

RSA[®]Conference2019 Asia Pacific & Japan

Singapore | 16–18 July | Marina Bay Sands



BETTER.

SESSION ID: FLE-W02

API Security Exposure for Gift Card Fraud: A 14-year old's guide

Tanay Deshmukh

High School Student
Amador Valley High School
Pleasanton CA, USA



#RSAC

About Me

- Just completed 9th grade
- Student at Amador Valley High School in Pleasanton
- Self taught and started coding at age 12
- Helped find vulnerabilities for Chipotle, Spotify, NCR, and JambaJuice
- Built Chrome extensions for buying high demand items
- Participant in HackerOne
- Platinum tier for US Cyberpatriot
- Github: t4nay



What will you learn and how can you use the learnings?

What will I talk about?

Securing API for services &
gift cards

What will you learn?

How hackers can exploit
vulnerabilities

How can you apply the learnings?

Use the best practices to
secure APIs and learn new
tools & techniques

Goals for my talk

- Understand how hackers exploit vulnerabilities using
 - Credential stuffing
 - SQL Injection
 - Web scraping
- Use techniques to protect by implementing
 - Captcha
 - Rate Limiting
 - Limiting public use, VPN access and increasing verifications

What is a Gift Card or Cash Card?

A **gift card** (also known as **gift certificate** in North America, or **gift voucher** or **gift token** in the UK) is a prepaid **stored-value money card**, usually issued by a **retailer** or **bank**, to be used as an alternative to cash for purchases within a particular store or related businesses.

What is a Subscription Account?

The subscription business model is a **business model** in which a customer must pay a **recurring price at regular intervals** for access to a product or service.

Biggest mistakes companies make with gift cards and subscription accounts

- Most gift cards have a clear pattern of gift card numbers so it's easy to guess the card number
- Overlooking the importance of securing the APIs
 - Websites are most secure
 - Mobile and APIs are least secure
- Captcha and rate limiting isn't implemented to the best of their ability
- Allowing VPNs or Public proxies to access the website without further verification
 - Suspicious login activity may not be reported to the user

Why are Gift card and Subscription accounts vulnerable?

Gift Cards:

Gift cards are vulnerable due to how they are generated and how balance checks are handled

Subscription Accounts:

Vulnerable from little to no protection from credential stuffing attacks on websites and old websites with recycled passwords

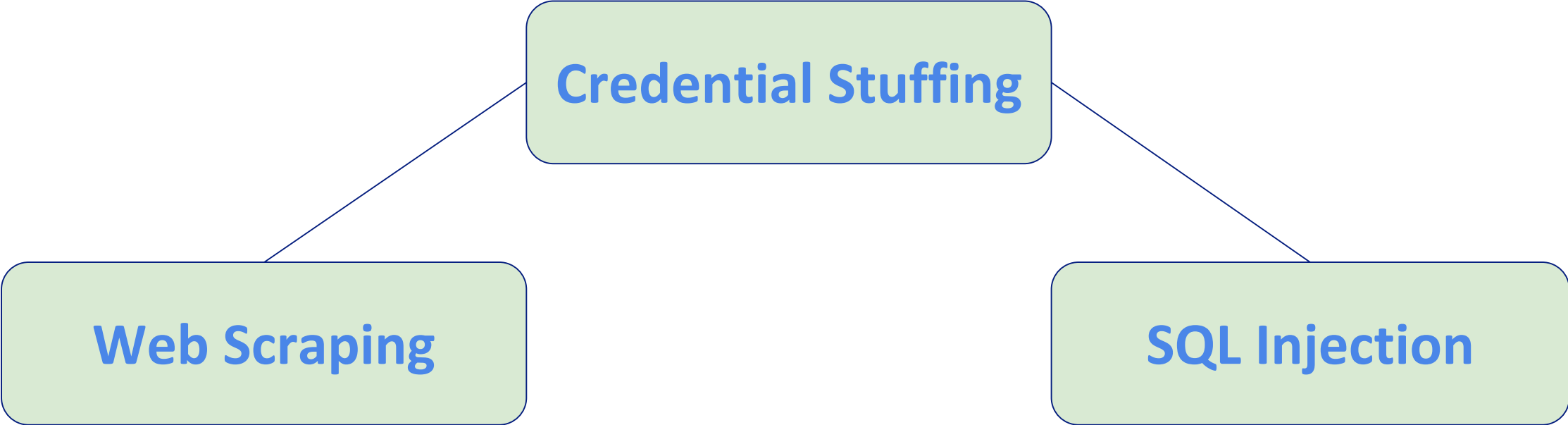
How did I find the vulnerabilities?

