[EX008] The exploit chain allows to take control of Zalo user accounts

blog.vincss.net/2021/11/ex008-exploit-chain-allows-to-take-control-of-Zalo-user-accounts.html

While using the Zalo application, one of the popular chat applications in Vietnam today (According to statistics from Wikipedia, since May 2018, Zalo has reached 100 million users), the **Threat Hunting team from VinCSS LLC** discovered some security vulnerabilities that allow the attacker to form an exploit chain to take control of Zalo accounts.

Beside that, while researching this attack chain, we also found it can exploit ZaloPay, an e-wallet and online payment platform that was also very successful in Vietnam.

A unique feature of the discovered exploit chain is that the bad guy can completely take control of any Zalo user account by tricking the victim into clicking on a sophisticated concealed link. When successfully accessing the Zalo user account, the Zalo application on the victim's phone will not appear in any new login session warning.

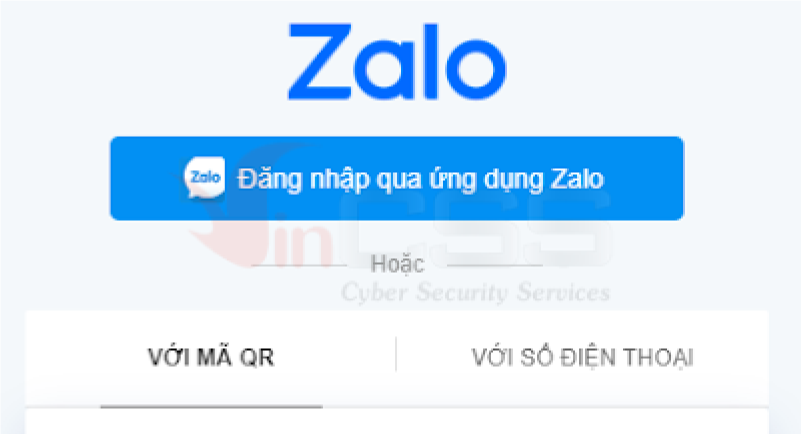
On August 10, 2021, VinCSS informed the security team of Zalo and immediately received positive feedback from the Zalo security team. By August 15, 2021, Zalo informed that it had fixed most of the vulnerabilities. A detailed timeline will be available at the end of this article.

This article will summarize technical information about the vulnerabilities that VinCSS has discovered, thereby helping businesses avoid similar vulnerabilities in the future.

I. Vulnerability in "login with Zalo" feature

In using the Zalo application, VinCSS discovered that the "**Login with Zalo**" feature exists an Open Redirection vulnerability that allows changing the address to receive tokens from the application.

Expressly, when using the Web-based Zalo application, or some other applications in the VNG ecosystem, users are provided with the option "Login with Zalo":



When using this feature, Zalo processes with the following flow:

Authenticate with the API at the following address to get the token:

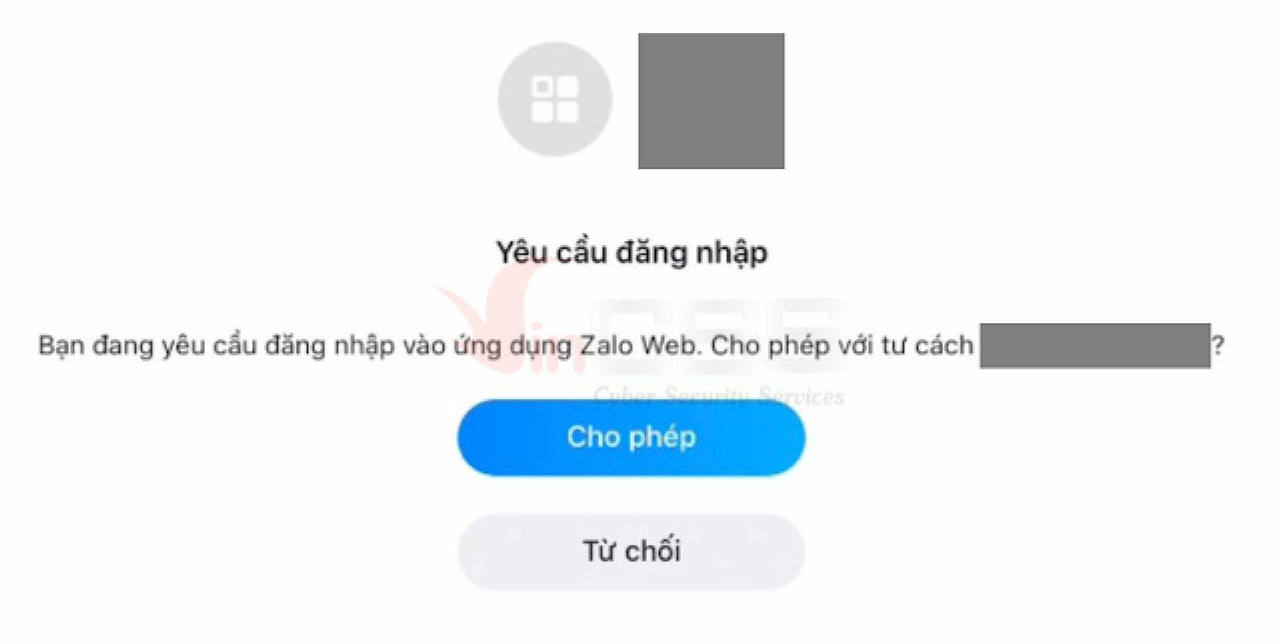
f'https://id.zalo.me/account/login/native/check-login-status' \

