

# Rozwiązania zadań

# Zadanie 1 - rozwiązanie



**LOGOWANIE**

sprzedawca@agh.pl ' ; --

.....

**ZALOGUJ SIĘ**

# Zadanie 2 - rozwiązanie - sposób I

```
if (isset($_POST['login']) && isset($_POST['password'])) {  
    if ($_POST['login'] == '' || $_POST['password'] == '') {  
        $message = "Pola nie mogą być puste.";  
    } else {  
        $login = $_POST['login'];  
        $password = crypt($_POST['password'], '$1$salt$');  
        $stmt = $dbh->prepare("SELECT * FROM users WHERE email = :email AND password = :password");  
        $stmt->execute([':email' => $login, ':password' => $password]);  
        $user = $stmt->fetch(PDO::FETCH_ASSOC);  
        if ($user) {  
            $_SESSION['uid'] = $user['uid'];  
            $_SESSION['email'] = $user['email'];  
            header('Location: /');  
        } else $message = "Niepoprawne dane.";  
    }  
}
```

# Zadanie 2 - rozwiązanie - sposób II

```
if (isset($_POST['login']) && isset($_POST['password'])) {  
    if ($_POST['login'] == '' || $_POST['password'] == '') {  
        $message = "Pola nie mogą być puste.";  
    }  
    else {  
        $stmt = $dbh->prepare("SELECT * FROM users WHERE email = :email");  
        $stmt->execute([':email' => $_POST['login']]);  
        $user = $stmt->fetch(PDO::FETCH_ASSOC);  
        if ($user) {  
            if (password_verify($_POST['password'], $user['password'])) {  
                $_SESSION['uid'] = $user['uid'];  
                $_SESSION['email'] = $user['email'];  
                header('Location: /');  
            } else $message = "Hasło niepoprawne.";  
        } else $message = "Nie ma takiego użytkownika.";  
    }  
}
```

# Zadanie 3 - rozwiązanie

```
toor@MSI: /mnt/d/AGH/Semes x + v

(toor@MSI)-[/mnt/d/AGH/Semestr V/BAWiM/pass]
$ ls
1.txt john.png odpowiedzi.txt passw passwords_to_crack.txt rockyou.txt

(toor@MSI)-[/mnt/d/AGH/Semestr V/BAWiM/pass]
$ john --wordlist=rockyou.txt --format=Raw-MD5 passwords_to_crack.txt
Using default input encoding: UTF-8
Loaded 3 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8x3])
No password hashes left to crack (see FAQ)

(toor@MSI)-[/mnt/d/AGH/Semestr V/BAWiM/pass]
$ john --show --format=Raw-MD5 passwords_to_crack.txt
ania:pass
piotr:alladin
szymek:szymek615243

3 password hashes cracked, 0 left

(toor@MSI)-[/mnt/d/AGH/Semestr V/BAWiM/pass]
$ |
```

# Zadanie 4 - rozwiązanie

Komunikat ze strony localhost

GRATULACJE! WYGRAŁEŚ BON O WARTOŚCI 1000ZŁ DO  
WYKORZYSTANIA W SKLEPACH BIEDRONKA. ABY ODEBRAĆ BON  
KLIKNIJ OK

OK

# Zadanie 5 - rozwiązanie - część 1

sprzedaj.pl

Wyloguj się Moje konto Dodaj ogłoszenie



**ciągnik Lamborghini**

**83500 PLN**

Kategoria: Rolnictwo

Stan: Używany

Użytkownik: **Janusz**

Telefon: **881536482**

Lokalizacja: **00-000, Poznań**

## Opis

```
<script type="text/javascript">alert("GRATULACJE! WYGRAŁEŚ BON O WARTOŚCI 1000ZŁ DO WYKORZYSTANIA W SKLEPACH BIEDRONKA. ABY ODEBRAĆ BON KLIKNIJ OK"); window.location = "https://biedronka.pl" </script>
```

# Zadanie 5 - rozwiązanie - część 2

```
if ($row) {  
    $title = $row['title'];  
    $category = $row['category'];  
    $path = $row['path'];  
    $description = htmlspecialchars($row['description']);  
    $status = $row['status'];  
    $price = $row['price'];  
    $postcode = $row['postcode'];  
    $location = $row['location'];  
    $phone_number = $row['phone_number'];  
    $username = $row['name'];  
}
```