Fortinet XPA2023 - ZTNA Track

Hands-On Lab

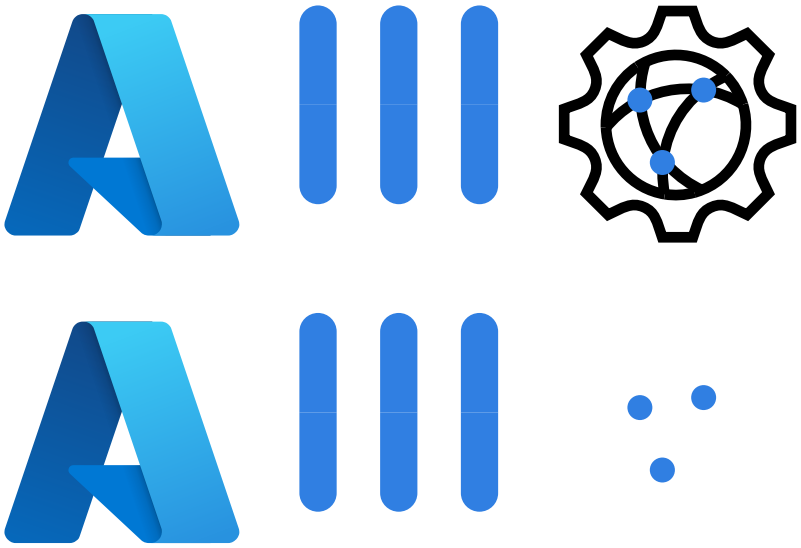
Fortinet Canada CSE Team

Last Update November 2023

Table of contents

1. Hands-On Lab: Fortinet Azure Blueprint

1.1 Comparative Analysis of Azure NSG, FortiGate, and FortiWeb for Web Application Security



1.2 Introduction

Welcome to this hands-on lab experience, designed to give you practical insights into protecting your Damn Vulnerable Web Application (DVWA). This exercise is divided into two distinct labs, each exploring different security solutions.

1.3 Lab 1: Exploring Network Security with Azure NSG and FortiGate

In the first lab, we will explore Azure Network Security Groups (NSG) and FortiGate functionalities to establish a secure environment for your DVWA application. The aim of this section is not only to demonstrate how these tools operate and can be fine-tuned for application security, but also to highlight their limitations. By examining the differences between NSG and FortiGate, we set the stage for the second lab focused on FortiWeb, which provides a more comprehensive security solution.

Components

- Azure Network Security Groups (NSG)
- FortiGate Firewall
- DVWA Web Application

1.4 Lab 2: Enhancing Web Application Security with FortiWeb

The primary objective of this second lab is to introduce the various security measures available for protecting web applications. You will gain firsthand experience in implementing these tools and will have the opportunity to compare their effectiveness, with a focus on demonstrating FortiWeb's superior protection capabilities compared to previous solutions.

Components

- FortiWeb Web Application Firewall
- DVWA Web Application

1.5 Network topology

There are multiple ways to install **FortiGate**, **FortiWeb** and **DVWA**. In this document, we will utilize a predefined template available for Azure:

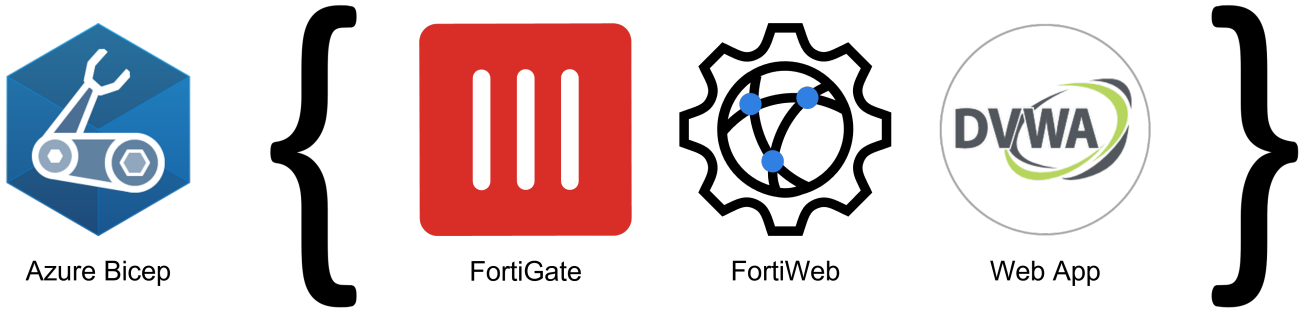
The Fortinet Reference Architecture for Azure

This template automatically deploys a **FortiGate** cluster, a **FortiWeb** cluster, and a **DVWA** instance, along with a predefined policy, enabling you to begin the demo immediately.

What is Fortinet Reference Architecture for Azure?

This architecture provides users with templates that deploy and preconfigure a perimeter solution to address dynamic security needs.

It features a **FortiGate** Next Generation Firewall, **FortiWeb WAF**, and **DVWA** Endpoint.



The WAF secures web servers against inbound attacks over HTTP/HTTPS, while the Next Generation Firewall supports various protocols, enabling connectivity, multi-protocol security, and serving as the primary egress mechanism. The FortiGate and FortiWeb solutions complement each other, with FortiWeb offering advanced features for HTTP/HTTPS traffic and FortiGate providing extensive capabilities for other protocols, routing, VPN termination, and SD-WAN.

Network Topology

This Azure BICEP template deploys a secure environment featuring **FortiGate** and **FortiWeb** for traffic inspection. The **FortiGate** setup receives non-HTTP(S) traffic, while **FortiWeb** handles HTTP(S) traffic, both using user-defined routing (UDR) and public IPs. Additionally, a **Damn Vulnerable Web Application** (DVWA) is included for security testing and learning purposes.

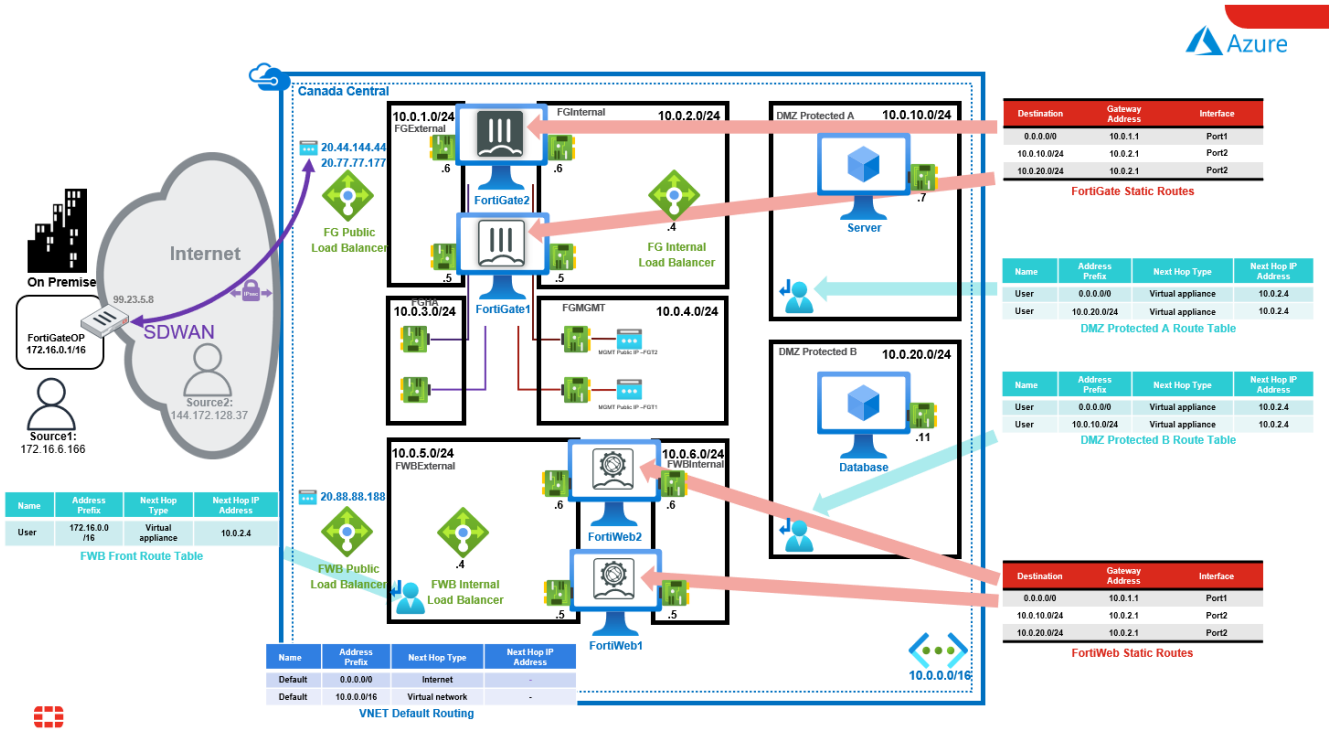
The environment includes:

- 2 x **FortiGate** Firewalls in an active/passive deployment
- 2 x **FortiWeb** WAFs in an active/active deployment
- 2 x Public Azure Standard **Load Balancers** for internet communication (1 x per cluster)
- 2 x Internal Azure Standard **Load Balancers** for forwarding traffic to Azure Gateways connected to ExpressRoute or Azure VPNs
- 1 x **VNET** with 1 protected subnet
- 4 x **Public IPs** for services and FortiGate/FortiWeb management
- **User Defined Routes** (UDR) for end-to-end communication via the FortiGate/FortiWeb deployment

VMs can be installed in different **Availability Zones** or **Availability Sets** for enhanced availability.

These templates can also be **extended** or **customized** based on your requirements, such as adding additional subnets and routing tables.

Click on the image if you want to enlarge it.

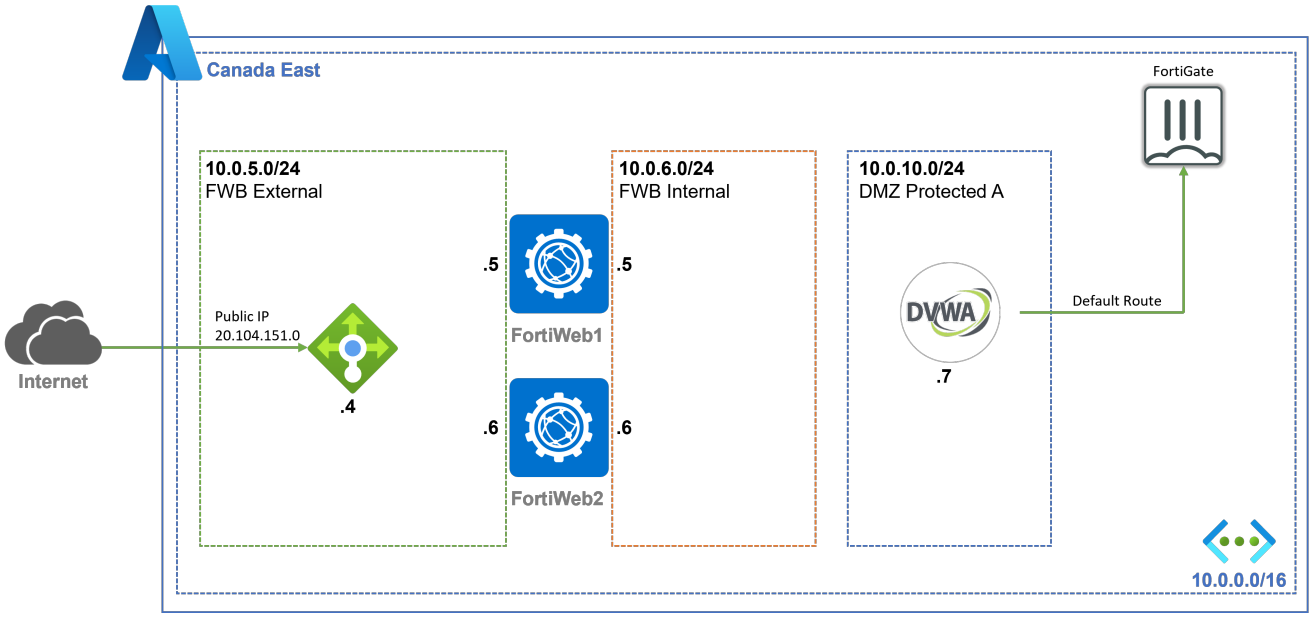


FortiWeb Deployment

FortiWeb is deployed with **2 interfaces** as an **active-active** cluster in **reverse proxy mode**.

