

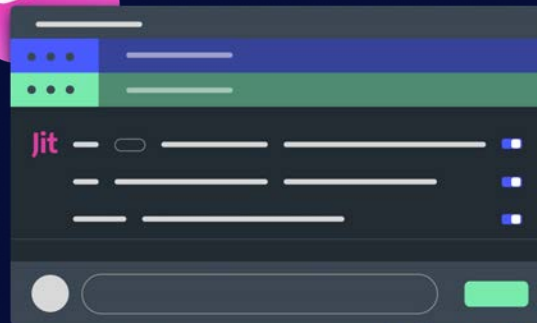


Kick Your Security Up a Notch

with Custom Queries

Gabriel L. Manor @ Conf42 DevSecOps


October 2022



{ }

</>

↑↑↑

 @gemanor



**CALLING ALL
~~SUPERHEROES!~~
DEVOPS**



Automate EVERYTHING!

Automate EVERYTHING!



3

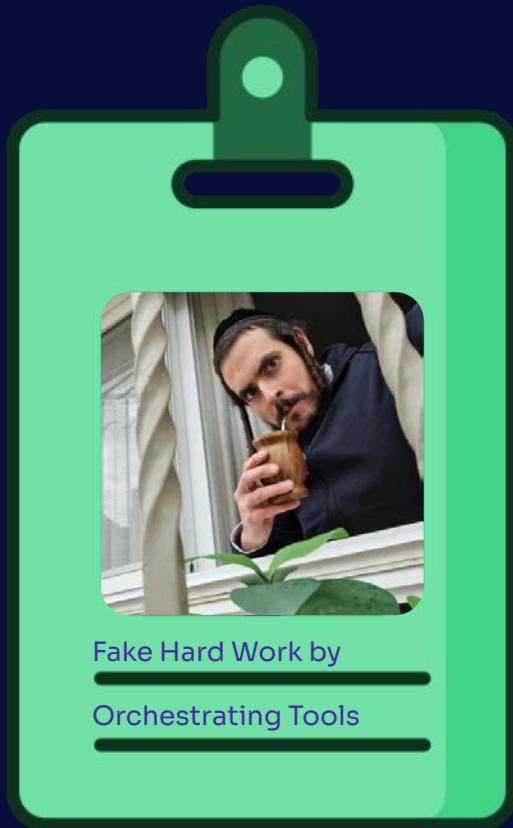
▶ Orchestrate Infrastructure and Operations

2

▶ Infrastructure as Code

1

▶ Automate Operations with Scripts



Gabriel Liechtman Manor

Tech Lead, DevSecOps


> 10y Fullstack Developer



@gemanor



<https://www.linkedin.com/in/gmanor>

 @gemanor



LAVANDERÍA BRILLANTE
INDUSTRIAL · UNIFORMES





By enabling Infrastructure as Code, you get complete **control** of the **continuous operation process**. Those documented **protocols** help you never make the same mistake twice.

Gustavo `Gus` Fring

Everything as Code



madrigal-electromotive / gus-playground Private


Unwatch 4 Fork 0 Star 0

Code Issues Pull requests 9 Actions Projects Wiki Security Insights

main 18 branches 0 tags

Go to file Add file Code

GustavoF Merge pull request #39 from jitsecurity-controls/Fix-jq-for-mfa-de... a0bd934 16 days ago 172 commits



About

Man as Corporation

- Readme
- 0 stars
- 4 watching
- 0 forks

Releases

No releases published
[Create a new release](#)

Packages

No packages published
[Publish your first package](#)



BETTER
CALL
Saul



guest.tf A ×

guest.tf

```
1 resource "azurerm_role_definition" "example" {
2     name          = "my-custom-role"
3     scope         = data.azurem_subscription.primary.id
4     description   = "This is a custom role created via Terraform"
5
6     permissions {
7         actions     = []
8         not_actions = ["*"]
9     }
10
11     assignable_scopes = [
12         data.azurem_subscription.primary.id,
13     ]
14 }
15
16 resource "azurerm_role_assignment" "example" {
17     name                = "00000000-0000-0000-0000-000000000000"
18     scope               = data.azurem_subscription.primary.id
19     role_definition_name = "Guest"
20     role_definition_id  = azurerm_role_definition.example.role_definition_resource_id
21     principal_id       = data.azurem_client_config.example.object_id
22 }
```





Search or jump to...

