CYBERSECURITY TEAM 1 REPORT

By: Uche Ogbuka, Redi Hoxhaj, Logan Connolly, Mario Welch

Affiliation: Kennesaw State University

Class: IT4983 – IT Capstone

Instructor: Donald Privitera

Table of Contents

Introduction/Background3

Website Backup/Plug-ins4

Saving Login Credentials5-6

HTTPS & SSL Certificates6-7

Disabling XML-RPC7-8

Change the default “ADMIN” username8

Automatic Logout8-9

Limit Login Attempts9-10

WordPress Scan for Malware and Vulnerabilities10-11

Firewalls11

Project Oversights11-12

Project Summary12-13

Introduction/Background

The first step of our capstone project was pointing out some of the obvious vulnerabilities on our given site. Our first observation was that the webpage had no initial backup. Backups help ensure that data on websites are saved in case of a potential attack. We also started downloading a few plugins, such as SSL, to strengthen security on our site. The website also seemed to save sensitive information, which is one of the biggest concerns when it comes to WordPress pages. We started conducting research to find out exactly what kinds of security methods to use on our website to decrease all the vulnerabilities and documented them below. The Akwaaba website we were given consisted of several security flaws which hackers can easily notice and perform malicious intentions. Most webpages nowadays show a user specific area in a website that might be vulnerable to things like viruses, malware, ransomware, and data breaches. This webpage alerts a user that their personal information such as credit cards, addresses, searches, and many other areas could be exposed to the public. Ransomware attack is a common issue associated with less secure webpages because it allows a hacker to encrypt and hold sensitive data. Ransomware is so dangerous and costly that "The attacker may even download and threaten to release sensitive data publicly if you do not pay by a deadline. Ransomware is the type of attack you're most likely to see reported in major news media." (Escobedo, 2021). In the case of our given site, someone who might want to order food/beverages from this page is at risk of falling victim to this malware. It is very important for a user to be cautious whenever saving payment methods to a website because most sites tend to save that data without permission. One of the best ways to protect against ransomware is to perform a thorough and frequent backup in a safe location. By enabling a backup to the target website, companies can easily perform a data cleanup or restoration to their site. This limits an attacker's, which could save company millions in damages.

Website backups/Plug-Ins

With a solid backup and recovery, an attacker loses leverage and cannot erase and restore data that has been affected. Website backups not only protect from hackers and malware, but it also protects against system failures that could occur unexpectedly. Our Akwaaba webpage seems to save data entered and does not have any protection for it, which is a vulnerability that attackers can notice instantly. When performing a backup, it is crucial to ensure all important data is secure. Scheduling backups is an effective way to keep track of current data and ensure that the restored site will be updated. Data breaches are common with unsecure websites as they allow an "unauthorized user to gain access to your private data." (Escobedo, 2021). Although the attacker might not be able to control the data, they can still view and make modifications easily. Plug-ins offered by open-source applications could help in surveying site files for any modifications made, which helps one become aware of suspicious activity. There are several plug-ins that work automatically, which could save time and money. The more plug-ins implemented on a webpage, the more secure the site will become. Some examples of popular plug-ins include Sucuri, IThemes Security, and Word Fence. Kinsta is a very effective plugin, and it can "monitors uptime, and automatically bans IPs with more than six failed login attempts in a minute." (Holcombe, 2022). With Kinsta, only encrypted connections such as SFTP and SSH are supported whenever a user attempts to access a WordPress site directly. Kinsta also features hardware firewalls and several active and passive security methods to prevent access to certain data. Relating back to website backups, Kinsta provides backups to all webpages on its servers and automatically creates up to two weeks of backups to restore if needed. Two-factor authentications is a method being used in many big companies and using Kinsta provided that extra layer of security when a user logs in.