- Web browsers connect to the public IP on Azure's Standard Load Balancers.
- FortiWeb decrypts and inspect the HTTP traffic, then forwards it to the DVWA via its internal IP
- Return packets are directed back to FortiWeb's internal IP.
- For DVWA OS updates or SSH connections, traffic is routed through FortiGate.

Click on the image if you want to enlarge it.



2. Getting Started

2.1 Accessing your Azure Account

This Hands-on-Lab is configured to allow each student to have their own training lab environment using pre-created Azure resource groups, all in one shared Azure Subscription.

Accessing the Azure Portal: Login Instructions

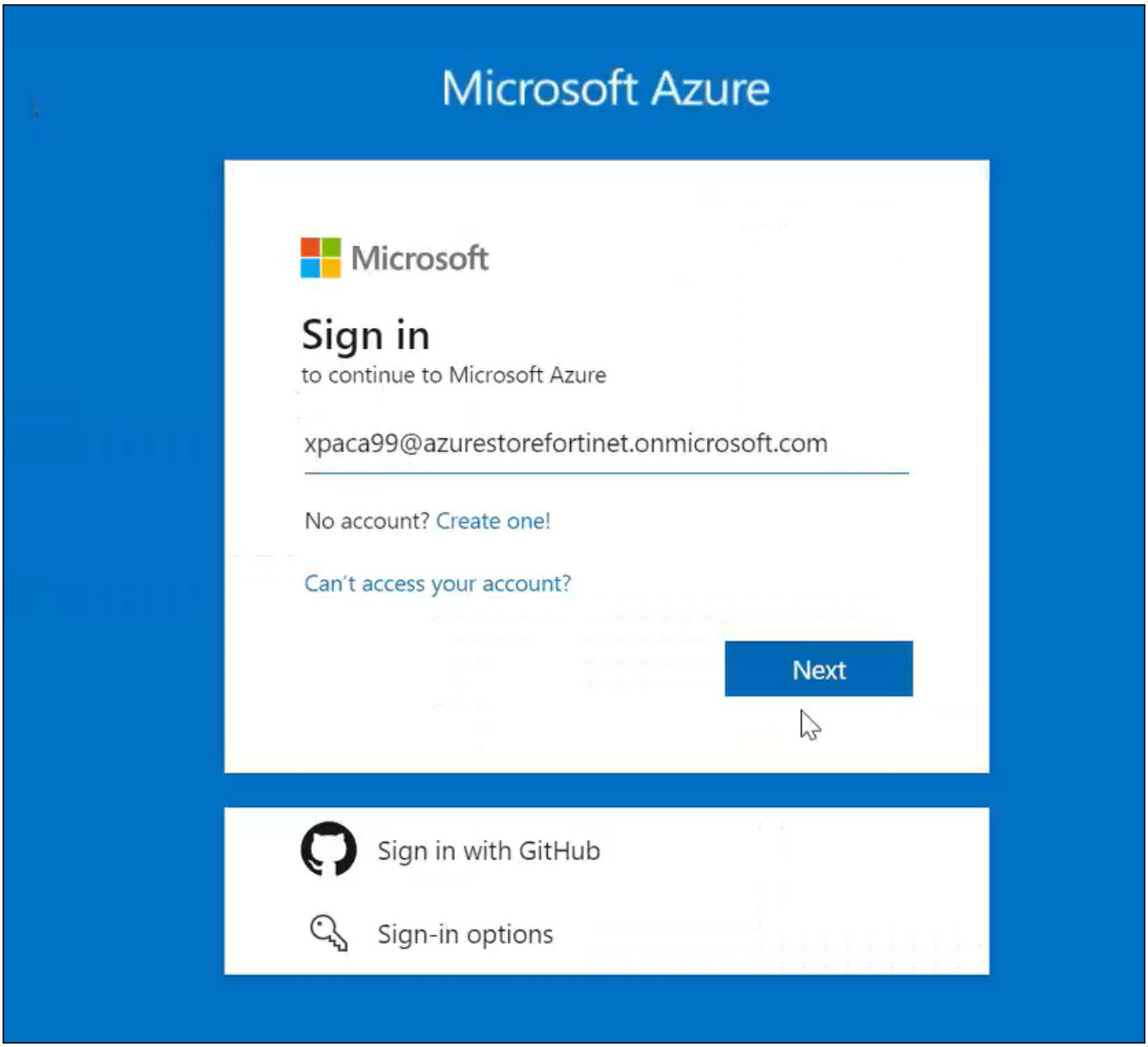
Accessing the Azure Portal

Browse to https://portal.azure.com

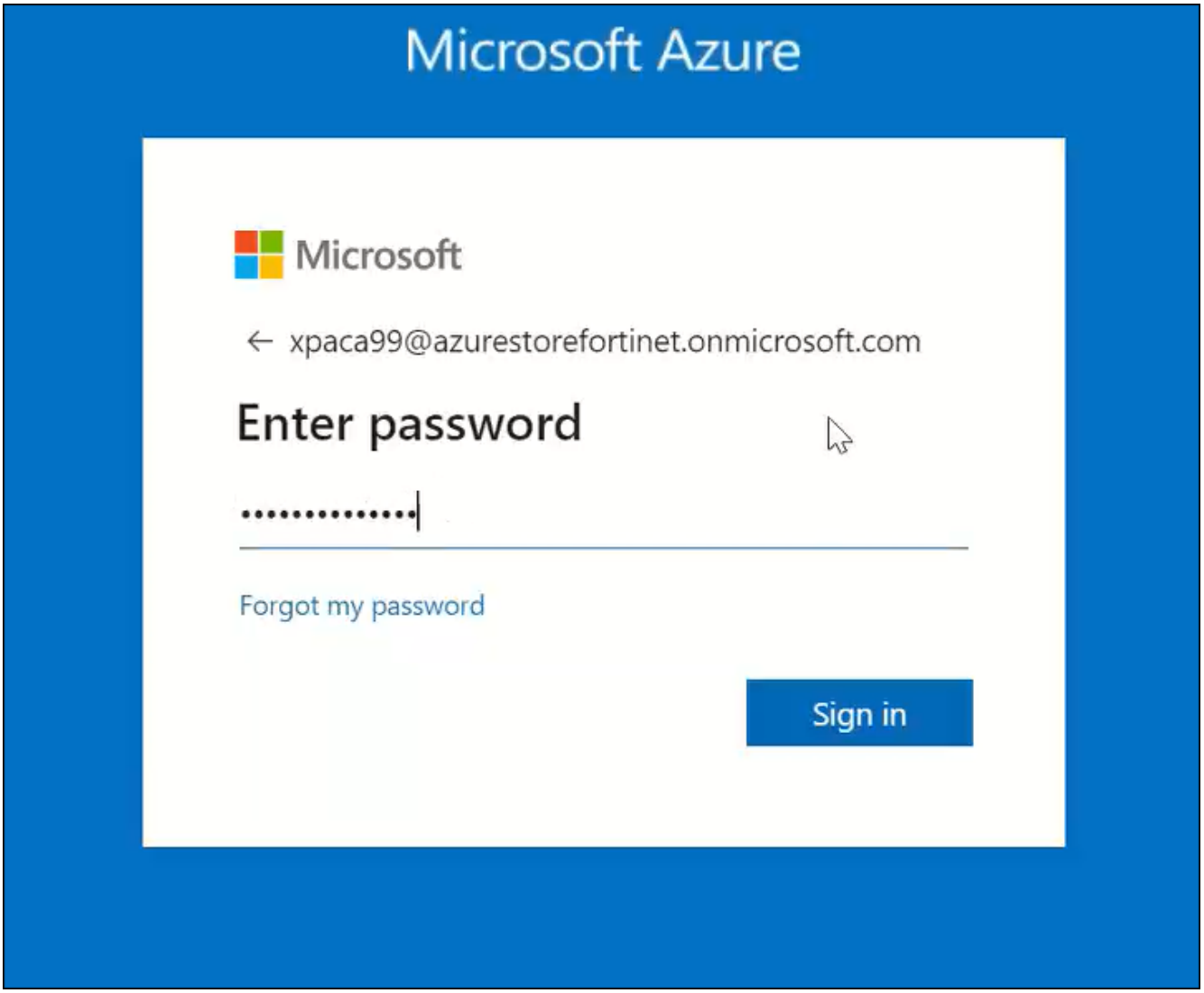
Use the credentials provided to you by your instructors.

If you can't find them, check your junk mail folder. Look for an email with the subject line: **MIS - Xperts Summit - Public Cloud Track - AZURE LAB Credentials**.

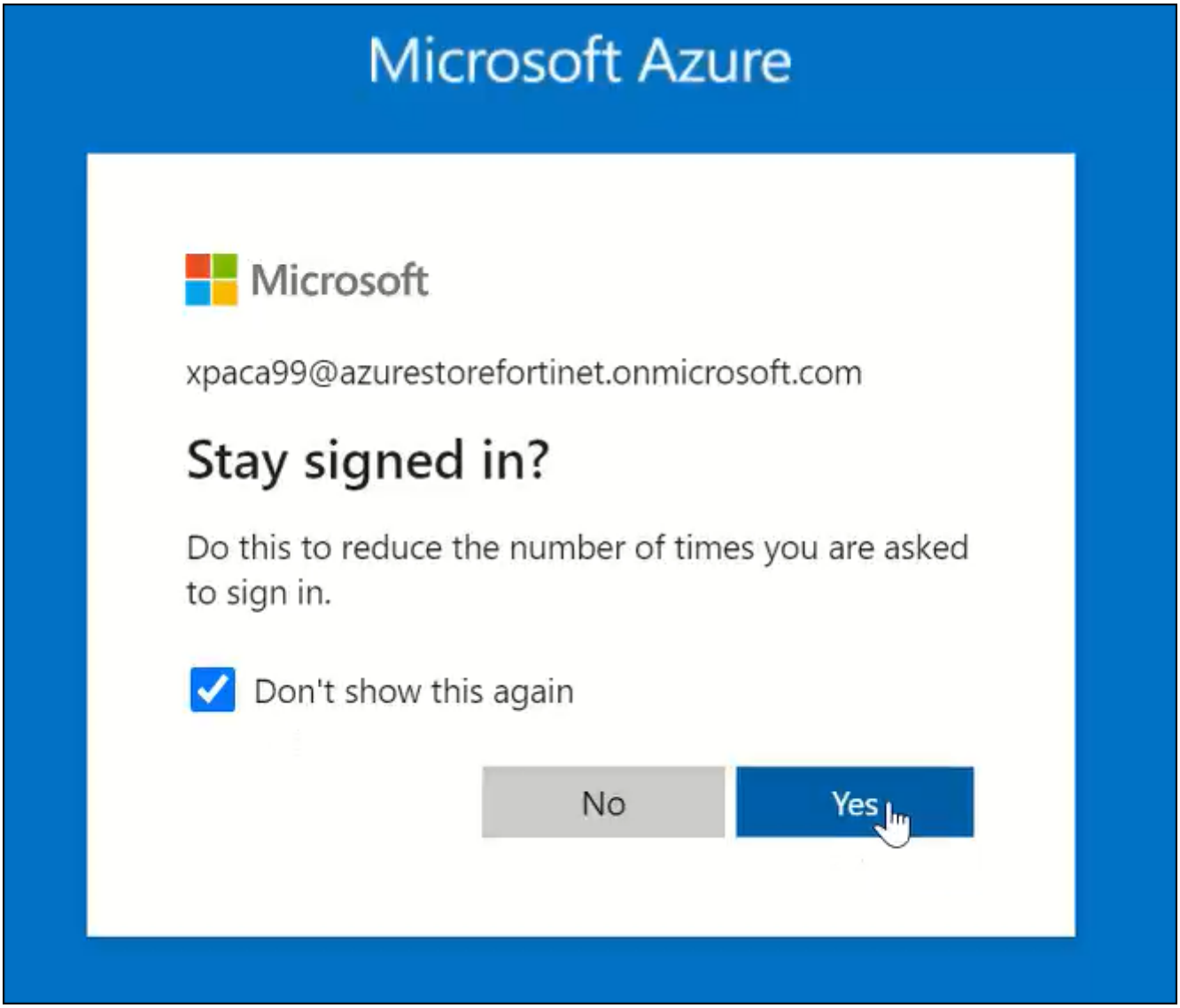
Username: xpaca**XX**@azurestorefortinet.onmicrosoft.com



