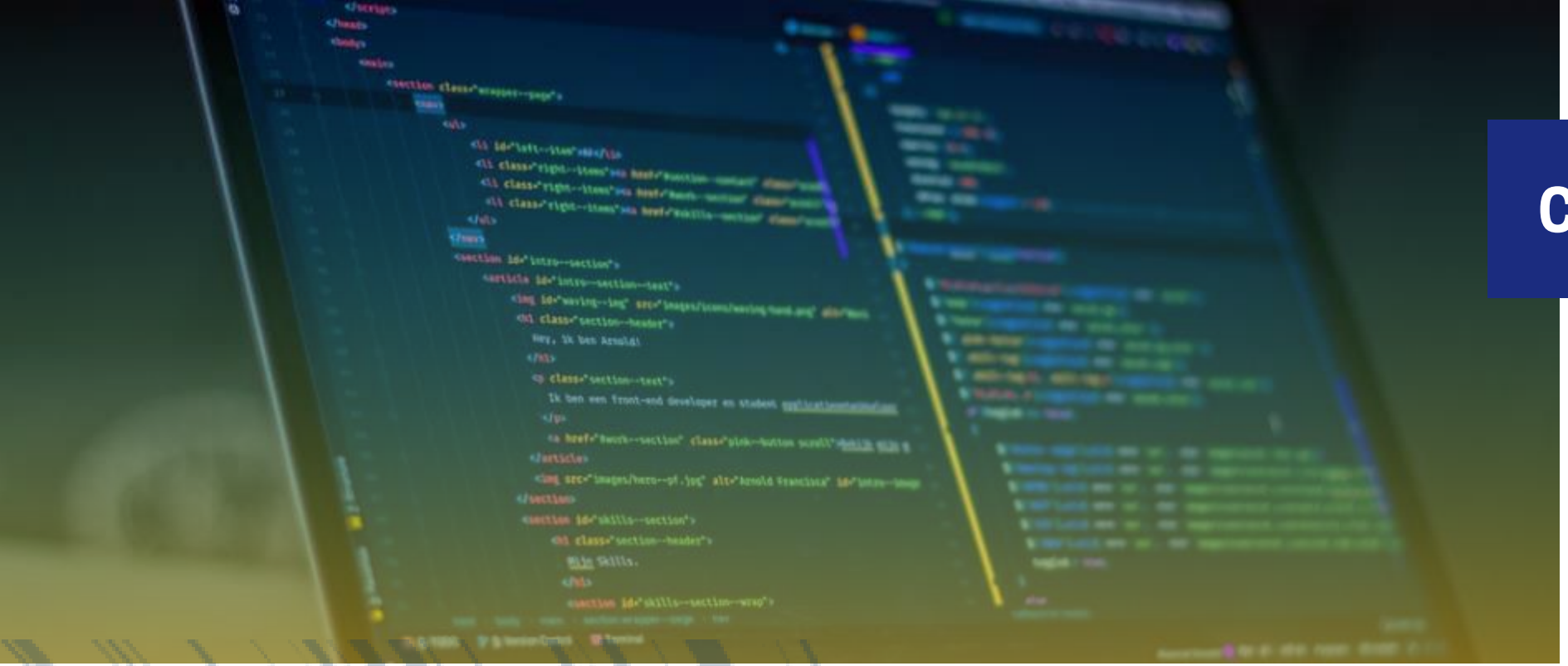


Checkmarx

A New Attack Vector

Infrastructure as Code

THE WORLD RUNS ON (CODE) WE SECURE IT.

ABOUT ME

Rusty Sides

DIRECTOR OF SALES ENGINEERING

- Security Evangelist
- Software Developer prior to AppSec
- Strong Believer in spreading Awareness for Software Security

Checkmarx Recognized by Gartner

5 Years in a Row

Checkmarx is positioned by Gartner® as a Leader in the April 2022 Magic Quadrant™ for Application Security Testing.

Gartner

Source: Gartner, Magic Quadrant for Application Security Testing
by Dale Gardner, Mark Horvath, Dionisio Zumerle, 18 April 2022

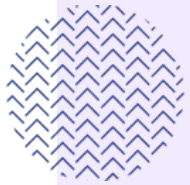
Figure 1: Magic Quadrant for Application Security Testing

Source: Gartner (April 2022)

EVERYTHING IS CODE

THE WORLD RUNS ON CODE WE'VE SECURED IT.

Checkmarx



Everything >>>>>

CAN BE TREATED LIKE APPLICATION CODE SUCH THAT WE CAN FOLLOW THE SAME SOFTWARE DEVELOPMENT LIFECYCLE PRACTICES

THE WORLD RUNS ON CODE. WE'LL SECURE IT.

Checkmarx

IT'S ALL "CODE"

01 Application Configuration

02 Operating System and Host Configuration

03 Cloud Resources

04 Network Elements

05 Firewalls

06 Load Balancers

07 Security Groups

08 IoT Devices

THE WORLD RUNS ON CODE WE SECURE IT.

Checkmar

THE BENEFITS OF CODE

- Automation
- GitOps
- Code Review
- Testing
- Version Control
- Reversibility

THE WORLD RUNS ON CODE WE'VE SECURE IT.

Infrastructure as code (IaC)

IS THE PROCESS OF **MANAGING AND PROVISIONING SOFTWARE** THROUGH MACHINE-READABLE DEFINITION FILES, RATHER THAN PHYSICAL HARDWARE CONFIGURATION OR INTERACTIVE CONFIGURATION TOOLS

WHAT IS INFRASTRUCTURE-AS-CODE (IAC)

IaC automates the manual tasks usually associated with computing infrastructure configuration and implementation.

IaC allows you to:

01

SPEED UP

Speed up configuration and implementation of new computing infrastructure

02

REDUCE THE COST

Reduce the cost and resource needed to scale and manage large infrastructure

03

ELIMINATE THE INCONSISTEN-CIES

Eliminate the inconsistencies that inevitably occur when multiple individuals manually configure new equipment or applications.

