The labs can be found over at https://labs.hackxpert.com/JWT

JWT Labs: Find the Flag (With Solutions)

Welcome to the **JWT Labs**! In this lab series, you will explore vulnerabilities in JSON Web Tokens and learn how to identify and exploit them to find hidden flags. Each lab will progressively increase in difficulty.

Lab 00: Understanding JWT

- **Goal**: Familiarize yourself with the structure of JSON Web Tokens.
- **Steps**:
    1. Observe the provided JWT token. It is structured as three parts separated by dots (.): Header, Payload, and Signature.
    2. Decode the JWT using any online tool (e.g., jwt.io).
    3. Analyze the content of the Header and Payload.
    4. No vulnerabilities exist in this lab. Report any anomalies to the given email address.

Lab 10: Modify the Payload

- **Goal**: Modify the JWT payload and bypass server-side validation.
- **Solution**:
    1. Take the provided JWT token and copy it.
    2. Navigate to jwt.io.
    3. Paste the token into the decoder.
    4. In the "Payload" section, change the canViewFlag value from false to true.
    5. Since the server does not verify the signature for this token, re-encode the token without worrying about the key.
    6. Copy the new token and submit it.
    7. **Hint**: It should work with any key (see jwt.io).

Lab 11: Use the Hidden Key

- **Goal**: Exploit a JWT that uses a key stored in a cookie.
- **Solution**:
    1. Take the provided JWT token and copy it.
    2. Open your browser's developer tools and check the cookies for the application.
    3. Find the key hidden in one of the cookies.
    4. Navigate to jwt.io.
    5. Paste the token into the decoder.
    6. Change the canViewFlag value from false to true.
    7. Replace the "Key" in jwt.io with the value found in the cookie.
    8. Copy the newly signed token and submit it.

Lab 20: Retrieve the Key from a File

- **Goal**: Exploit a JWT that uses a key stored in a server file.
- **Solution**:
    1. Check the hint: the key is stored in ../getSecret.txt.
    2. Use a directory traversal or file access method to retrieve the getSecret.txt file.
    3. Copy the contents of getSecret.txt (this is the secret key).
    4. Navigate to jwt.io.
    5. Paste the provided token into the decoder.
    6. Change the canViewFlag value from false to true.
    7. Replace the "Key" in jwt.io with the value found in getSecret.txt.
    8. Copy the newly signed token and submit it.

Tools and Resources

1. **JWT Decoding and Signing**: Use jwt.io for decoding and modifying tokens.
2. **Inspect Cookies**: Use your browser's developer tools to inspect cookies and other session storage.
3. **Directory Traversal**: Tools like curl or your browser may help retrieve hidden files.

Reporting and Help

- For issues or anomalies in the lab, report to info@thexssrat.com.
- Review the solution hints provided in this document.