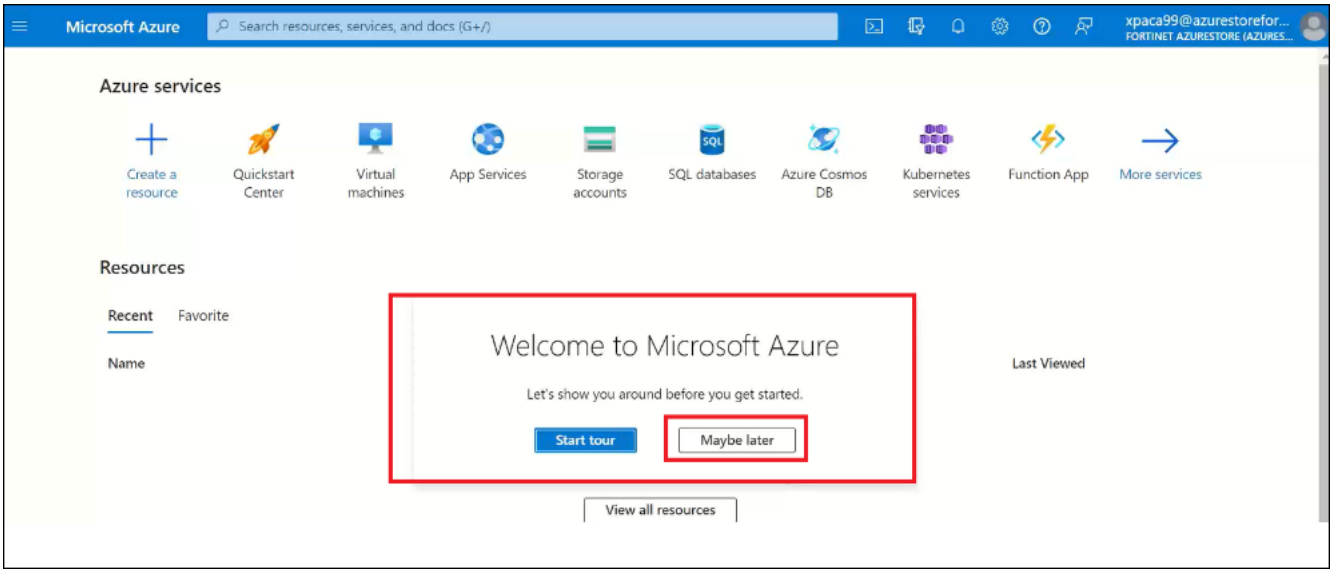
Password: *<password provided by email>*



Click to log in, and optionally select "Yes" to stay signed in.



When the **Welcome to Microsoft Azure** window appears, skip the tour.



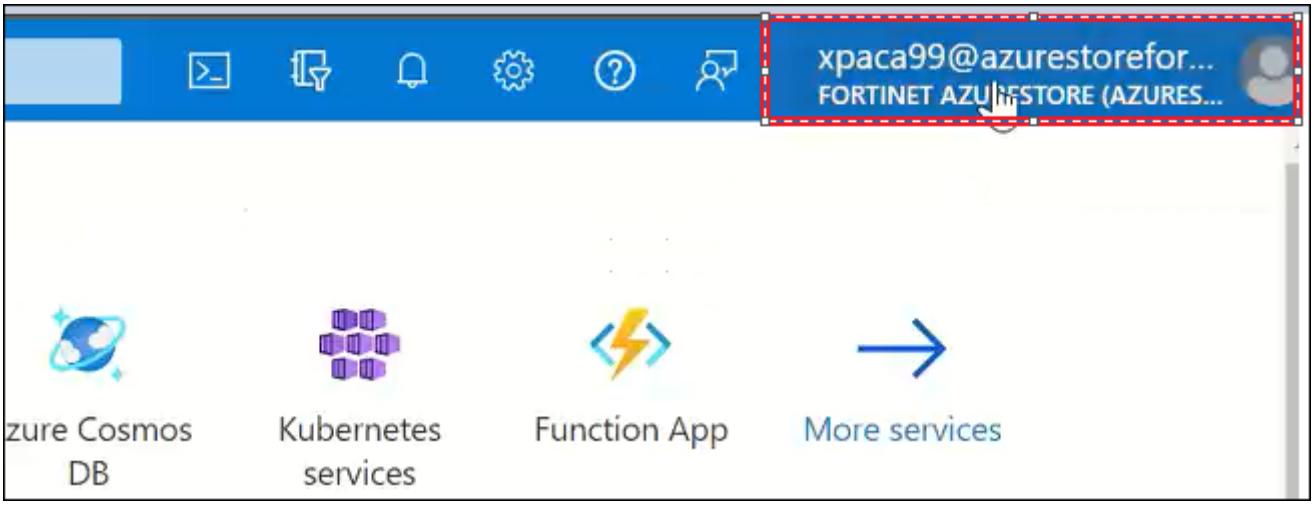
Now that you've signed in, you are on the Azure Portal Dashboard.

Notice your **username** in the top right corner.

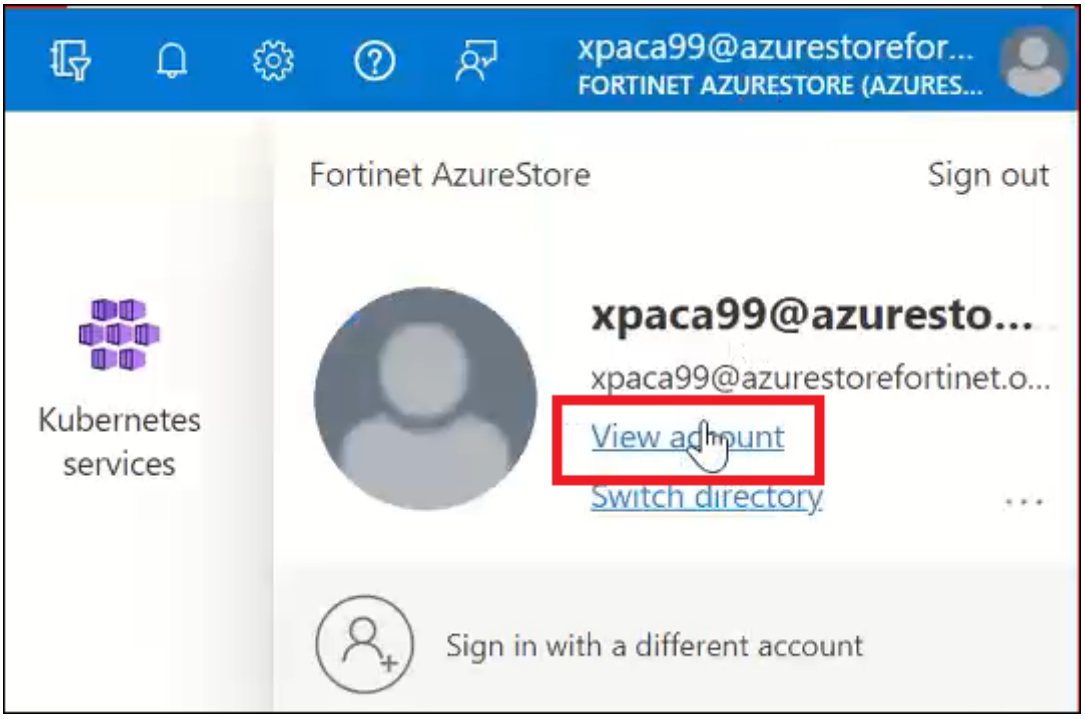
Changing Your Password

Changing Your Password

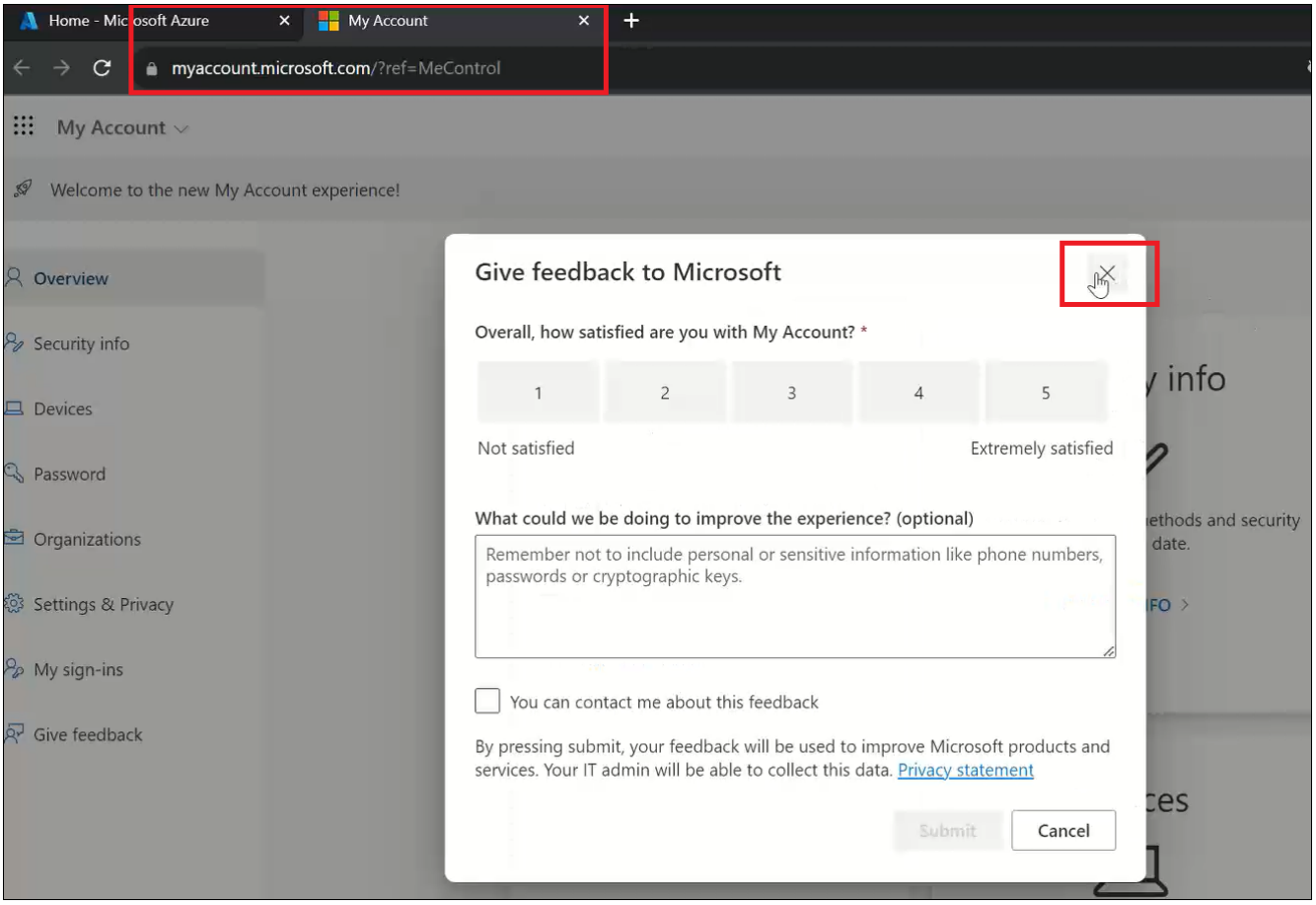
Click on your **username** located in the top-right corner of the screen.