f'?browser={redirect_url}&continue=https%3A%2F%2Fchat.zalo.me%2F'

Use the token obtained in step 1 to send to the Zalo application on your phone via a shared deep link for both iOS and Android platforms:

f'zalo://login/?browser=chrome&token={token}'

The phone will switch to the Zalo application, and Zalo will display a message **Requires login to the Zalo Web application**.



[redacted]

Yêu cầu đăng nhập

Bạn đang yêu cầu đăng nhập vào ứng dụng Zalo Web. Cho phép với tư cách [redacted]?

- When the user presses click **Allow** button, the application will open the default browser on the phone with the link to the **redirect_url** address with a token used to log in (If you press the **Reject** button, the token will not be sent).
  By arbitrarily changing the **redirect_url** address in step 1, the bad guys can redirect the authenticated user to a website that they own or have taken control of, thereby obtaining the token. to log into the user's account.
- Continues to interact with the API below to convert the token obtained in step 4 into cookies:

```
url = f'https://id.zalo.me/account/login/native/verify?token={verify_token}'

resp = requests.get(

   url,

   headers={'User-Agent': user_agent},

   cookies={'zvid': check_login_cookie},

   allow_redirects=False)
```

To interact with this API, the bad guy needs to save the value of the cookie name **zvid** (issued together with the token in step 2). In addition, it should be noted that the **user_agent** parameter value will be the value used by Zalo to display in the **Settings ® Account and Security ® Login history** of the user account.

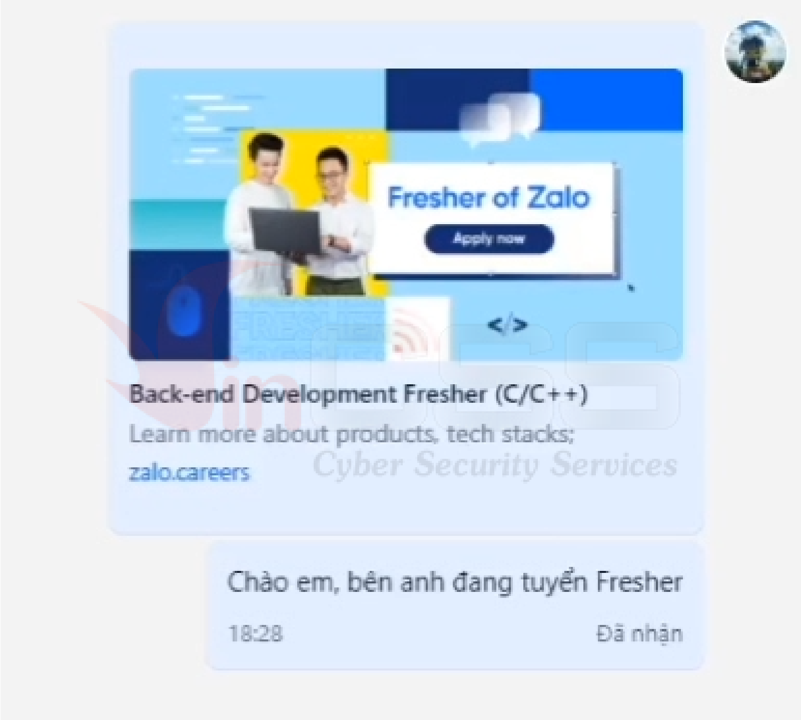
After exploiting this vulnerability, the bad guys obtained Cookies that allowed access to the victim's account. However, we quickly recognize 03 limitations if the bad guys only exploit this vulnerability:

- Difficult to trick users into clicking on the link because the link will look very "strange"
- There is a login notification message when using the token and comply with the processing flow of the Zalo Web application.
- After a period of use, the expired cookie will not be able to log in again.

So need to exploit this vulnerability with the following sequence of vulnerabilities to exploit it more effectively.