Pull requests Issues Marketplace Explore

Checkmarx / kics Public

<> Code Issues 76 Pull requests 16 Discussions Actions Projects 2 Security Insights

master 24 branches 63 tags

Go to file

Add file

Code



cxMiguelSilva fix(masked_secrets): Mask Secrets in All Vulnerability Prev... a52e458 13 hours ago 4,579 commits

.github	ci(deps): bump docker/login-action from 2.0.0 to 2.1.0 (#5926)	7 days ago
assets	Merge pull request #5951 from Checkmarx/fix_query_5859	yesterday
cmd	fix(memory consumption): improved SplitLines function calls (#5680)	2 months ago
docker	Merge branch 'feature/kicsbot-update-docs-index'	8 days ago
docs	docs(kicsbot): update images digest (#5935)	3 days ago
e2e	fix(masked_secrets): Mask Secrets in All Vulnerability Preview (#594...	13 hours ago
examples	chore(gitlab-ci): add --ci flag to gitlab examples (#5682)	29 days ago
internal	code coverage improvements (#5744)	23 days ago
lib	feat: support filter pattern expressions for CIS benchmark regarding ...	13 months ago
pkg	fix(masked_secrets): Mask Secrets in All Vulnerability Preview (#594...	13 hours ago



> 1600 Security and Misconfiguration Tests!



Ansible

Azure Resource Manager

CloudFormation

Dockerfile

Docker Compose

Kubernetes

OpenAPI

Google Deployment Manager

gRPC

Terraform


KICS.



Privilege Escalation Allowed, Severity: HIGH, Results: 5

Description: Containers should not run with allowPrivilegeEscalation in order to prevent them from gaining more privileges than their parent process

Platform: Kubernetes

[1]: ../../code/positive2.yaml:17

```
016:         image: nginx
017:         securityContext:
018:           capabilities:
```

[2]: ../../code/positive1.yaml:21

```
020:         image: images.my-company.example/log-aggregator:v6
021:         securityContext:
022:           runAsUser: 2000
```



Most Found Misconfiguration Issues



According to Jit Metrics

1. No Global And Operation Security Defined (v2)
2. EC2 Instance Has Public IP
3. Azure Instance Using Basic Authentication
4. Privilege Escalation Allowed
5. Storage Account Allows Insecure Transfer
6. Missing User Instruction
7. NET_RAW Capabilities Not Being Dropped
8. S3 Bucket Without Enabled MFA Delete
9. S3 Bucket SSE Disabled
10. Array Without Maximum Number of Items (v2)



Image source: <https://www.openpolicyagent.org/>



```
1 package play
2
3 import future.keywords.if
4
5 default hello := false
6
7 hello if input.message == "world"
```

KICS Query Building Blocks



[query.rego](#)

The actual query policy



[metadata.json](#)

Query metadata and
configuration

The Regalo Trucks Check



```
specInfo := k8sLib.getSpecInfo(document)
container := specInfo.spec[types[x]][c]

containerCtx := object.get(container, "securityContext", {})
not common_lib.valid_key(containerCtx, "allowPrivilegeEscalation")
startswith(container.name, "regalo_")
```

Custom Query Mounting



```
> docker run -t \  
-v $CUSTOM_QUERY_LOCATION:/app/bin/assets/queries/k8s/privilege_escalation_allowed \  
-v $(pwd)/test:\code \  
checkmarx/kics scan -p /code -o /code/jit-report -f json \  
--exclude-severities INFO,MEDIUM,LOW --disable-secrets
```

```
.0MO.  
OMMMx  
;NMX;  
...  
WMMMd      cWMMMO.  KMMMO      ;xKWMMMMNOc.      ,xXMMMMMWXkc.  
WMMMd      .0MMMN:  KMMMO      :XMMMMMMMMMMMMWl  xMMMMMWMMMMMMl  
WMMMd      lWMMMO.  KMMMO      xMMMMKc... 'lXmk  ,MMMMx      ;dXx  
WMMMd      .0MMMX;  KMMMO      cMMMMd      'MMMMNl'  
WMMMMNWMMMMl  KMMMO      0MMMN      oMMMMMMMMXkl.  
WMMMMMMMMMMMO  KMMMO      0MMMX      .ckKWMMMMMM0.  
WMMMMWokMMMMk  KMMMO      oMMMMc      .      :OMMMO  
WMMMK.      dMMMM0.  KMMMO      KMMMMx'      ,kNc      :W0c.      .NMMMX  
WMMMd      cWMMMX.  KMMMO      kMMMMMWXNMMMMMd .wMMMMWKO0NMMMMl  
WMMMd      ,NMMMN,  KMMMO      'xNMMMMMMMNx,  .l0WMMMMMMMMwk,  
xkkk:      ,kkkkx  okkk      ;xKXKx;      ;d0KKkc
```



DON'T



Before designing a query we should think of **every single configuration** that could be **harmful**. Same as we do with **Unit Tests**.

