Alyssa
MILLER

SANS CYBER CAMP

Next-Level App Hacking

Threat Modeling for Better Attacks

Hacker For Life

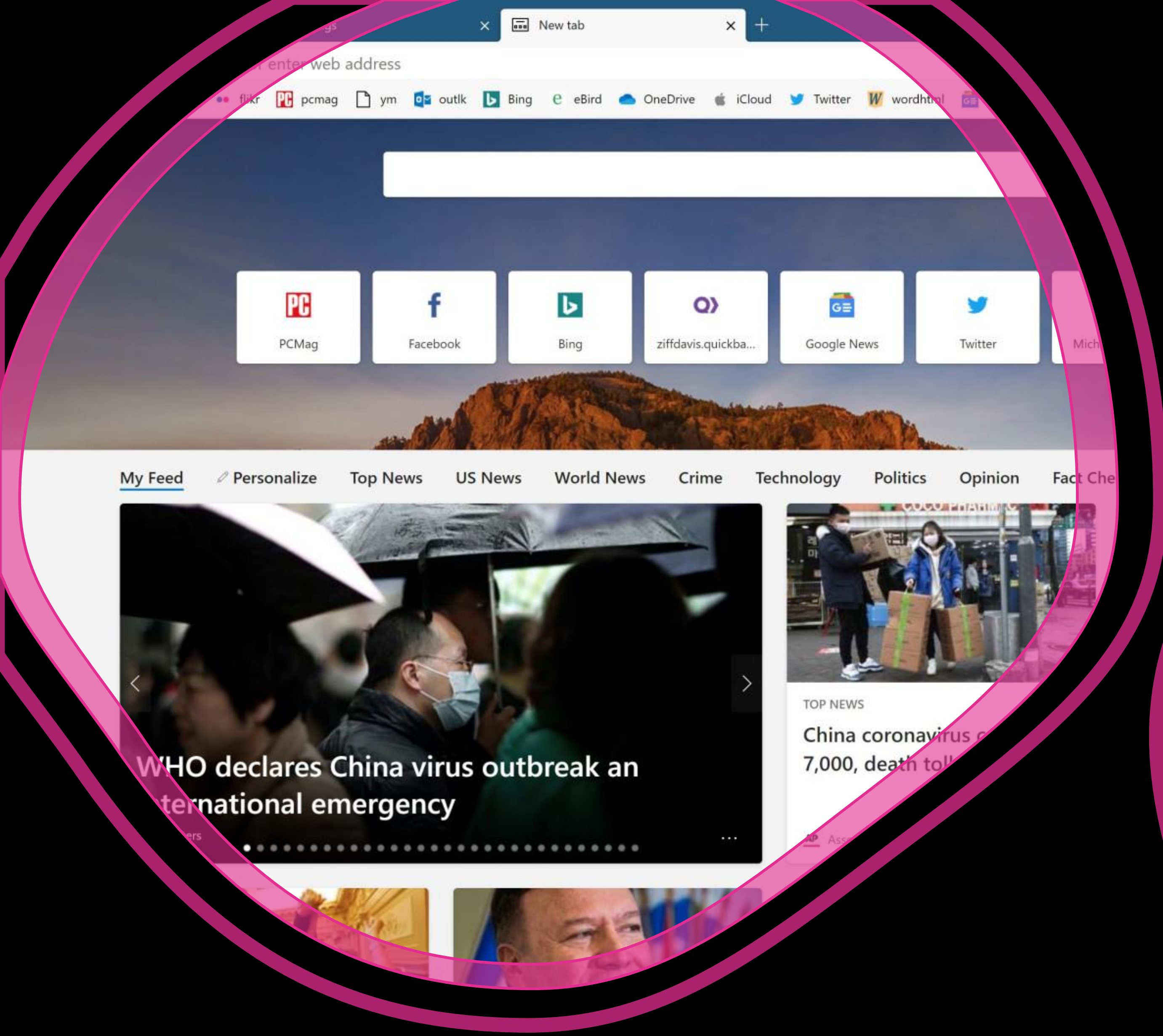
Security Advocate & Speaker

Former Software Developer

Author, Blogger, Podcaster

Threat Modeling ==

WHAT COULD
POSSIBLY GO
WRONG?
quickmeme.com



WHO declares China virus outbreak an
ternational emergency

TOP NEWS

China coronavirus c
7,000, death toll

What’s Important?

Why is it important?

