

```
*****
*****CyberXploit*****
*****
```

CyberXploit is an easy to use vulnerable web application with the aim of creating awareness on vulnerabilities in web applications and how they occur.

```
##### Installation #####
## Tools
```

a. XAMPP Control panel - This application was used to connect phpMySQL to the web application as the backend database.

```
*****Install XAMPP*****
```

1. Download and run XAMPP for your operating system. Get latest version of XAMPP here <https://www.apachefriends.org/download.html>
 2. Select and install all components. No special configuration needed during installation. Process takes about 10 -15 minutes
 3. Open XAMPP Control Panel and start the Apache and MySQL modules. If MySQL module is not running on port [3306] click the [Config] button close to the module to access the [my.ini] text file and change the port to 3306 (i.e. port = 3306). You may also have to set the User Account Settings to [Never Notify Me] for the installation duration.
 4. Access the phpMyAdmin MySQL database here: <http://localhost/phpmyadmin>
 5. When in phpMySQL first create a new database name [nodejs-login] and then from the IMPORT tab, import SQL file from application folder with name: [database -> users.sql] . Database details as follows [host: 'localhost', user: 'root', password: '']
- For any installation and configuration issues read this short guide: [\[https://www.cloudways.com/blog/setup-mysql-database-localhost/\]](https://www.cloudways.com/blog/setup-mysql-database-localhost/)

b. Node js - The environment for creating Backend server for application

```
*****Install Node js*****
```

1. Download and install Node Js for your operating system. Get it here: <https://nodejs.org/en/>
2. To check whether you have node installed by typing into Hyper Terminal [node -v]. This shows you the version of node installed.

c. Hyper Terminal CLI - Command line platform to run the web application server

```
*****Install Hyper*****
```

1. Download Hyper for your Operating System here. [<https://hyper.is/>]
2. Run Hyper
3. Download and extract the web application zip file from Github: [<https://github.com/Richard-Quartey/dissert>] and in Hyper navigate to downloaded project folder [dissert-master]
4. In dissert-master directory run [npm install] without brackets, to install needed dependencies from package.json file
5. Subsequently run application server with [node app.js] to run web application
6. Start web application on localhost in web browser [localhost:3000]

```
##### Usage (How To Guide) #####
```

CyberXploit comprises of 5 major vulnerability tasks. The user is supposed to

read this guide before
beginning.

1.Task 1 - SQL Injection â€

To do this task navigate to the Signin page (i.e. Account -> Signin). Then enter [" or ""="] without brackets, in both the Email address and Password fields. This allows you to select all the email addresses and password in the database.

2. Task 2 - Broken Access Control â€â€

To do this navigate to the path: [http://localhost:3000/admin] without brackets. This gives you direct access to the admin page without any authentication whatsoever and in turn giving you unauthorised access to the admin account.

3. Task 3 - Cross-site Scripting â€â€â€

To do this task, you should have completed task 2 (Broken Access Control) and on the admin page. The search box on the admin page http://localhost:3000/admin will be needed to perform this task. On the admin page insert the script:

(([])) without three brackets in the search box and hit enter. This injects javascript into the page and gets information about cookies(which is basically information about a users session).

In this case the cookies reveals information about how to authenticate yourself as the admin providing you with an email and a password (i.e. email=admin@admin.com password=admin). This information be used by the user to login as the admin.

4. Task 4 - Broken Authentication â€â€â€â€

To do this task , you should have completed task 3 (Cross-site Scripting). This is because you need the information about the email and password of the admin to perform this task. Click logout (i.e. Account -> Logout) and subsequently login (i.e Account -> Login) as the admin with credentials (email=admin@admin.com password=admin).

5. Task 5 - Security Misconfiguration â€â€â€â€â€

To do this task, you need to logout ((i.e. Account -> Logout) from the admin page or simply click the cyberXploit text logo(on the top left corner) to take you to the home page. On the homepage scroll down to the [Click Me] button and click it. This takes you to an wrongly configured error 404 page which shows you how to access the secret message on the web application. Simply append to the current path: [http://localhost:3000/secrets] , [file/pages/secret]. This takes you to [http://localhost:3000/secrets/file/pages/secret] where you can access the secret message via a Secret link.

Contributing and License

Application files are accessible to be pulled and recommendations on updates are also welcome.