RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: **HT-W11**

API Security Exposure for Gift Card Fraud: A 15-year old’s guide

Tanay Deshmukh

High School Student
Amador Valley High School
Pleasanton, CA

About Me

- High school sophomore
- Student at Amador Valley High School in Pleasanton
- Self taught and started coding at age 12
- Found major 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.

Source - Wikipedia

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.

Source - Wikipedia

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

Common methods used by hackers

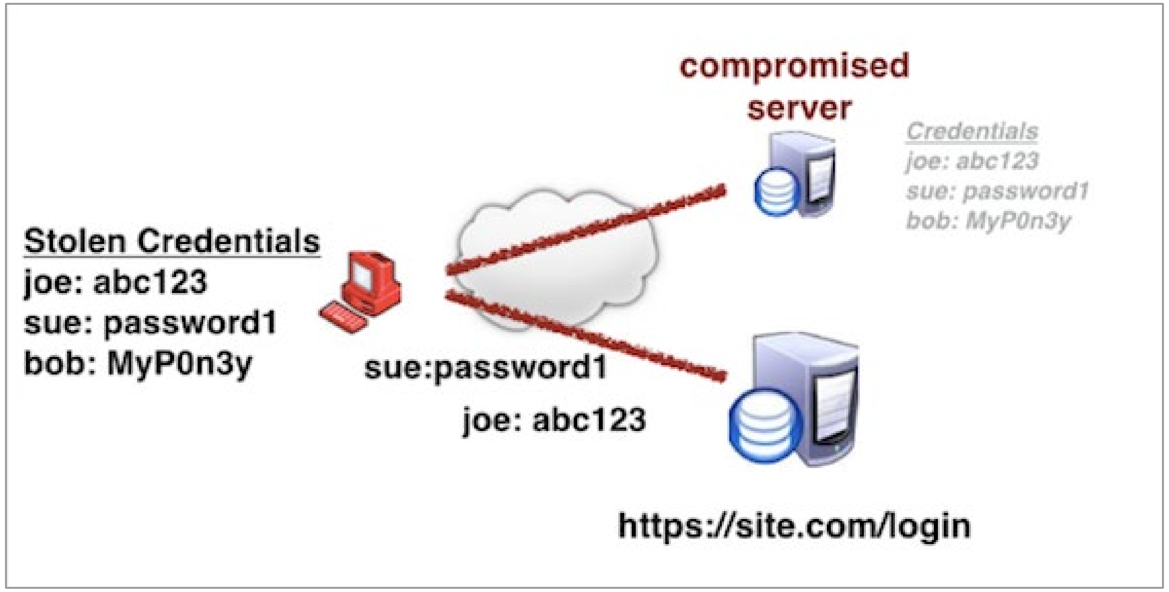
Credential Stuffing

Web Scraping

SQL Injection

What is Credential Stuffing?

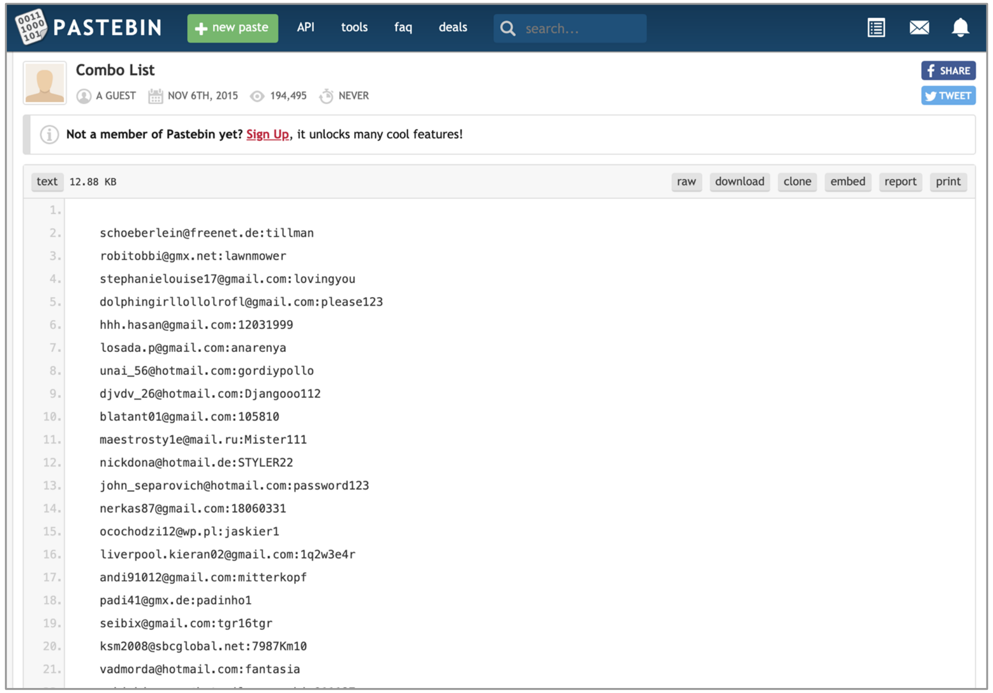
Credential stuffing is the **automated injection of breached username/password pairs** in order to fraudulently gain access to user accounts.