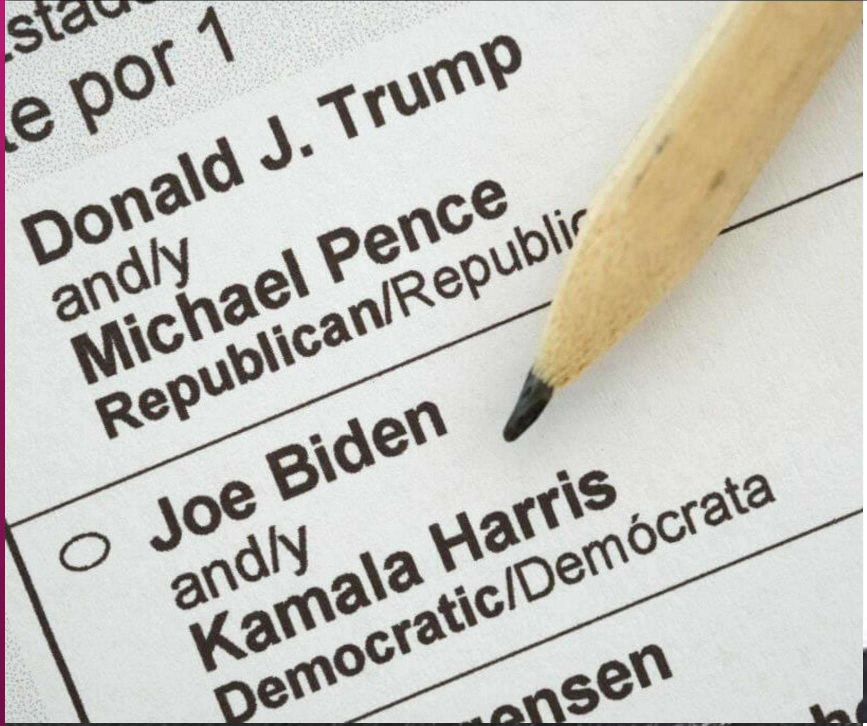
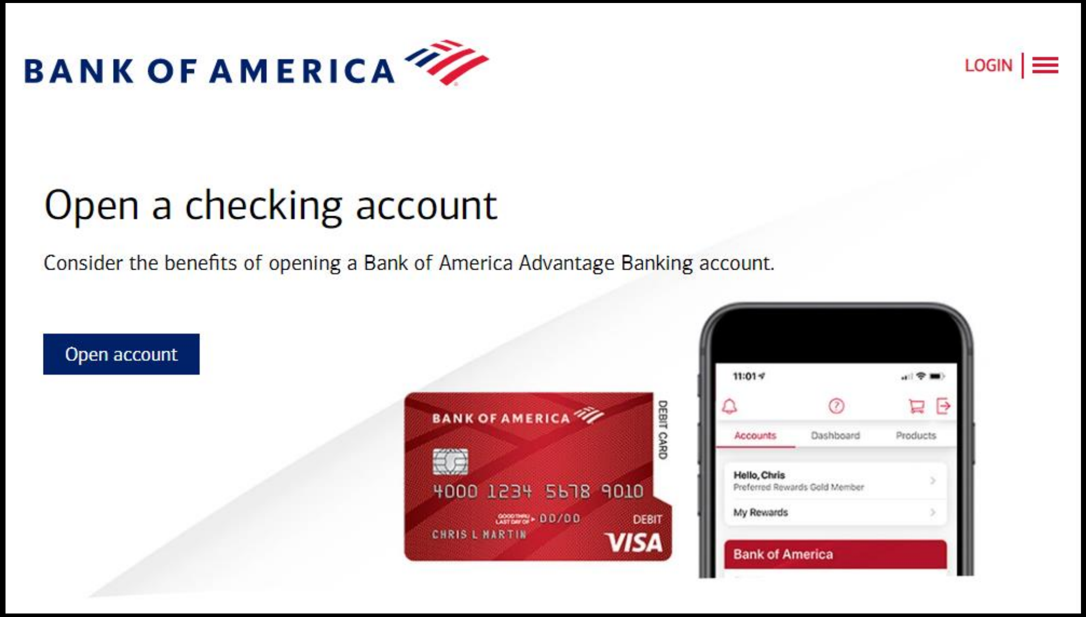


Image: Premium Credit Cards by



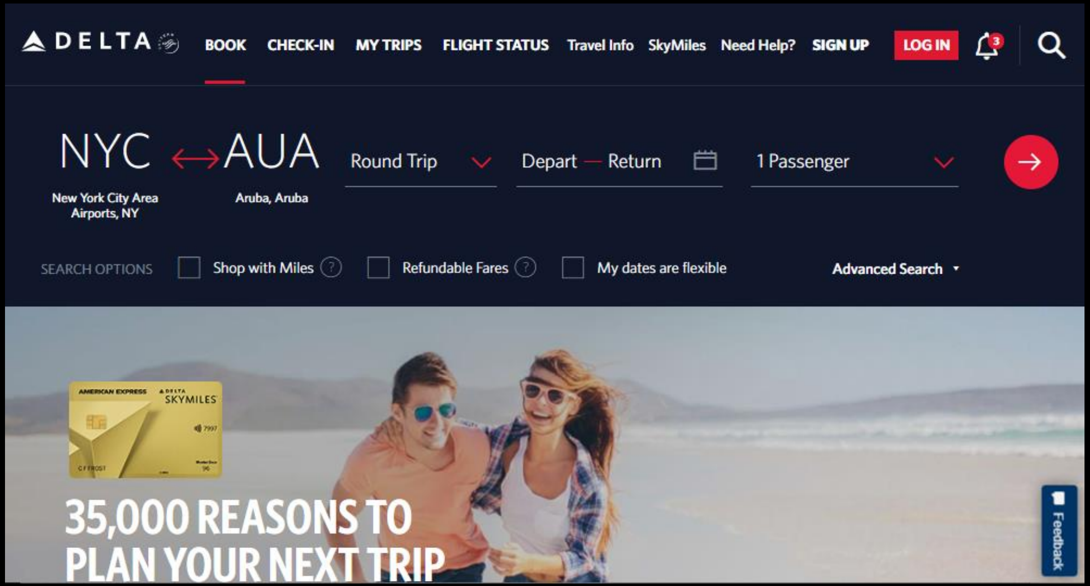
BANK OF AMERICA

LOGIN

Open a checking account

Consider the benefits of opening a Bank of America Advantage Banking account.