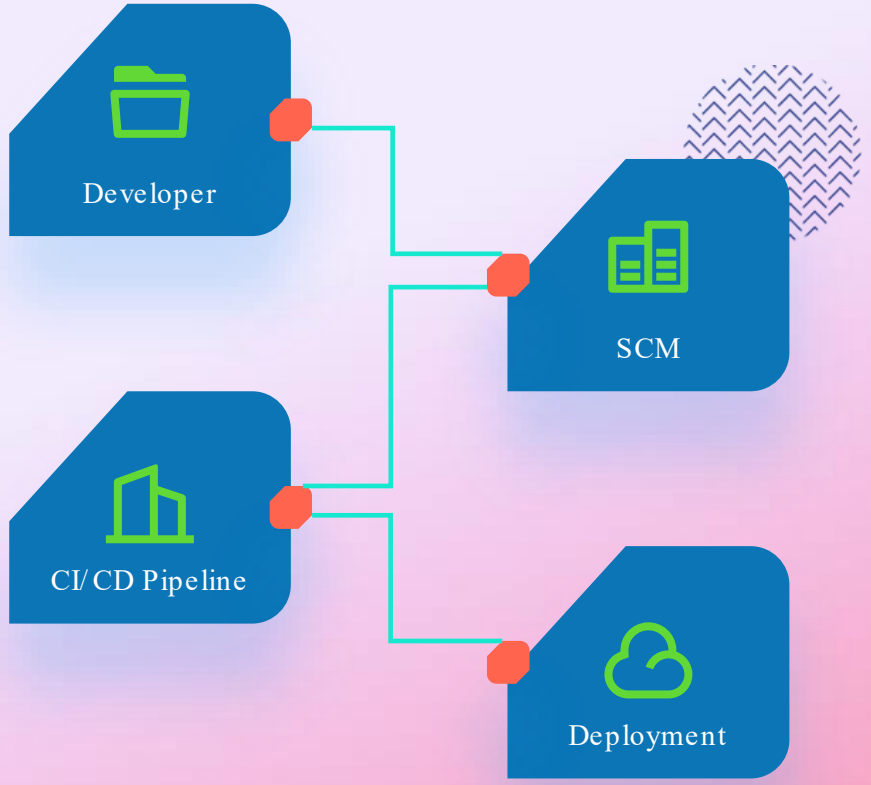
INFRASTRUCTURE AT THE SPEED OF DEVOPS

Moving to cloud-based infrastructure opens doors to building and managing infrastructure in completely new ways:

01 Infrastructure can be provisioned in seconds

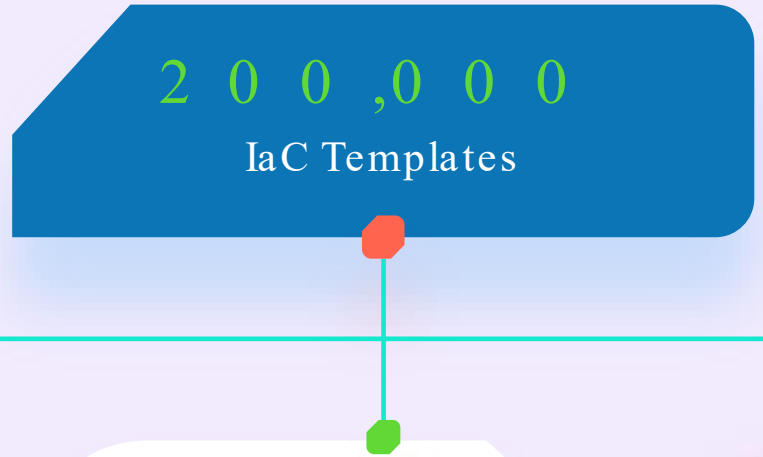
02 Scale can be achieved without capacity planning

03 API-driven cloud infra allows us interact with it via code



SO, WHAT'S THE PROBLEM?

IAC SECURITY IS A CONCERN



48%

of AWS S3 buckets do not have server-side encryption enabled

42%

CloudFormation config files contained at least one insecure configuration

55%

of cloud user-configured S3 buckets do not have logging enabled

Source: https://start.paloaltonetworks.com/unit-42-cloud-threat-report

An SSRF, privileged AWS keys and the Capital One breach

Riyaz Walikar Follow

Aug 4, 2019 · 9 min read

This post attempts to explain the technical side of how the Capital One breach occurred, the impact of the breach and what you can do as a user of cloud services to prevent this from happening to you.

Updated 3rd December 2019 — Please note: AWS released an additiona security defences against the attack mentioned in this blog post. While the methods described here will work with the legacy version of Instance Met Data Service (IMDSv1), they will be thwarted by IMDSv2. Read our extensive blog post on how to utilise AWS EC2 IMDSv2 and add the additional defences for your EC2 machines

02 What We Can Learn from the Capital One Hack

AUG 19

On Monday, a former **Amazon** employee was arrested and charged with stealing more than 100 million consumer applications for credit from Capital One. Since then, many have speculated the breach was perhaps the result of a previously unknown "zero-day" flaw, or an "insider" attack in which the accused took advantage of access surreptitiously obtained from her former employer. But new information indicates the methods she deployed have been well understood for years.

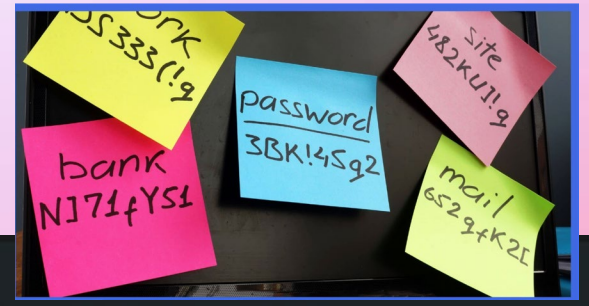
SECURITY RISKS IN IAC IMPLEMENTATIONS

- Vulnerabilities in IaC can serve as a thread entry point to the core infrastructure
- Misconfigured IaC templates can expose sensitive data

SECRETS STORAGE

Keep it secret, Keep it safe

- Storage of secrets is necessary for connecting to managed infrastructure.
- Storing such data inside source code management (SCM) systems or plain text files is dangerous and irresponsible.
- Bots scrape public SCM sites like Github looking for secrets to exploit and compromise




```
/*public static void main(String[] args) {
    // Endpoint以Region: 华东1为例，其他Region请按实际情况填写
    String endpoint = "https://datahub.cn-shanghai-shga-d01.dh.alicloud.ga.sh";
    String accessId = "0iWV0NCs805VuAAu";
    String accessKey = "iEwlgpCnXDwT93YMVDb2G60my9ne81";
    String projectName = "sjc_rwzx";
    String topicName = "task_center_platform_request";
    RecordSchema schema = new RecordSchema();
```