Text source: Wikipedia. Image: OWASP

How does Credential Stuffing work?

1. Obtain credentials
2. Obtain proxies (optional)
3. Create/use existing config for website



Combo List

A GUEST NOV 6TH, 2015 194,495 NEVER

Not a member of Pastebin yet? Sign Up, it unlocks many cool features!

text 12.88 KB

```

    schoeberlein@freenet.de:tillman
    robitobbi@gmx.net:lawnmower
    stephanielouise17@gmail.com:lovingyou
    dolphingirllollolrofl@gmail.com:please123
    hhh.hasan@gmail.com:12031999
    losada.p@gmail.com:anarenya
    unai_56@hotmail.com:gordiypollo
    djvdv_26@hotmail.com:Djangooo112
    blatant01@gmail.com:105810
    maestrosty1e@mail.ru:Mister111
    nickdona@hotmail.de:STYLER22
    john_separovich@hotmail.com:password123
    nerkas87@gmail.com:18060331
    ocochodzi12@wp.pl:jaskier1
    liverpool.kieran02@gmail.com:1q2w3e4r
    andi91012@gmail.com:mitterkopf
    padi41@gmx.de:padinho1
    seibix@gmail.com:tgr16tgr
    ksm2008@sbcglobal.net:7987Km10
    vadmorda@hotmail.com:fantasia
```

Image source: pastebin

Ways to prevent Credential Stuffing

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

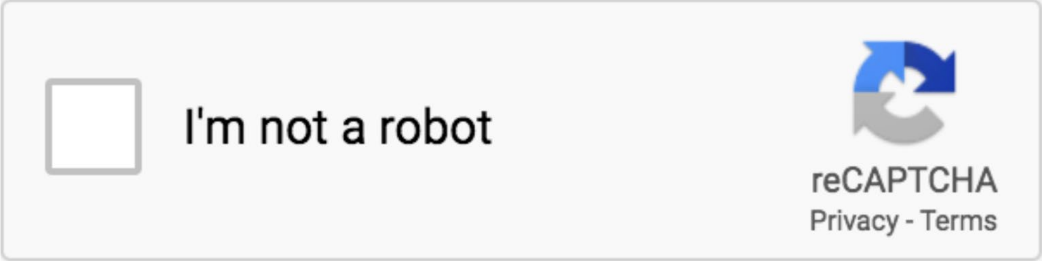


Image source: google image search

SQL Injection

- SQL Injection is the main method attackers use to gain access to credentials
  - Compromised databases are used for accessing credentials

