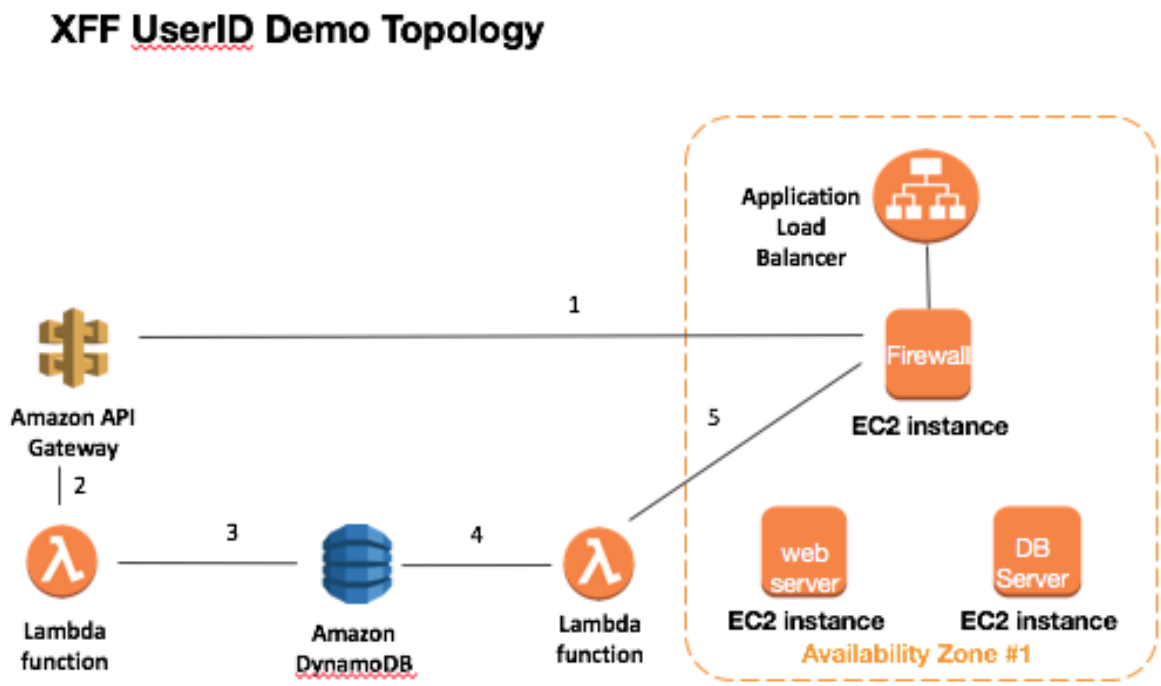
Overview

The components shown below are deployed in this demo



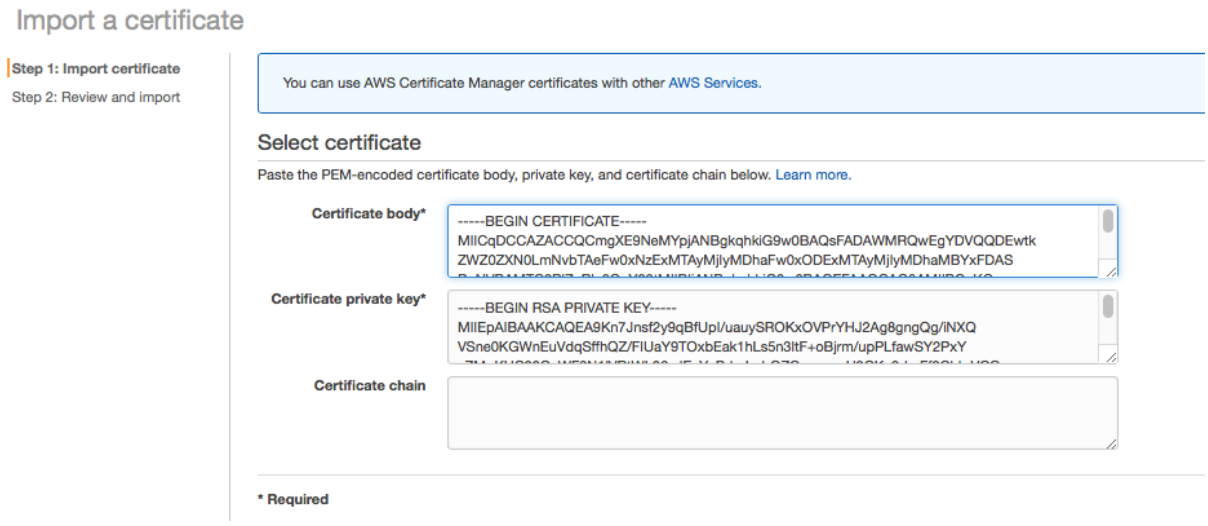
Introduction

The demo performs the following actions.

1) In this demo we use the DVWA http://www.dvwa.co.uk to generate detectable threats between a browser and the web server. In this case we use a SQL Injection attack for demonstration purposes
2) The firewall will detect the SQL Injection threat and forward the log data to the AWS API Gateway via an HTTP log forwarding action.
3) The AWS API Gateway invokes a lambda function that queries the firewall for additional information based on the sessionID of the detected threat. The additional information includes the IP address in the X-Forwarded-For HTTP header. The additional data is written to a DynamoDB database.
4) A second Lambda function that is triggered from a Cloudwatch timer triggered event reads the current entries in the DynamoDB database and forwards them to the UserID database in the firewall.
5) The IP address from the X-Forwarded-For header is added to the “bad user” group and is then subject to a blocking policy in the firewall.

