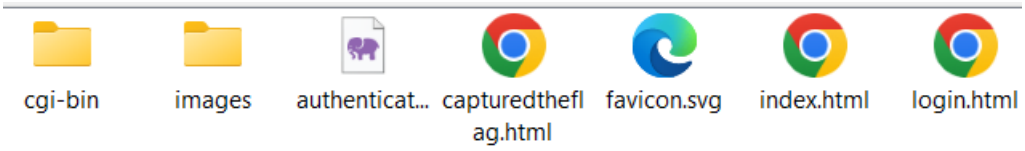
בס"ד

הסבר

בתיקייה זו ישנם 4 קבצי html, דף פתיחה, דף התחברות ודף סיום



כמו כן, דף ה login מתקשר עם קובץ נוסף שרשמתי, authentication.php, שתפקידו יהיה לנהל את הבדיקה של הסיסמא הנכונה, ו redirection לדף סיום במידה והסיסמא באמת נכונה.

הייתי חייב לעשות את זה בצד שרת, אחרת הלקוח היה יכול פשוט לעשות inspect ולראות או מה הסיסמא הנכונה, או פשוט לאן הוא אמור להגיע במידה והוא מכניס את הסיסמא הנכונה.

הנה הקוד:

```
    <script>

        document.getElementById('loginForm').addEventListener('submit',
function(event) {
            event.preventDefault(); // Prevent the form from submitting

            var username = document.getElementById('username').value;
            var password = document.getElementById('password').value;

            // Send POST request to authenticate.php
            fetch('authenticate.php', {
                method: 'POST',
                headers: {
                    'Content-Type': 'application/json'
                },
                body: JSON.stringify({ username: username, password: password
})
            })
            .then(response => {
                return response.json().then(data => {
                    return {status: response.status, body: data};
                });
            })
            .then(data => {
                if (data.status === 200 && data.body.authenticated) {
                    window.location.href = data.body.redirect_url; // Redirect
on successful login
                } else {
                    document.getElementById('errorMessage').innerText =
'Invalid username or password'; // Display error message
                    document.getElementById('errorMessage').style.display =
'block'; // Show error message
```

```
                }
            })
            .catch(error => {
                console.error('Error:', error);
                document.getElementById('errorMessage').innerText = 'Failed to
authenticate. Please try again.'; // Generic error message
                document.getElementById('errorMessage').style.display =
'block'; // Show error message
            });
        });
    </script>
```

מה שקורה פה זה ככה:

כל פעם שהמשתמש מכניס סיסמא, הדפדפן עושה Http POST עם הנתונים, וזה מגיע אל השרת. בצד לקוח זה מחכה לתגובה, ובהתאם לתגובה עושה את הפעולות המתאימות. במידה והוא מקבל שגיאה, הוא מדפיס invalid, אחרת, הוא עושה redirect לדף שאותו שלח ה server.

בצד שרת יש קוד php, שתפקידו לקבל שם משתמש וסיסמא, לבדוק אם הם נכונים, ואם כן לשלוח בחזרה response עם ה redirection page המתאים. במידה והם לא נכונים, הוא ישלח קוד בהתאם.

```
<?php
// Replace with your actual username and password
$correctUsername = 'EliCopter';
$correctPassword = 'MossadRules';

// Check if the request is a POST request
if ($_SERVER['REQUEST_METHOD'] === 'POST') {
    // Retrieve POST data
    $postData = json_decode(file_get_contents('php://input'), true);

    // Check if username and password are provided
    if (isset($postData['username']) && isset($postData['password'])) {
        $username = $postData['username'];
        $password = $postData['password'];

        // Simple authentication logic
        if ($username === $correctUsername && $password === $correctPassword)
{
            // Authentication successful
            $response = array('authenticated' => true, 'redirect_url' =>
'capturedtheflag.html');
            http_response_code(200);
        } else {
            // Authentication failed
            $response = array('authenticated' => false);
            http_response_code(401);
        }
    } else {
```

```
        // Invalid request
        $response = array('error' => 'Invalid request');
        http_response_code(400);
    }
} else {
    // Method not allowed
    $response = array('error' => 'Method not allowed');
    http_response_code(405);
}

// Return JSON response
header('Content-Type: application/json');
echo json_encode($response);
?>
```