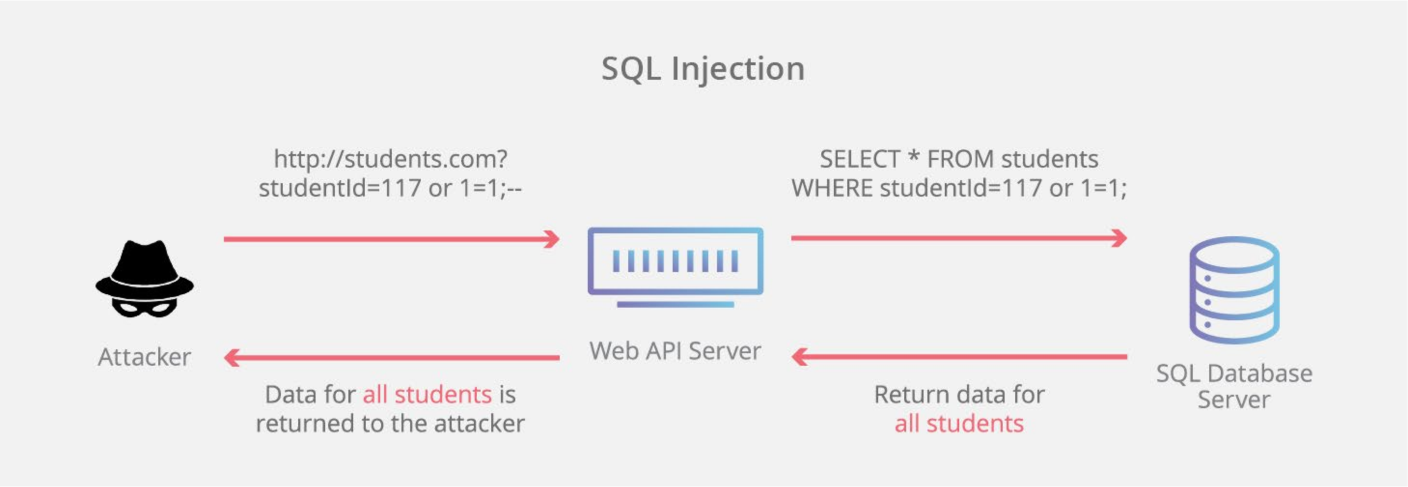
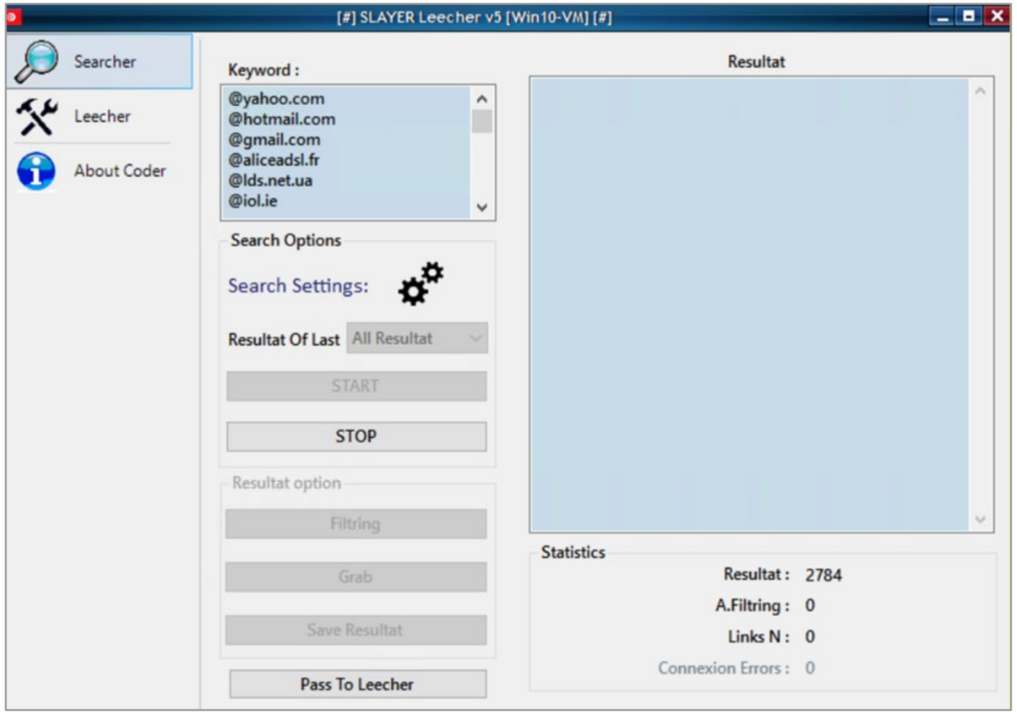


Image source: google image search

Web Scraping

- Credentials can also be found on publicly on the internet easily
    - Links are scraped from keywords and are the program parses credentials



[#] SLAYER Leecher v5 [Win10-VM] [#]

Keyword :

```
@yahoo.com
@hotmail.com
@gmail.com
@aliceadsl.fr
@lds.net.ua
@iol.ie
```