Open account



DELTA

BOOK CHECK-IN MY TRIPS FLIGHT STATUS Travel Info SkyMiles Need Help? SIGN UP LOG IN

NYC ⟷ AUA

New York City Area Airports, NY

Aruba, Aruba

Round Trip

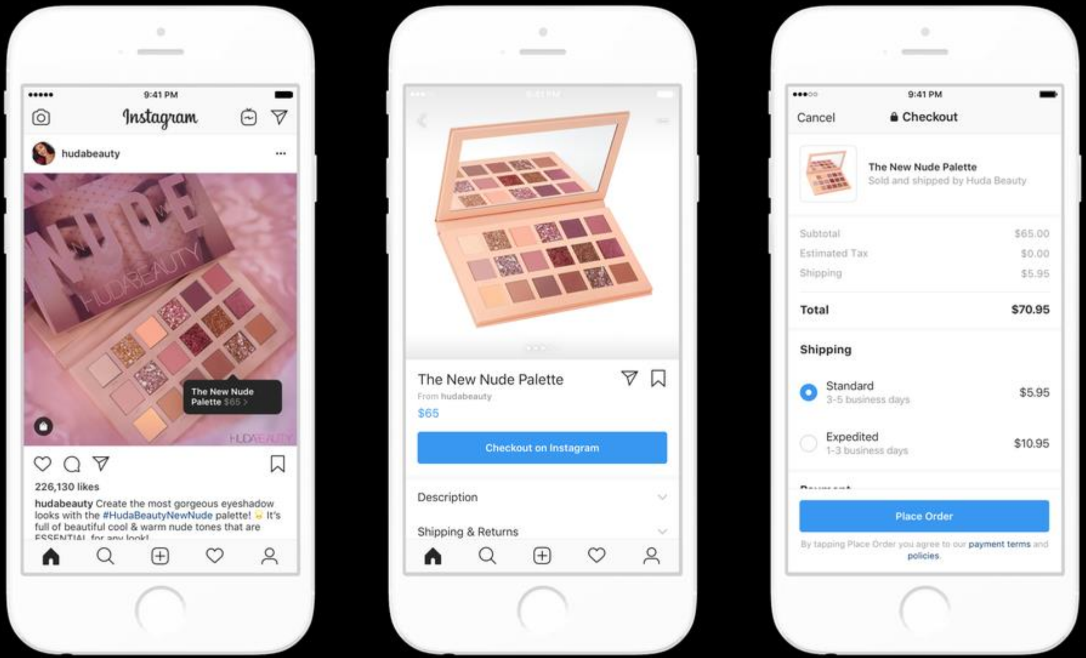
Depart — Return

1 Passenger

SEARCH OPTIONS □ Shop with Miles ? □ Refundable Fares ? □ My dates are flexible

Advanced Search ▾

35,000 REASONS TO PLAN YOUR NEXT TRIP



9:41 PM

Instagram

hudabeauty

The New Nude Palette $65 >

226,130 likes

hudabeauty Create the most gorgeous eyeshadow looks with the #HudaBeautyNewNude palette! 👑 It's full of beautiful cool & warm nude tones that are ESSENTIAL for any look!

