Headline

Credential stuffing attacks and step-by-step response strategies

Senior Manager, ICT MSS Biz. Team, Park Nam−chun

■ Outline

With the recent increase in credential stuffing attacks targeting Korean companies and government agencies, related cyber threats have also been increasing significantly. Between June and July of last year, there was a credential stuffing attack on the Korea Employment Information Service’s Worknet, Korea's representative recruitment and job search site, resulting in the leakage of personal information of about 236,000 people. A similar attack targeting the website of the Korea Student Aid Foundation resulted in the leakage of personal information of about 32,000 people.

Credential stuffing is one type of attack that leaks personal information or data. For this purpose, the attacker builds account information such as the user's ID/password (PW) into a large-scale database, and then randomly inserts this account information into several web/app services to attempt to log in. As credential stuffing attacks using automated technology targeting many companies and government agencies have recently become a social issue, this headline report will present cases of damage from credential stuffing attacks and explain response strategies.

Article 48 of the Information and Communications Network Act[1] considers credential stuffing an illegal act, and also prohibits the use of illegal programs related to it.

Article 48 of the Information and Communications Network Act (Prohibition of Intrusive Acts on Information and Communications Networks)
① No one shall intrude on an information and communications network without the rightful authority for access or beyond the permitted authority for access. * Imprisonment of up to 5 years or a fine of up to 50 million Korean won

For a credential stuffing attack, the attacker attempts to log in to multiple websites simultaneously using authentication information obtained through the dark web. Because most users tend to use the same password across multiple accounts, problems can occur even if login information is leaked from just one account. Therefore, special caution is required. In particular, with the recent increase in personal information leakage or hacking accidents, the probability of success in credential stuffing attacks also on the rise, requiring further attention.

Credential stuffing appears to be a normal login, and because of this, it is difficult to identify attack patterns and completely block them. Therefore, to prevent attacks for data theft, account takeover, and other fraudulent activities, you must use secure passwords, be careful to avoid an infection with malicious software, and take measures including updating your security solution.

[1] Information and Communications Network Act: Act on the Promotion of Information and Communications Network Utilization and Information Protection

■ Cases of damage from credential stuffing

The table below summarizes cases of damage caused by credential stuffing attacks that have recently occurred in Korea. All victims were attacked through exposed or leaked personal information. In addition to primary damage such as system errors and personal information leakage, additional financial damage such as surcharges and fines has occurred.

Date	Target	Description
Jan. 2024	Online education website	· Personal information of XX thousand members was leaked due to a credential stuffing attack and a cross-site scripting (XSS) attack on the bulletin board. · The attacker took over Member A's account through a credential stuffing attack that utilized an ID and password obtained in advance, and additionally leaked personal information by inserting a malicious script into the bulletin board for reporting illegal usage through Member A's account.
Nov. 2023	Lottery website	· The attacker changed the member's password and performed a fraudulent login. · Personal information (name, date of birth, phone number, email and virtual account) was leaked. · The website took steps to reset the passwords of members who were identified as having suffered damage.
Oct. 2023	Sports website	· In the Asian Games soccer quarterfinal match between Korea and China, over 90% of people cheered for the Chinese team in XX Sports' click rooting service. · On this website, click rooting is possible without logging in. The attacker used a macro to click root through 2 foreign IPs
Jul. 2023	Coffee shop website	· The attacker logged in to the app without permission using a credential stuffing attack and made purchases using the customer's (member) prepaid charges. · The attacker mainly purchased tumblers that were easy to cash out, and the coffee company compensated the customer for the entire prepaid amount · No separate secondary authentication was required at the login or transaction stage.
Jul. 2023	Employment information website	· Personal information was leaked through over XX thousand unauthorized logins from foreign IPs, including ones in China. · 13 registered personal information items, including name, gender, year of birth, address, and landline number, were leaked.

Table 1. Cases of credential stuffing attacks in Korea

■ Examples of credential stuffing attacks

Recently, credential stuffing attacks are becoming more sophisticated. In addition to existing hacking through simple ID/PW input, attackers are attempting various attacks as follows to obtain information:

- Attacks in which the attackers continuously substitute input values for a specific API value/page/parameter and check the response.

- Attacks conducted with a specific purpose and attempted through various points (before/after login, using normal service logic or support functions for the service, etc.)