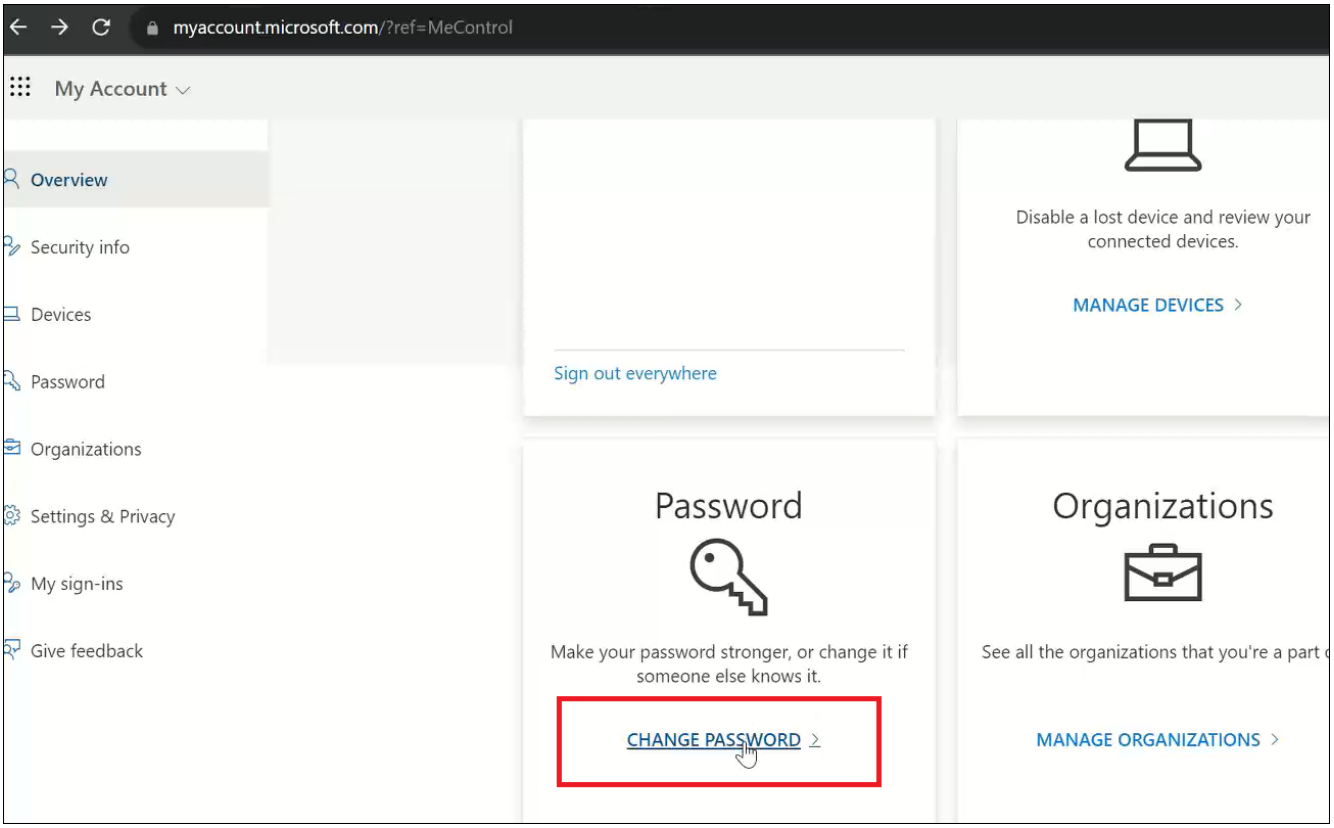
Select **View Account**. This action will automatically open a new tab.



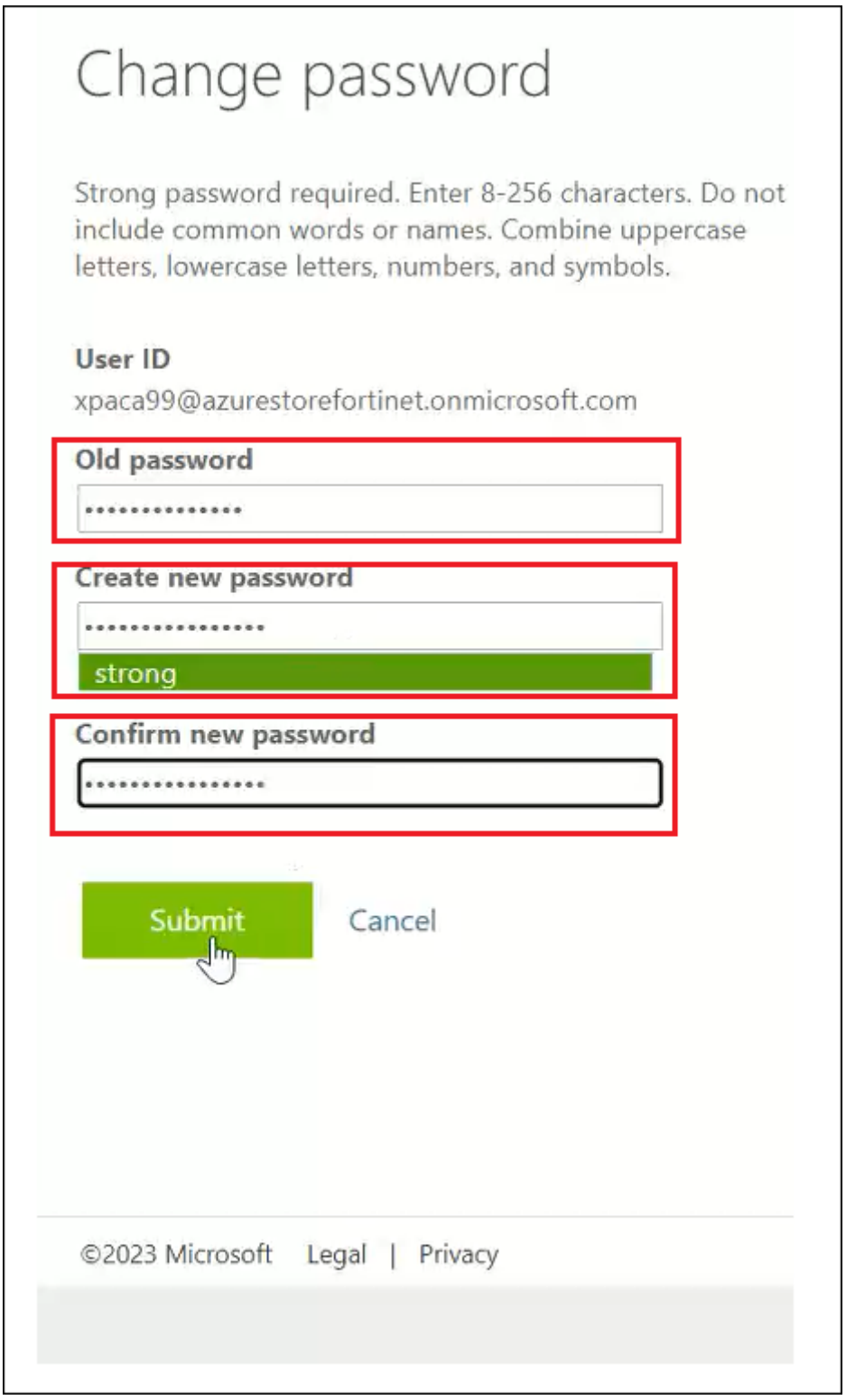
You can skip the Microsoft feedback in this new tab.



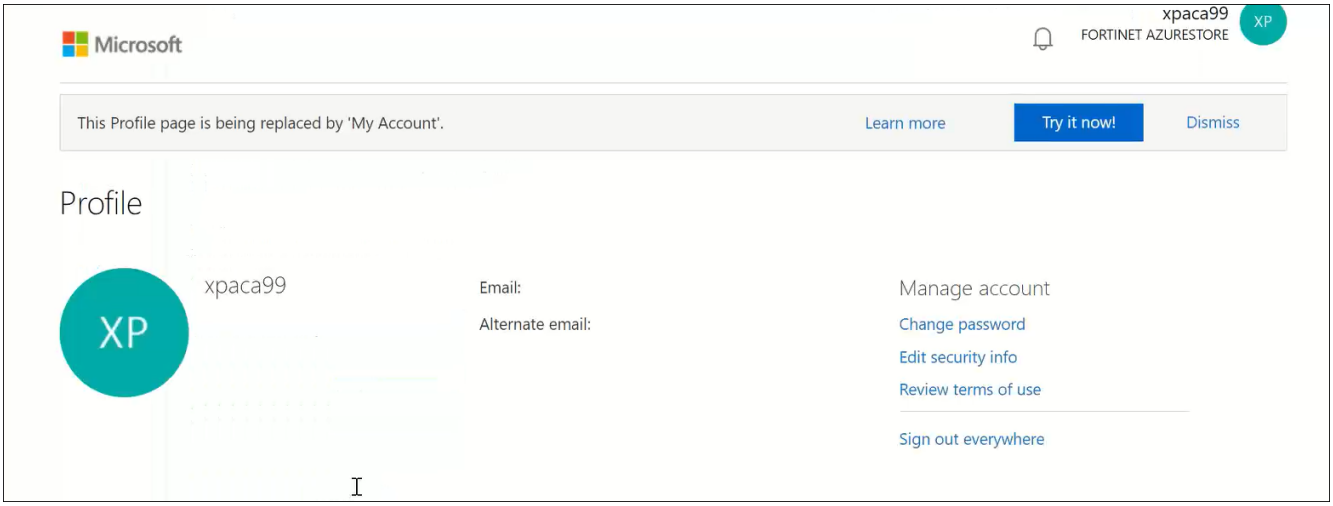
Scroll down, if needed, and click on **Change Password**.



Fill in the required fields to change your password and click **Submit**.



Once you see the confirmation screen, you can close this tab. Your password has been successfully changed.

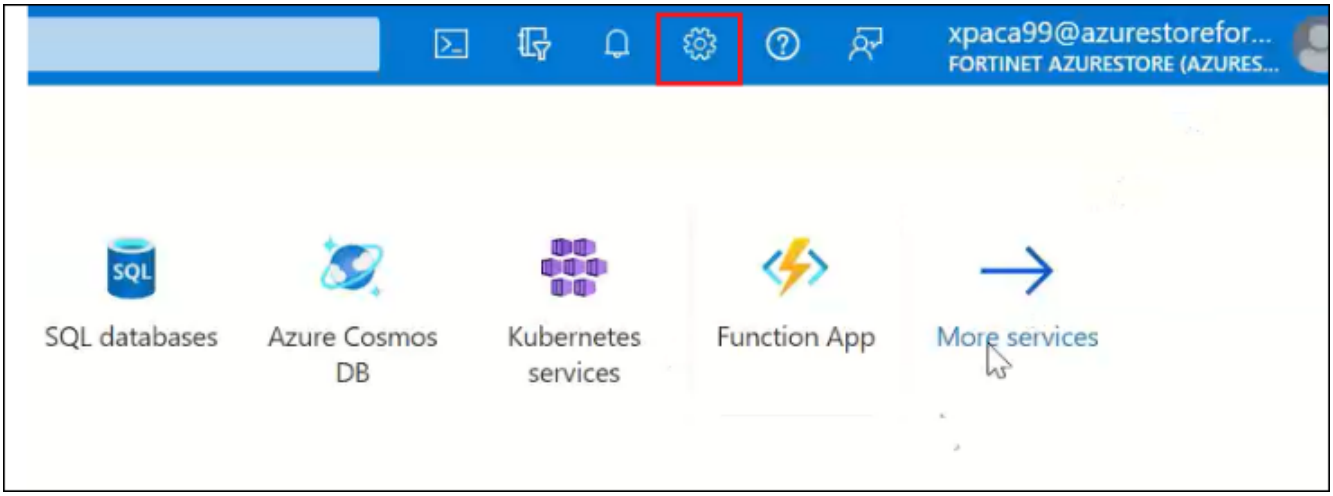

Microsoft
xpaca99
FORTINET AZURESTORE
XP
This Profile page is being replaced by 'My Account'.
Learn more
Try it now!
Dismiss
Profile
XP
xpaca99
Email:
Alternate email:
Manage account
Change password
Edit security info
Review terms of use
Sign out everywhere

Switching Language Settings

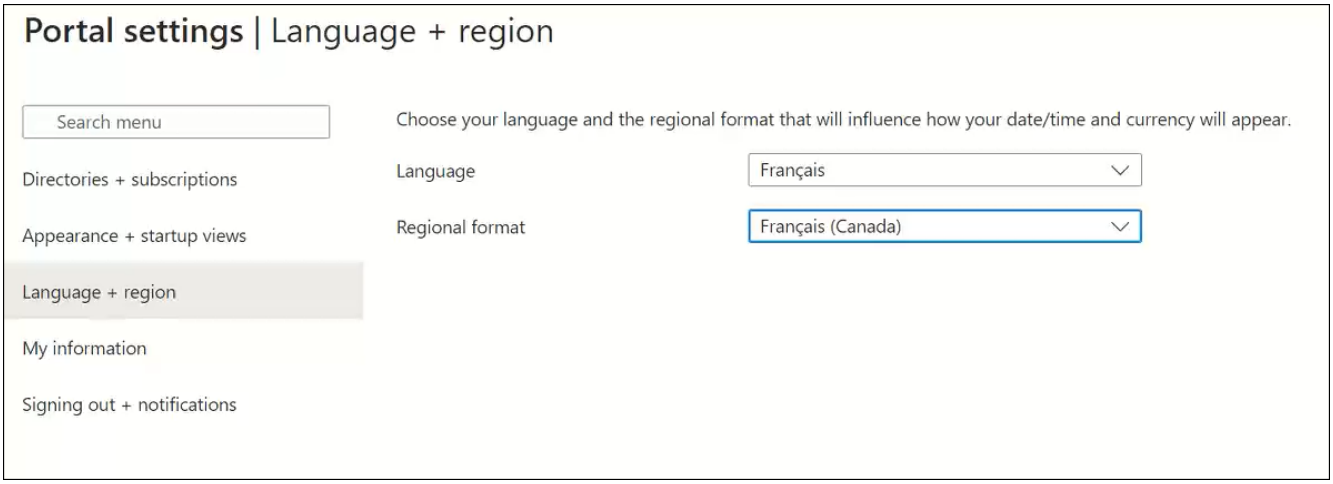
Switching Language Settings

If you wish to change the language of your Azure dashboard, follow these steps.

