**Video Demo Script – Final Submission**

👋 **Intro:**  
"Hello, my name is [Your Name], and this is my final demo for the Web Security Assignment. In this video, I’ll walk through the vulnerable app I created, demonstrate some common web vulnerabilities, show how I fixed them, and explain the security measures I implemented."

**🧱 1. Vulnerable Code (Before Fixes)**

(Open server.js or your main backend file)

"This is the original Node.js Express app. It includes basic signup and login functionality. Initially, it was vulnerable to several common attacks:

* NoSQL Injection in the login form
* Cross-site Scripting in the profile page
* Weak password storage without hashing
* No input validation for empty fields"

**🧪 2. Demonstrating Vulnerabilities**

(Open browser, use signup/login form with test payloads)

**For NoSQL Injection:**  
"I'll enter this payload in the login field:

json

CopyEdit

{ username: { $ne: null }, password: 'any' }

This lets me log in without valid credentials — a NoSQL Injection."

**For XSS:**  
"Now, if I signup with a username like <script>alert('XSS')</script>, it will be rendered directly on the profile page, triggering a JavaScript alert — that's Cross-Site Scripting."

**🔧 3. Fixes and Improvements**

(Back to the code editor, show fixed sections)

"Here are the changes I made:

* Added manual validation to prevent empty inputs.
* Used bcrypt to hash and salt passwords before saving them to the database.
* Used EJS’s auto-escaping (<%= %>) to prevent XSS.
* Avoided using raw user input in database queries to prevent NoSQL injection."

**📦 4. Nmap Port Scan**

(Switch to terminal, show the Nmap result)

"I used Nmap to check for open ports. The command was:

css

CopyEdit

nmap -sV -p 3000 localhost

It shows that only port 3000 is open and running a Node.js Express app, confirming that no unnecessary services are exposed."

**🧾 5. Log File Content (Live Logging)**

(Show security.log file being updated live)

"I’ve added logging using the winston library. Each signup, login, and error event is logged.  
Let me refresh the login page and try a login — as you can see, a new entry has appeared in the security.log file."

**🛠️ 6. Tools Used**

"Here are the tools I used throughout this project:

* **VS Code** for development
* **Browser** for form testing and rendering
* **Nmap** for scanning open ports
* **Postman** for testing POST requests (optional)
* **winston** for logging"

**✅ 7. Final Summary**

"To summarize:

* I built a vulnerable app and demonstrated NoSQL injection, XSS, and other issues.
* I then fixed those vulnerabilities using proper validation, escaping, and password hashing.
* I tested the app using Nmap and added logging for security monitoring.
* All changes are documented in the final report and pushed to my GitHub repository."

👋 **Outro:**  
"Thank you for watching. This concludes my final demo."