Mason Competitive Cyber

AWS That Isn’t Just EC2

News since last meeting

- UMDCTFers
  - High schoolers are good, man
- CYSE IAB

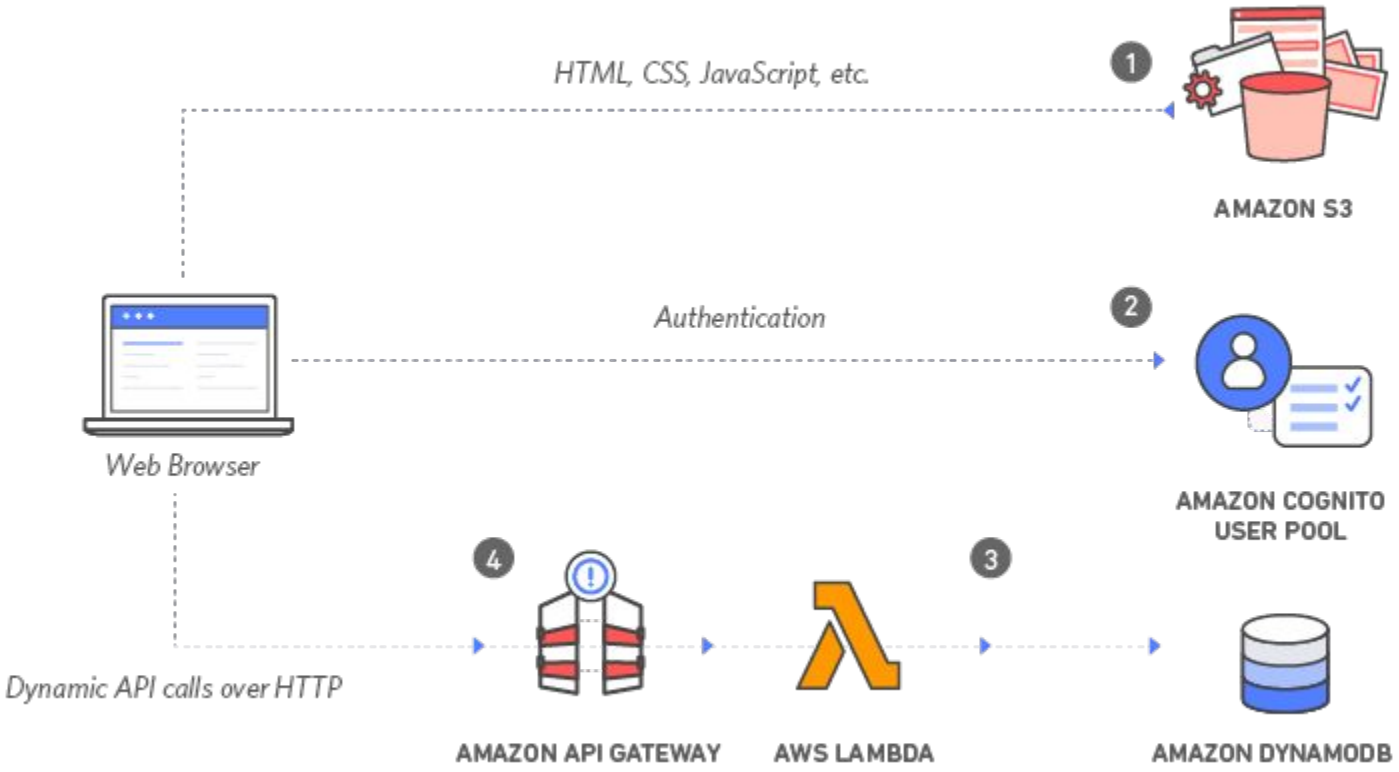
Disclaimer

- This is far from our first AWS talk
- I am far from perfect/infallible in this content