After logging into your Azure account, click on the **gear icon** in the upper-right corner.

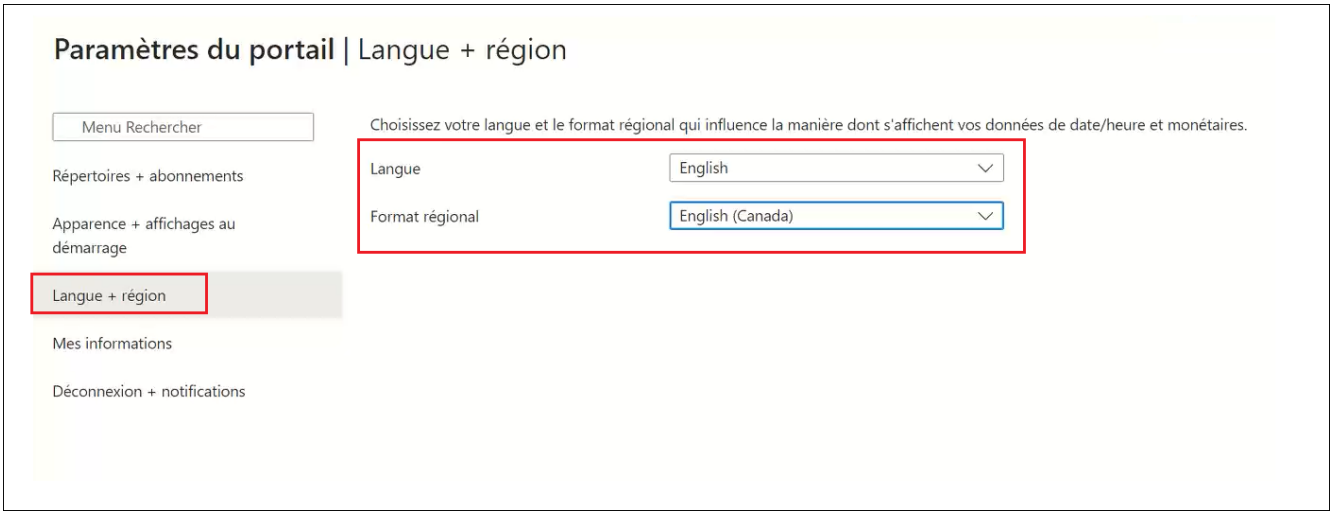


Next, select **Language + Regional Format**.

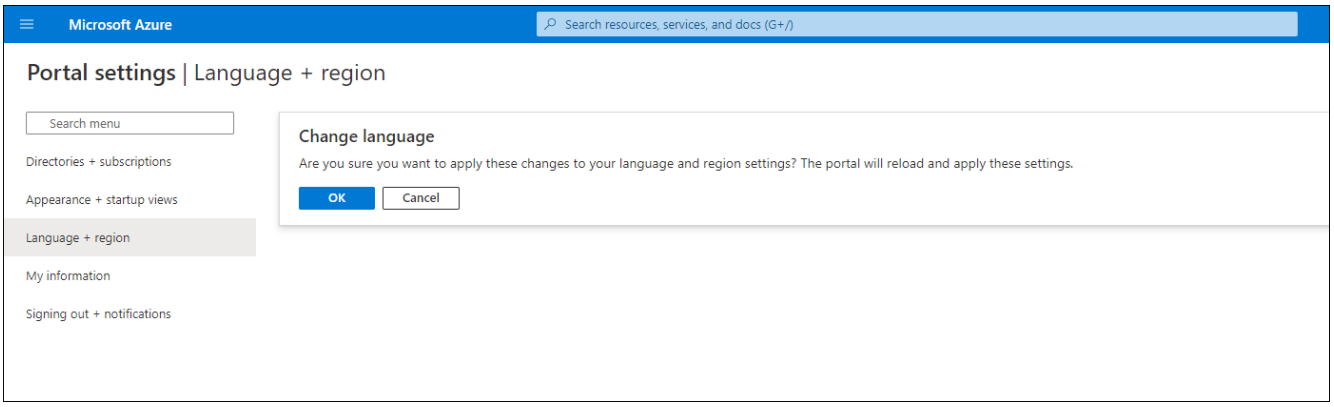


Choose your preferred language and regional format.

For example, if you select “English (Canada)," it will change the Dashboard language to Canadian English.



Click **Apply**. A message will appear asking for confirmation. Click **OK** to confirm the language change.

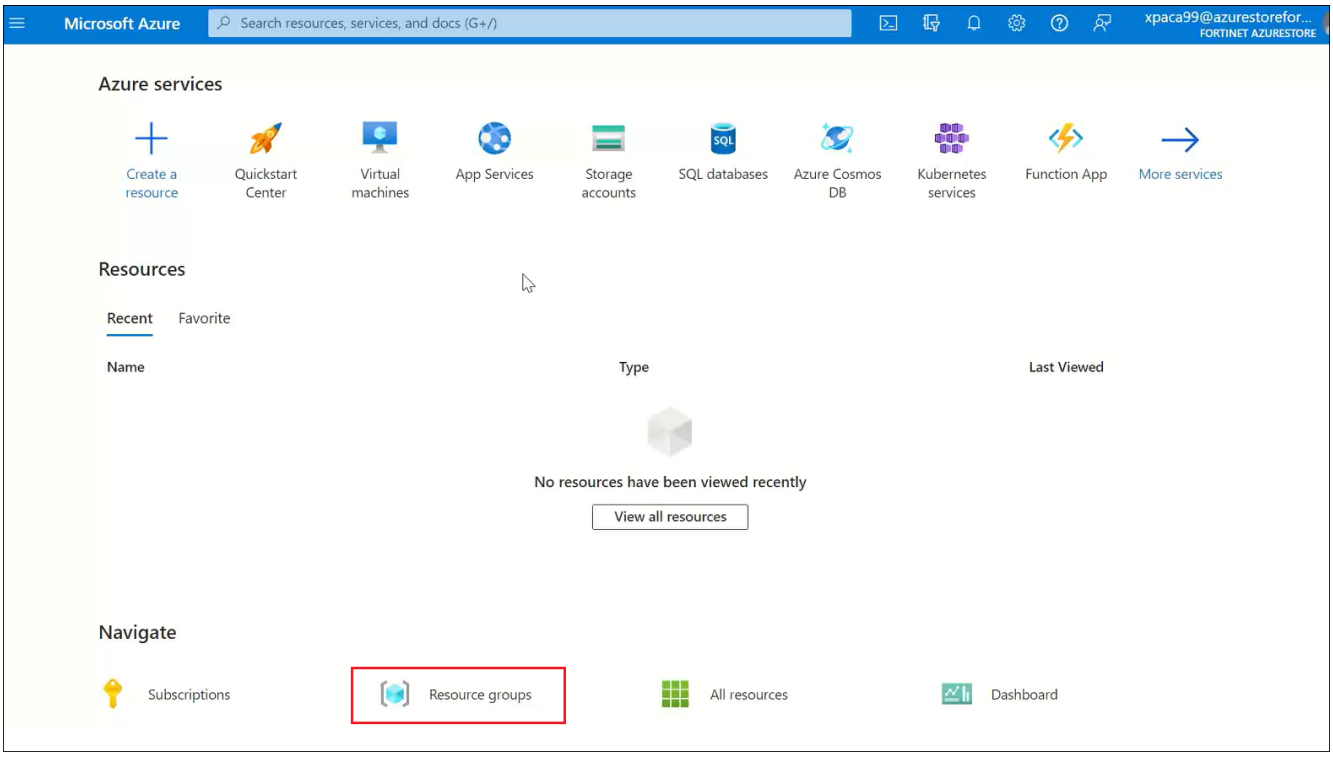


Verifying Resource Groups

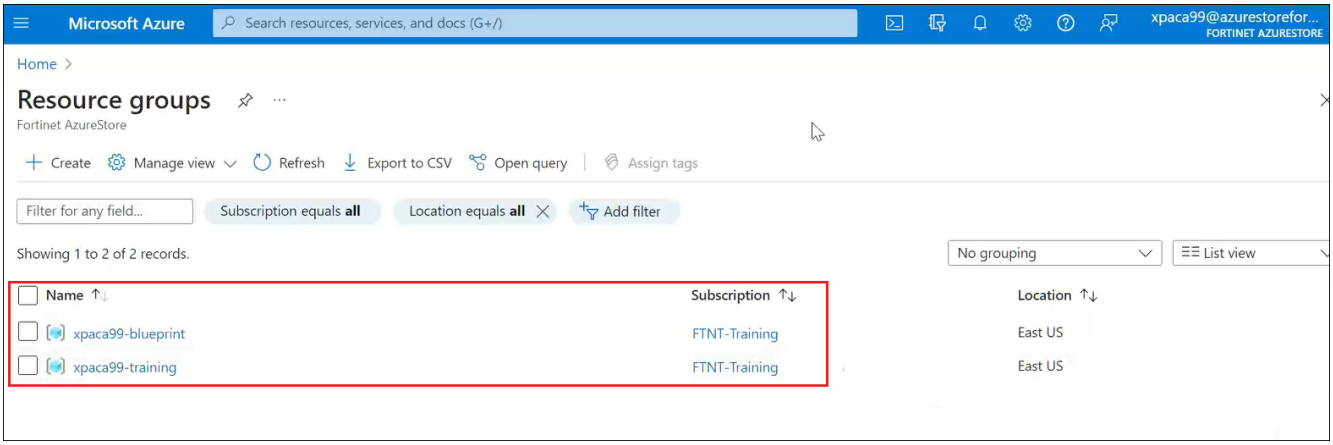
Verifying Resource Groups

In a new Azure subscription account, only two resource groups will be pre-existing. These will be used in this lab for security customization.

Navigate to **Resource Groups** on the main page.



Make sure **two** resource groups are displayed, prefixed with your student number.

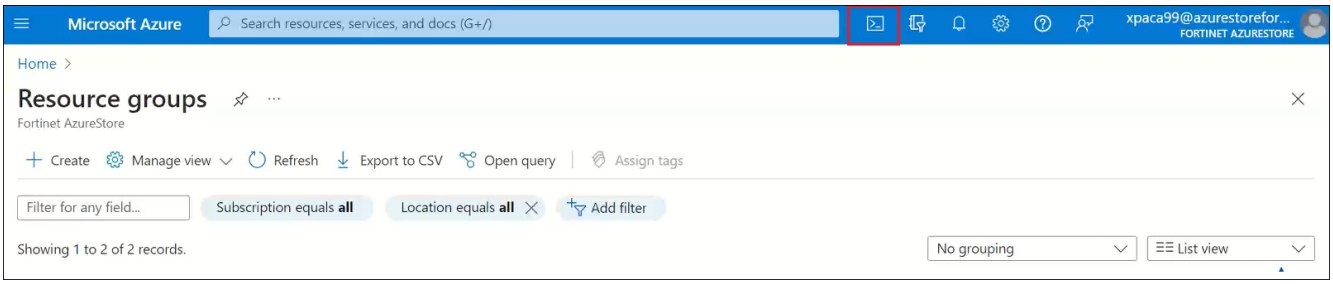


Launching CLI & Setting Up Storage Account (mandatory)

