Waiming Ham

CYB 333

Project

I went based on the status code that is used for the web server, I used the website w3.org to see what codes are known for websites. This is useful for sites that have purchases options to make sure that they have a secure website. One example is having https for the website, https allows the site to have a more secure communication and prevents any type of attackers, it encrypts the communication between the client side and the host side.

The idea is to allow the user to see what vulnerabilities they may have in their website and what they should do to prevent that. As I mentioned the user can add https to have a more secure site however they should also plan ahead and add security naturally on it which is to have a minimal amount of add-ons and have little plug-ins, sometimes the plug-ins may have spyware and the user maybe unaware thus causing the user to have their data hijacked. The user should also be aware that the attackers can attack the ACL which is the access control lists and the root directory. This will allow the user to access any type of personal data

Based on acunetix website it states “An Access Control List is used in the authorization process. It is a list which the web server’s administrator uses to indicate which users or groups are able to access, modify or execute particular files on the server, as well as other access rights.” (Acunetix, 2019)

There are several ways to prevent this and it’s to add a web firewall, this will prevent any attacks, one good program is cloudbric, they help users prevent any type of leaked information. They also use web application firewall as mentioned earlier, and lastly, they have an SSL certificate that allows the user to have their communication encrypted between the client and the host server. This is overall a very useful tool that any type of websites should have.

The other is having an SSL certificate as I mentioned lightly in the last paragraph SSL is a very important tool to have for the user to have on their website. One of which is of course to protect your personal data from attackers, secondly SSL confirms the identity of the user. What that means is if the user goes to a website, they believe they know but later find out that it’s a fake website, SSL prevents that to happen to the user, one good example is a verified profile, it could be a celebrity or a political figure. This will allow the user to know the difference between the real one and the fake one.

The outcome is to see what attacks can happen in a website, this applies heavily in sites that has a payment method, one good example is many attacks happen to amazon and eBay. This is since they have payment methods and personal information as their name and address. This can lead to identity theft.

For the timeline I took about 5 hours for the coding this was during week 3-4, for the research of prevention was 3 hours did that in week 4. One of the major issues I was dealing with was creating a type of code, the purpose I went for this code was to show the users that creating a penetration type code to see what issues that website may have and how to prevent it. I also added comment lines in the code to describe what each line of code is mean to do.

Sources

W3.org. (2019). World Wide Web Consortium (W3C). [online] Available at: https://www.w3.org [Accessed 22 Nov. 2019].

HTTP - Hypertext Transfer Protocol. (n.d.). Retrieved from https://www.w3.org/Protocols/.

What is a Directory Traversal Attack? (2012, October 16). Retrieved from https://www.acunetix.com/websitesecurity/directory-traversal/