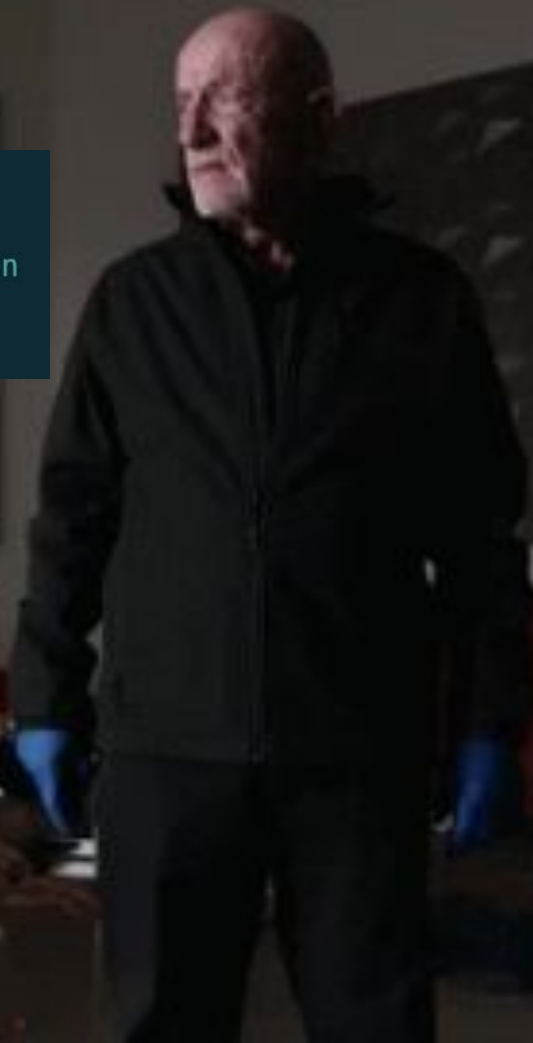
```
headers:
```

```
  ehrmentraut-inspection:
```

```
    description: Mike's request validation token
```

```
    schema:
```

```
      type: string
```





EXPLORER

- ✓ KICS
 - assets
 - libraries
 - queries
 - template / query.
 - test
 - negative.tf
 - positive_expected_result.json
 - positive.tf
 - metadata.json
 - query.rego

Positive and Negative Cases



```
! positive.yaml U x
assets > queries > openAPI > mike_header > test > ! positive.yaml
1  #this is a problematic code where the query should report a resu
2  info:
3    title: Simple API overview
4    version: 1.0.0
5  paths:
6    "/":
7      get:
8        operationId: listVersionsv2
9        summary: List API versions
10       responses:
11         "50":
12           description: Server error response
13           content:
14             application/json:
15               examples:
16                 foo:
17                   value:
18                     versions:
19                       - status: CURRENT
20                         updated: "2011-01-21T11:33:21Z"
21                         id: v2.0
22                         links:
23                           - href: http://127.0.0.1:8774/v2/
24                             rel: self
25         "6xx":

! negative.yaml U x
assets > queries > openAPI > mike_header > test > ! negative.yaml
1  openapi: 3.0.0
2  info:
3    title: Simple API overview
4    version: 1.0.0
5  paths:
6    "/":
7      get:
8        operationId: listVersionsv2
9        summary: List API versions
10       parameters:
11         - in: header
12           name: ehrmentratut-inspection
13           schema:
14             type: string
15             format: uuid
16             required: true
17       responses:
18         "50":
19           description: Server error response
20           content:
21             application/json:
22               examples:
23                 foo:
24                   value:
25                     versions:
```



`{}` metadata.json U X



assets > queries > openAPI > mike_header > `{}` metadata.json > ...

```
1  {
2    "id": "f969e51a-e3f0-4da5-902f-6e4bc0abcf0",
3    "queryName": "API Endpoint Without Mike Header",
4    "severity": "HIGH",
5    "category": "Access Control",
6    "descriptionText": "Every API key must have declared Mike's header on it.",
7    "descriptionID": "f969e51a",
8    "platform": "OpenAPI"
9  }
```