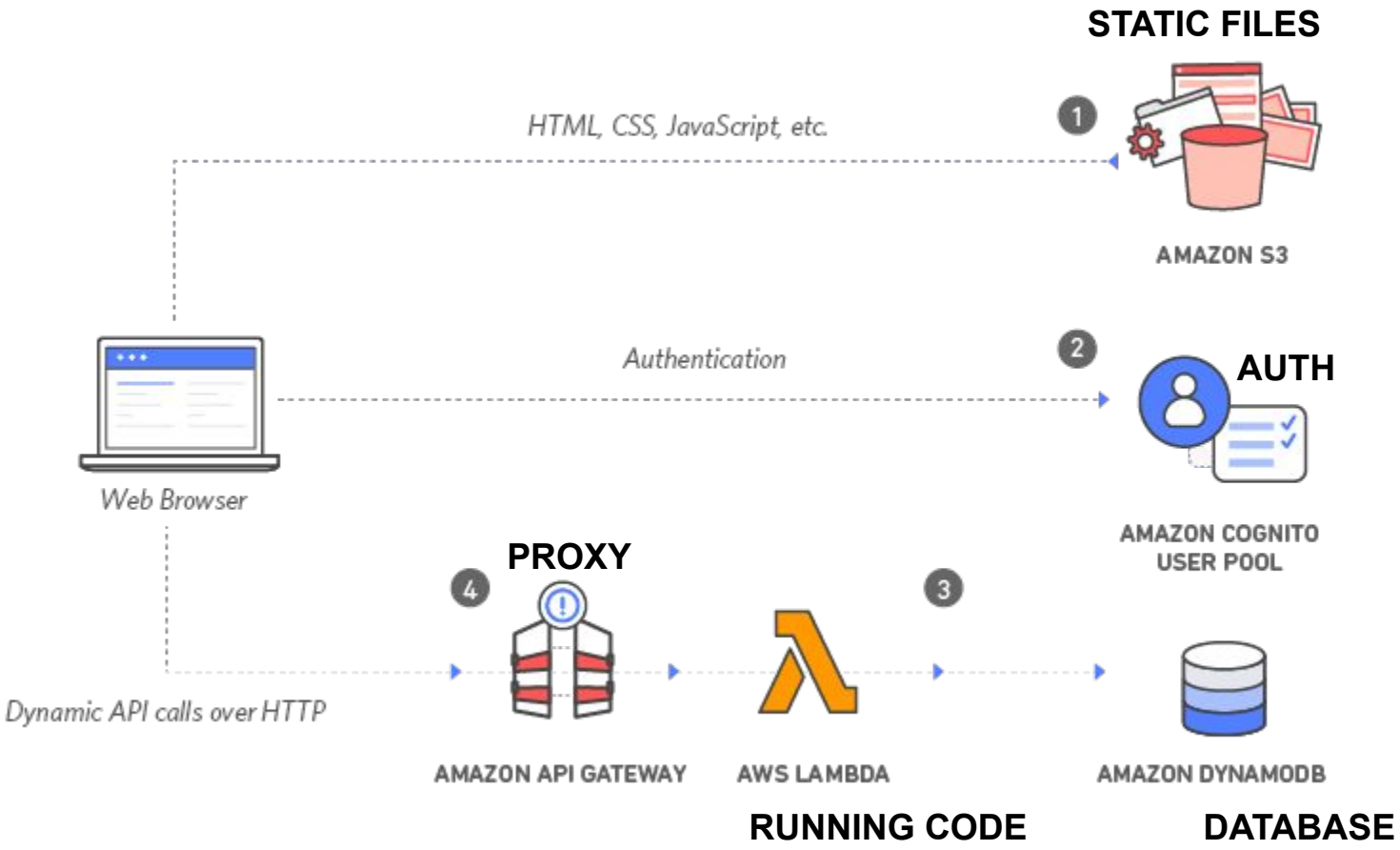
AWS Primer

- Owns at least 30% of the cloud market
  - Easily programmable cloud infrastructure
  - Offers like 100+ services to do a variety of tasks
    - S3, EC2 most common
- Traditionally known as expensive, reliable
- CloudGoat can make you a playground
  - DVWA for AWS (also aws.flaws if you're a poor)
- Tries to ship secure by default
  - Doesn't always achieve that

Example of non-noob application



So what are we looking at...



First a primer on IAM…

- Root account vs IAM Account
  - If you have an account today it's likely root
  - Mason CC runs on a root account (whoops)
- Conventional Login
  - Username, password, optional 2FA
- Roles
  - "Temporary Security Credentials"
  - Auto-rotating, auto-scoped keys that grant AWS access to AWS
- Keys
  - API keys, used for pretty much all tools
    - AWS doesn't do oauth-y stuff
  - Secret and key
  - Prone to leakage, accidental disclosure, looting

What do roles look like?

- In EC2, metadata service
  - 169.254.169.254
- In Lambda and elsewhere, env vars
  - AWS_REGION, AWS_ACCESS_KEY_ID, etc
- ASIA* keys vs AKIA* keys
- Harder to extract than to run within context
  - I’ve had little/no luck

Keys

- Stored in ~/.aws/credentials
  - non-sensitive in ~/.aws/config
  - includes Windows' ~
- AKIA…..
  - There may be alternate formats I'm not aware of
- AWSCLI can do essentially all you need

What does looting AWS earn you?

- Sensitive data you'd expect to see anywhere
- **Look for roles**
  - I've personally had zero success pulling directly and re-applying
  - Dump keys and you'll at least know
    - Nimbostratus

Other Service Considerations

- DocumentDB
  - AWS's MongoDB
  - MongoDB tends to be deployed poorly, in AWS it's Salted Challenge Response Authentication Mechanism (SCRAM, mutual auth)
- RDS
  - Loot the underlying instance, loot the database
    - Can ask RDS to reset RDS's passwords

APIs, SDKs

- 

Common Ones

- Don’t hand-craft API requests, please
- boto3 - python
- Rest are essentially *AWS SDK for* _____
- Follow similar themes: Resource or Client
  - I like Client SDKs
  - Pseudo-code:
    - Establish client: client = boto3.client(‘s3’)
      - May include authentication, unless a role is in play
    - Use that client: buckets = client.list_buckets()

- AWS rolls a shitload of their own object types

Walking through TCTF

walkthrough

Proud Sponsors

Thank you to these organizations who give us their support:

BATTELLE

CYSE

It can be done™

CRYPSIS™