USER PRIVILEGES

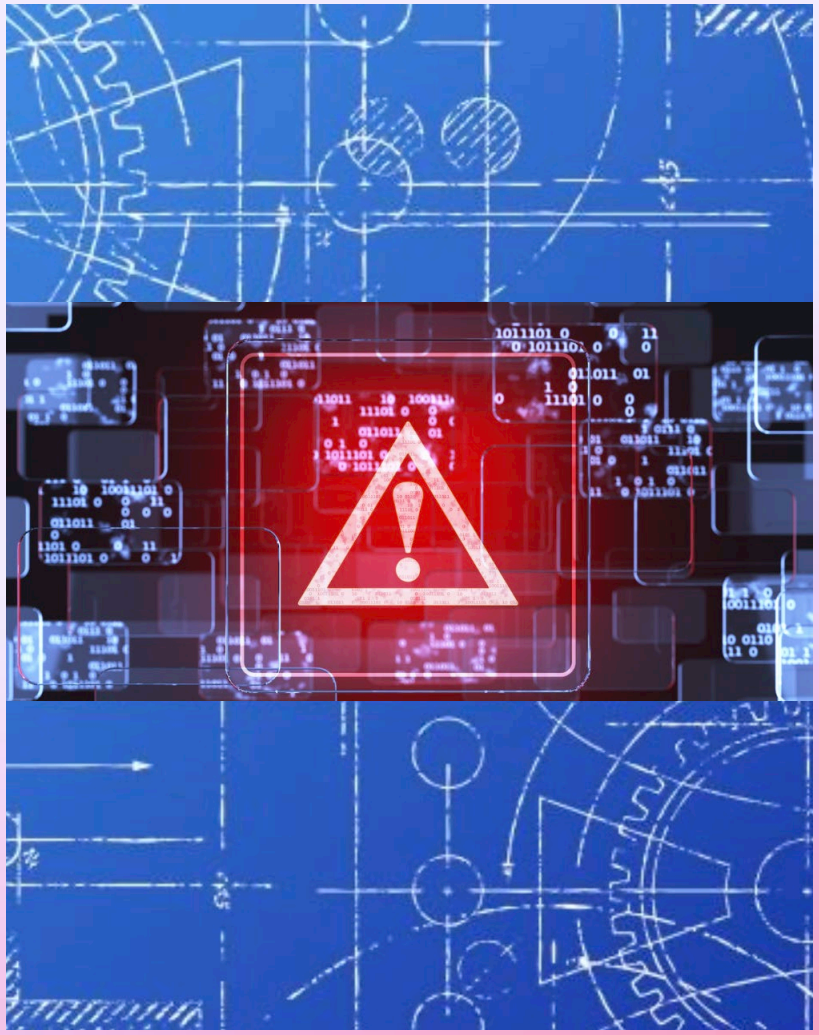
Least privilege

- Application deployment is unlikely to require root privileges on the target machine
- Least privilege may be more challenging but mitigates the risk of compromise

I A C T E M P L A T E S

Do you trust the source?

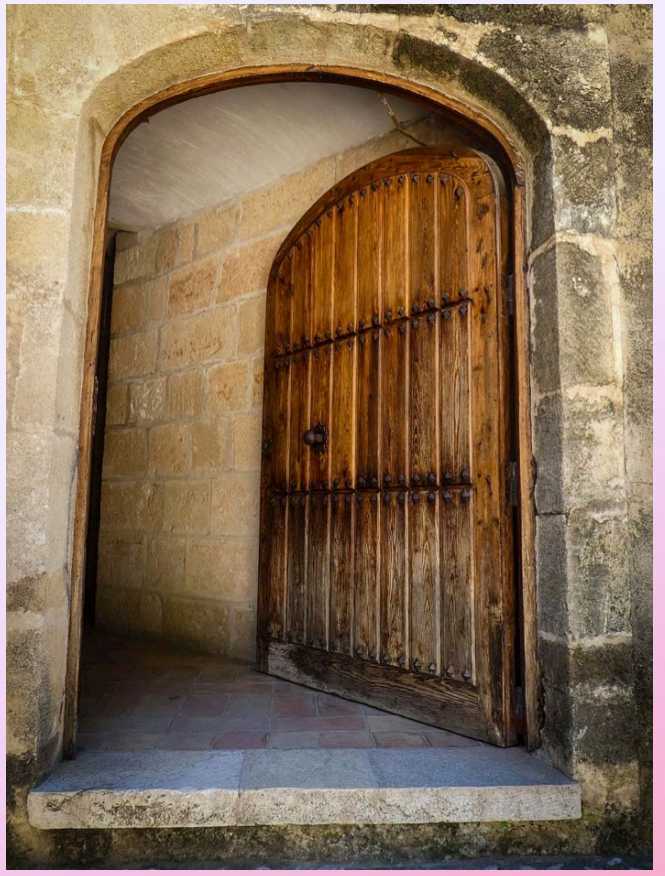
- IaC Templates can have vulnerabilities and insecure default configurations that could lead to data exposure
- IaC Templates can unintentionally use OS or container images from untrusted sources



NETWORK EXPOSURES

New platforms, New problems

- Insecure IaC configurations can expand the attack surface
- Open Security Groups
- Public SSH Access



EXAMPLE OF IAC

AWS CLOUDFORMATION

ElasticBeanstalkSample.template

```
{
 "AWSTemplateFormatVersion" : "2010-09-09",

 "Description" : "AWS CloudFormation Sample Template ElasticBeanstalkSample: Configure and

 "Parameters" : {
   "KeyName" : {
     "Description" : "Name of an existing EC2 KeyPair to enable SSH access to the AWS Elast
     "Type" : "String"
   }
 },

 "Resources" : {
   "sampleApplication" : {
     "Type" : "AWS::ElasticBeanstalk::Application",
     "Properties" : {
       "Description" : "AWS Elastic Beanstalk Sample Application",
       "ApplicationVersions" : [{
         "VersionLabel" : "Initial Version",
         "Description" : "Version 1.0",
         "SourceBundle" : {
           "S3Bucket" : { "Fn::Join" : ["-", ["elasticbeanstalk-samples", { "Ref" : "AWS::R
           "S3Key" : "elasticbeanstalk-sampleapp.war"
         }
       }],
       "ConfigurationTemplates" : [{
         "TemplateName" : "DefaultConfiguration",
         "Description" : "Default Configuration Version 1.0 - with SSH access",
         "SolutionStackName" : "64bit Amazon Linux running Tomcat 7",
```

CloudFormation

aws

KICS IS OPEN-SOURCE

Public GitHub repository

(https://github.com/Checkmarx/kics)

Live chat with Gitter

(https://gitter.im/kics-io/community)

Public website

(https://kics.io/)

Managed completely from GitHub

(Issues / Projects)

SUPPORTED PLATFORMS

- Terraform
- Kubernetes
- Docker
- AWS CloudFormation
- Ansible
- Helm
- Google Deployment Manager
- AWS SAM
- Microsoft ARM
- OpenAPI 3.0

KICS: SECURITY POLICIES

- Access Control
- Availability
- Backup
- Best Practices
- Build Process
- Encryption
- Insecure configurations
- Insecure defaults
- Networking and Firewall
- Observability
- Resource management
- Secret management
- Supply-Chain

Supports top Infrastructure-as-Code tools with over 2000 security policies

KICS: VULNERABILITY EXAMPLE

```
resource "azurerm_network_security_rule" "positive4" {
    name                        = "example"
    priority                    = 100
    direction                   = "Inbound"
    access                      = "Allow"
    protocol                    = "TCP"
    source_port_range           = "*"
    destination_port_range      = "22"
    source_address_prefix       = "0.0.0.0"
    destination_address_prefix  = "*"
    resource_group_name         = azurerm_resource_group.example.name
    network_security_group_name = azurerm_network_security_group.example.name
}
```

01 Terraform for Azure

02 Access policy for a resource

03 SSH port 22 is left open leaving the possibility of unauthorized access, ports scanning attacks and remote take-over of your infrastructure

KICS: INTEGRATION FLOW DIAGRAM

Developer

Run KICS locally for immediate feedback.

SCM

Integrate KICS w/ git repo of choice

CI/CD Pipeline

Run KICS as part of CI/CD pipeline, on every pull request.

Security Check

Run KICS as a gated check prior to deploying to production

LIVE DEMO

THE WORLD RUNS ON CODE WE'VE SECURED IT.

Checkmarx

https://kics.io

HOME ABOUT CONTRIBUTE

Scan your IaC

Get results immediately

Supported file types: zip .tf .json .yaml .yml .dockerfile (max size 4MB)

Enter GitHub URL

Or drag & drop, or browse file

I agree to the terms of service

START YOUR SCAN

KICS finds security vulnerabilities, compliance issues, and infrastructure misconfigurations in following Infrastructure as Code solutions: Terraform, Kubernetes, Docker, AWS CloudFormation, Ansible. 1900+ queries are available.