II. Vulnerability in Link Preview feature

When the first vulnerability above was discovered, VinCSS also noticed that when pasting a link into Zalo chat, the Zalo bot would conduct a link check by crawling the destination page with a special **user_agent**. This mechanism also allows Zalo to display the content of the destination page for users to preview. Suppose the Zalo bot checks and gets the response as the **302 Moved Temporarily** redirect status code. In that case, the **Zalo application will only display the website's content being redirected,** not **the link address.** This mechanism allows bad guys to hide the phishing link, easily tricking users into clicking the link because then only the website content is displayed like the real thing. Check out the phishing chat below. Will you click or try to check the destination page before clicking?



Back-end Development Fresher (C/C++)

Learn more about products, tech stacks;

zalo.careers

Chào em, bên anh đang tuyển Fresher

18:28 Đã nhận

When this vulnerability is exploited in combination with the first vulnerability, hackers will lure users, as shown above. When the user clicks and is redirected to the bad guy's server, the token will be automatically logged and redirected the user to the actual destination website. Since the redirect is so fast, the user, after clicking on the phishing link, will only see that they are being redirected to a legitimate and utterly normal destination website.

III. Vulnerability in Relogin mechanism

VinCSS also discovered that Zalo uses a re-login mechanism, allowing users to re-login the Zalo Web session with the logged-in session's cookie. However, the **re-login mechanism still works with the session that has never been logged in, hiding the logged in message on the new device.**

Specifically, the Zalo Web application will interact with an API as follows:

```
url = 'https://id.zalo.me/account/checksession?type=ajax&login_type=relogin' \

      '&continue=https%3A%2F%2Fchat.zalo.me'

response = requests.get(url, headers={'Referer': 'https://chat.zalo.me/login'}, cookies=
{'zpsid': cookie_value})

continueUrl = response.json()['data']['continueUrl']
```

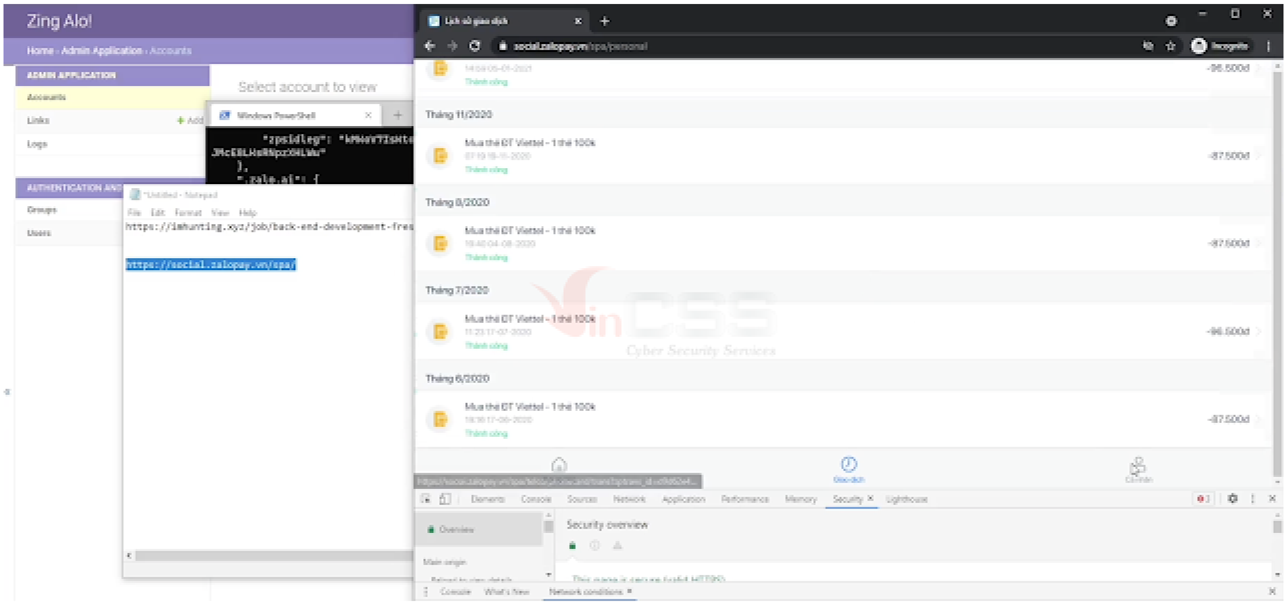
Using the **continueUrl** link in a brand new browser, Zalo will automatically set the necessary cookies and allow access to Zalo Web. Also, don't show an unknown login session warning to the user.

IV. Vulnerability related to the Session expiration time

In using the Zalo application, VinCSS discovered that when exploiting the relogin mechanism as described in the above security error, the session corresponding to the **zpsid** value will exist for a very long time. Bad guys can take advantage of this bug to access user accounts and take control of accounts for a long time.

