|  |  |
| --- | --- |
| Course Name | ITD 3243 – Server Side Programming |
| Instructor | Mark L. Pranger |
| Student Name | Sharyl Hammer |
| Due date | April 12, 2018 |
| Grade | 100 |
| Grading Comments | <instructor comments here> |

In the module, the topic of authentication is covered.  One problem security has is the delicate balance between secure and usable.  Too much security makes a system, app, program, website, etc. to hard to use.  Making some extremely usable (user friendly) can lead to a very lax security model on the system.  There needs to be the balance between being secure and being usable by the users.  There are several authentication methods, not just the ones discussed in the text.  For this discussion, a little research into various authentication methods.will need to be done.  Share after your research, what methods or methodologies you find along with the advantages and disadvantages of the methods.  Discuss how much is too much and how much is too little when it comes to securing websites.  What methods should not be used due to lack of usability or security itself?

**Authentication Methods for Websites**

HTTP Basic Authentication

Simplest possible way to enforce access control using a user name and password. This type of authentication sends an authentication header with every request it makes. The user name and password are not encrypted. The user name and password and sent every request which can potentially expose them. This type of authentication is connected to SSL/TLS and if the website uses weak encryption an attacker can break into the connection and the username and passwords will be exposed. Changing the user name and password is not trivial the user has to change the password.

Cookies for Authentication

Always use HTTP Only cookies. HTTP Only prevents cookies from showing up in document.cookies. Always use signed cookies a server can tell if a cookies was modified by the client. If the transport layer gets exposed your credentials are easy to access with this type of authentication.

Tokens of JWT

Consists of three parts which the header which contains type of token and hasting algorithm, payload which contains the claims and signatures which calculated with HMAC sha256. When using JWT (Json Web Token) in the browser you have to store it either Local Storage or Session Storage which can lead to XSS attacks. If the transport layer is exposed then the credentials can be easily accessed.

I found that in my research the type of web authentication depends on how the web app will be used. If the web application is for the internet only then cookies or tokens should be used. When the web app will use mobile clients then token based authentication should be used.