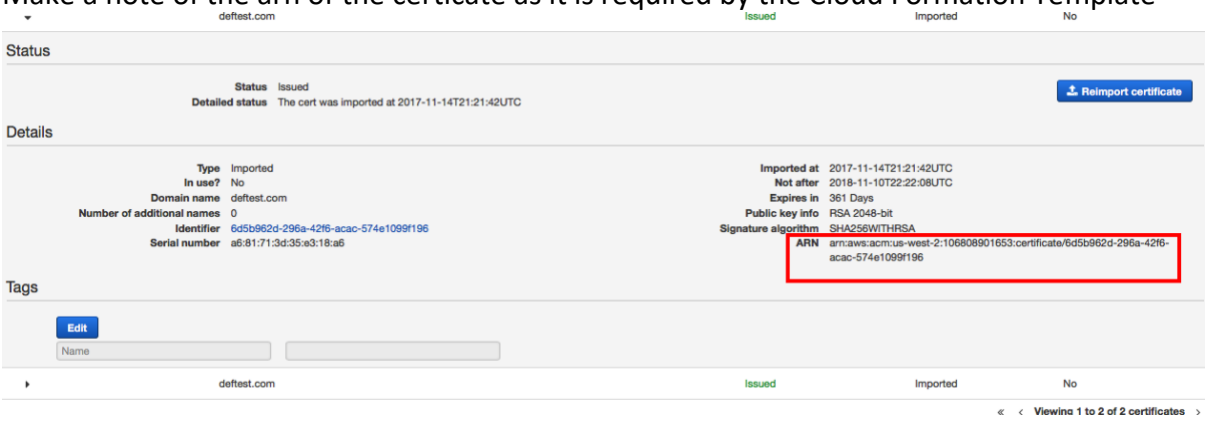
Initial Setup

1) Load The Application Load Balancer Certificate
   The application load balancer will require a certificate. Access the AWS Certificate Manager and select “Load Certificate”.



Paste in the text for the public and private key.

Make a note of the arn of the certicate as it is required by the Cloud Formation Template



2) Create the Bootstrap Buckets
   More documentation required here but we can import from the existing Wordpress Demo.

3) Deploy the Cloud Formation Template

Create stack

Select Template
Specify Details
Options
Review

Specify Details

Specify a stack name and parameter values. You can use or change the default parameter values, which are defined in the AWS CloudFormation template. Learn more.

Stack name XFF-Demo-Stack

Parameters

BootstrapBucketName xff-[illegible] Bucket name for FW bootstrap configuration

CertificateARN arn:aws:acm:[illegible]653:cert Enter arn for the certificate

ELBName public-elb Enter the name of the External Classic Load Balancer

LambdaBucketName xff-[illegible] Bucket name for FW bootstrap configuration

NumberOfAZs 2 Total Number of AZs which will be used in this deployment (Default 2)

ServerKeyName AWS-[illegible]
Name of an existing EC2 KeyPair to enable SSH access to the FW (Hint: You MUST have its private key)

VpcAzs us-west-2a × us-west-2b ×
Enter the list of Availability Zones (Based on Number of AZs above)

Check that the template deployment completes and make a note of the Wordpress URL which is the DNS name of the Application Load Balancer and the firewall management IP

XFF-Demo-Stack

Stack name: XFF-Demo-Stack

Stack ID: arn:aws:cloudformation:us-west-2:106808901653:stack/XFF-Demo-Stack/27949c10-c98a-11e7-9bcb-50a68a2012f2

Status: CREATE_COMPLETE

Status reason:

Termination protection: Disabled

IAM Role:

Description Install Web Server, Firewall and Application LB to Demonstrate XFF Header IP extraction for use in policy

Outputs

Key	Value	Description
WordpressURL	https://XffALB-272684332.us-west-2.elb.amazonaws.com/dvwa/setup.php	Web server
FirewallManagementURL	https://34.208.95.62	VM-Series management interface URL