Complete

KICS finds security vulnerabilities, compliance issues, and infrastructure misconfigurations in following Infrastructure as Code solutions: Terraform, Kubernetes, Docker, AWS CloudFormation, Ansible. 1900+ queries are available.

KICS is easy to install and run, easy to understand results, and easy to integrate into CI.

Open Source

KICS is open and will always stay such. Both the scanning engine and the security queries are clear and open for the software development community.

Extensible

From day one KICS is built for extensibility.

First, it includes over 1900 fully customizable and adjustable heuristics rules, called queries. These can be easily edited, extended, and added. Second, its robust but yet simple architecture allows quick addition of support for new Infrastructure as Code solutions.

Checkmarx

KICS REPORT v1.5.3

HIGH	99	MEDIUM	61	LOW	21	INFO	62	TOTAL	243

PLATFORMS Terraform, Dockerfile, Common
START TIME 19:44:19, Jul 14 2022
END TIME 19:44:59, Jul 14 2022
SCANNED PATHS:
- git::https://github.com/bridgecrewio/terragoat.git

AD Admin Not Configured For SQL Server

Results 1

Severity HIGH
Platform Terraform
Category Insecure Configurations

Description

The Active Directory Administrator is not configured for a SQL server

git::https://github.com/bridgecrewio/terragoat.git/terraform/azure/sql.tf:9

Expected: A 'azurerm_sql_active_directory_administrator' is defined for 'azurerm_sql_server[example]'

App Service Managed Identity Disabled

Results 2

Severity HIGH
Platform Terraform
Category Resource Management

Description

Azure App Service should have managed identity enabled

git::https://github.com/bridgecrewio/terragoat.git/terraform/azure/app_service.tf:43

Expected: 'azurerm_app_service[app-service2].identity' is defined and not null

git::https://github.com/bridgecrewio/terragoat.git/terraform/azure/app_service.tf:22

Expected: 'azurerm_app_service[app-service1].identity' is defined and not null

App Service Not Using Latest TLS Encryption Version

Results 1

Severity HIGH
Platform Terraform
Category Encryption

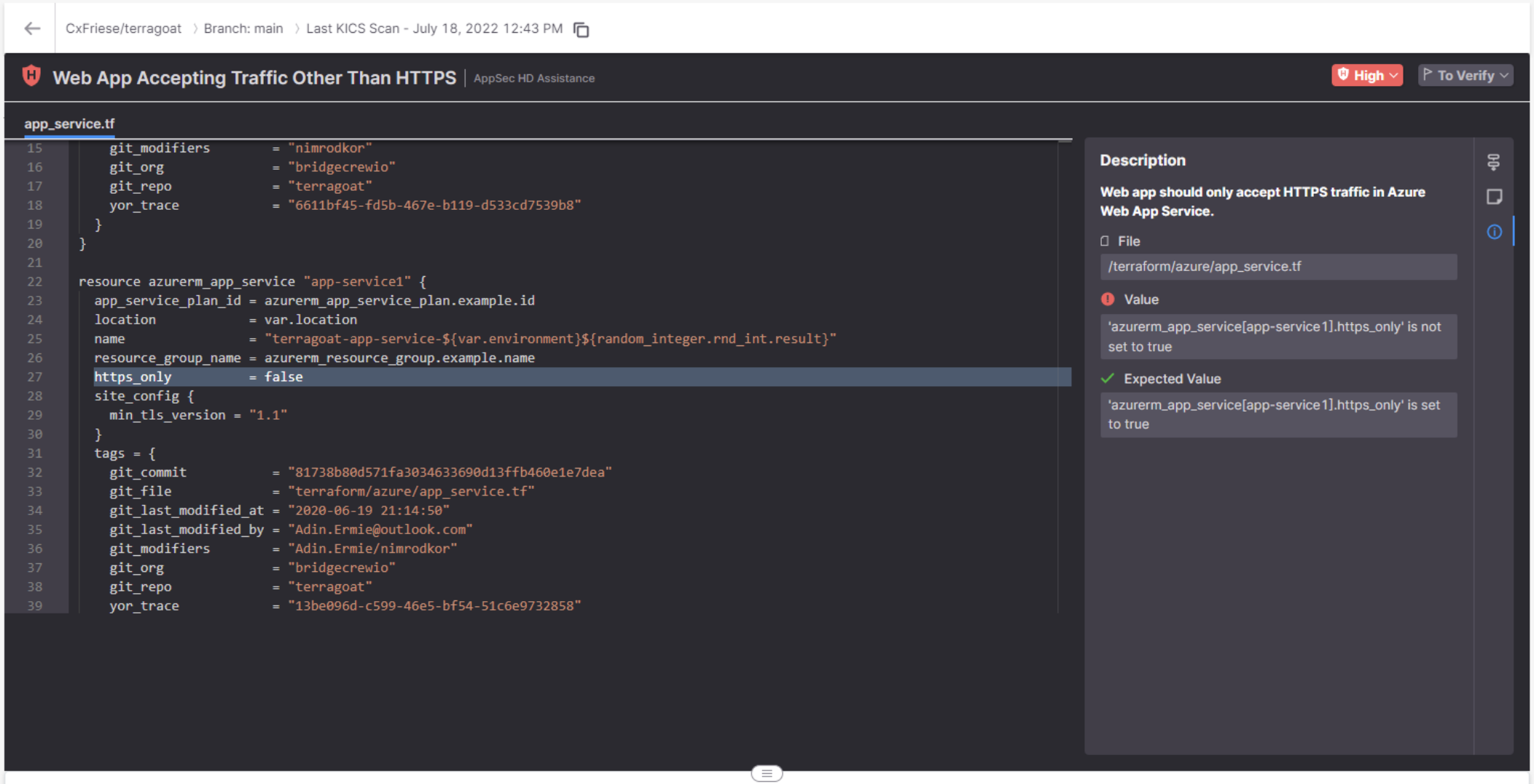
Description

Ensure App Service is using the latest version of TLS encryption

git::https://github.com/bridgecrewio/terragoat.git/terraform/azure/app_service.tf:29