Saving Login Credentials

As already observed, our given site is also at risk of exposing user's login credentials. Most websites have the option of saving usernames and passwords, which is very risky for an unsecure site. The use of multifactor authentication can reduce the risk of an attacker stealing one's information by providing an additional layer of protection. There are several authentication applications like Duo, Google Authenticator, Authy, and more. A password manager does help keep and organize several passwords to sites, but there needs to be an additional step like a biometric scan or passcode to ensure only authorized personnel can gain access to the credentials, which will decrease the chance of attacks. Another advantage of a password manager is to alert someone about the strength of their passwords or if they have used it on a previous website. Many people tend to utilize the same passwords across websites and hackers can quickly take notice of this, steal those credentials, and launch a cyber-attack. Most webpages have a feature that requires a password to meet certain conditions such as length, numbers, and special characters. Escobedo states that "Therefore, for any level of access, all passwords should be of sufficient length and complexity. A strong password should include 18 characters minimum, and the longer, the better. Password length increases security more than complexity." (Escobedo, 2021). Two-way authentication also plays into this by protecting a login even when guessed correctly. Norton, Dash line, and LastPass are all great examples of password managers to ensure passwords are not being recycled throughout websites. In a situation where an attacker utilizes several passwords attempts to gain access to a site, network, or any platform, most webpages will place a restriction on that user for an amount or time and instruct them to reset the password. Saved passwords also pose a threat to the devices they are stored on. A hacker that seeks to access an account does not need to be physically present to access the devices. There are several viruses and malware that do the job easily and remotely steal data. If a device is no longer in use, A security action to take is to always full wipe and clear all data to restrict attackers from stealing any possible credentials.

HTTPS & SSL Certificate

SSL stands for Secure Sockets Layer, a security protocol that creates an encrypted link between a web server and a web browser. An SSL certificate "authenticates a website's identity and enables an encrypted connection" (Kaspersky, 2022). We need SSL certificates to keep user data secure, verify ownership of the website, prevent attackers from creating a fake version of the site and make the website more trustworthy to the users. Several companies utilize SSL certificates to provide security for online transactions and restrict unauthorized access to customer information. SSL also keeps internet connections secure and prevents hackers from stealing or changing information that is transferred between two systems. To tell a website is protected by an SSL certificate, there is a padlock icon located next to the URL in the address bar. The process of SSL is vague, but it starts with a browser attempting to connect to a webpage. The webserver then sends the browser a copy of the SSL certificate. The browser then checks to verify the SSL certificate and signals the webserver. The web server then "returns a digitally signed acknowledgement to start an SSL encrypted session", which results in data sharing between the browser/server and webserver." (Kaspersky, 2022). Hypertext transfer protocol secure (HTTPS) is the secure version of HTTP, which is the primary protocol used to send data between a web browser and a website. HTTPS is an additional layer of security that also uses SSL certificates in encrypting the data shared between a browser and a server, which protects from data breaches. At the current state, our page does feature a HTTP protocol which makes it more secure and less penetrable. By adding that extra layer of protection we make sure that the communication is encrypted. Encryption is done by using asymmetric public key infrastructure and the extra layer of protection comes from TLS (Transport Layer Security) protocol. Both TLS and SSL are the same, but SSL is the more updated way to refer to it.

Disabling XML-RPC

XML-RPC is enabled by default in WordPress, and it is used to make your site connect with other web and mobile apps. Back in the days, before WordPress became today's WordPress, the connectivity speeds were quite slow and making changes was very time consuming. This is where developers created this offline client where you would build your content and then connect it with the blog and publish it. Exactly this connection was done through XML-RPX. There are numerous functionalities that empower the developers to perform many tasks in a fast and easy way. This kind of API is a phenomenal tool that empowers developers to complete somewhat CRUD operations remotely to their website. As WPHacked states in their blog, “XMLRPC.PHP authorizes remote updates to WordPress from various applications”, but because of its added functionality and complexity it also comes with drawbacks. Hackers will try and brute force their way into the site by using a special function called system. MultiCall. By using that, they would attempt hundreds of logins but with less request. In our case it is recommended to disable it. Another way that hackers will try to exploit its vulnerabilities is through DDoS via pingbacks. Since the xml-rpc is enabled, it also offers the hacker a long list of IP addresses for them to send these attacks and that could to thousands of sites at once.