While learning about web development and how to secure web applications to the best of my ability -- started finding some security holes

- Mobile API was not as secure as the browser
 - Mobile API's typically do not have as much rate limiting as web applications do
- Credential stuffing is an attack which can easily be performed on most websites

My intentions were to learn and I found a way to help companies fight fraud

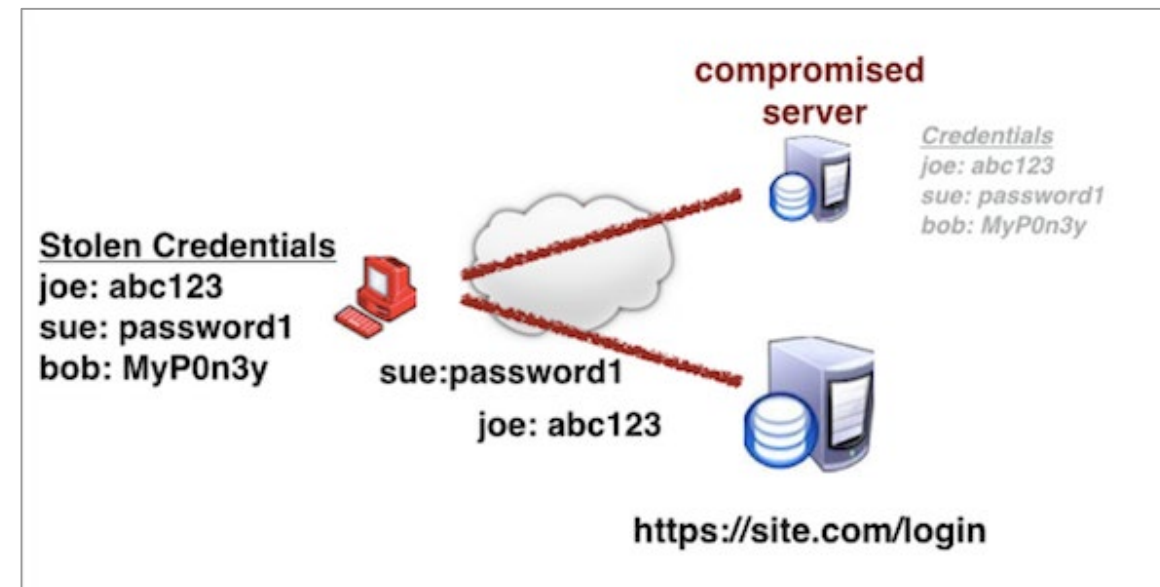
Methods used by hackers



What is Credential Stuffing?

Credential stuffing is the **automated injection of breached username/password pairs** in order to fraudulently gain access to user accounts.

Large numbers of spilled credentials are automatically entered into websites until they are potentially matched to an existing account, which the attacker can then hijack for their own purposes.



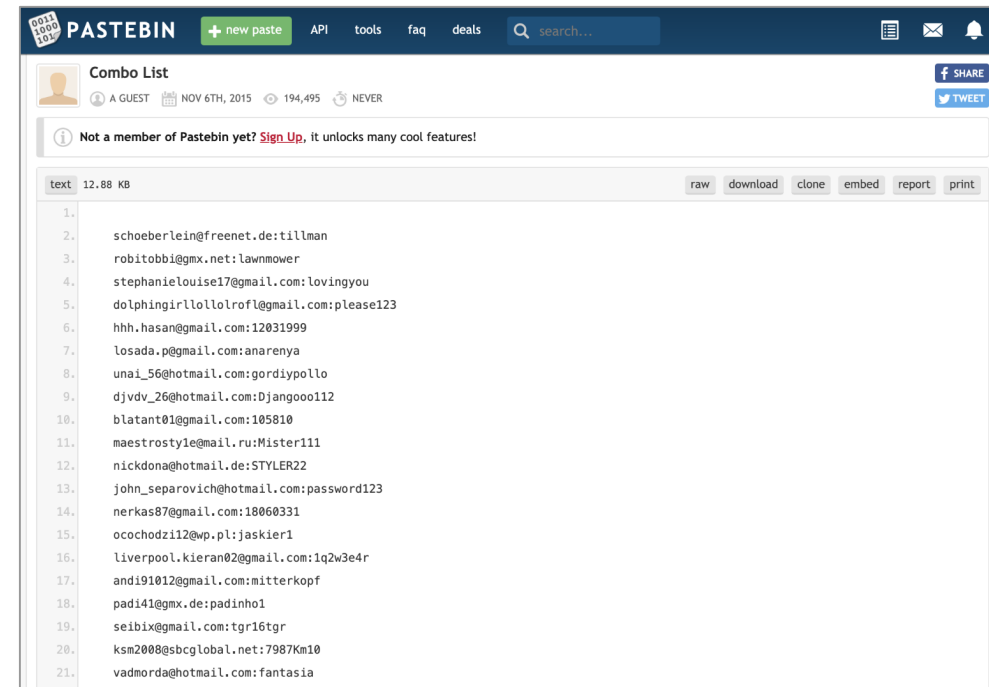
How does Credential Stuffing work?

