# **CS 405 5-1 Case Study: Triple A and Defense in Depth**

# **Austin Donaubauer**

# **Southern New Hampshire University**

# **CS-405 Secure Coding**

# **Wasim Alim**

# **August 3rd, 2025**

# **CS 405 5-1 Case Study: Triple A and Defense in Depth**

* Introduction
  + Name of case and link

LinkedIn Data Scraping

<https://news.linkedin.com/2021/june/an-update-from-linkedin>

* + Date of case

April 2021

* + Why did this case make the news?

It made the news because of all the users it affected as it affected ~700 million of LinkedIn users.

* Describe the breach
  + Type of security or data breach or combination

The type of breach was data scraping. The attackers didn’t hack into LinkedIn, but were able to access the data using bots and automated scripts to get user data and then sell it online.

* + Why was this company a target?

LinkedIn is a target for hackers because of all the data it contains from its users. Users provide LinkedIn with their email, phone number, job info, educational information, and other personal information. This is valuable to many different people which is what makes LinkedIn an ideal target for hackers to try to exploit.

* Identify the threat(s)
  + Immediate threat(s)

The people that scraped the data were selling it online. This creates potential threats from people using the data for scamming or phishing people with illegitimate actions. This could cost people and cause them issues where they could be hacked or attacked by others.

* + Potential threat(s) if the vulnerability goes unresolved

The continuing of this data scraping would still create issues where user data is being sold to people. It also would hurt the reputation of LinkedIn and cause many users to delete their accounts and not use their website anymore.

* What could a developer have done to prevent this breach?
  + Which policy or policies will help prevent this type of attack?

More security around user access to help protect against bot login would have helped because the attack stemmed from the ability of the data scrapers to use bots and automated scripts to access the data. Also, session time would only allow access for a certain amount of time would have helped limit the amount of data retrieved. Authentication also could have been improved to prevent bot login, like CAPTCHA so that bots could be prevented.

* Summarize the case by explaining the role of best practices, Triple A and defense in depth in preventing future attacks.
  + Authentication

The data scraping didn’t directly attack through breaking authentication, but it just shows that improved authentication processed like multifactor authentication and or CAPTCHA could prevent illegitimate users from accessing the system.

* + Authorization

Controlling what users are allowed to do is important. This case shows that because there weren’t more strict authorization permissions the bots and automated scripts were able to access the data. Improved AuthZ policies could help prevent access to public data in the future.

* + Accounting

Logging user activity could help detect unusual activity. Reviewing this activity will help create an earlier response to protect and limit the amount of data that is potentially retrieved.

* + Defense in depth

Defense in depth was in place for LinkedIn as its outer defense layers were exploited but the inner layers were secure and prevented further access from the bots and automated scripts. Improving the outer layers with additional security policies for bot and automation detection is necessary to make the outer layers more secure and prevent this from reoccurring.

References:

Communications        Share      LinkedIn      Facebook      Twitter, L. C. (n.d.-a). *An update on report of scraped data*. An update from LinkedIn. <https://news.linkedin.com/2021/april/an-update-from-linkedin>

Communications        Share      LinkedIn      Facebook      Twitter, L. C. (n.d.). *An update on report of scraped data*. An update from LinkedIn. <https://news.linkedin.com/2021/june/an-update-from-linkedin>

*Help linkedin help*. Prohibited software and extensions | LinkedIn Help. (n.d.). <https://www.linkedin.com/help/linkedin/answer/a1341387/prohibited-software-and-extensions?src=or-search&veh=www.google.com%7Cor-search>

Sharma, S., Barker, P., Constantin, L., & Plumb, T. (2025, August 1). *The 20 biggest data breaches of the 21st Century*. CSO Online. <https://www.csoonline.com/article/534628/the-biggest-data-breaches-of-the-21st-century.html>