Expected: 'azurerm_app_service[app-service1].site_config.min_tls_version' is set to '1.2'


```
efriese@mint-clean:~/tmp/kics/bin$ ./kics scan -p ../../terragoat/ --report-formats json

                  .0MO.
                  0MMMx
                  ;NMX;
                   ...           ...             ....
WMMMd     cWMMM0.  KMMMO      ;xKWMMMMNOc.     ,xXMMMMMWXkc.
WMMMd   .0MMMN:    KMMMO    :XMMMMMMMMMMMMWl   xMMMMMWMMMMMMl
WMMMd  lWMMMO.     KMMMO   xMMMMKc...'lXMk   ,MMMMx   .;dXx
WMMMd.0MMMX;       KMMMO  cMMMMd        '    'MMMMNl'
WMMMNWMMMMl        KMMMO  0MMMN               oMMMMMMMXkl.
WMMMMMMMMMMo       KMMMO  0MMMX                 .ckKWMMMMMM0.
WMMMMWokMMMMk      KMMMO  oMMMMc               .     .:OMMMM0
WMMMK.  dMMMM0.    KMMMO   KMMMMx'    ,kNc   :WOc.     .NMMMX
WMMMd    cWMMMX.   KMMMO    kMMMMMWXNMMMMMd .WMMMMWKO0NMMMMl
WMMMd     ,NMMMN,  KMMMO     'xNMMMMMMMNx,   .l0WMMMMMMMWk,
xkkk:      ,kkkkx  okkkl        ;xKXKx;          ;dOKKkc


Scanning with Keeping Infrastructure as Code Secure snapshot-7e8b65d9


Preparing Scan Assets: Done
Executing queries: [----------------------------------------------------] 100.00%

Files scanned: 51
Parsed files: 51
Queries loaded: 1311
Queries failed to execute: 0

-----------------------------------

Variable Without Type, Severity: INFO, Results: 7
Description: All variables should contain a valid type.
Platform: Terraform

        [1]: ../../terragoat/terraform/aws/consts.tf:20

                019:
                020: variable "profile" {
                021:   default = "default"


        [2]: ../../terragoat/terraform/gcp/variables.tf:16

                015:
```



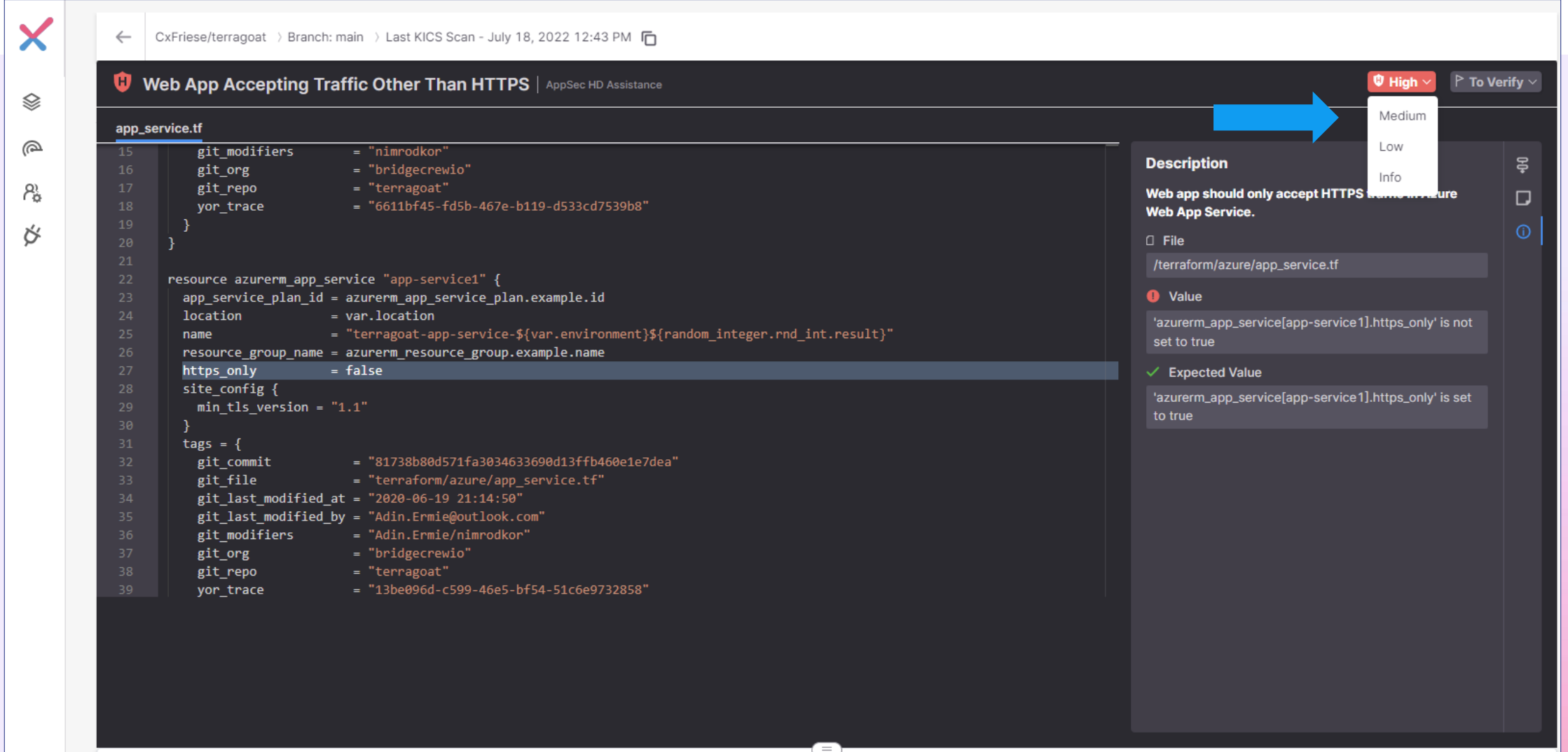
243 Vulnerabilities

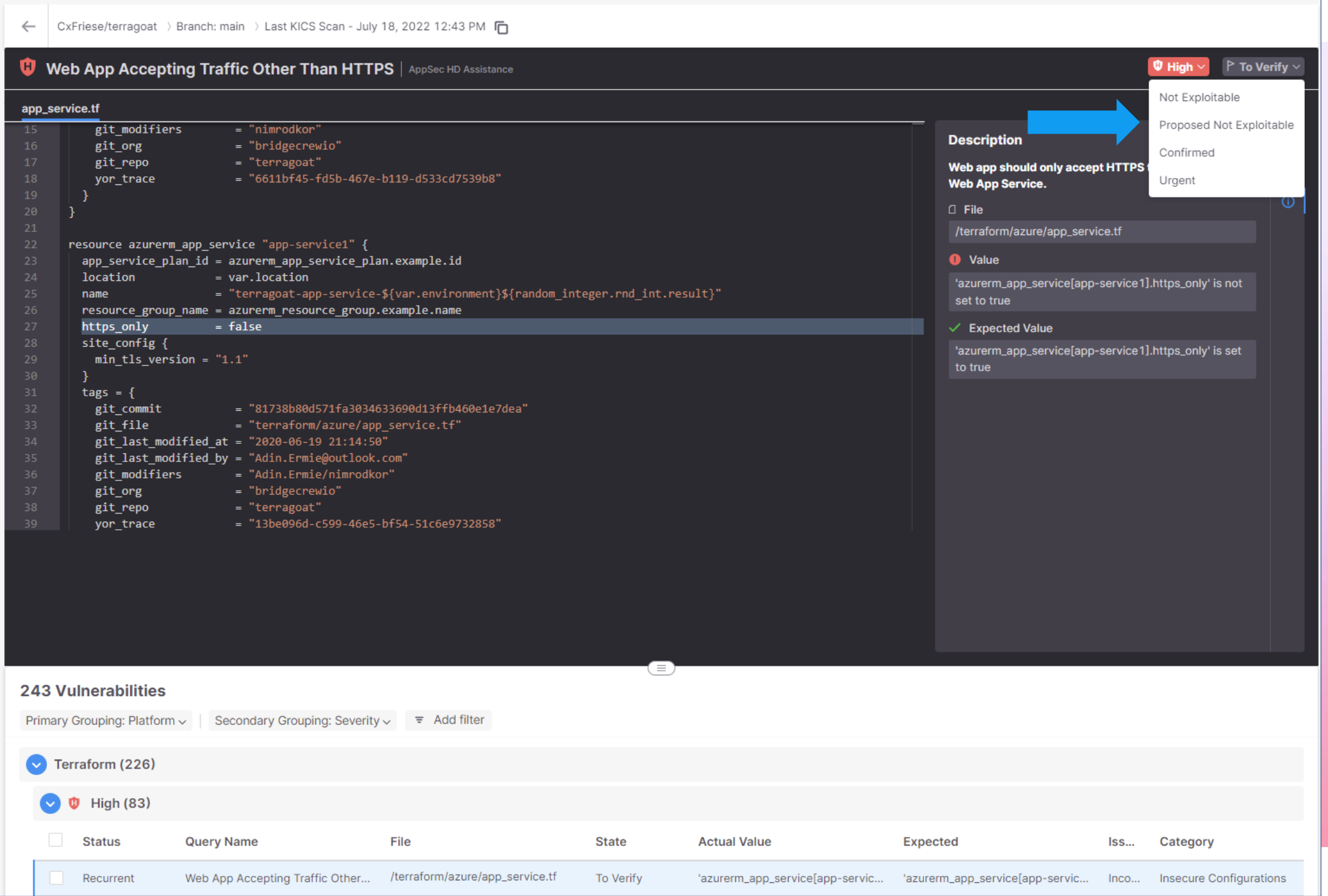
Primary Grouping: Platform | Secondary Grouping: Severity | Add filter