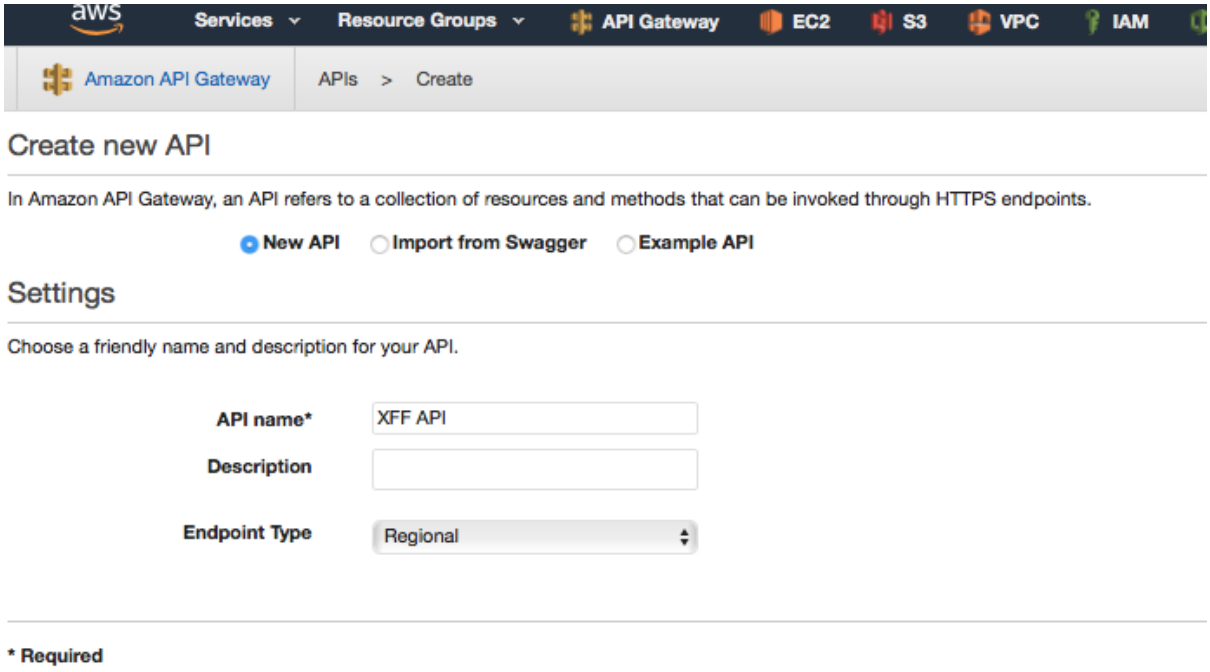
Resources

Events

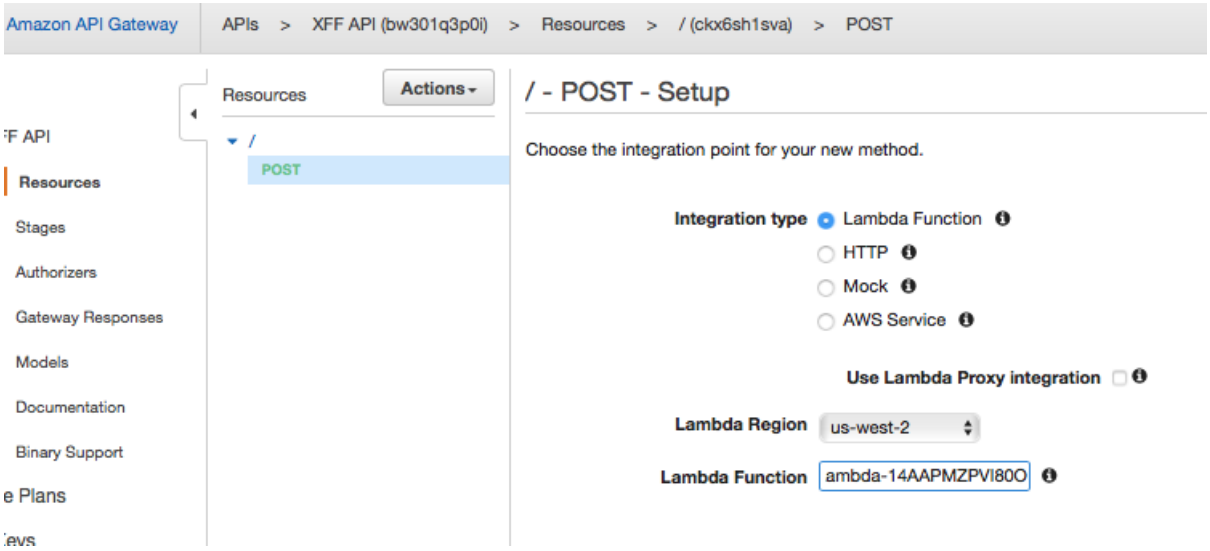
2017-11-14	Status	Type	Logical ID	Status reason
22:26:44 UTC+0000	CREATE_COMPLETE	AWS::CloudFormation::Stack	XFF-Demo-Stack	