KICS Supported Libraries



github.com/Checkmarx/kics/tree/master/assets/libraries

Checkmarx / kics Public


Code Issues 76 Pull requests 16 Discussions Actions Projects 2 Security Insights

master - kics / assets / libraries /

Kicsbot and gabriel-cx bump: updating software versions to new release (#5918) 4c2856 3 days ago History

..		
ansible.rego	fix(cli): fixing bug related to flag -q + adding new cli flag related...	14 months ago
azureresource manager.rego	fix(query): fixed 59cb3da7-f206-4ae6-b827-7abf0a9cab9d and 2ade1579-...	12 months ago
buildah.rego	feat(buildah): added support to Buildah (#4740)	9 months ago
cloudformation.rego	Merge branch 'master' into release/1.6	last month
common.json	bump: updating software versions to new release (#5918)	3 days ago
common.rego	Merge branch 'master' into release/1.6	last month
crossplane.rego	queries(pulumi): add pulumi gcp security queries (#5654)	3 months ago
dockercompose.rego	feat(analyzer): Docker Compose support (#4851)	7 months ago
dockerfile.rego	update(query): Apt Get Install Pin Version Not Defined (#5176)	6 months ago
googledeploymentmanager.rego	feat(parser): added google deployment manager to platforms (#4530)	10 months ago
grpc.rego	feat(grpc): added support to gRPC (#4532)	10 months ago
k8s.rego	Correct k8s Query	last month
knative.rego	feat(knative): add knative security query and k8's pod queries intero...	2 months ago
openapi.rego	fixed function check_schemes of openapi lib (#5433)	5 months ago
pulumi.rego	queries(pulumi): add pulumi gcp security queries (#5654)	3 months ago
serverlessfw.rego	merge	2 months ago
terraform.rego	fix lambda_function_with_privileged_role (#5833)	23 days ago

<https://github.com/Checkmarx/kics/tree/master/assets/libraries>

 @gemanor

```
go run ./cmd/console/main.go scan -p "pathToTestData" -d "pathToGenerateJson"
```

So for example, if we wanted to transform a .tf file in ./code/test we could type:

```
go run ./cmd/console/main.go scan -p "./src/test" -d "src/test/input.json"
```

Example of input.json

```
{
  "document": [
    {
      "resource": {
        "aws_cloudtrail": {
          "positive1": {
            "name": "npositive_1",
            "s3_bucket_name": "bucketlog_1"
          }
        }
      },
      "id": "02926636-f2c1-46c3-93cc-c7dc2a79791f",
      "file": "/assets/queries/terraform/aws/cloudtrail_multi_region_disabled"
    },
    {
      "resource": {
        "aws_cloudtrail": {
          "positive2": {
            "name": "npositive_2",
            "s3_bucket_name": "bucketlog_2",
            "is_multi_region_trail": false
          }
        }
      },
      "id": "4b27da84-4d38-4422-b2b5-fa85029dad2a",
      "file": "assets/queries/terraform/aws/cloudtrail_multi_region_disabled"
    }
  ]
}
```



≡ query.rego U ×

assets > queries > openAPI > 3.0 > mike_header > ≡ query.rego

```
1  package Cx
2  import data.generic.common as common_lib
3  import data.generic.openapi as openapi_lib
4
5  CxPolicy[result] {
6      doc := input.document[i]
7      openapi_lib.check_openapi(doc) == "3.0"
8      paths := doc.paths[name]
9      not common_lib.valid_key(paths, "parameters")
10
11     result := {
12         "documentId": input.document[i].id,
13         "searchKey": sprintf("paths.%s.parameters", [name])
14         "issueType": "MissingAttribute",
15         "keyExpectedValue": "mike's header",
16         "keyActualValue": "no parameters",
17     }
18 }
```



 Dockerfile M ×

 Dockerfile > ...

You, now | 1 author (You)

```
1 FROM checkmarx/kics:latest
2
3 COPY assets /app/bin/assets
4
5 ENTRYPOINT [ "scan", "-p" ]
6
```

Gus Protocol for Happy Life



✓ Exclude

✓ Customize

✓ Create



Thank You!

Let keep in touch!



@gemanor




@gemanor



<https://www.linkedin.com/in/gmanor>



 @gemanor