Terraform (226)

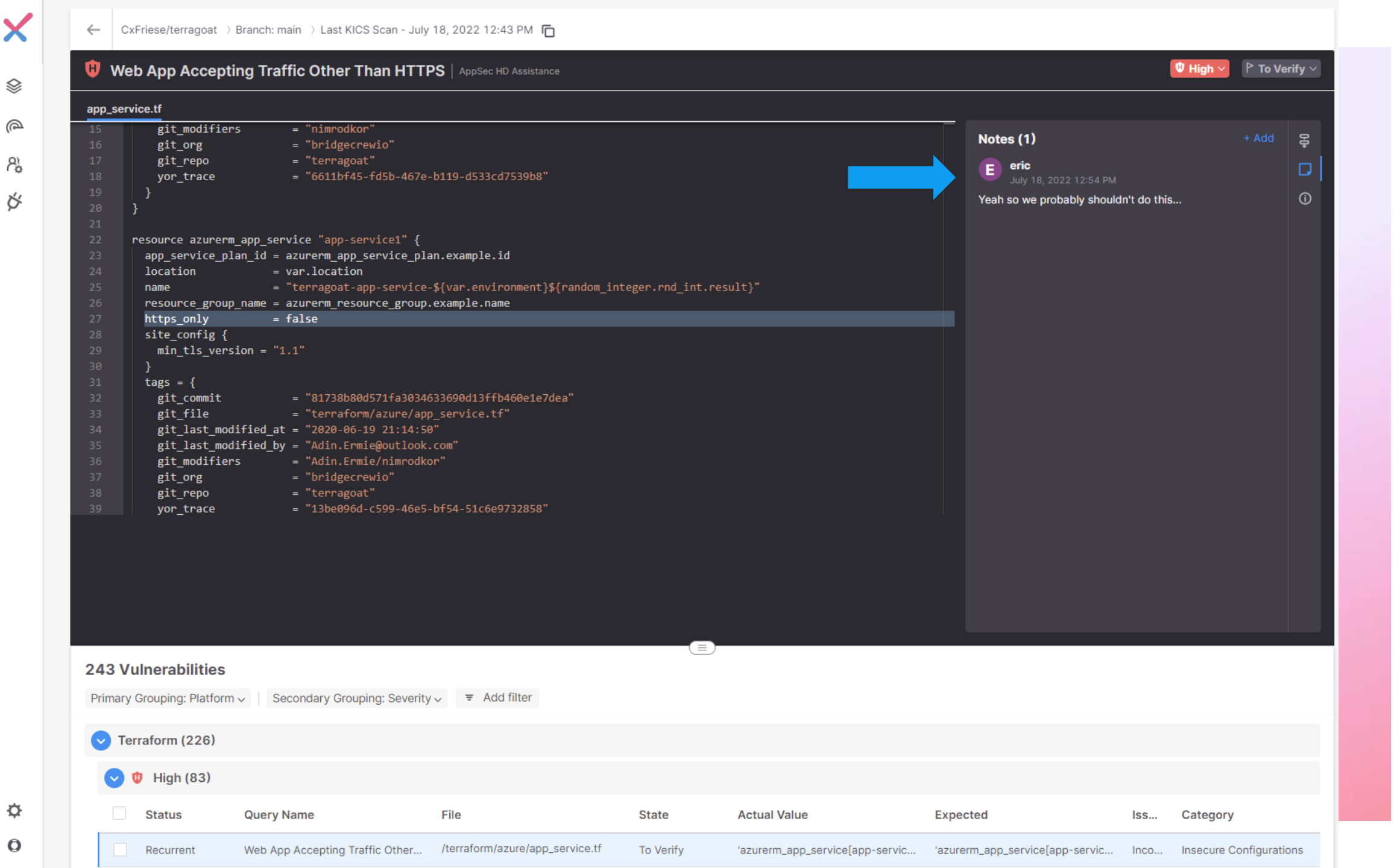
High (83)

Status	Query Name	File	State	Actual Value	Expected	Iss...	Category
Recurrent	Web App Accepting Traffic Other...	/terraform/azure/app_service.tf	To Verify	'azurerm_app_service[app-servic...	'azurerm_app_service[app-servic...	Inco...	Insecure Configurations