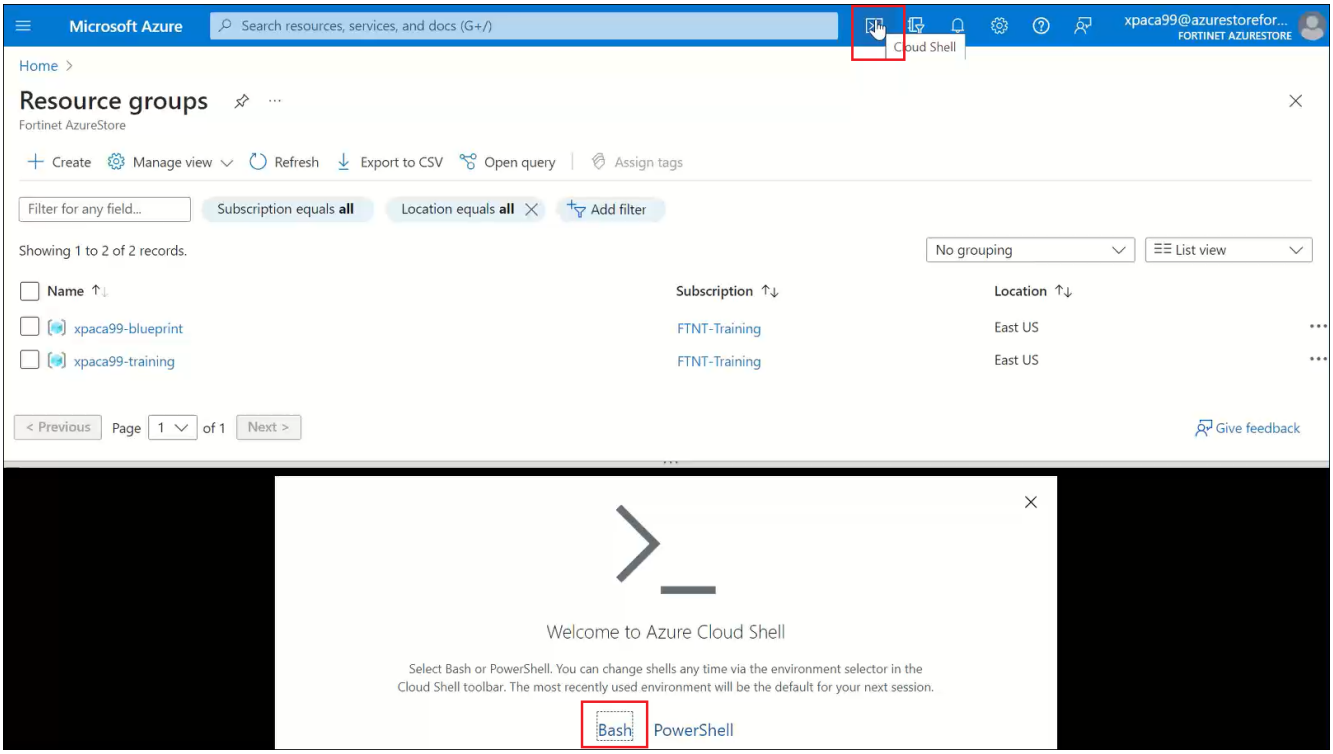
Launching CLI & Setting Up Storage Account

We'll next connect to the **Azure CLI**, which plays a key role in facilitating automated deployments. To do this, you'll need to have a storage account configured.

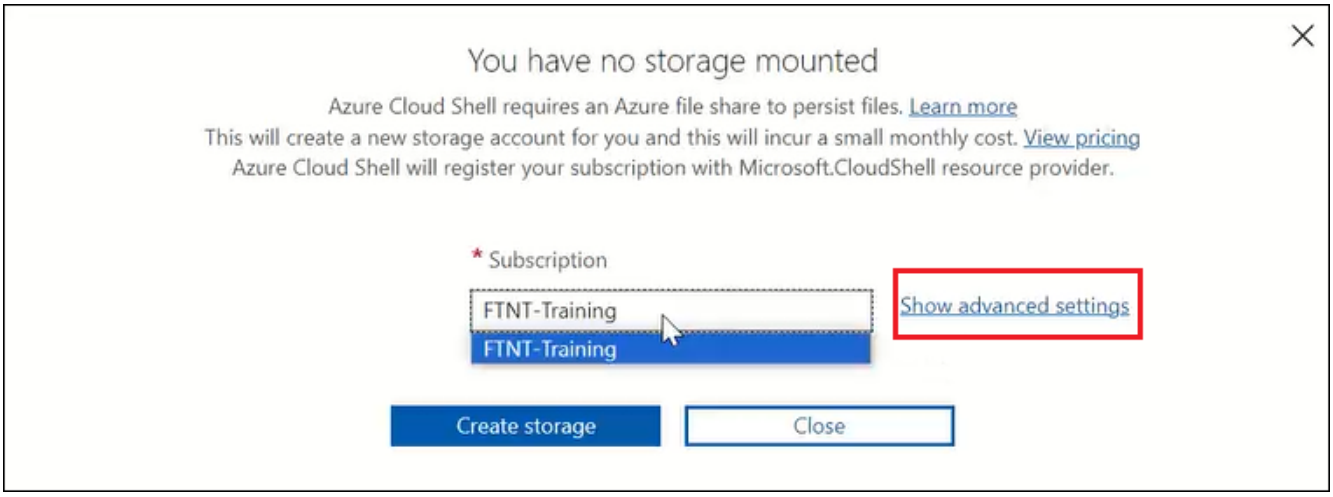
Click on the **CLI Icon**, found in the top-right corner.



This will open the CLI Shell at the bottom of the screen. Select **Bash Shell**.



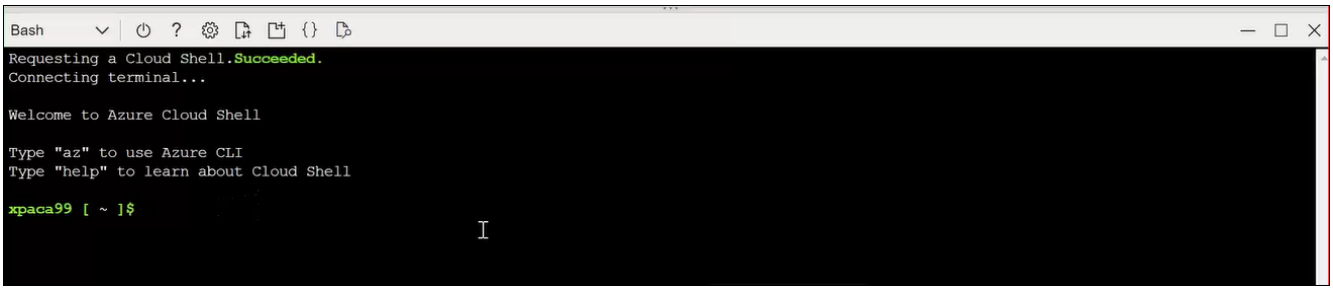
Select your **FTNT-Training** subscription and click on **Show Advanced Settings**.



These advanced settings allow you to select existing resources. Note that the default settings may not align with where our Resource Groups are located.

Adjust your settings to match the example below. **Note**: Your student number may differ.

You are now welcomed to the *Azure Cloud Shell*.



Congratulation! You are all set to proceed with the lab activities.

2.2 Your Lab Environment

The accounts provided as a part of **Fortinet XPERTS Academy** have adjusted resource quotas to reflect the demands of this Hands on Lab. The subcription has also accepted the terms of the required marketplace offers.

Deploying your Lab Environment in Azure

This section will guide you through the essential steps to deploy your Lab Environment in Azure with the Fortinet Reference Architecture for Azure.

Tip

Click on the images to view them in a larger format.

Define your Prefix, Region and Ressource Groupe Name

Before you proceed, complete the form below to personalize your Hands-on Lab experience by setting your **Prefix**, **Region**, and **Resource Group Name**.

Prefix:

xpacaXX

This prefix will be applied to all resources created during this lab for easier management and identification. Your prefix will be **xpacaXX** where **XX** is your student number.

Region:

eastus

You need to choose the **eastus** region (Richmond, Virginia) because this is where our Lab Quota is available. Outside of this HOL session, you could select any region in Canada such as **canadacentral** (Toronto, Ontario) or **canadaeast** (Quebec City, Quebec).

Resource Group Name:

xpacaXX-blueprint

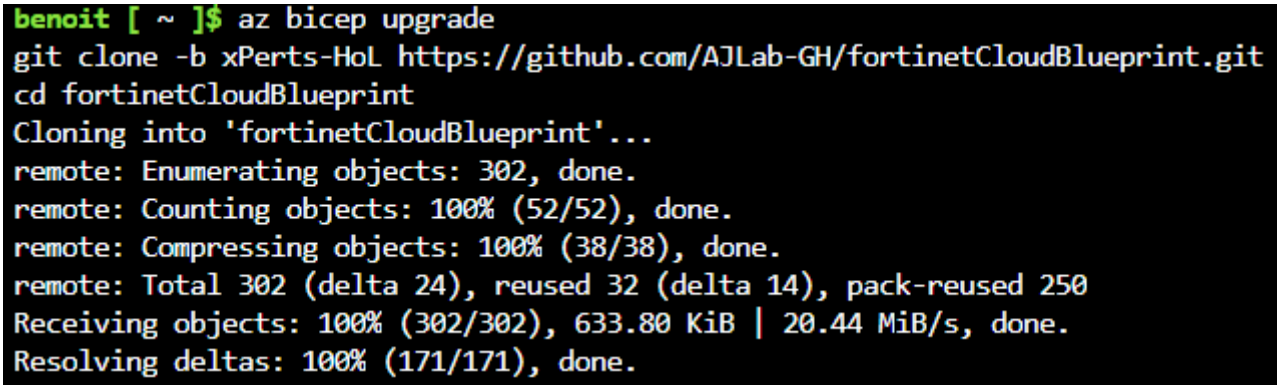
This will be the name of the Azure Resource Group where all your lab resources will be contained. Your Azure Resource Group will be **xpacaXX-blueprint** where **XX** is your student number.

Submit

Deploy the Lab Environment with Bicep

- Access the Azure Cloud Shell either through the Azure Portal or directly via https://shell.azure.com.
- Log into the Azure Cloud Shell.
- Run the following commands in the Azure Cloud:

```
az bicep upgrade
git clone -b xPerts-HoL https://github.com/AJLab-GH/fortinetCloudBlueprint.git
cd fortinetCloudBlueprint
```



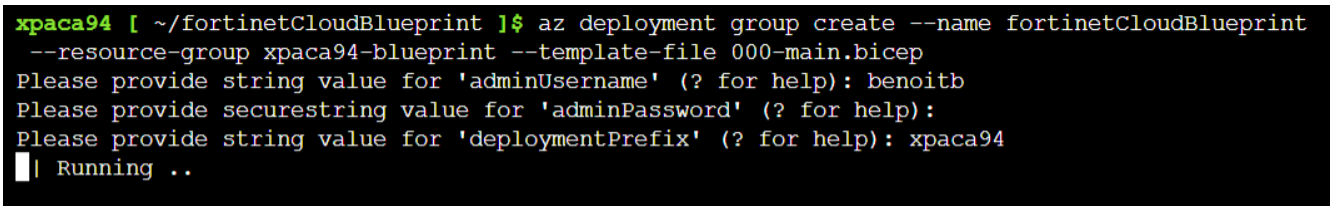
- Deploy the template

```
az deployment group create --name fortinetCloudBlueprint --resource-group @RESOURCE_GROUP_NAME --template-file 000-main.bicep
```

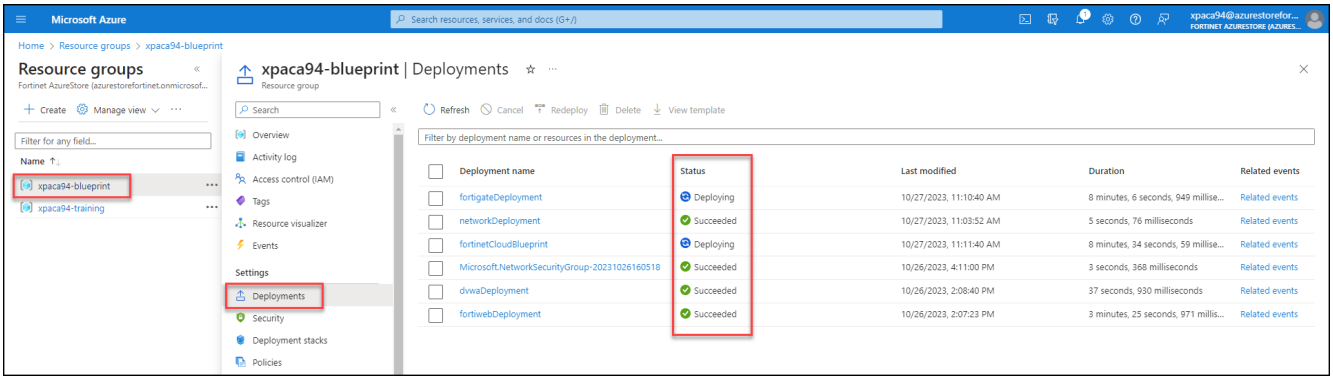
- When you execute the script, it will prompt you with a few questions to configure the necessary settings for deployment. You'll need to provide answers for these specific settings.