V. Login to ZaloPay with the token obtained

When using the relogin mechanism described in vulnerability III, in addition to the new session access path of Zalo Web, the API also returns many ways to log in to other Zalo applications, including ZaloPay. When changing the browser's **user_agent** to the format of the mobile device, can access the ZaloPay application via the link https://social.zalopay.vn/spa.



```
        "zpsidleg": "kMHWYTIsHt
JMcE8LHsRNpzOHLWu"
      },
      ".zalo.ai": {
```

```
https://imhunting.xyz/job/back-end-development-fres

https://social.zalopay.vn/spa/
```

14:59 05-01-2021 Thành công -96.500đ

Tháng 11/2020

Mua thẻ ĐT Viettel - 1 thẻ 100k 07:19 18-11-2020 Thành công -87.500đ

Tháng 8/2020

Mua thẻ ĐT Viettel - 1 thẻ 100k 19:40 04-08-2020 Thành công -87.500đ

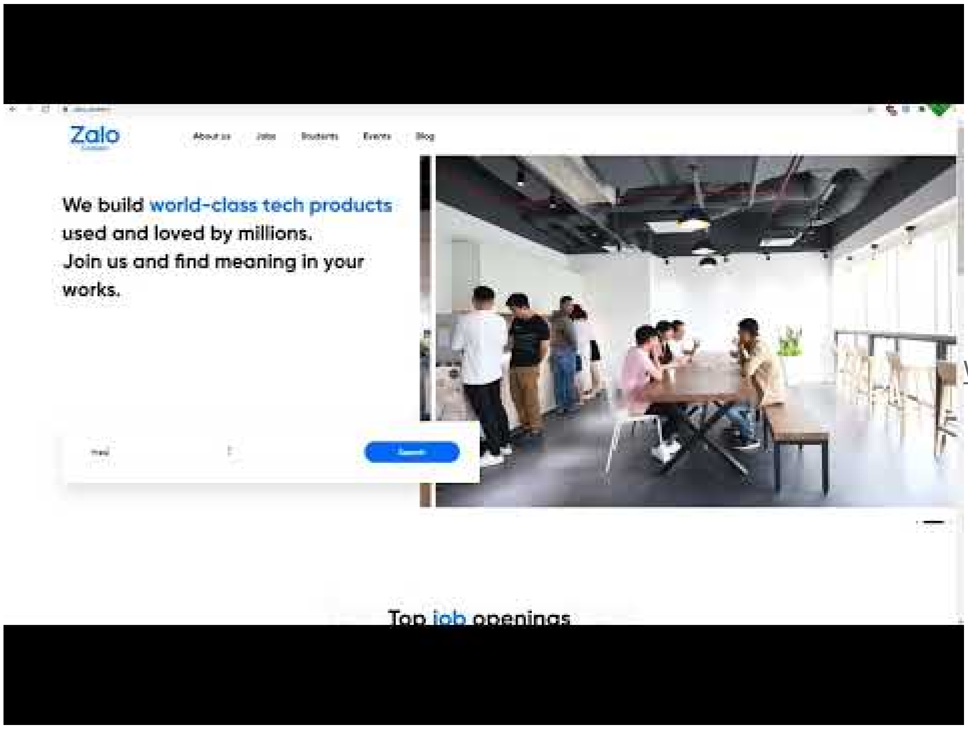
Tháng 7/2020

Mua thẻ ĐT Viettel - 1 thẻ 100k 11:23 17-07-2020 Thành công -96.500đ

Tháng 6/2020

Mua thẻ ĐT Viettel - 1 thẻ 100k 18:18 17-06-2020 Thành công -87.500đ

Demo:



We build world-class tech products used and loved by millions.
Join us and find meaning in your works.

Top job openings

Watch Video At:

https://youtu.be/AbEO4ucta4E

Summary

It is possible to form an exploit chain aimed at Zalo users when combining the five vulnerabilities presented above. Fortunately, the problem was dealt with quickly. Not only Zalo but any application can also have serious cyber security problems even with strict security. So, besides Bug bounty programs to attract bug hunters, the role of Red teams is equally important.

At VinCSS, the Threat Hunt teams are constantly monitor customers' IT resources from the bad guys' perspective, continuously targeting and simulating possible hazards to clients. From there, VinCSS can provide early and honest warnings to customers to promptly detect and deal with complex cyber threats.

Timeline

- August 10, 2021: Report to Zalo Security team.
- August 10, 2021: Zalo replied that it has received the report and is processing it.
- August 15, 2021: Zalo Security team informed that 4/5 vulnerabilities have been fixed.
- August 15, 2021: VinCSS verify and confirm.
- November 6, 2021: VinCSS sent an email to Zalo to ask about the status of the last vulnerability and requested to publish information about the vulnerability to the community when it was almost 90 days from the reporting date.
- November 9, 2021: Zalo Security team confirmed to have fixed all of vulnerabilities and VinCSS published the research paper.

Click here for Vietnamese version.