Restricting website access

How to prevent unauthorized access to my website?

At the moment anyone can access our Catering Application to create sessions and issue order and as you can imagine this can be a problem. A solution must be implemented that is suited for my case in order to prevent such a thing from happening. There are multiple ways in which I can achieve this and we are going to explore them further along this document.

Password Protection.

One of the method to protect it by password is with HTTP Basic Authentication which is supported by most web browsers and is easy to set up. However the downside of it is that it is not very secure as the password is sent in plain text over the network.

A second solution would be with Form-based Authentication which involves creating a login form on your website where users can enter their credentials (username and password). The form is then submitted to the server, which checks the credentials and logs the user in if they are correct.

Using a third-party authentification service can be another option and there are there are several third-party authentication services that you can use to add password protection to your website. Some popular options include Auth0, Okta, and OneLogin. These services provide a secure and easy-to-use solution for managing user accounts and passwords.

IP address filtering

To implement IP address filtering, I can use a firewall or other security tool to create rules that specify which IP addresses are allowed or blocked. For example, you might allow access to your website only from certain IP addresses belonging to your company.

One of the security tool that will allowe me to achieve my goal is Web Application Firewalls. WAFs can be configured to allow or block traffic based on the IP address of the client requesting access. Another one that can be taken into consideration is Network Access Control, a security tool that controls access to a network based on the identity and security posture of the client device. NAC systems can be configured to allow or block access based on the IP address of the client.

Geolocation technology

Geolocation technology allows you to determine the location of a device or user based on the IP address of the device or other factors.

Comparing the location of the device from which the issue has been ordered with the latitude and longitude coordinates of the restaurant will allow to secure unrestricted access of the website

What solution is best suited for my case?

Truth be told, none of the solutions as on their own are 100% secure as all of them can be bypassed, so in order to at least make it difficult for mallicious access I would need a combination of Form-based Authentification and Geolocation technology. The password will be encrypted in our database and only a limited amount of people will have access to the username and password.

To use a geolocation API I will need to sign up for an API key the API provider and also include the API key in the API requests.

Conclusion

It is very important to take this security aspect into account because it can cause financial damage to the business and will create awkward and unwanted problems within the restaurant.

As for now we only make use of API keys so that we restrict anyone else from using or issuing orders within a session, however in further iterations we will be implementing the above mentioned solution.

Sources

<https://www.ibm.com/docs/en/cics-ts/5.4?topic=concepts-http-basic-authentication>

<https://medium.com/@niitwork0921/what-is-a-form-based-authentication-fac2adde13ac>

<https://resources.infosecinstitute.com/topic/third-party-authentication-oauth-good-or-bad-for-security/>

<https://blogs.oracle.com/advertising/post/understanding-ip-filtering-common-techniques-and-pitfalls>

<https://www.isaca.org/resources/isaca-journal/issues/2016/volume-5/geolocationthe-risk-and-benefits-of-a-trending-technology>