The New Nude Palette

From hudabeauty

$65

Checkout on Instagram

Description

Shipping & Returns

9:41 PM

Cancel 🔒 Checkout

The New Nude Palette

Sold and shipped by Huda Beauty

Subtotal	$65.00
Estimated Tax	$0.00
Shipping	$5.95
Total	**$70.95**

Shipping

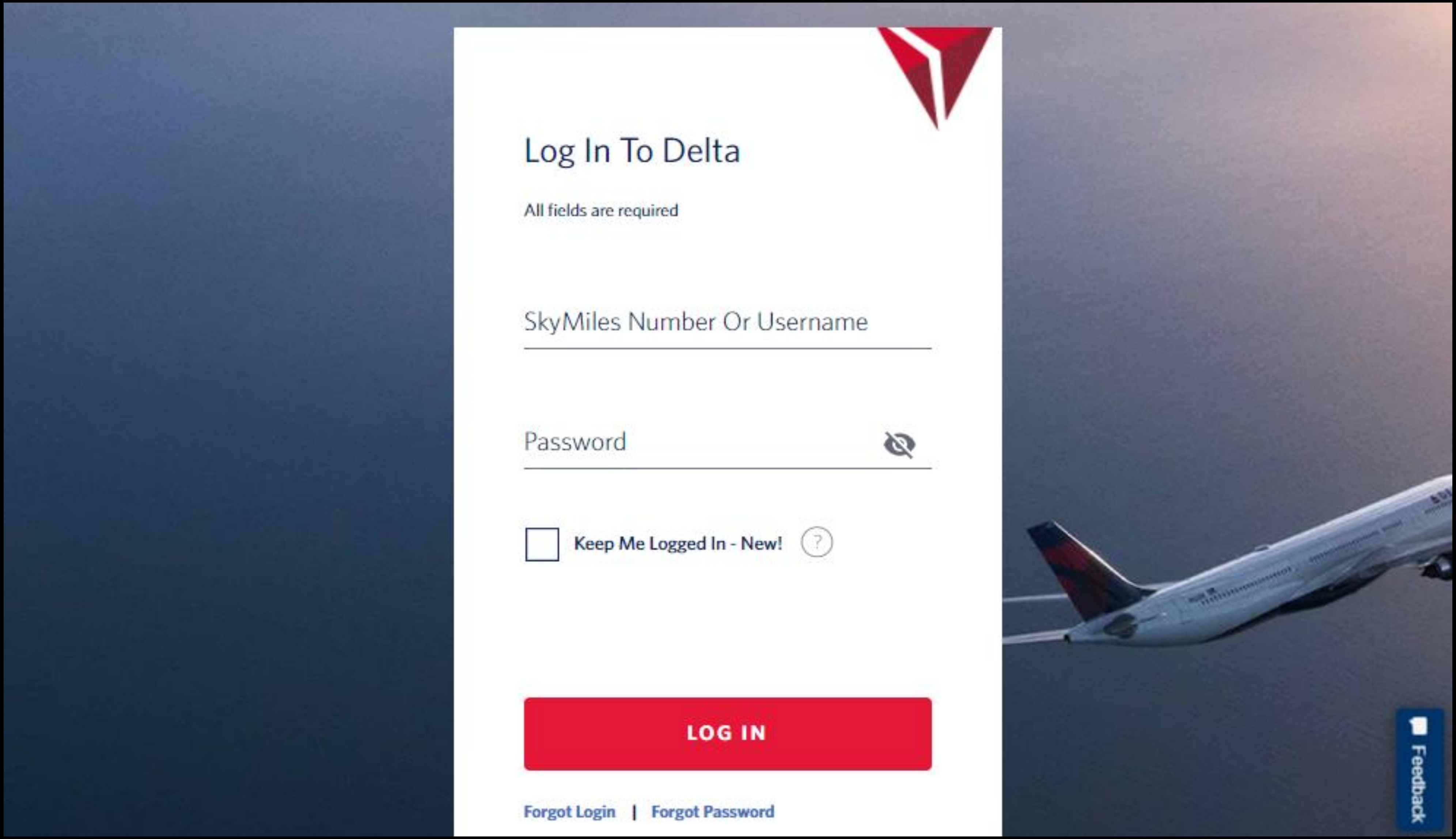
● Standard 3-5 business days $5.95

○ Expedited 1-3 business days $10.95

Payment

Place Order

By tapping Place Order you agree to our payment terms and policies.