4) Create the API Gateway

Go to the AWS console and select API gateway

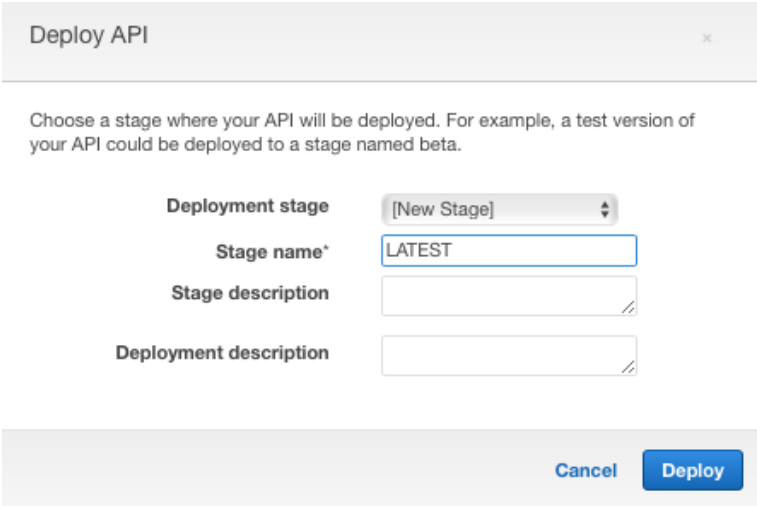


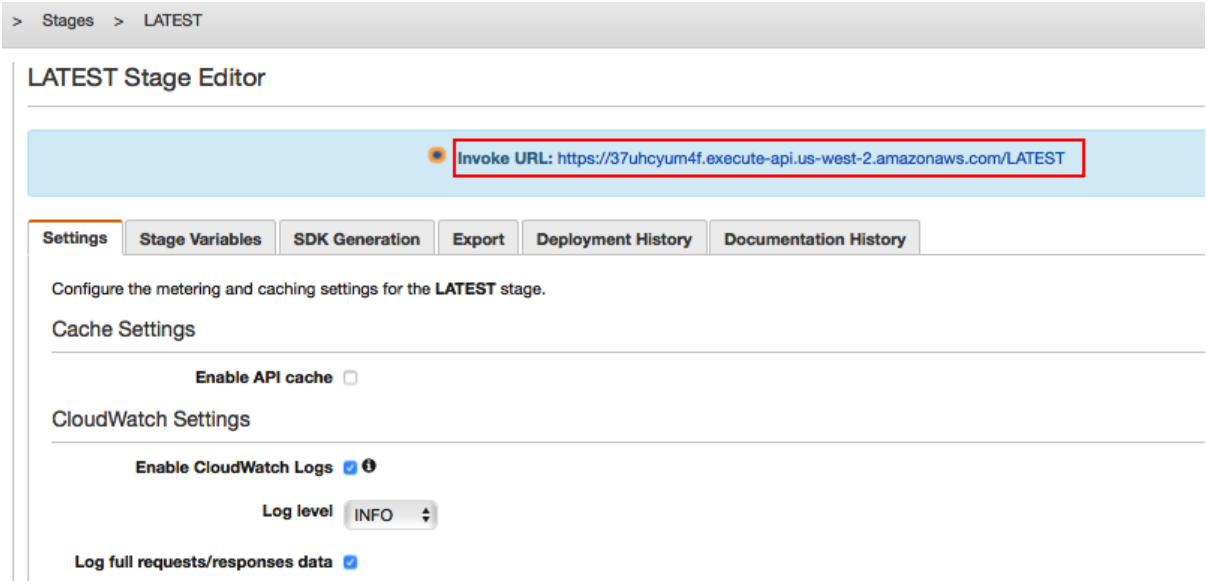
Select Actions and create a POST method



Add the lambda region and then the function.
The Lambda function will have the name {Stack Name}-GetXFFHeaderLambda-*
Next Deploy the gateway to a stage

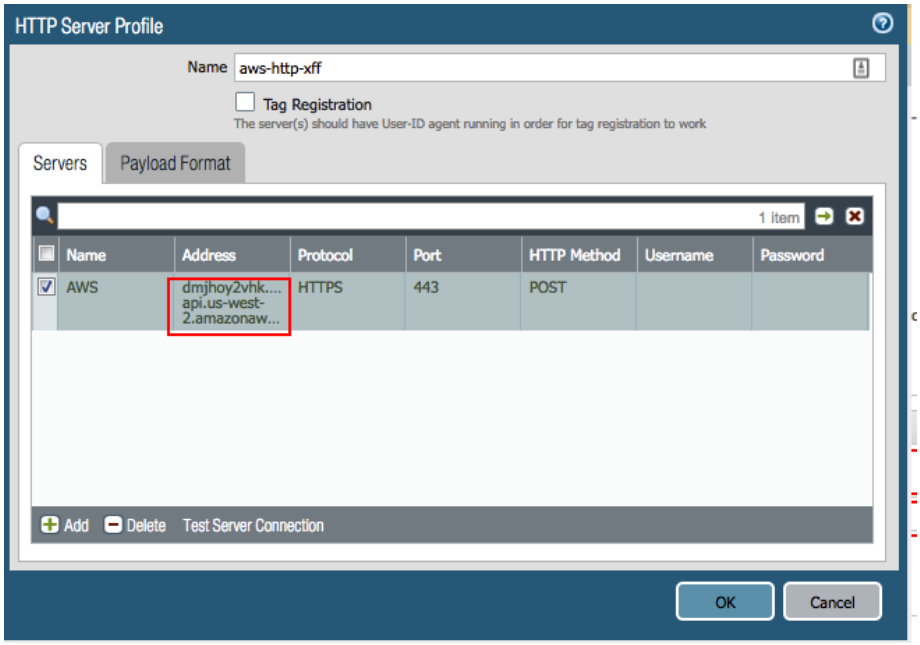
After deployment copy the URL from the summary screen
Select Actions and then Deploy