- Modification and SQL injection attacks using vulnerabilities of a large number of parameters may also be classified as credential stuffing attacks (Recognizing unique patterns through responses/results of repetitive performance, and checking the consistency of information)

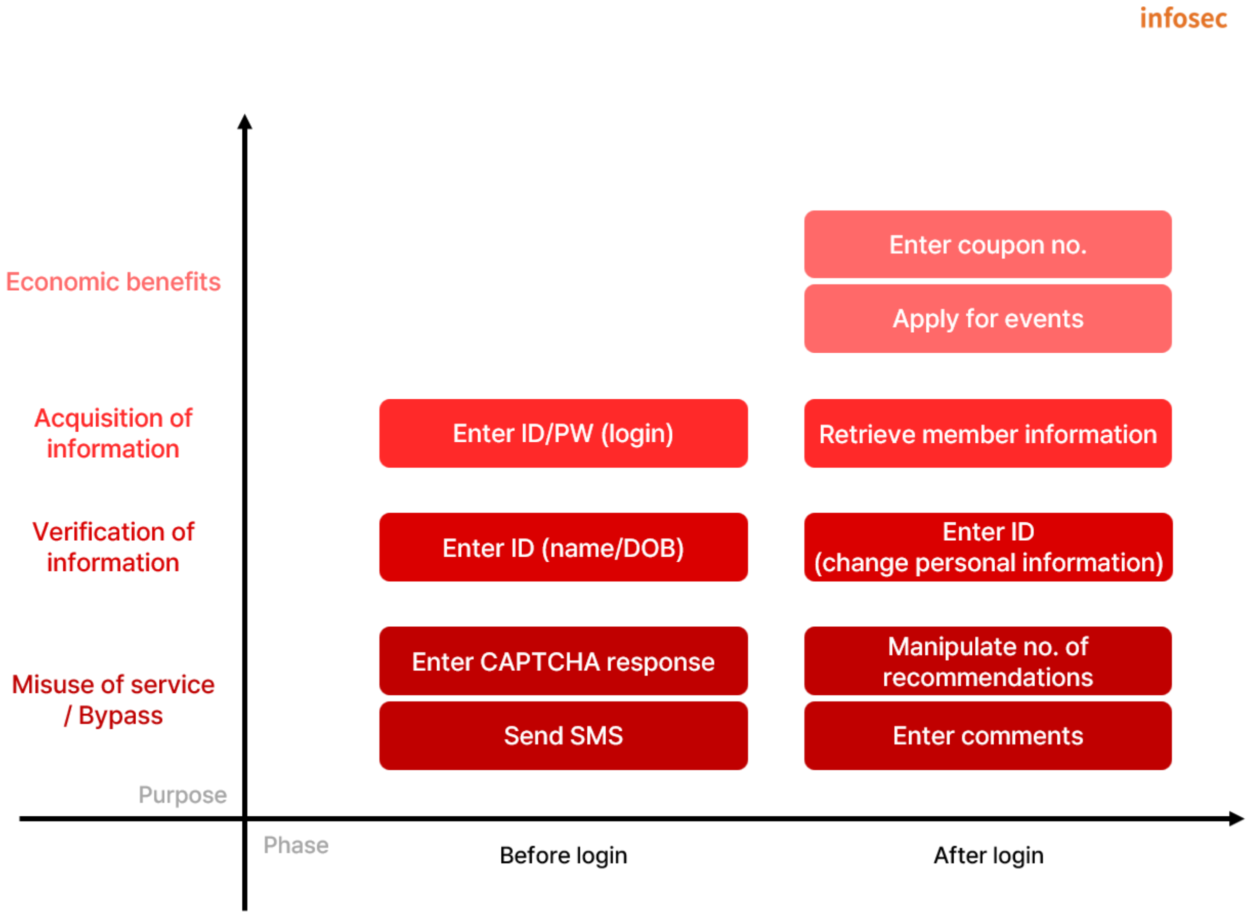
infosec
Economic benefits
Enter coupon no.
Apply for events
Acquisition of information
Enter ID/PW (login)
Retrieve member information
Verification of information
Enter ID (name/DOB)
Enter ID (change personal information)
Misuse of service / Bypass
Enter CAPTCHA response
Send SMS
Manipulate no. of recommendations
Enter comments
Purpose
Phase
Before login
After login

Figure 1. Examples of attacks on various service points

■ Step-by-step response strategies to credential stuffing

This section summarizes the step-by-step measures that security personnel can take in the event of a credential stuffing attack.