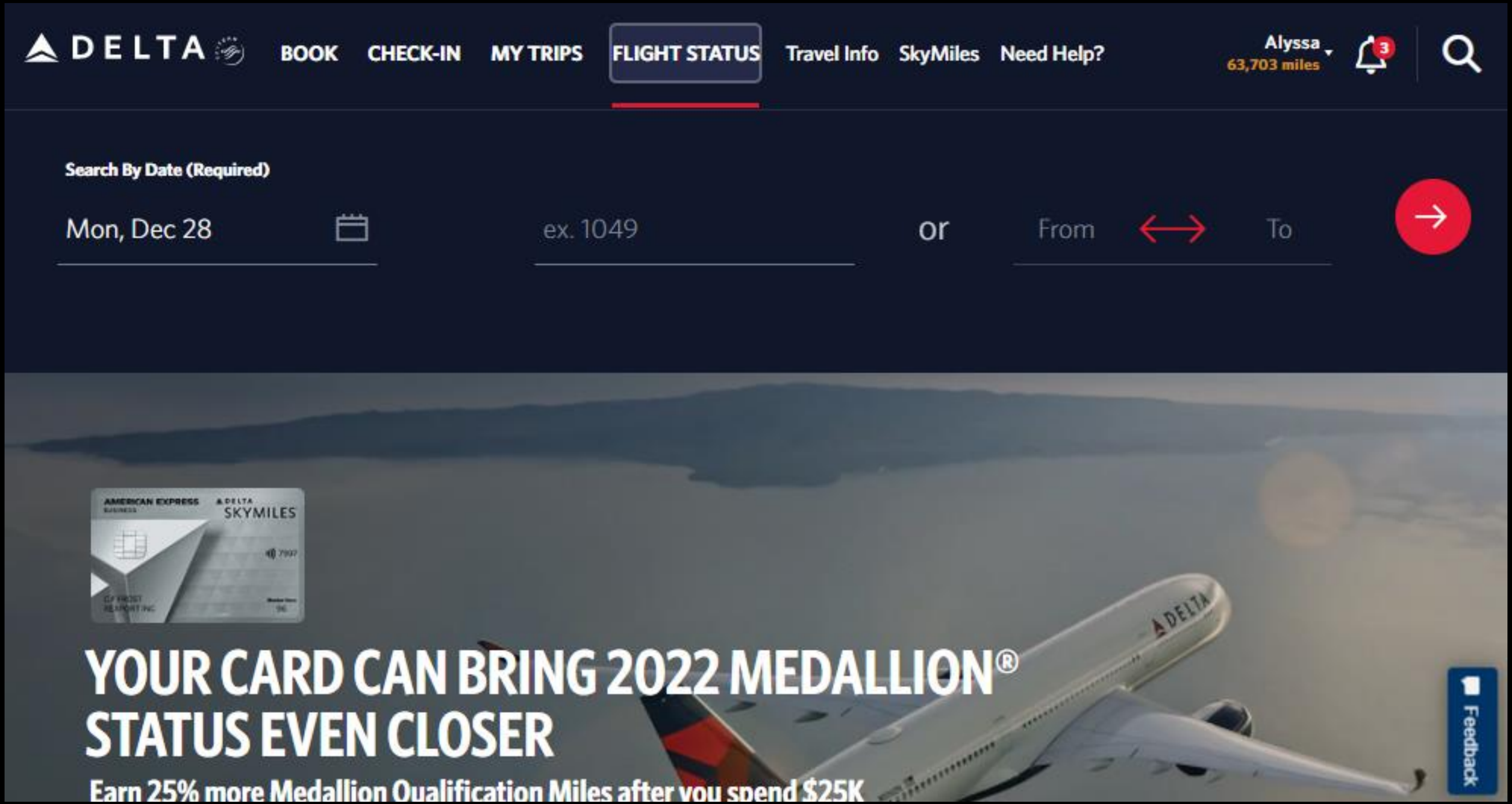
Log In To Delta

All fields are required

SkyMiles Number Or Username

Password

□ Keep Me Logged In - New!

