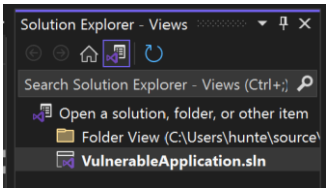
Bypass of CSRF Middleware in Astro Deployment

Dependencies

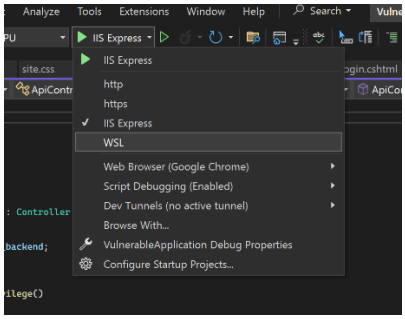
- SQL Server Management Studio 20 (Express)
- Visual Studio 2022
    - .NET 8
- Visual Studio Code
    - NPM v9.3.1
    - WSL (Latest)

First-Time Setup

- Vulnerable Application Setup
    - Please open Visual Studio 2022 with .NET 8 packages installed, upon opening the software you will be greeted with a screen for cloning a repository. This is the recommended first step. Here is the link to the challenge contents.
    - Once you've cloned the repository, please find the solution inside of the solution explorer (top right).

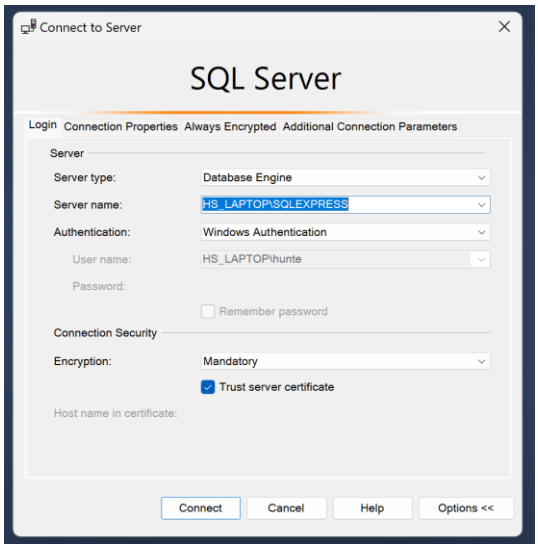


    - Next, where the big play button is, please select the drop-down menu and run the solution with IISExpress. Additionally, in this menu you will find "VulnerableApplication Debug Properties". Please select this option and take note of the App SSL URL inside of the IISExpress section. This will be crucial for forging the CSRF attack.

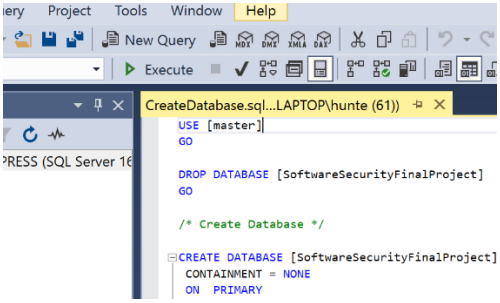


    - The last step which is crucial to this application running properly is the database! Once you're ready, please boot up SQL Server Management Studio (SSMS). I'm using my own local SQL Express database, although if you're running from a server,

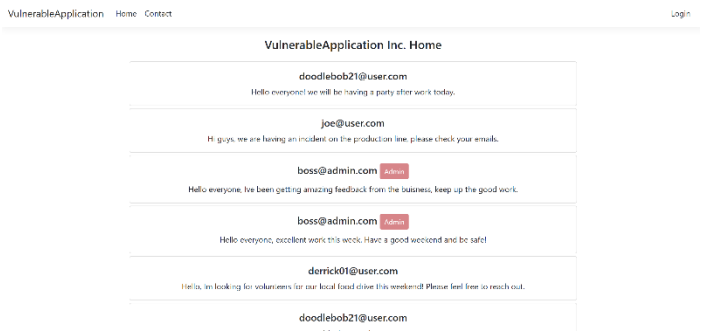
feel free to change the appsetting's connection string in the Vulnerable Application Project. Here is an example of my connect screen.



- Next, please open the "CreateDatabase.sql" script from the Github Repository, and execute the query.



- Lastly, try running the VulnerableApplication inside of Visual Studio verifying the application has data visible from the home screen. If it's a blank screen you're in trouble! It should look something like this:



- Malicious Application Setup
  - Please open the "Malicious Application" folder in Visual Studio Code. Then in the WSL terminal, please run "npm run dev". Once this has finished it will have built the malicious project completely, and will display the website url inside of the terminal.

Take note of the file “src/pages/index.astro”. This contains the html, css, and javascript for completing the malicious request.

Challenge Regeneration

- Re-run the “CreateDatabase.sql” script inside of SSMS.
- Re-boot both applications.

Description & Hints

- This information can be found in “WriteUp.pdf”.

Completed Challenge

- Be the only admin left or manipulate the other admin’s accounts by changing their passwords.
- Delete at least one forum post and change at least one forum post to something funny.
- Hide your tracks, try to manipulate the astro file and phishing email to draw low attention. Once your dirty work is complete, revoke your own admin access.