Sensitive Data Exposure

Description:

Sensitive Data Exposure most likely occurs when an application does not have a proper protect sensitive information. Data varies and the exposed are any from passwords, credit cards, etc. For example, you have accidentally uploaded something to somewhere. A weak crypto can only mean that attacker could be able to get information to you and because of less of headers which is preventing the browser form caching it.

How to Prevent:

The first thing to do is that you must find out the data that is possible to be a sensitive one and must be protected.

Then make sure the followings:

* The data should never be placed in a text that is very clear.
* Data should not transmit in a very clear text.
* Make sure that the algorithms that you used for encrypting is strong enough.
* Check If the key was secured or not secured
* The browser should not able to cache when the data is being turned in to the end-user

Injection

Description:

Injection is the most popular or the number one list on OWASP. This was more on a type of looking that was like a category which includes lots of types of vulnerabilities, where any application gives a not secured data in an interpreter. Mostly, injection can be found on databases, some of the examples are the commands in operating systems when someone or the user input is being delivered as arguments in the program.

Some of the Remediations:

1. The remediation may likely vary from the problem based on the type of vector you were talking about. One of the possible solution to be done is by using an API which will be avoiding an interpreter or will give an interface which is being parameterized.
2. If you encounter some queries which have been parameterized, those will not be a possible solution to be followed. The work would be done depending on the interpreter that was used, and anything that you must check.
3. Also, an alternative would be by using a whitelist for the validation input, but many of the cases cannot be used because an application is needing characters that are special as an input to it. One example of it would be, someone wants to give permissions to the users to have their comments by means of quotes, even if the case is that it is character that may be used to get out form a query. If these was the case, go with the two solutions above.

Broken Authentication

Description:

Broken Description will include all types of flaws which are mostly caused by some errors in implementing a management session. Because of having a very broad range of so many kinds or types of vulnerabilities, this will cause to a not very easy to know or define what are its unique, or most important properties.

Remediation:

The security would be badly needing to be as a part of the whole in the process of developing until from the very beginning. This will be the one and only way to make sure nothing can be over used in away that was not planned to when or during its development process. As of those types of vulnerabilities are hard to find or look at afterwards.

Almost all the types of vulnerabilities that includes in the category is there or is existing because of the many programmers or developers gets problems in many ways.

Security Misconfiguration

Description:

Security Misconfiguration is a type, or a component is very susceptible to a configuration that has many insecurities and is being classified as a protector or as a security that leads to a misconfiguration. This is acceptable as a look a like or the same vulnerability regardless of whatever the misconfiguration is occurring or happening in a web server, in a custom mode or in a database.

How to Prevent:

* You should always make sure that all has been updated. When creating the system, you should make it very easy to give or deploy all the updates of the software as well as all the patches.
* The configuration staging must not be different and must be the same every time. Almost all of the misconfigurations are because of the inconsistencies.
* A large percentage of us is very good in committing mistakes, and that is why we should make sure that we automate all the things that can be automated. If the set-up will be the same as well as the procedure is being processed often, it would be recommended that you must make sure it will be secured and then just repeat everything.
* You should do some scanning, or you should do some auditing which must be done regularly to learn or discover the misconfigurations that will be possible to occur.
* When it will be possible, the system must surely be configured with you keeping in mind that the system will be compromised since is very likely or same. When there is a security breach, the attacker will be limited to only to do a very small amount of damage.

Cross-Site Scripting (XSS)

Description:

Cross-Site Scripting is yet another kind of an attack being done, that can be tag along or carried out on compromised people or the users of a website. The deployment or exploitation of the a Cross-Site Scripting flaw will enable any attacker to have an injection to a script that are client-side into all web pages that can be see or can be viewed by the users.

WE can say that the cross-site scripting or XSS means JavaScript, but in some cases may include a for example a VBScript.

XSS Remediation:

It has very high chance or is very potential for every not wanted or very dangerous characters to be surely sanitized or be escaped or went out. This can be done in many ways and it will be depending on what will be the context, and many of the most cases will be the article or information about the knowledge of us on databases be enough or sufficient.

The application must also always be developed or created with the XSS having so many risks in your thought, and this will make all those harmful, little or big, to most likely happen if there is a XSS vulnerability.

Insufficient Logging and Monitoring

Description:

Insufficient Logging and Monitoring, instead of having so many vulnerabilities, is a category of OWASP that handles and covers having less of many good practices that may turn on become on preventing or stopping.

This type or category covers everything from all the events that have not been logged are recorded, all logs that have not been recorded or kept properly and warnings which has no action or work is being taken from within a reasonable time.

Remediation

You must always make sure that the logs or the records have always a backed up and is in synchronized to a different server. The attacker will surely will not have the ability to remove or clear all the records after hacking the chosen server and just by doing it would be prevented.

You must also go and check everything from the system and must be made sure that all sensitive actions are recorded. This will include all logins, transactions that are important, changing the passwords, etc. This is very important when knowing if it has been act afterwards.