There are several ways to disable XML-RPC. The first option would include a line of script in a specific where the xmlrpc returns false. Another option would include installing a plugin that once you complete the installation and activate it, it will automatically disable. For this to work, WordPress version must be 3.5 and above.

Change the default "ADMIN" username

Usually, the default name for the username is "admin" and since this makes about half of the login information it is imperative to make it the most unique. The default username, and sometimes even password, may be fantastic for connecting and getting the application or device up and running quickly, but you must change them as soon as possible to prevent snoopers or potential attackers from getting in. Hackers will try and use brute force otherwise to crack the password and thus gain access to sensitive information. There are also other ways to be hacked when the usernames and password are very easily guessed. As stated in Blog Vault, "It doesn't have to be human hackers, bots are also built to scavenge for vulnerabilities in your website." They are automated to scan and exploit mistakes made by humans and unfortunately the login credentials are one of the weakest links in a website and specifically in WordPress. As the login site opens the gates to the website, many more hackers focus most of their attention on that specific part. What makes it worse is that they don't have to stay and try each combination of usernames and passwords one by one. Bots that use brute force or Dictionary attacks will exploit that information by using millions of most common combinations to gain access.

Automatic Log out

Many websites with sensitive data inside such as banks or other institutions have security measures that log the users out after a certain period. It is an important feature as users often leave their station without logging out and it can potentially be hijacked by hackers. They do this by seeing that the account is without any activity and will try to hijack the session and the cookies. On our website we can do that by installing a plugin called Inactive Logout. It will let us set a certain idle timeout and display a message after logging it out. This plugin comes in with a few more features such as Disabling Concurrent Login which will prevent the user signing in in two or more different devices at the same time. Another feature is Enable Redirect which will make the user redirect to the login screen after timeout. After, say, five minutes of inactivity, online banking services log users out automatically. Naturally, this timer is reset each time a system screen is refreshed. However, if you fail to do so, a notification stating that you can prolong your session is displayed two to three minutes before checking out (Daniel Viquez, 2019). This is especially helpful if you want to browse at some previous operation lists because doing so would take longer than a session if you didn't want to leave the screen. Browser sessions on bank websites do expire, but not on sites like Facebook. However, a laptop, phone, or tablet session's external security system is there to secure it. Because of this, even though there is a strong reliance on the security of an external system, security in these situations is typically not compromised (Daniel Viquez, 2019).

Limit Login attempts

Even though WordPress has proven to be secure CMS, hackers, or everyone else that would want to get something out of the site, will always find a way to do it. Having a certain amount of tries to login is a good thing to have as there are times where you just keep getting it wrong. However, a legitimate user will only need a few tries to get it right as opposed to a hacker which would need a lot more. Saying that, it is imperative to limit the Login Attempts for your website. This is a feature that by default WordPress has turned on as in unlimited tries. This can be exploited by using brute force attacks. A plugin called Login Lockdown will let us change the limit of the attempts made from the specific IP address. This feature will temporarily or permanently lock that person as a precaution thus making the website more secure. Unfortunately, some users who repeatedly enter their password erroneously find themselves locked out of their own WordPress website. Password lockout has the potential for a denial-of-service attack, which is one disadvantage. A malicious party might simultaneously run a hacking script on all the institution's accounts. In a healthcare facility, reaching the password lockout threshold for every account may be exceedingly problematic, especially if the only option to unlock the passwords involves going via an administrator. It can take hours to fix. The normal barrier should be greater than 10 attempts, at the very least. If the account owner given 20 chances to remember their password, they would presumably either succeed or give up and reset it to something they can remember before being locked out. A hacker's success rate at guessing a password in 20 tries is incredibly low (*What are the benefits and drawbacks of a password lockout?*).