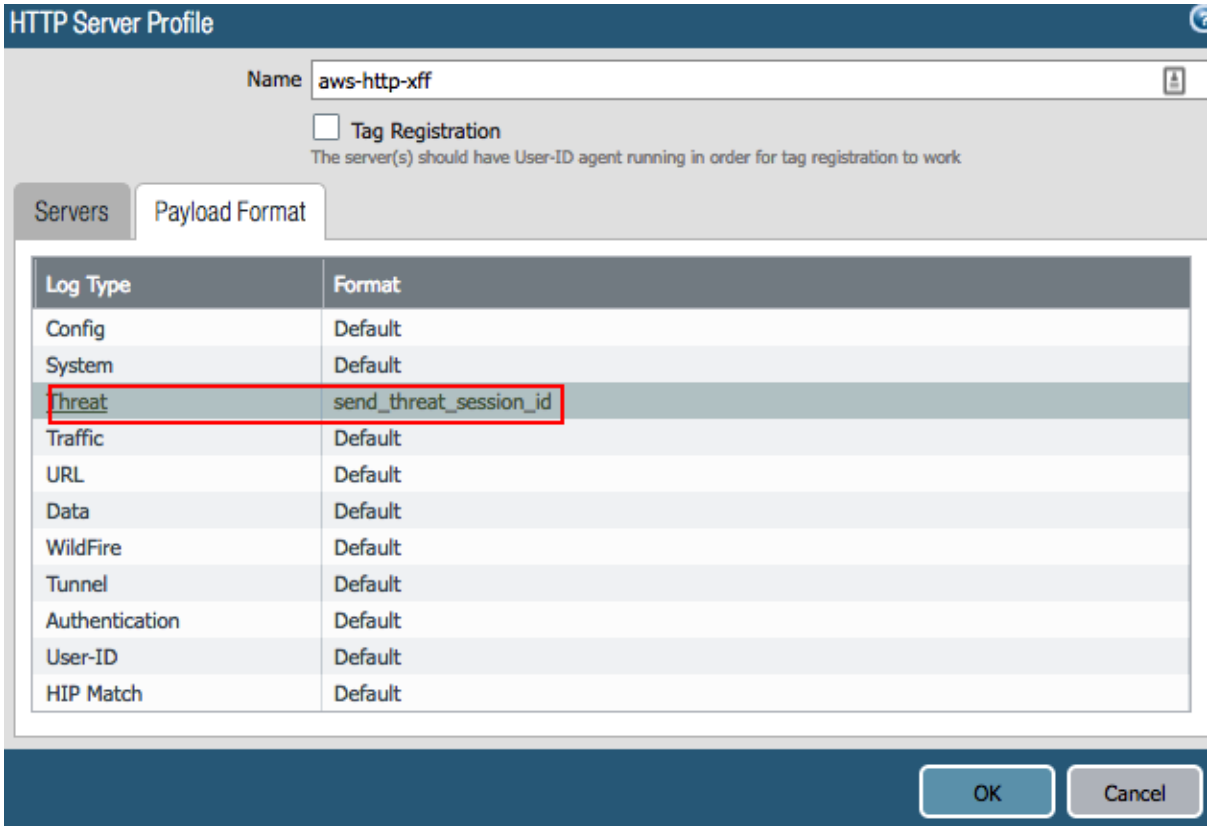


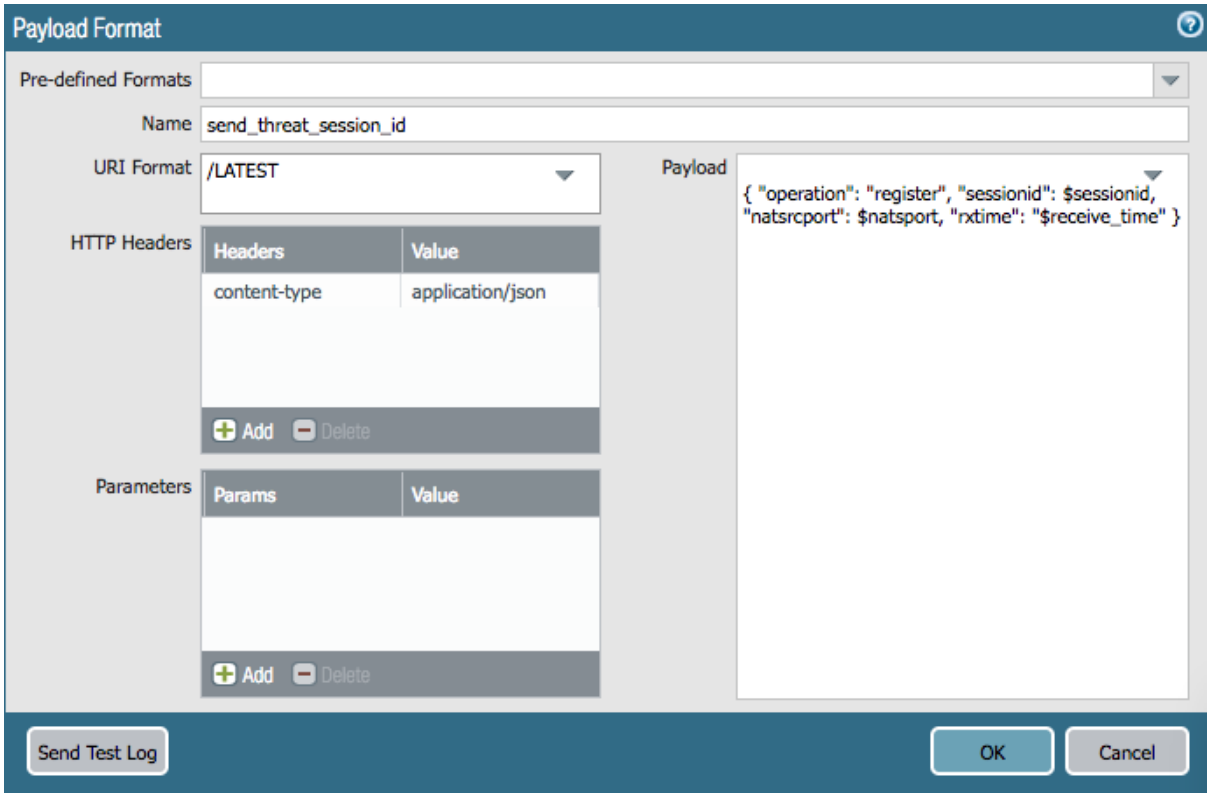
Login to the firewall with credentials Password for the firewall is admin/Pal0Alt0