Parameter	Description	Requirements
USERNAME	The username you provide will grant you access to the FortiGate / FortiWeb GUI and SSH management interface. This username can differ from your Azure account username.	Username **admin** is **not** allowed.
PASSWORD	The password that will be used to log in to the FortiGate / FortiWeb GUI and SSH management interface. It's crucial to use a unique password that hasn't been used elsewhere, as it will appear in plaintext in the bootstrap process.	At least 12 characters long and must include characters from at least three of the following categories: uppercase, lowercase, numbers, special characters (excluding '\' and '-').
PREFIX	Enter **@PREFIX**. It will be applied to all the resources created to make them easier to manage, use, and identify.	Needs to be **unique**.

- To proceed, please enter the necessary variables when prompted.



- Deployment can take up to 15 minutes. Time for a coffee break, maybe even two.
- While the template is deploying, you can monitor its progress by navigating to the resource group **@PREFIX-blueprint** and selecting the **Deployments** menu.



- After deployment, you can output essential information such as public IP addresses that you will need to connect to your deployment:

```
az deployment group show -g @RESOURCE_GROUP_NAME -n fortinetCloudBlueprint --query properties.outputs
```

```
xpaca94 [ ~ ]$ az deployment group show -g xpaca94-blueprint -n fortinetCloudBlueprint --query properties.outputs
{
  "dvwaHTTPviaFortiGate": {
    "type": "String",
    "value": "http://xpaca94-fgt-to-dvwa.eastus.cloudapp.azure.com:80"
  },
  "dvwaHTTPviaFortiWeb": {
    "type": "String",
    "value": "http://xpaca94.eastus.cloudapp.azure.com:80"
  },
  "dvwaSSHviaFortiGate": {
    "type": "String",
    "value": "4.157.173.242:22"
  },
  "fortiGateAManagementConsole": {
    "type": "String",
    "value": "https://4.157.173.231:443"
  },
  "fortiGateBManagementConsole": {
    "type": "String",
    "value": "https://4.157.173.238:443"
  },
  "fortiWebAManagementConsole": {
    "type": "String",
    "value": "https://xpaca94.eastus.cloudapp.azure.com:40030"
  },
  "fortiWebBManagementConsole": {
    "type": "String",
    "value": "https://xpaca94.eastus.cloudapp.azure.com:40031"
  }
}
```

Connect to FortiWeb

Once the deployment is complete, use the following **URLs** and **ports** to connect to your instances:

Instance	HTTPS Ports	SSH Ports
FWB-A	https://@PREFIX.@REGION.cloudapp.azure.com:40030	50030
FWB-B	https://@PREFIX.@REGION.cloudapp.azure.com:40031	50031
DVWA	https://@PREFIX.@REGION.cloudapp.azure.com:443	N/A

FAQ

Why is it hard to predict which FortiWeb unit will handle my traffic?

Traffic is distributed across both FortiWeb units, FWB-A and FWB-B. Due to this load-balancing mechanism, it's unpredictable to determine in advance which unit will manage a particular flow of traffic. That is said, we have enabled **connection persistence** on the external Azure Load Balancer. This ensures that once you've identified the correct FortiWeb unit, your traffic should consistently be managed by that unit.

What should I do if I find the traffic log empty?

If the traffic log is empty on one of the FortiWeb units, you'll need to log in to the other unit to see if the traffic is being managed there.

Why do I get logged out of one GUI when logging into the other?

Both FortiWeb units share the same domain and, consequently, the same cookies. Logging in to one GUI will overwrite the cookie for the other, automatically logging you out.

How can I stay logged into both GUIs simultaneously?

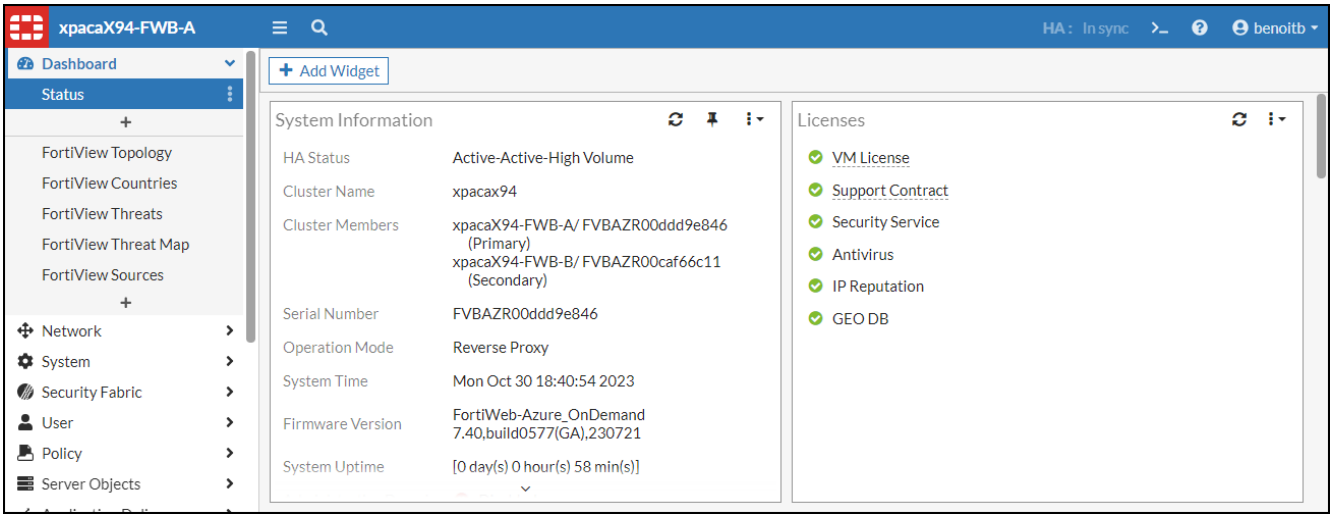
If you wish to keep both GUIs open at the same time, you will need to use two different web browsers. This will allow you to maintain separate sessions for each FortiWeb unit.

You can use the az **deployment group show** command to display all resources along with their URLs and ports.

```
az deployment group show -g @RESOURCE_GROUP_NAME -n fortinetCloudBlueprint --query properties.outputs
```

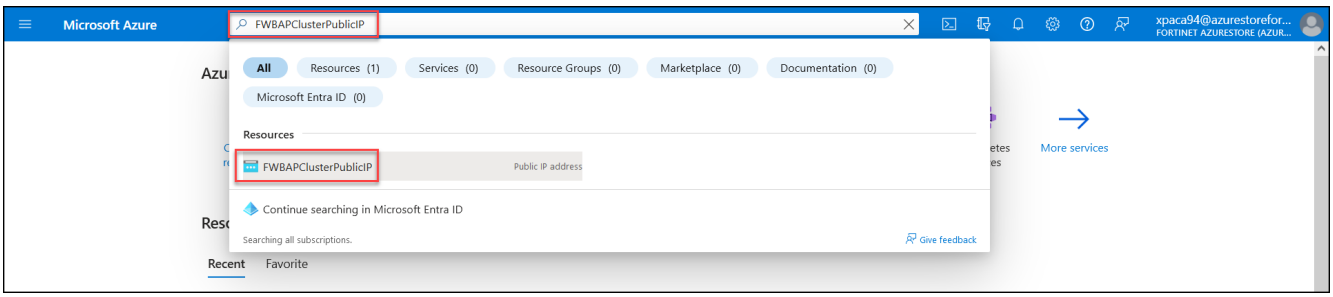
```
xpaca94 [ ~ ]$ az deployment group show -g xpaca94-blueprint -n fortinetCloudBlueprint --query properties.outputs
{
  "dvwaHTTPviaFortiGate": {
    "type": "String",
    "value": "http://xpaca94-fgt-to-dvwa.eastus.cloudapp.azure.com:80"
  },
  "dvwaHTTPviaFortiWeb": {
    "type": "String",
    "value": "http://xpaca94.eastus.cloudapp.azure.com:80"
  },
  "dvwaSSHviaFortiGate": {
    "type": "String",
    "value": "4.157.173.242:22"
  },
  "fortiGateAManagementConsole": {
    "type": "String",
    "value": "https://4.157.173.231:443"
  },
  "fortiGateBManagementConsole": {
    "type": "String",
    "value": "https://4.157.173.238:443"
  },
  "fortiWebAManagementConsole": {
    "type": "String",
    "value": "https://xpaca94.eastus.cloudapp.azure.com:40030"
  },
  "fortiWebBManagementConsole": {
    "type": "String",
    "value": "https://xpaca94.eastus.cloudapp.azure.com:40031"
  }
}
```

When connecting to FortiWeb GUI, use the username and password that you provided when deploying the template. You should then be logged in to the main Dashboard.

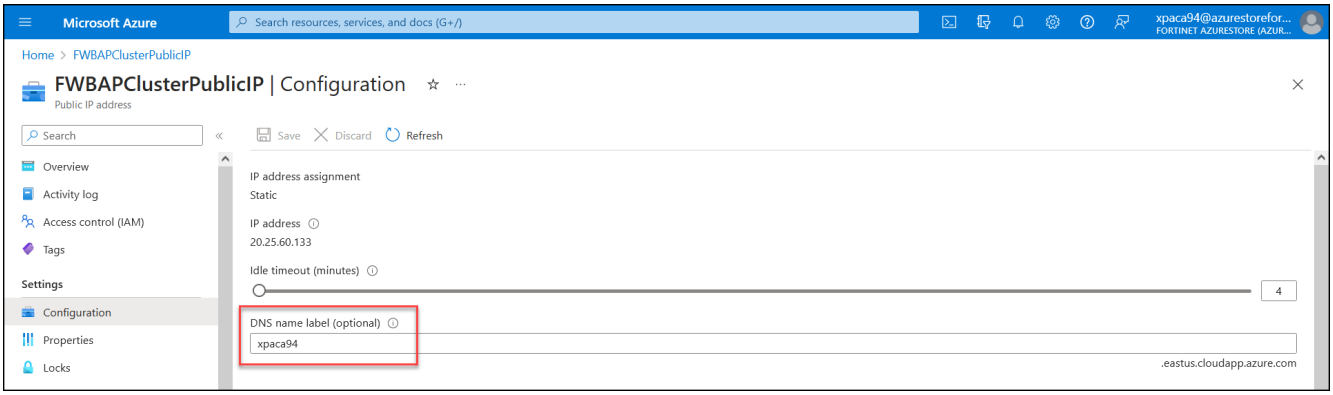


You can double check your **DNS configuration** in the Azure Public IP settings.

In the Azure portal, search for **FWBAPClusterPublicIP**.



You will find the DNS configuration under the configuration menu.