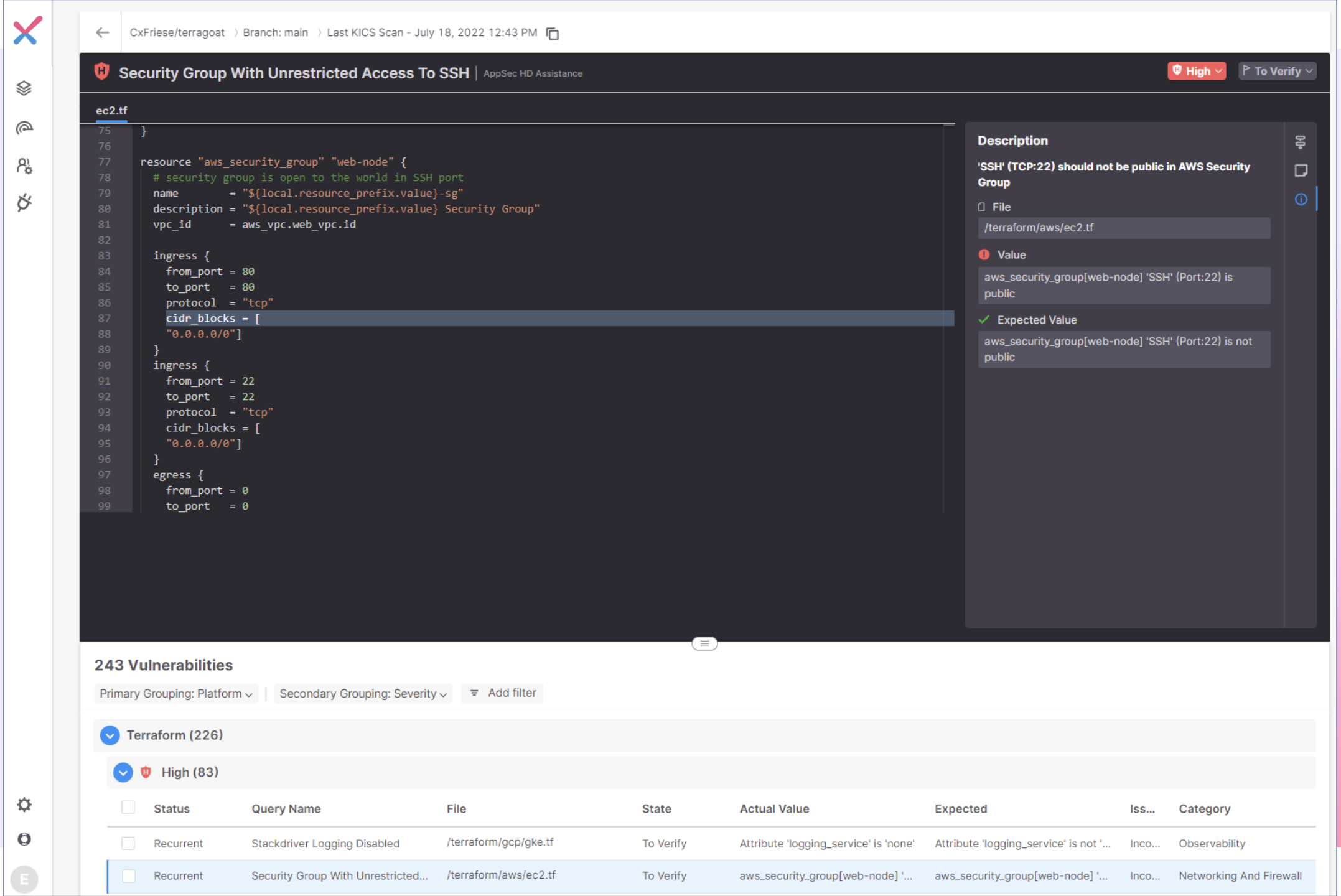


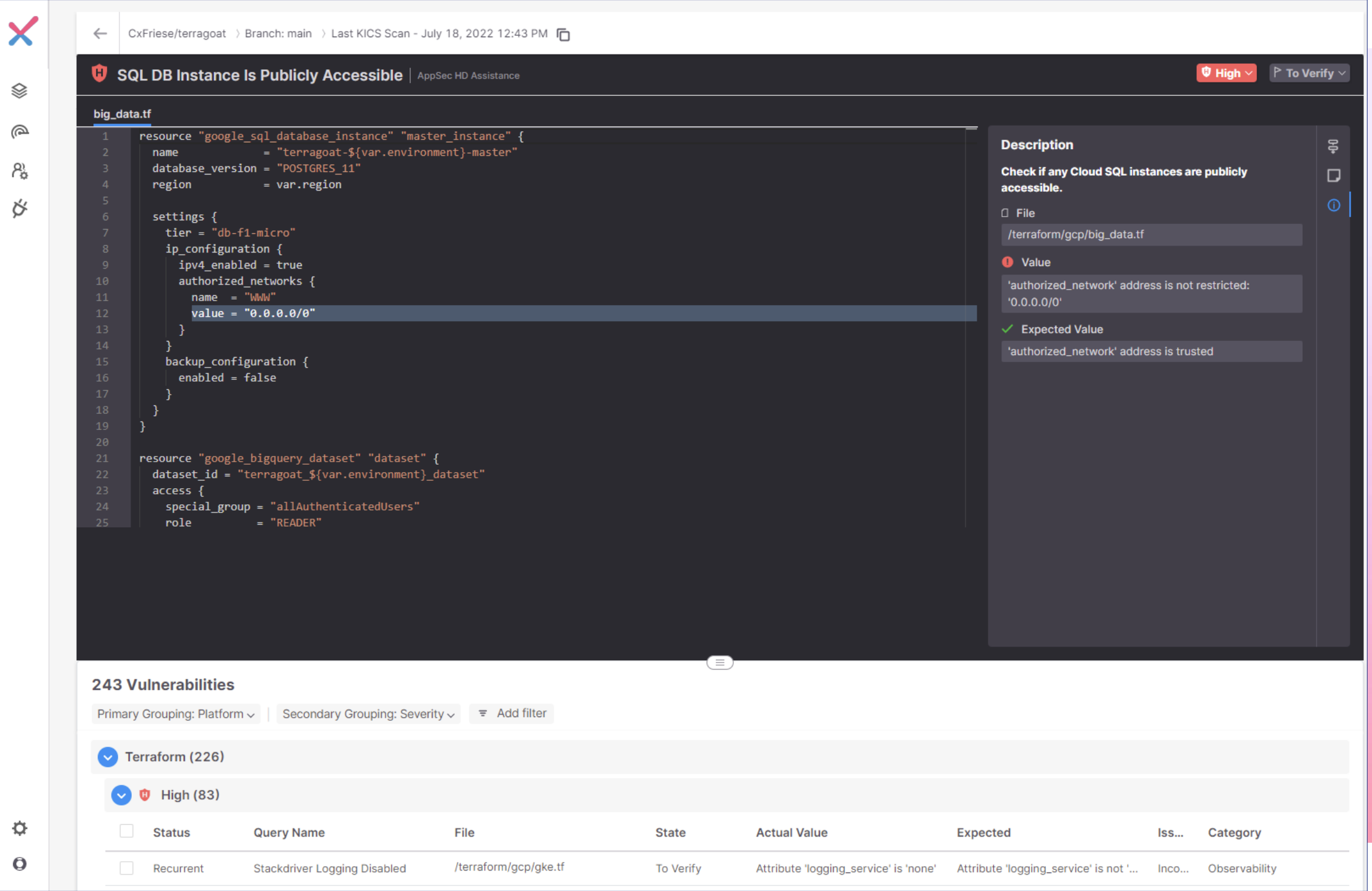


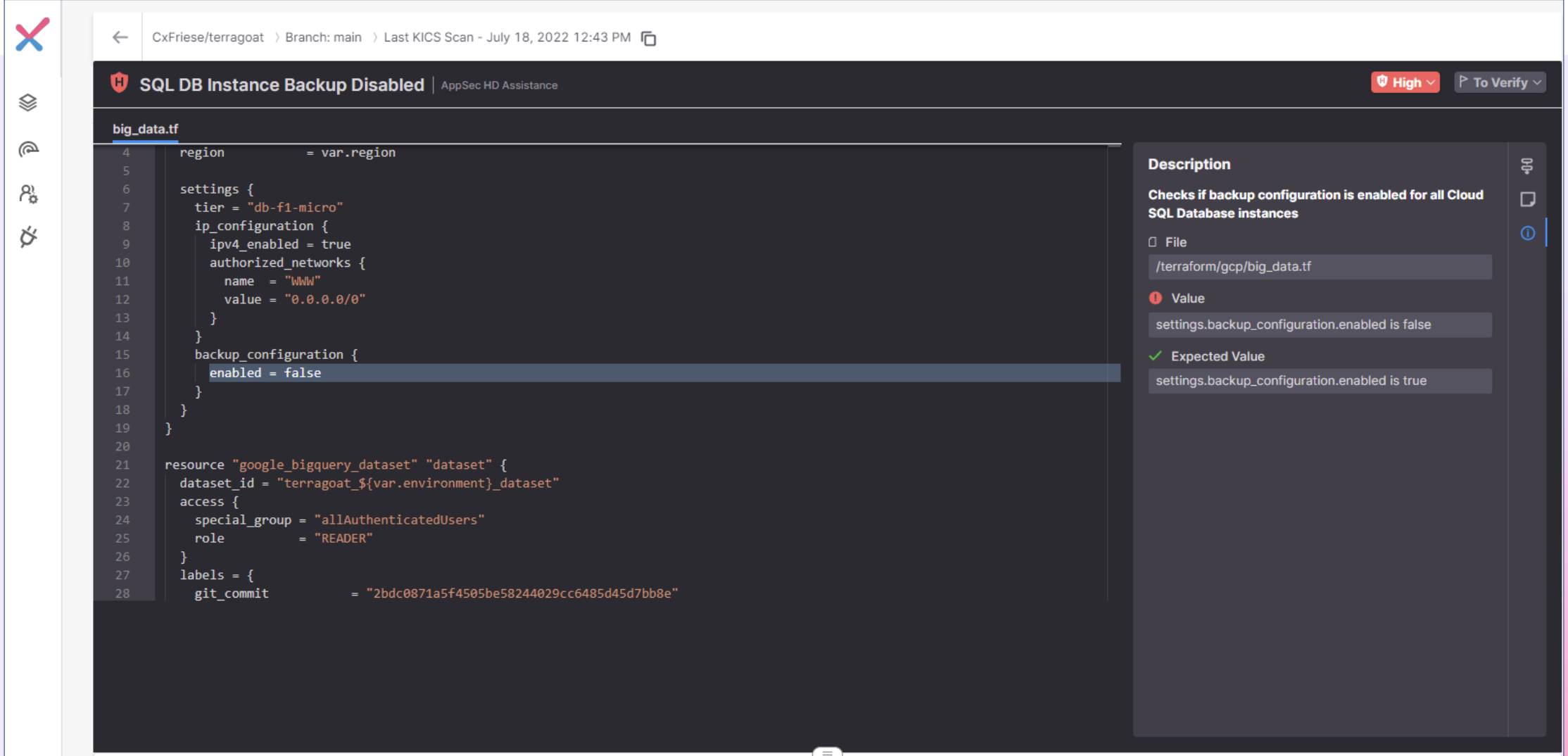
THE WORLD RUNS ON CODE. WE SECURE IT.