1. Obtain credentials

- Easily found on pastebin or dedicated forums
- Can use SQL injection
- Can be formatted as User:Pass or Email:Pass

2. Obtain proxies (optional)

3. Create/use existing config for website

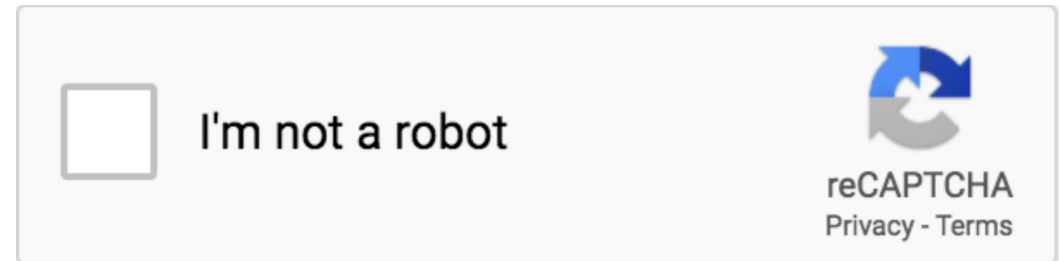


The screenshot shows a Pastebin page titled "Combo List". The page contains a list of 21 entries, each consisting of an email address followed by a colon and a password. The entries are numbered 1 through 21. The page also includes a search bar, a "new paste" button, and various utility buttons like "raw", "download", "clone", "embed", "report", and "print".

```
1.
2. schoeberlein@freenet.de:tillman
3. robitobbi@gmx.net:lawnmower
4. stephanielouise17@gmail.com:lovingyou
5. dolphingirl1lolrofl@gmail.com:please123
6. hhh.hasan@gmail.com:12031999
7. losada.p@gmail.com:anarenya
8. unai_5@hotmail.com:gordiypollo
9. djvdy_26@hotmail.com:Django00112
10. blatant01@gmail.com:105810
11. maestrosty1e@mail.ru:Mister111
12. nickdona@hotmail.de:STYLER22
13. john_separovich@hotmail.com:password123
14. nerkas87@gmail.com:18060331
15. ocochodzi12@wp.pl:jaskier1
16. liverpool.kieran02@gmail.com:1q2w3e4r
17. andi91012@gmail.com:mitterkopf
18. padi41@gmx.de:padinho1
19. seibi@gmail.com:tgr16tgr
20. ksm2008@sbcglobal.net:7987Km10
21. vadmorda@hotmail.com:fantasia
```

Ways to prevent Credential Stuffing

- Rate limiting
 - Use a commercial or open source software
 - Build it in application logic
- Captchas
- 2-step verification

