gathered in order to provide feedback on the gathering of information as well as on the detection phases of those vulnerabilities. Take this situation as an example, if ever the tester was able to gain a list of the credentials of the users or a connection from a network to those other additional servers, then this access is going to be leveraged in the process of testing.

By means of using additional information, the tester has the ability to uncover those other vulnerabilities that can be remained hidden. After all the technical testing has been made and completed, the Lean security is going to consider each of the vulnerabilities found in the context. In this way, it will allow all of us to fully understand the impact on the business of those vulnerabilities a well as those appropriate ratings of the risk that can be assigned in each one. The process of reporting is going to consider the following things:

- the vulnerability's nature
- the skill needed in order to exploit as well as to detect the vulnerability
- the impact it has on the web applications where I has been found as well the business
- if there are some mitigating controls in order to reduce the possibility of those further risks

The report will give detailed recommendation with regards on how to remediate the detected vulnerabilities as well as mitigate the risk if ever the use of full remediation is not that practical to do. Once the report has been done and delivered, the Lean Security is going to schedule a debrief question as well as a question and answer session within the staff of the client.

DELIVERABLES

After the conclusion of the testing has been made, the Lean security is going to deliver a report which contains the following information:

- The methodology used in the conduct of the testing
- The detailed findings of the technicians for each insecure configuration vulnerability
- an analysis of the business risks which considers the all context of the vulnerabilities
- a detailed recommendation that describes the best thing to be done and method in order to provide solution to the problem
- a high level of recommendation that make sure those ongoing security in the website

Once all the important information has been done in the report and has been delivered, the Lean security will now be available for about one hour of debrief sessions. This debrief sessions will be effectively tailored by the technical staff of the senior management which has been required to have by the client.

The report provided is very important to take into consideration and to follow because it helps a lot in providing the best methodology as well as the most appropriate way in making the software application and computer system secure and safe. It is done in detailed for the clients to easily to follow and understand.

Security in computer systems as well as in software applications is an important thing to have, most especially for those businesses because it contains all the important information with regards on the nature of a business, the operations that takes place and other important things.

So if you are a business owner and you want to secure the security of the information provided in your website as well as on the software application that you use, then it is very important to fully understand the things state above. By knowing them all and understanding each things they has to offer, you will be able to see a great help in the management of the information located in your business website.

Nowadays, with the emergence technology, there are more and more businesses that rely more on online, particularly on the aspect of doing business transactions, plans and strategies. On the other hand, there are also more and more malicious and suspicious acts that takes place online which aims to detect the information you have and us it in an illegal way and then after that, destroy your website of your account.

By means of understanding the things above and through effectively learning the things they can offer, business individuals as well as the other website owners and software applications will be able to use these things in providing security in the information they have.

When you feel and see that there are malicious acts and unnecessary things that take place on your software application, and then it is very important to report it immediately in order to provide an immediate solution to it. Always remember that as early as you see those vulnerabilities in your software, you should provide an immediate solution to it for you to retrieve all the important things you have in it. Always remember that security is a thing that all of us should take in consideration for the first place. When you provide security on the important information you have, you can rest assure that all your files will be exclusively kept for your eyes only and no one could take the courage to access it.

ABOUT LEAN SECURITY

SECURITY SOLUTIONS YOU CAN RELY ON

For dedicated managed security and IT solutions that are guaranteed effective and reliable, more online business owners are choosing Lean Security over any other internet security firm period. We are the only firm that works laterally with our clients every step of the way to ensure their needs are met and their web applications are secure at all times. When you need a team of experts who will listen and respond to your IT needs, trust Lean Security to show you what we can do for you today.

THE SECURITY SOLUTIONS YOU NEED

Headquartered in Sydney, Australia and serving the international business community, Lean Security was founded under the principle of offering our clients real-world solutions to all of their online business needs. We are more than an IT consultancy, we offer managed security solutions designed to keep your web applications secure and your business running smoothly. We are an Australian owned and operated company and you can be assured that your data is controlled by us, right here in Australia.

OUR PHILOSOPHY

Our team of experienced professionals strive to provide a higher level of service and support that our clients can't get anywhere else. We offer best in class products and rely on our over 10 years of practical security industry experience to provide our customers with truly world class online business solutions.

Lean Security showcases the best value for the IT and online security products and offers our clients a wide range of customizable services including:

- Secure Managed Cloud Hosting
- WAF Managed Service
- Managed Web Application Security Testing
- Managed DDoS Protection
- Managed Event Correlation /SEIM Solutions
- Managed Network Vulnerability Assessments

CHOOSE LEAN SECURITY AS YOUR APPLICATION SECURITY PROVIDER

We at LEAN SECURITY furnish organizations and associations with a simple and savvy method for dealing with the security dangers connected with corporate web and versatile applications. LEAN Security gives oversaw helplessness examining and web application infiltration testing administration. This implies establishing the data cen5teres without any need of equipment or programs to be installed, you can pay as per your need which means you can start with the little and then you may extend if you need more services, it totally up to you. Thirdly there will be so compelling reason to employ and prepare any web IT Security staff. Let our expert group handle all the specialized testing. And yes, you will be having a very simple fixed pricing per application (or per subscription) makes it easier to manage the budget.

At LEAN Security, we will be helping you through:

1. **Our Technology:** We use an assortment of business and open source apparatuses and items to convey the best security administrations to our clients. A rundown of the apparatuses utilized include:

    - **Nessus Vulnerability Scanner:** The most widely organized vulnerability assessment & management solution
    - **Qualys Vulnerability Scanner:** Qualys is a source of cloud security, compliance and related services for small and medium-sized businesses and large companies
    - **Metasploit:** Penetration Testing Software
    - **Netsparker:** Work as a False Positive Free Web Application Security Scanner
    - **SQLMap:** Automatic SQL injection and database takeover tool
    - **Burp Suite:** Burp Suite is an cohesive platform for execution security testing of web applications.

2. **Process:** For getting the services, you don't need to wait some weeks or even months until your website is verified by a security consultancy. Our SLAs are very simple and you get results much faster and provide you the reliability that you will not regret on your decision. Our SLA's provide:

    - **Basic Assessment** - branding web sites and mobile applications without the data collection features in 3 business days only.
    - **Standard Security Assessment** - corporate web sites with data collection functions and simple web applications (reservations, order handling etc.) in 5 business days only.
    - **Premium Assessment and Penetration Testing** - ecommerce applications or complex web applications with multiple roles and privileges in 10 business days only.

3. **Our Consultants:** Our customers will get enthusiastic account managers and project managers to help accomplish the project goals and results. Our team will help you to:

    - Analyze your business necessities and find the clarifications to address your challenges.
    - Generate a security assessment plan to meet timelines
    - Provide inclusive reporting on the position of the project
    - Intensify any issues that need quick and speedy resolutions
    - Track you resources and budget

Moreover, all your projects are checked by our skilled professionals with respected industry certifications like:

- **CISSP** - Certified Information Systems Security Professional
- **CISA** - Certified Information Systems Auditor
- **CISM** - Certified Information Security Manager
- **GPEN** - GIAC Penetration Tester
- **GCIH** - GIAC Certified Incident Handler
- **GWAPT** - GIAC Web Application Penetration Tester
- **GXPN** - GIAC Exploit Researcher and Advanced Penetration Tester