Extract the DNS name from the URL and modify the HTTP log forwarding values

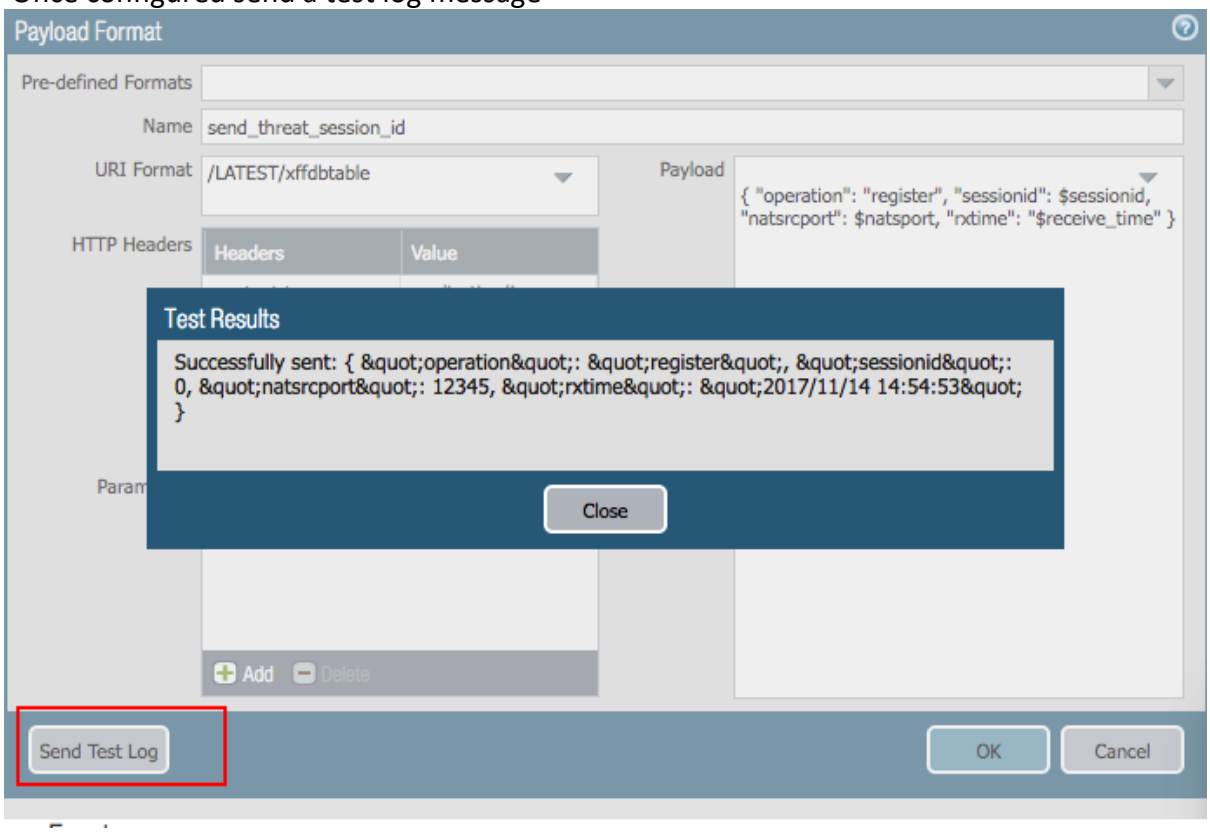


Modify the “URI Format” under “Payload Format”





Once configured send a test log message



Test the deployment

Open a browser and browse to the URL from the output of the cloud formation template
Setup the DVWA database

XFF-Demo-Stack

Stack name:	XFF-Demo-Stack
Stack ID:	arn:aws:cloudformation:us-west-2:106808901653:stack/XFF-Demo-Stack/27949c10-c98a-11e7-9bcb-50a68a2012f2
Status:	CREATE_COMPLETE
Status reason:	
Termination protection:	Disabled
IAM Role:	
Description	Install Web Server, Firewall and Application LB to Demonstrate XFF Header IP extraction for use in policy

▾ Outputs

Key	Value	Description
WordpressURL	https://XffALB-272684332.us-west-2.elb.amazonaws.com/dvwa/setup.php	Web server
FirewallManagementURL	https://34.208.95.62	VM-Series management interface URL

Setup Check

Operating system: ***nix**
Backend database: **MySQL**
PHP version: **7.0.22-0ubuntu0.16.04.1**

Web Server SERVER_NAME: **xffalb-272684332.us-west-2.elb.amazonaws.com**

PHP function display_errors: **Disabled**
PHP function safe_mode: Disabled
PHP function allow_url_include: Enabled
PHP function allow_url_fopen: Enabled
PHP function magic_quotes_gpc: Disabled
PHP module gd: Installed
PHP module mysql: Installed
PHP module pdo_mysql: Installed

