# logo_ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ

# ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΚΑΙ ΕΦΑΡΜΟΣΜΕΝΩΝ ΕΠΙΣΤΗΜΩΝ

# ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

# cslogo

# EPL425: Internet Technologies

Team 05

Elena Kissopoda 915172

Constantinos Diomedous 934991

For the implementation of the authentication process we first created a “Login” page, where the user can write his username and password. The user pushes the button “Enter the site”. If the username given exists in the database, then we fetch the corresponding hashed password. We take the input password, hash it with the bcrypt algorithm and compare it with the one that we fetched from our database. The way we stored them in the database is with the use of bcrypt . If the combination of username and password don’t match with the ones that we have in our database then an error message appears, else the user moves to the next page. The user can try logging in 3 times, after that is blocked.

If the user successfully enters the site, a unique token is given to him. The token will be used when the user wants to access the API. Specifically as he request the API we check if the provided token is matched. If yes, the API is available to him, else he gets an “Access denied” message.

The token is been generated with the following code:

<?php

function generate\_token($username){

// Create token header as a JSON string

$header = json\_encode(['typ' => 'JWT', 'alg' => 'HS256']);

// Create token payload as a JSON string

$payload = json\_encode(['username' => $username]);

// Encode Header to Base64Url String

$base64UrlHeader = str\_replace(['+', '/', '='], ['-', '\_', ''], base64\_encode($header));

// Encode Payload to Base64Url String

$base64UrlPayload = str\_replace(['+', '/', '='], ['-', '\_', ''], base64\_encode($payload));

// Create Signature Hash

$signature = hash\_hmac('sha256', $base64UrlHeader . "." . $base64UrlPayload, 'mysecretestring', true);

// Encode Signature to Base64Url String

$base64UrlSignature = str\_replace(['+', '/', '='], ['-', '\_', ''], base64\_encode($signature));

// Create JWT

$jwt = $base64UrlHeader . "." . $base64UrlPayload . "." . $base64UrlSignature;

return $jwt;

}

function validatetoken($username,$token){

if(generate\_token($username)!=$token){

echo "You are not authorized to access this data";

die();

}

}

?>