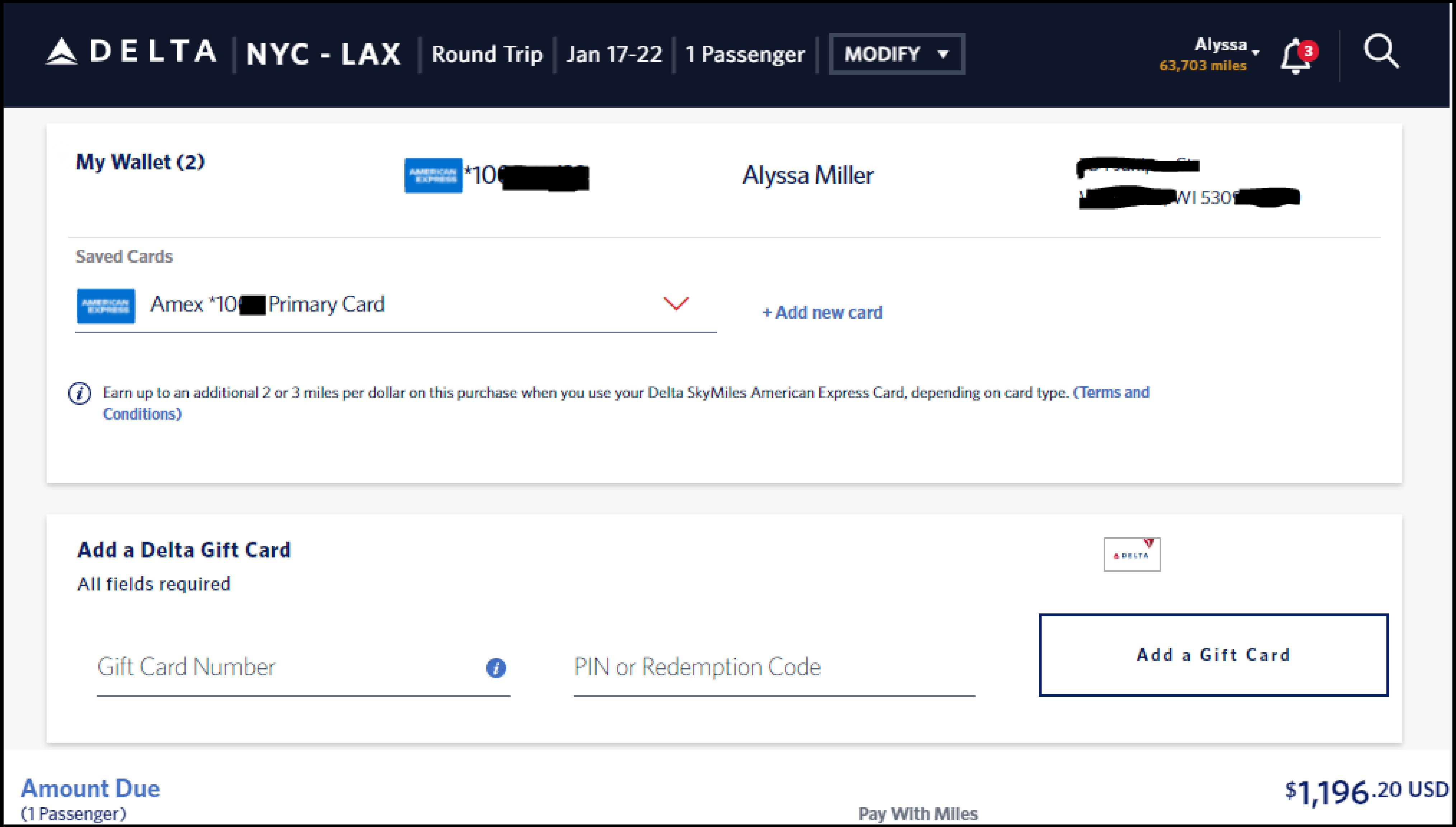


Search By Date (Required)

Mon, Dec 28

YOUR CARD CAN BRING 2022 MEDALLION® STATUS EVEN CLOSER

Earn 25% more Medallion Qualification Miles after you spend $25K



DELTA | NYC - LAX | Round Trip | Jan 17-22 | 1 Passenger | MODIFY ▾

Alyssa ▾
63,703 miles

3

My Wallet (2)

*10[redacted]

Alyssa Miller

[redacted]
[redacted]WI 530[redacted]

Saved Cards

Amex *10[redacted] Primary Card

+ Add new card

Earn up to an additional 2 or 3 miles per dollar on this purchase when you use your Delta SkyMiles American Express Card, depending on card type. (Terms and Conditions)

Add a Delta Gift Card

All fields required

Gift Card Number

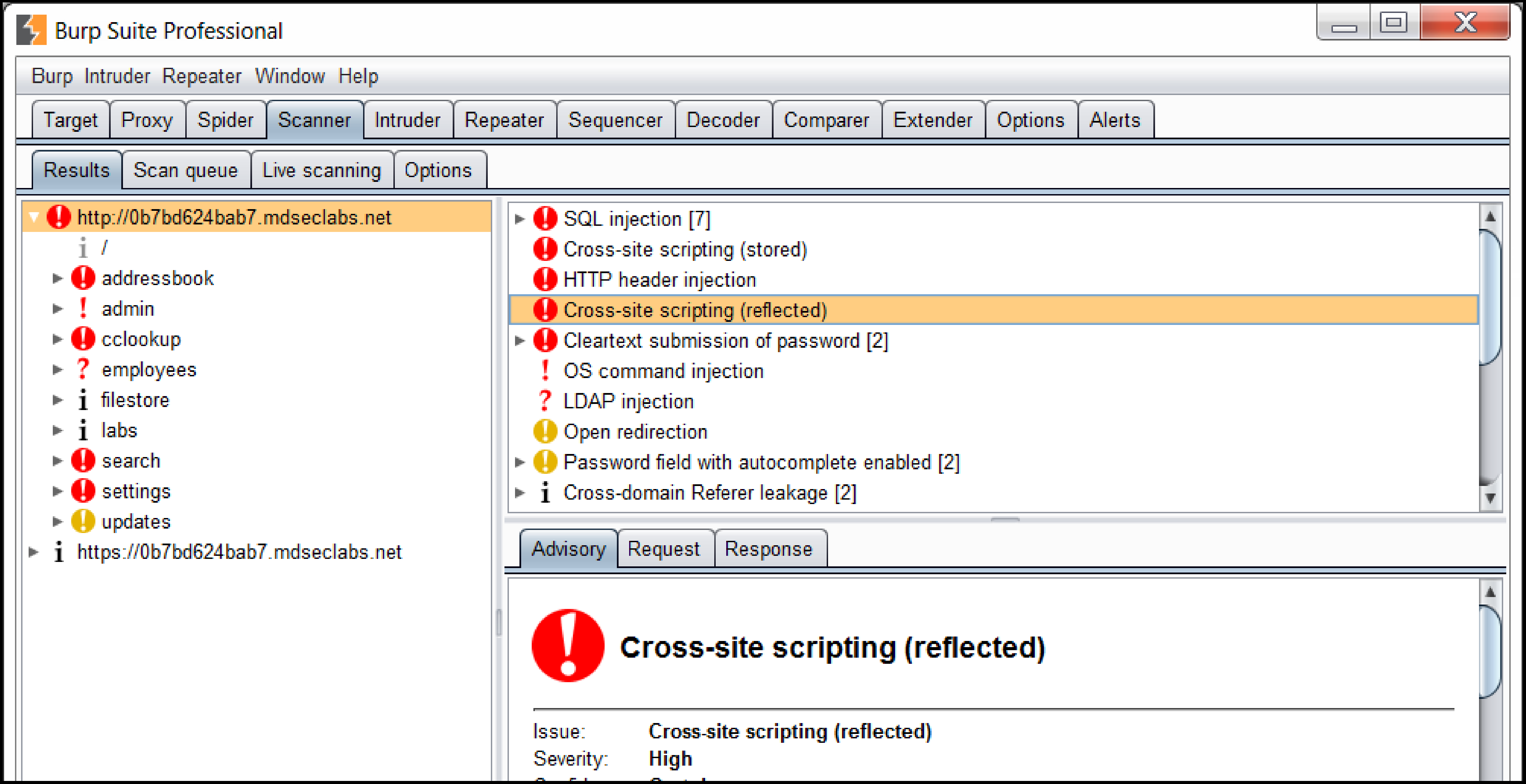
PIN or Redemption Code

Add a Gift Card

Amount Due
(1 Passenger)