MySQL username: **root**
MySQL password: ******
MySQL database: **dvwa**
MySQL host: **127.0.0.1**

reCAPTCHA key: **Missing**

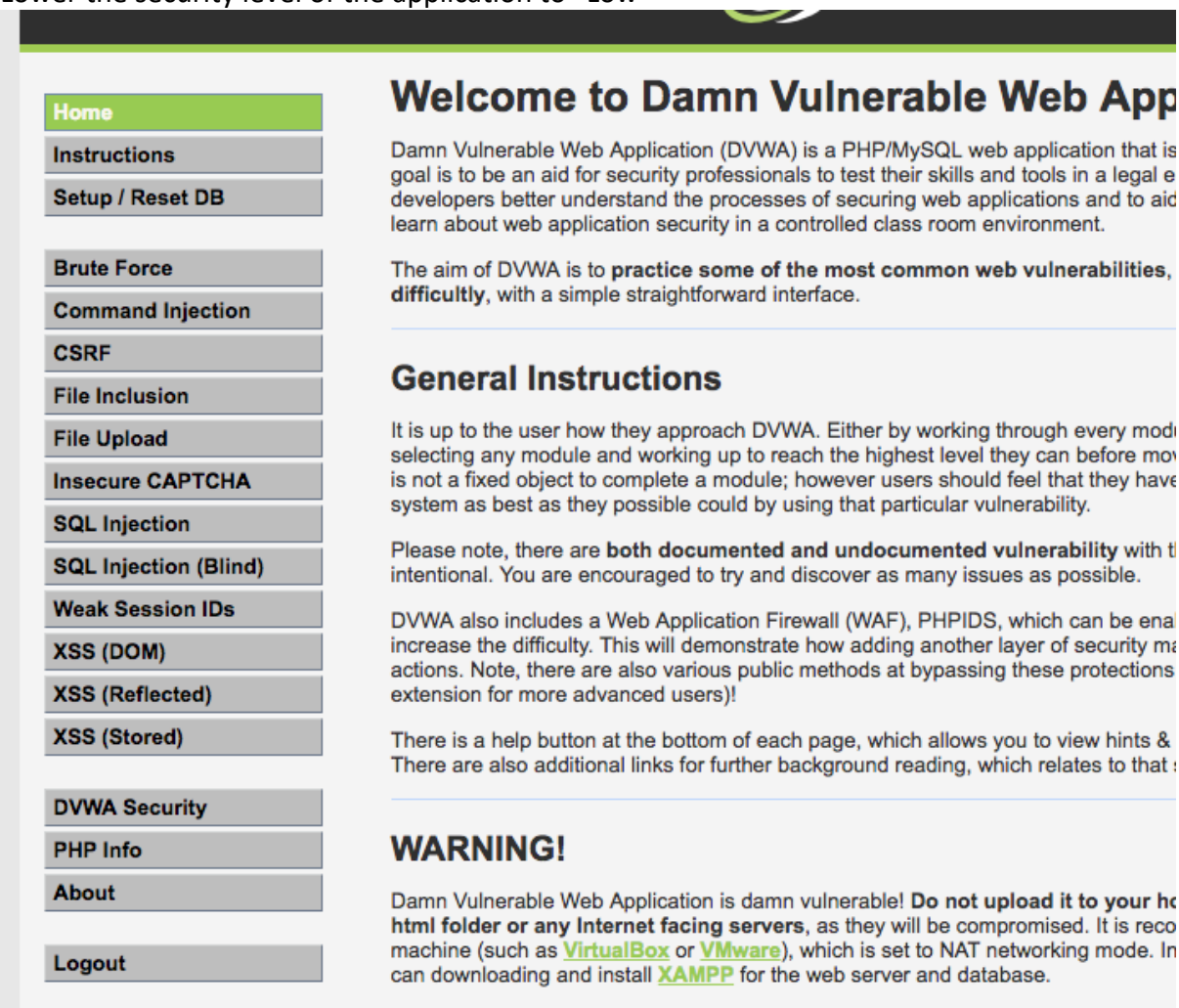
[User: root] Writable folder /var/www/html/dvwa/hackable/uploads/: Yes
[User: root] Writable file /var/www/html/dvwa/external/phpids/0.6/lib/IDS/tmp/phpids_log.txt: Yes

***Status in red**, indicate there will be an issue when trying to complete some modules.*

Create / Reset Database

Login to the application using admin / password credentials

Lower the security level of the application to “Low”



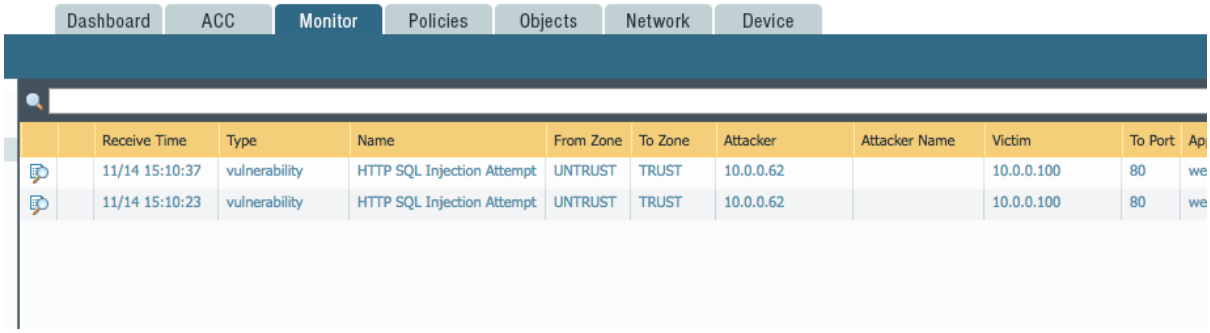
Next generate Threats using the SQL Injection tab