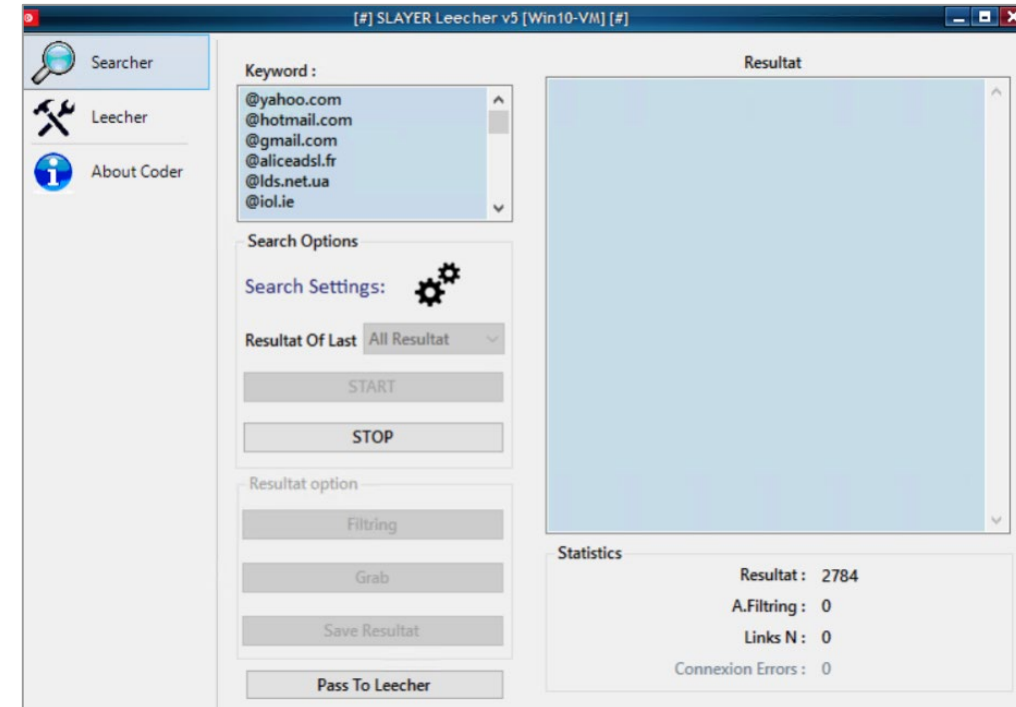


SQL Injection

- To perform SQL injection SQLi dumper can be used
 - Search terms referred to as dorks are used to find vulnerable urls on search engines such as google or bing
 - VPNs or proxies are used similarly to prevent rate limiting on search engines
 - Once the urls have been collected the program checks them for vulnerabilities and the attacker can dump the emails, usernames, and passwords from the database

Web Scraping

- Credentials can also be found on publicly on the internet easily
 - Websites used to scrape links include **Google**, **Pastebin**, and **Bing**
 - Programs such as **Slayer Leecher** are utilized using keywords
 - Links are scraped from keywords and are the program parses whatever format is selected (USER:PASS, EMAIL:PASS)



Tools used

- For credential stuffing a wide variety of tools can be used
 - **SentryMBA**
 - Original program for credential stuffing and the most popular
 - **SNIPR**
 - Costs money
 - Has a public and private repo for configs built in
 - Built in proxy scraper and leecher
 - **OpenBullet**
 - Can use selenium and has a simple system of making configs
- **SQLi Dumper**
 - Has many different versions and is the primarily used program for SQL injection

RSA®Conference2019 **Asia Pacific & Japan**

Demo



How to fix the problems?

- **Captcha**
 - Companies were allowing balance checks on cards through their web api
 - o Captchas make it harder for bots to send automated requests
 - o It was added additional steps to perform an attack
 - o Forces the attacker to pay for a captcha solving service (ex: 2captcha)
- **Rate Limiting**
 - Rate limiting limits the number of requests from a specific IP address within a certain amount of time
 - Companies can use this to limit the number of requests and prevent bots from sending requests at a faster rate
 - Adding a commercially available rate limiting software can also prevent websites slowing down due to bots sending a large amount of requests in a short period of time

What did I do after finding the vulnerabilities?

- Reached out to the customer service department and in some cases the InfoSec team on what I had found
- In some cases, used HackerOne to submit the vulnerabilities
- Sent a screenshot of the problem identified
- Made myself available for a call with the team
- Shared my findings and fixes that were needed

What's next for me?

- Continue learning more about vulnerabilities, security tools and techniques
- Help companies with preventing fraud if I find something new
- Learn and share what I find
- Summer research at UC Berkeley
- Continue my high school for next three years -- enter a Computer Science program
- Learn more programming languages

RSA®Conference2019 **Asia Pacific & Japan**

Questions?

Thank You!

tanayemail@gmail.com