Pay With Miles

$1,196.20 USD

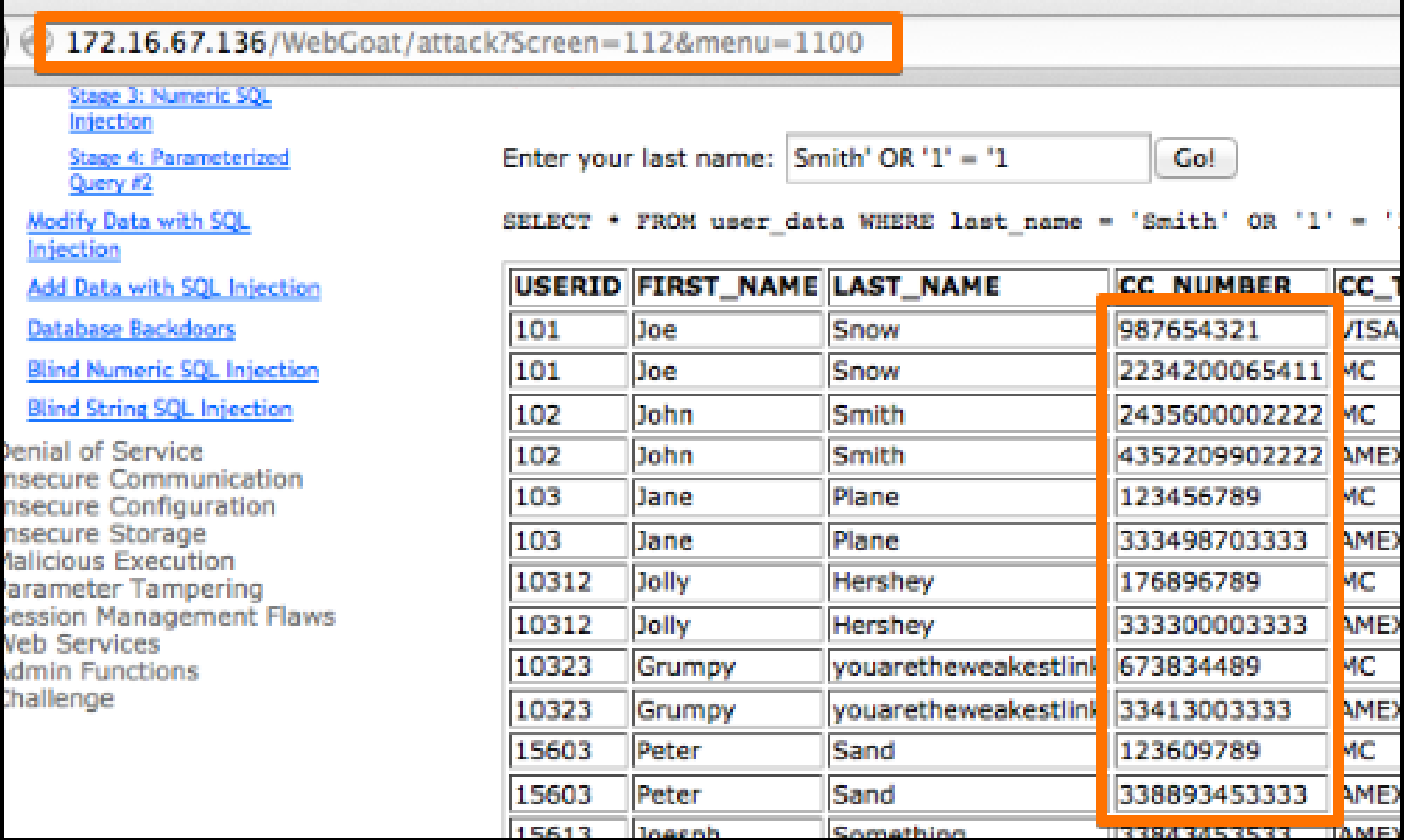

Burp Suite Professional
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Results Scan queue Live scanning Options
Advisory Request Response

- http://0b7bd624bab7.mdseclabs.net
  - /
  - addressbook
  - admin
  - cclookup
  - employees
  - filestore
  - labs
  - search
  - settings
  - updates
- https://0b7bd624bab7.mdseclabs.net

- SQL injection [7]
- Cross-site scripting (stored)
- HTTP header injection
- Cross-site scripting (reflected)
- Cleartext submission of password [2]
- OS command injection
- LDAP injection
- Open redirection
- Password field with autocomplete enabled [2]
- Cross-domain Referer leakage [2]

Cross-site scripting (reflected)