WordPress Scan for Malware and Vulnerabilities

Security plugins are an essential tool which will keep the website running safely. Taking measures to secure the website is the first steppingstone into having a healthy website. But that does not end there, as most attacks can cause worse problems when they go undetected which would be continuous bleeding. Therefore, having a scan tool run for any malware is imperative. Most of the plugins will run routine checks and catch any signs of breaches. Sometimes there will be cases where we will want to check it manually if we see any drop to the website traffic. Doing it is very straightforward and we will just need to input our URL into the security plugin, and it will go through the website and look for any possible known malware. Using the default ‘wp-admin’ WordPress URL left open many vulnerabilities since this gave a hacker instant access to our entire webpage’s backend. This could allow a hacker to completely remove our websites layout from the inside or remove it all together. Creating a new URL for the page adds an extra layer of protection from threats.

Firewall

A firewall is used to filter access to a protected network, all traffic to a webpage must pass through the firewall. The firewall will authorize traffic to pass through if it meets the defined security policy. Though, “A firewall is by its nature perimeter defense, and not geared to combating the enemy within...” (Habtamu Abie, 2000) Acknowledging this fact meant that despite all the tools provided through the security system there also had to be a level of proactive defense on our network.

Setting this defense layer up brought a lot of tools that could be easily implemented to our security. By adding the firewall, we were able to set automated scans to monitor any malicious web traffic. Packet filtering allowed us to have the ability to verify IP addresses, the port # available, and grant or deny access to our webpage. The ability to set up a blacklist for certain IPs meant that any malicious IPs detected could be blocked from accessing our webpage.

Project Oversights

The biggest oversight that our project had was forgetting to change the default password to our server infrastructure that was set during the beginning of the semester. While installing plugins, changing hyperlinks, and setting new passwords for the WordPress login, we had overlooked the biggest vulnerability our project had. This ended with the unfortunate event of our website being easily crashed by the other team within the same day of the IP addresses being received, which is the same timeframe we thought to change this default password.

One of the biggest difficulties we faced during this project was that each team member had never taken a Cyber Security class before this project. This led to all of us starting from square one when it came to setting up proper defenses for our webpage, this lack of understanding lead to us doing many unnecessary implementations during the start of the project. This caused us to ignore the simple vulnerabilities that we ended up facing. A large amount of our time was spent attempting to get our SSL certificate secured, this ended up being an unnecessary step overall and it was impossible to get working for free without paying for a service.

Project Summary

Everywhere we go or everything we do it is impossible not to interact with technology. As technology has become a way of life so it has protecting it. Protecting it from hackers or programmed bots from exploiting vulnerabilities, from impersonating other persons or from stealing data or information that could be used for malevolent intentions. On this semester long project, we were tasked with a business restaurant website called Akwaaba. Upon getting the necessary information to access the website, we were tasked with finding all the key points where it lacked protection.

Some of the key findings that we discovered after thorough research were unprotected URL with the latest HTTPs protocols, scanning mechanism not in place, a backup mechanism not implemented, Login credentials easily guessed, Firewall and preventive measures not in place. Upon identifying these vulnerable points each team member extended their research and learned as much as possible about not only the kind of attacks that they may cause but also the repercussion that it may inflict on the website. Being a website that deals with client's data we were focused on patching up all the vulnerabilities by converting the previous HTTP protocol into HTTPs protocol, installing various plugins that will ensure the longevity of the website in a sudden attack such as back up plugin.

During this long semester project, we were also tasked to monitor the website for any suspicious activities and any breach that could have been executed by outside sources. After extended research of each member, we were able to install some very useful plugins that would help in the monitoring but also in the overall security. WPScan was on the plugins that ran periodically scan and detected any intrusion or looked for common breach patterns. As part of the monitoring phase each member was tasked to take turns and look over the website for any intrusion. As a precaution or preventive measure in case of attacks we have also implemented a backup plugin which was ready to launch the website at any time if the latter resulted in down time.