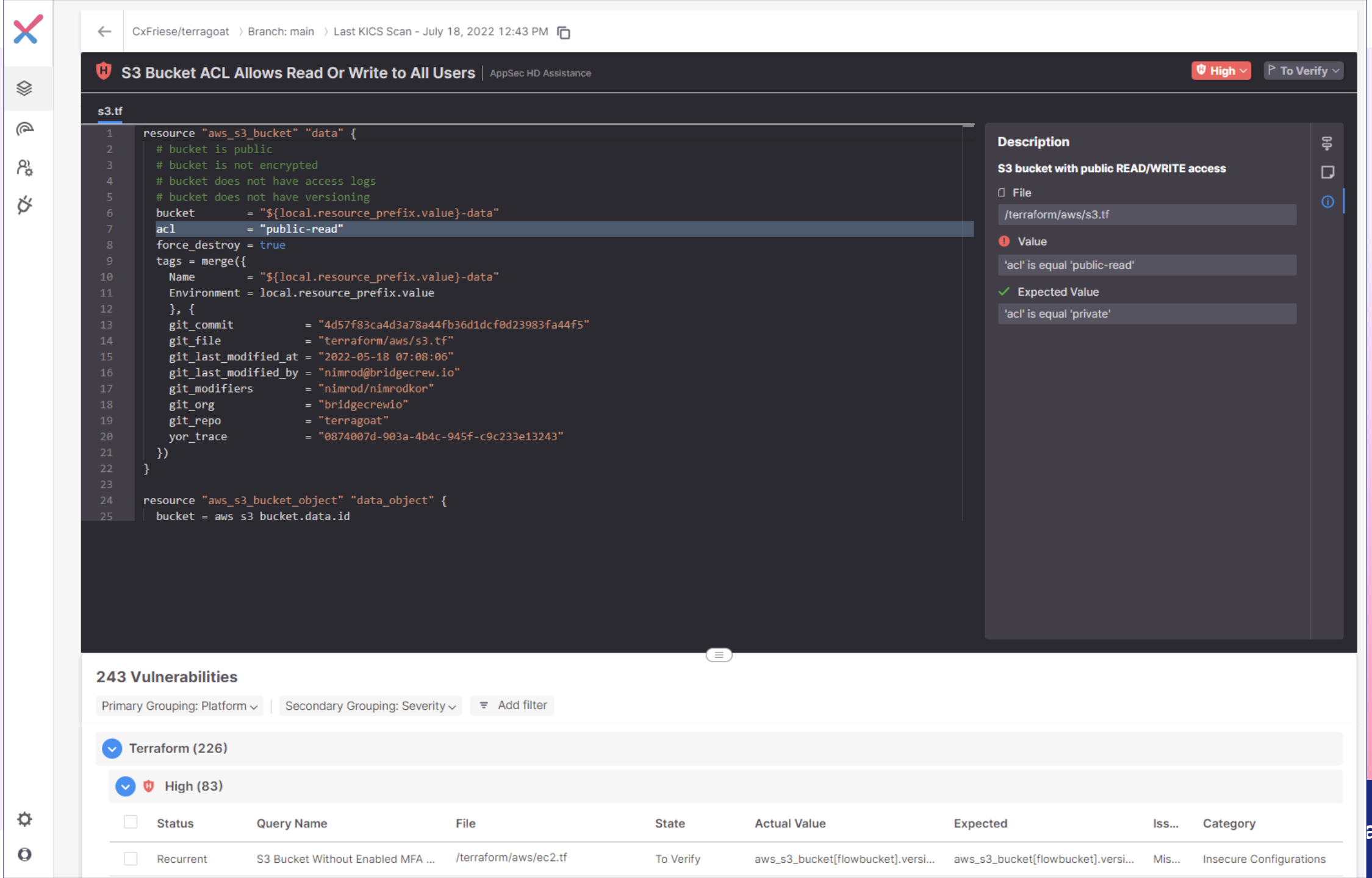


THE WORLD RUNS ON CODE. WE SECURE IT.









THE WORLD RUNS ON CODE WE SECURE IT.

Thank you!

>>>>>