Issue: **Cross-site scripting (reflected)**
Severity: **High**

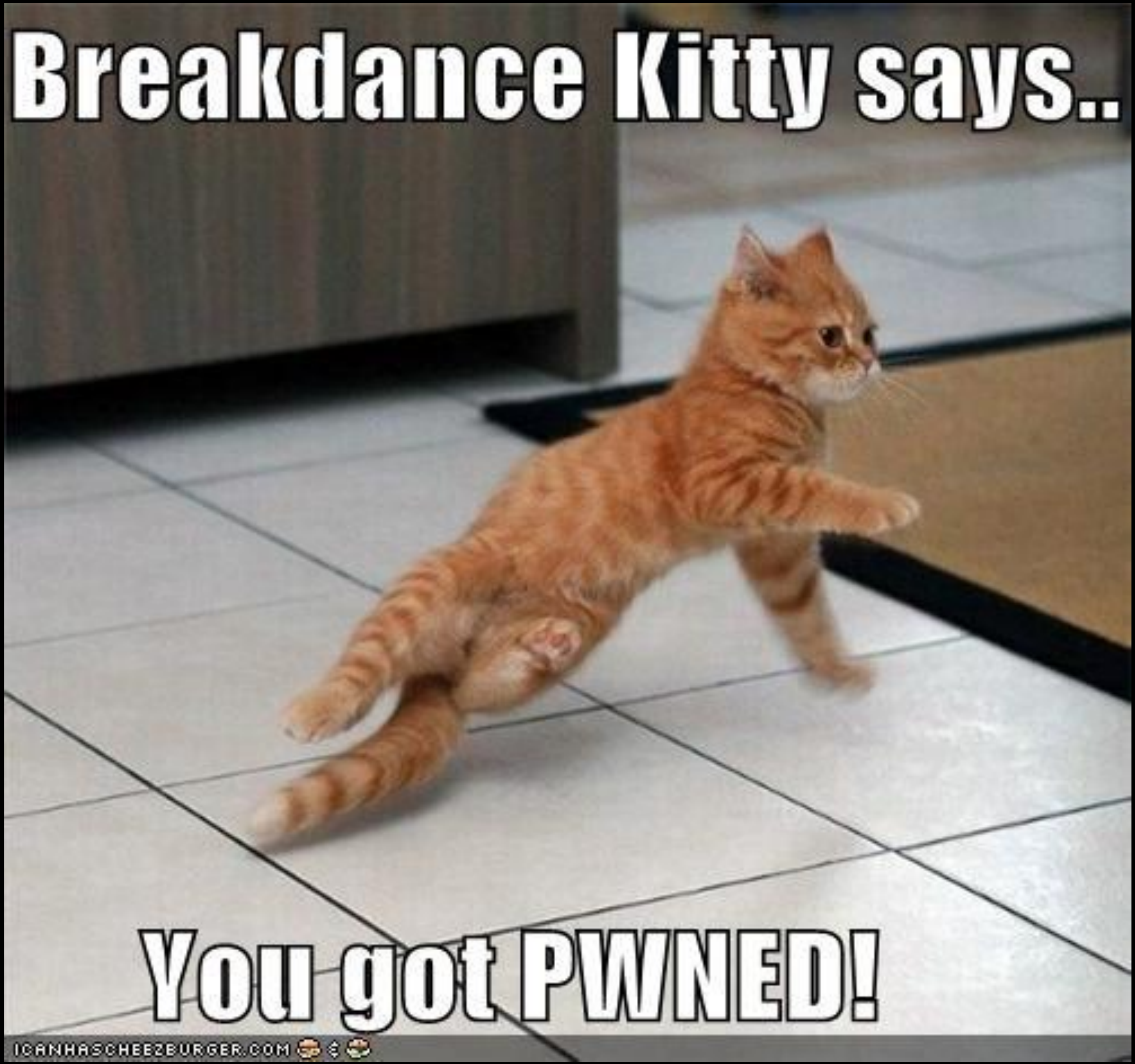


172.16.67.136/WebGoat/attack?Screen=112&menu=1100

Enter your last name: Smith' OR '1' = '1

```
SELECT * FROM user_data WHERE last_name = 'Smith' OR '1' = '
```

USERID	FIRST_NAME	LAST_NAME	CC_NUMBER	CC_T
101	Joe	Snow	987654321	VISA
101	Joe	Snow	2234200065411	MC
102	John	Smith	2435600002222	MC
102	John	Smith	4352209902222	AME
103	Jane	Plane	123456789	MC
103	Jane	Plane	333498703333	AME
10312	Jolly	Hershey	176896789	MC
10312	Jolly	Hershey	333300003333	AME
10323	Grumpy	youaretheweakestlink	673834489	MC
10323	Grumpy	youaretheweakestlink	33413003333	AME
15603	Peter	Sand	123609789	MC
15603	Peter	Sand	338893453333	AME
15613	Joseph	Something	33843453533	AME


Breakdance Kitty says..
You got PWNED!
ICANHASCHEEZBURGER.COM

@AlyssaM_Infosec

/in/alyssam-infosec

https://alyssasec.com

Thank You

Alyssa
MILLER