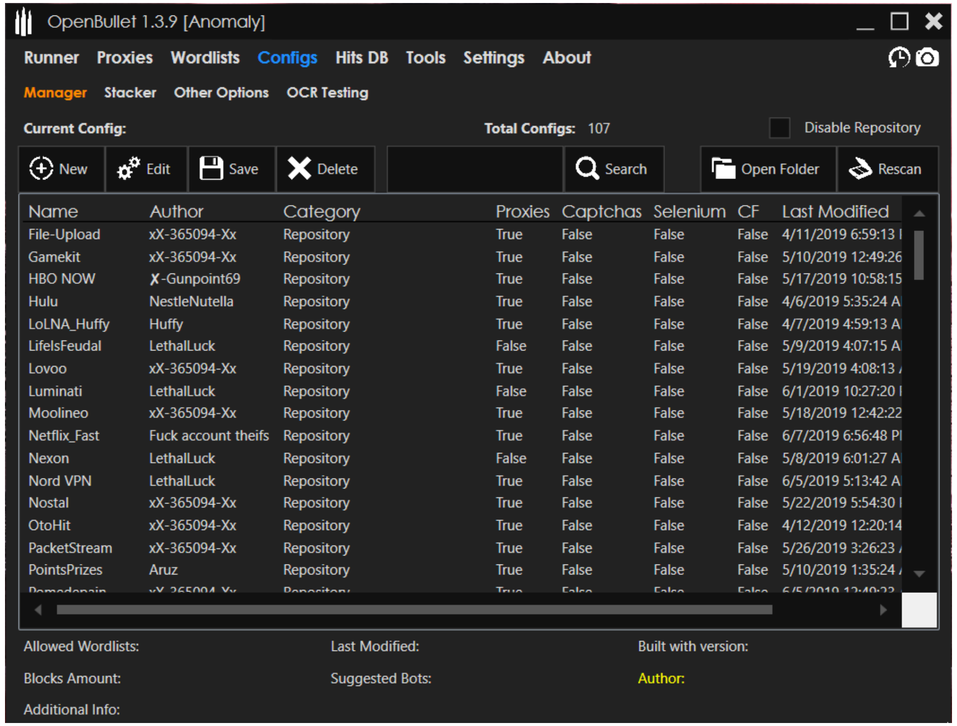
Resultat Of Last: All Resultat

Statistics

Resultat : 2784
A.Filtring : 0
Links N : 0
Connexion Errors : 0

What is a Config?

- Configs are files which instruct the program the series of requests and responses to check for a valid login



Current Config:

Total Configs: 107

Name	Author	Category	Proxies	Captchas	Selenium	CF	Last Modified
File-Upload	xX-365094-Xx	Repository	True	False	False	False	4/11/2019 6:59:13
Gamekit	xX-365094-Xx	Repository	True	False	False	False	5/10/2019 12:49:26
HBO NOW	Ӿ-Gunpoint69	Repository	True	False	False	False	5/17/2019 10:58:15
Hulu	NestleNutella	Repository	True	False	False	False	4/6/2019 5:35:24 A
LoLNA_Huffy	Huffy	Repository	True	False	False	False	4/7/2019 4:59:13 A
LifeIsFeudal	LethalLuck	Repository	False	False	False	False	5/9/2019 4:07:15 A
Lovoo	xX-365094-Xx	Repository	True	False	False	False	5/19/2019 4:08:13
Luminati	LethalLuck	Repository	False	False	False	False	6/1/2019 10:27:20
Moolineo	xX-365094-Xx	Repository	True	False	False	False	5/18/2019 12:42:22
Netflix_Fast	Fuck account theifs	Repository	True	False	False	False	6/7/2019 6:56:48 P
Nexon	LethalLuck	Repository	False	False	False	False	5/8/2019 6:01:27 A
Nord VPN	LethalLuck	Repository	True	False	False	False	6/5/2019 5:13:42 A
Nostal	xX-365094-Xx	Repository	True	False	False	False	5/22/2019 5:54:30
OtoHit	xX-365094-Xx	Repository	True	False	False	False	4/12/2019 12:20:14
PacketStream	xX-365094-Xx	Repository	True	False	False	False	5/26/2019 3:26:23
PointsPrizes	Aruz	Repository	True	False	False	False	5/10/2019 1:35:24
Pomodonain	xX-365094-Xx	Repository	True	False	False	False	6/5/2019 12:40:23

Allowed Wordlists:

Last Modified:

Built with version:

Blocks Amount:

Suggested Bots:

Author:

Additional Info:

Tools used

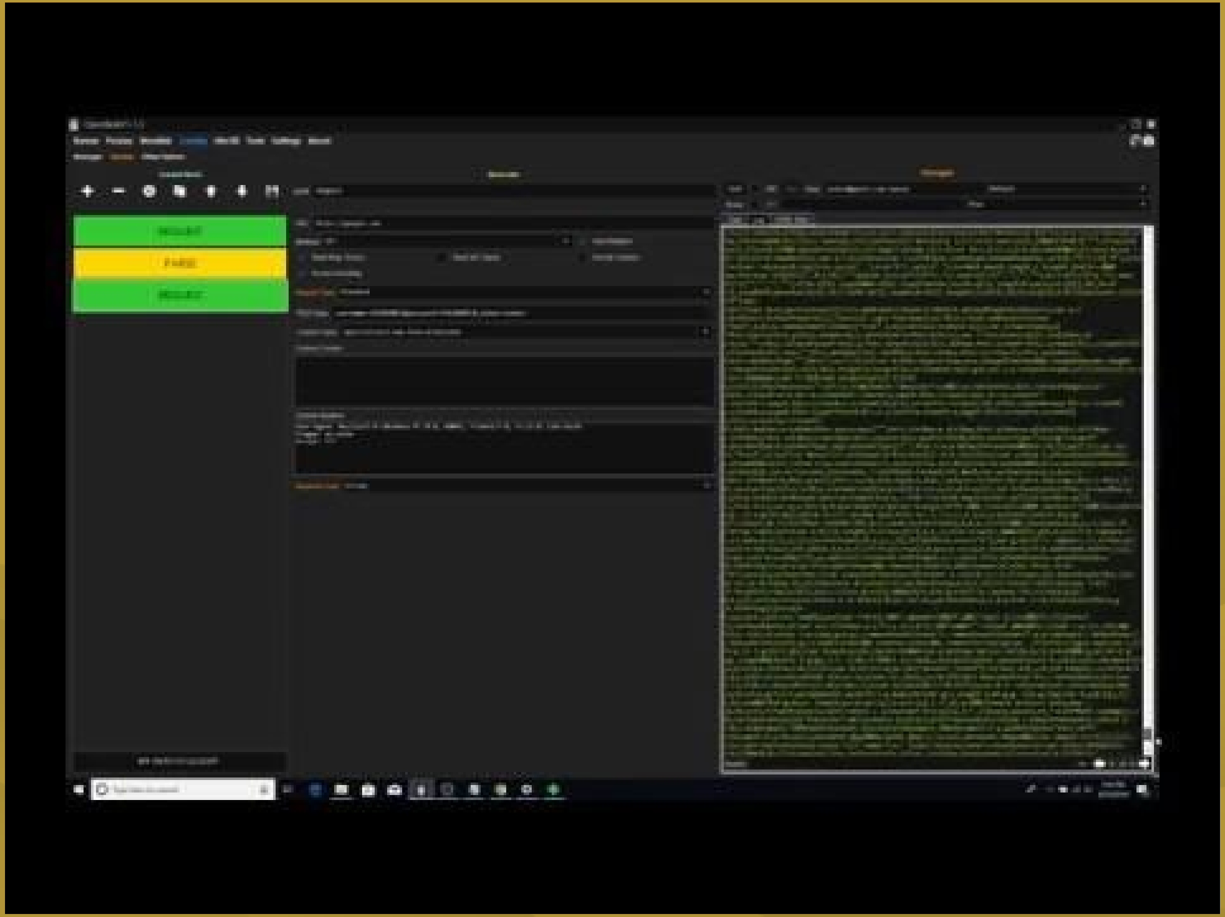
- For credential stuffing a wide variety of tools can be used
  - **SentryMBA**
    - Original program for credential stuffing and the most popular
  - **SNIPR**
    - Costs money
    - Has a public and private repo for configs built in
    - Built in proxy scraper and leecher
  - **OpenBullet**
    - 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

RSAConference2020

Demo



How to fix the problems?

- **Captcha**
  - Captchas make it harder for bots to send automated requests
    - It adds additional steps to perform an attack
    - Forces the attacker to pay for a captcha solving service (ex: 2captcha)
- **Rate Limiting**
  - Prevent bots from sending requests at a faster rate
  - Prevent websites slowing down from 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
- Continue my high school for next three years -- enter a Computer Science program
- Learn more programming languages
- *Looking for short or long term research opportunities - I would love to talk*

Questions?

Thank you!

Contact: tanayemail@gmail.com