Details of SQL injection attacks that can be performed can be found here https://www.computersecuritystudent.com/SECURITY_TOOLS/DVWA/DVWAv107/lesson6/index.html

For simplicity use `%' or '0'='0`

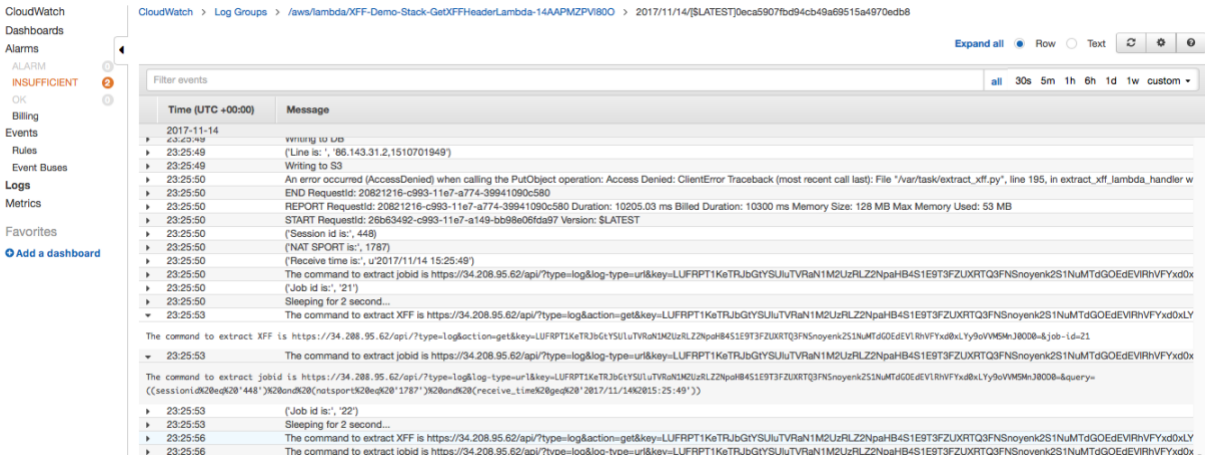
The firewall should block the attack and the browser will return a 502 bad Gateway error.

Check the firewall for threat logs

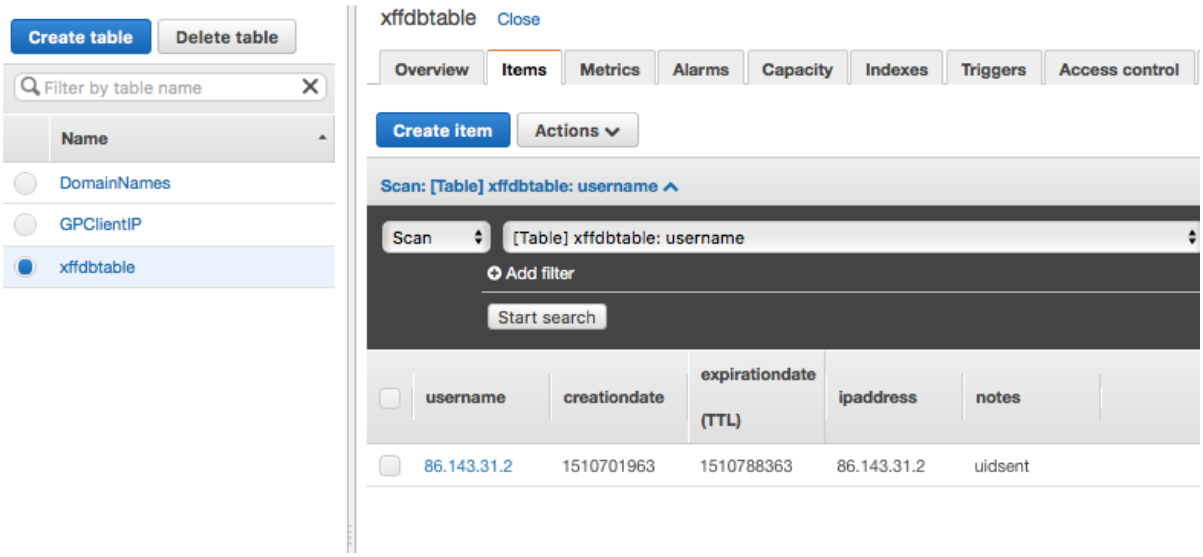


Check the cloudwatch logs.

If the threat log has been forwarded and processed logs will appear in cloudwatch under the log group corresponding to the lambda function



Checking DynamoDB should show the IP address in the database



If the notes column indicates uidsent then the username IP has been sent to the firewall

```
admin@aws-test-drive-fw> show user ip-user-mapping all

IP              Vsys   From    User                            IdleTimeout(s) MaxTimeout(s)
--------------- ------ ------- ------------------------------- -------------- -------------
86.143.31.2     vsys1  XMLAPI  86.143.31.2                     711            711
Total: 1 users

admin@aws-test-drive-fw>
```

You should now receive a block page from the original URL