1. Identify the attacker's purpose and current situation

- What is the purpose of the page under a credential stuffing attack?

: Identify information (personal information) that an attacker can obtain from the page.

- What fields/parameters and response values (inputs) does the attacker manipulate?

: Identify what information the attacker is trying to check for consistency.

: Identify what personal information items are included in the input values.

: Identify what unique information is included in the response values.

- How many attempts and how?

: Determine whether it is a credential attack or a simple attack.

: Sequential increase/decrease of input values or sequential addition of strings has a low success rate.

2. Consider blocking the credential stuffing completely

- Consider a response method that limits the number of attempts per user.

: Limit the number of attempts using a user classification method.

(Login session, Src_IP, Pre-login session, User-Agent, etc.)

- Prevent damage from unauthorized logins

: Defense through multiple/complex authentication

3. Consider obstructing attacker actions

- Defense using restrictions on access to the target page (URL) by IP

: If it is difficult to implement the function in the app (server), implement it through an NW security solution (e.g., dedicated equipment).

: Support the threshold access blocking response function in AWS/Azure.

: Respond using WAF and SSL decryption traffic at OnPrem.

- Defense through implementing CAPTCHAs

: For pages where attacks/issues occur frequently, such as in the case of membership registration or identity verification, apply CAPTCHAs unconditionally.

: In the case of pages that general users frequently access (for example, login page), apply CAPTCHAs when abnormal behavior is detected.

4. Apply techniques to detect credential stuffing block bypasses
- Use techniques to detect connections bypass blocking : It is necessary to detect attempts to bypass the CAPTCHA through a manual method rather than an automatic method. **- Detection and analysis techniques (example)** : When accessing specific pages only : When accessing with a changed HTTP header : Detect persistent entry attacks (small number of accesses over a long period of time). : If necessary, perform monitoring by expanding the IP search criteria to C/B Classes.

5. Respond while considering service stability
- NAT IP band with many users : Recognize normal access by multiple users, not just one user, and handle it as an exception. **- Seek various response methods other than blocking** : Apply CAPTCHAs/additional authentication. : Notify users/administrators of blocking information. : Clear the block after a certain period of time.

6. Preventive and follow-up measures
- Design safe service logic against brute-force attack when implementing an app : Implement user-friendly security functions; implement protection processes **- Take action against attempted credential stuffing attacks** : Cancel illegal event wins, warn through user verification, etc. **- Respond to accounts that have been exposed to the dark web** : If necessary, implement an automated response process using services that provide dark web information. : Lock/change/guide measures for login to exposed accounts.

Table 2. Step-by-step response against credential stuffing

■ Conclusion

We have learned about cases of damage from credential stuffing attacks and step-by-step response strategies.

If a credential stuffing attack occurs, there is a risk that the leaked personal information may be used for hacking attacks on other services or in other ways, so thorough preparation is necessary. Furthermore, as the damaged company or institution can become subject to punishment, special caution is required at the company level.

In particular, the development of AI technology is accompanied by the advancement of credential stuffing attacks using this technology. Instead of attacking through existing simple automation tools, AI can attack by using the human-like threshold method. Therefore, preparation for this is necessary. In addition, such attack attempts are expected to increase further due to the active sale of personal information and accounts on the dark web.

In order to respond to credential stuffing attacks, it is necessary for security managers, developers, and operators to closely cooperate with each other. The most basic measures include implementing and expanding strong security policies, such as frequent password changes and the use of multi-factor authentication. In addition, perimeter monitoring must be thorough to detect suspicious activity.

SK Shieldus, a leader in the Korean information security industry, provides customized security consulting to prevent security incidents. In particular, penetration testing consulting helps prevent credential stuffing attacks. SK Shieldus has the largest number of penetration testing experts in Korea and provides customized services using differentiated methodologies and accumulated technology. Recently, the company has been using the generative AI ChatGPT to conduct AI mock-hacking simulations to identify PC or web vulnerabilities and detect the possibility of them being used in cyber attacks. More detailed information can be found on the SK Shieldus website.