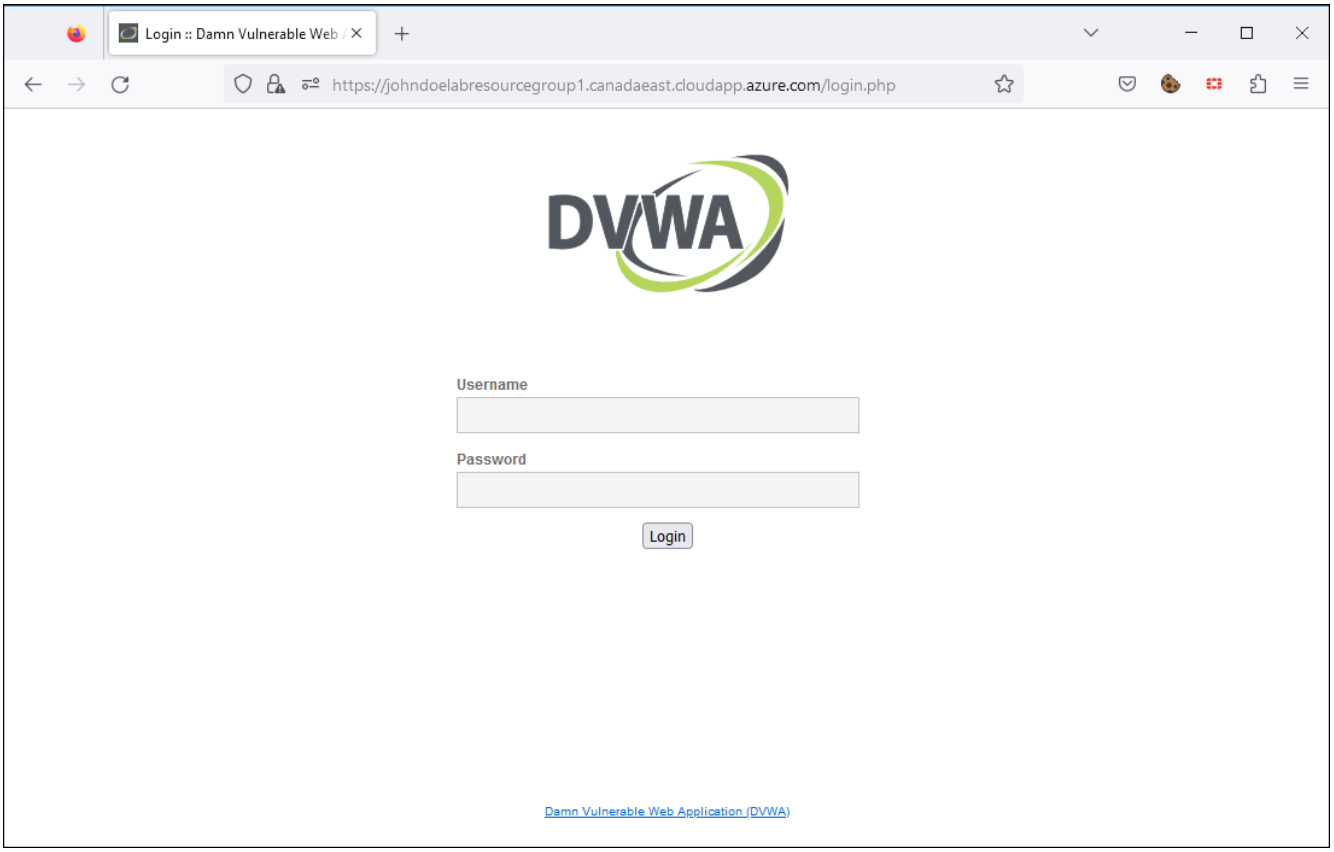


Ensure that your environment is operational

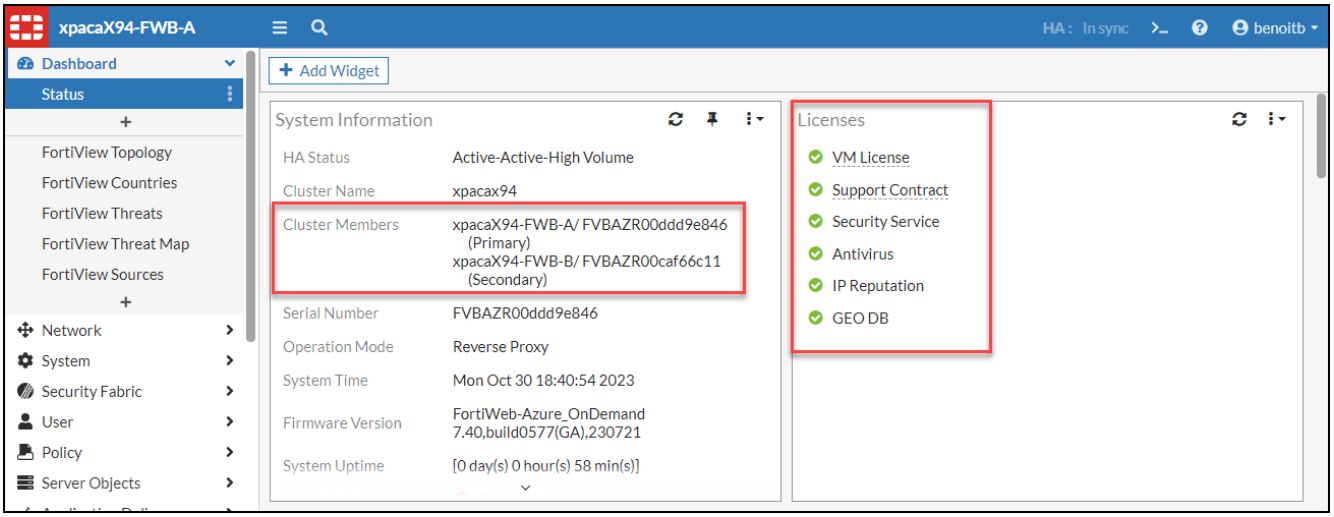
Ensure your environment is set up correctly by following this three-step checklist.

1 - You should be able to navigate to the DVWA application: https://@PREFIX.@REGION.cloudapp.azure.com

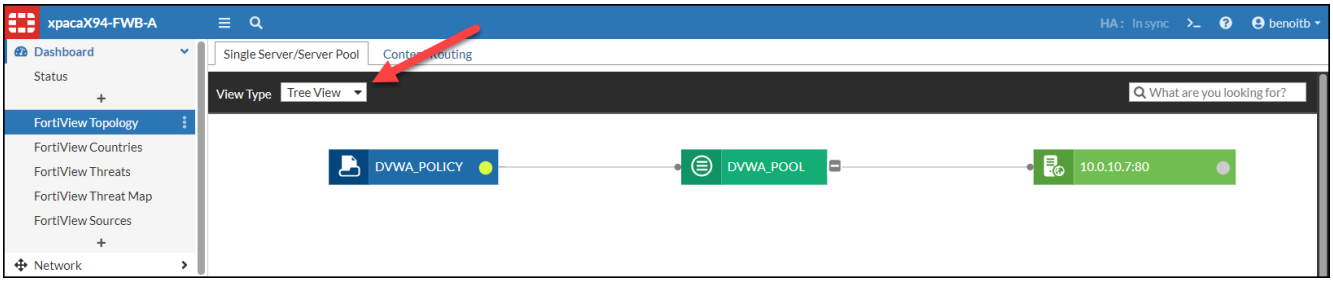
If you encounter a FortiWeb block page, clear your browser cache and try again.



2 - Verify the presence of the two FortiWeb instances on the main dashboard by navigating to `Dashboard > Status`. Additionally, check the status of your license. **Note**: we are using PAYG License model for this Lab.



3 - Verify the topology by going to the menu `Dashboard > FortiView Topology`



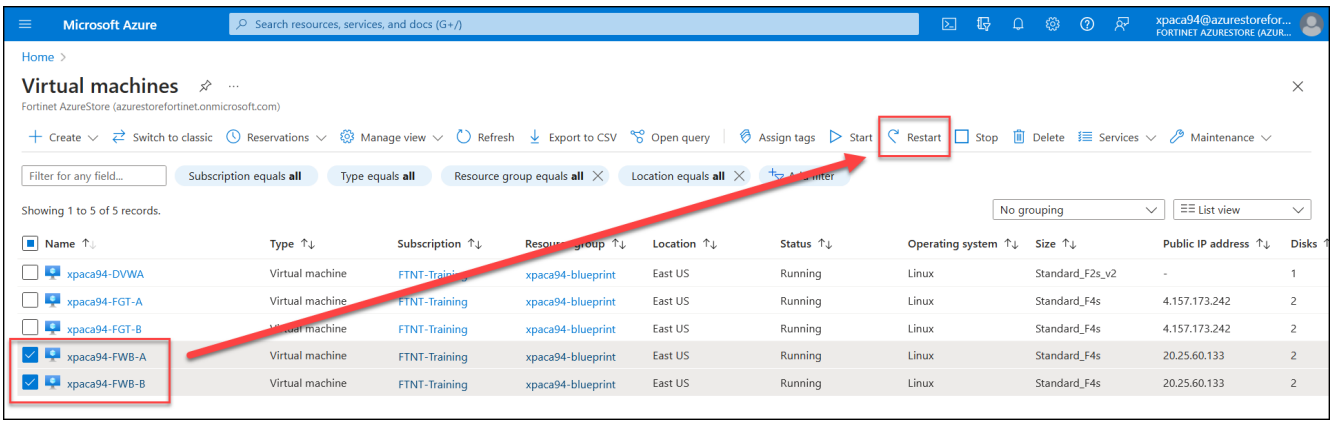
If you encounter any issues, refer to the following troubleshooting sections or consult your instructor.

Troubleshooting - What to do if the cluster is not operational?

During the initial startup, there's a possibility that **ARP on port2** may malfunction, which could render the cluster inoperative, as port2 is deemed faulty. In such cases, you'll need to restart both FortiWeb VMs via the Azure console.

Note that restarting the FortiWebs from the GUI will not resolve the ARP issue; only a restart from the Azure portal will fix it.

Navigate to the **Virtual Machines** menu in the Azure portal. Select the two FortiWeb VMs and click on **Restart**.

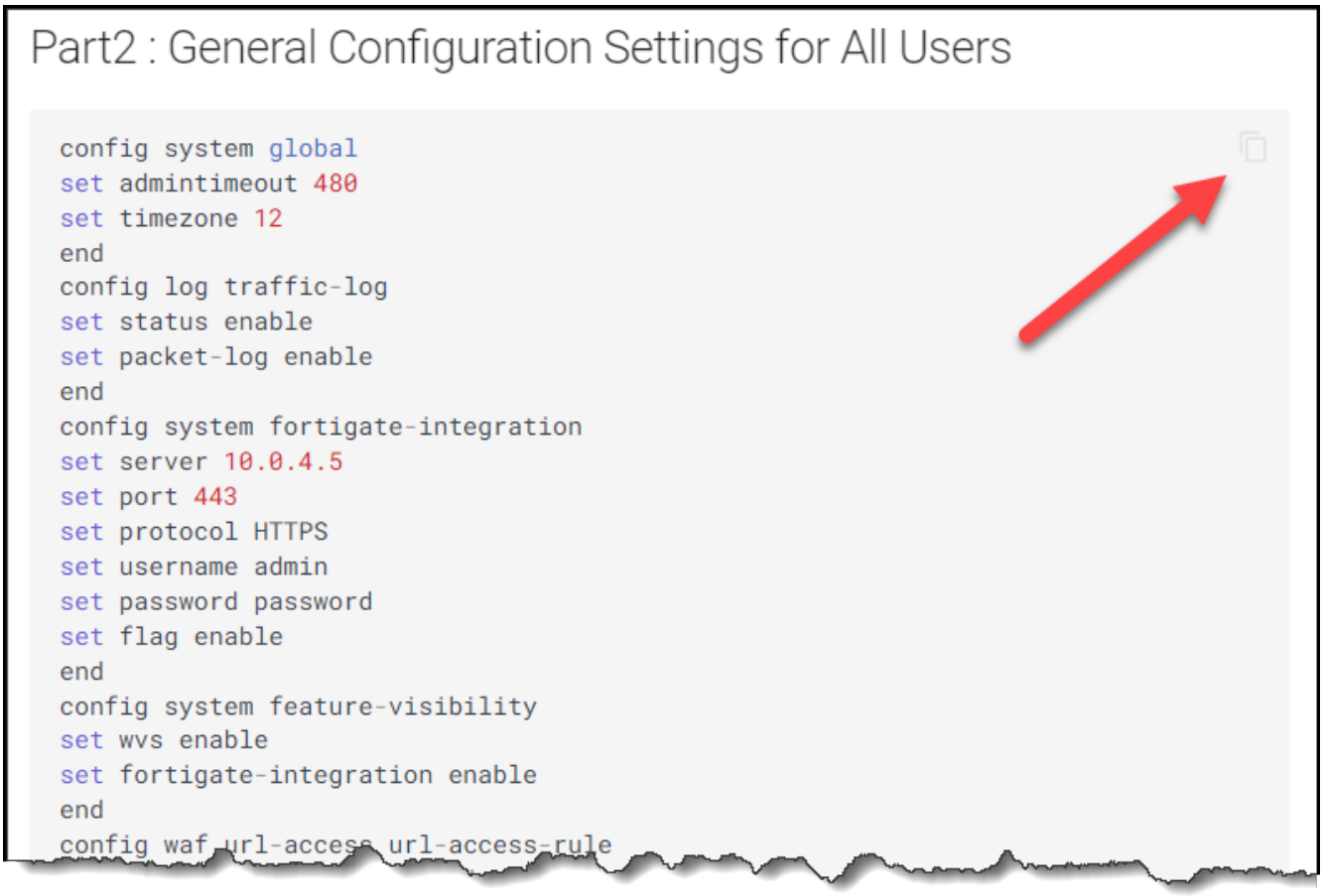


Troubleshooting - What to do if there is no policy in place, or if DVWA is not accessible?

The FortiWeb configuration, including the WAF policy, is automatically loaded when the VM is created. We achieve this by using the Azure **cloud-init** feature. Cloud-init is a widely used method for customizing a VM as it boots for the first time. However, there may be circumstances where the configuration doesn't load correctly. If this happens to you, you can simply manually import our configuration file.

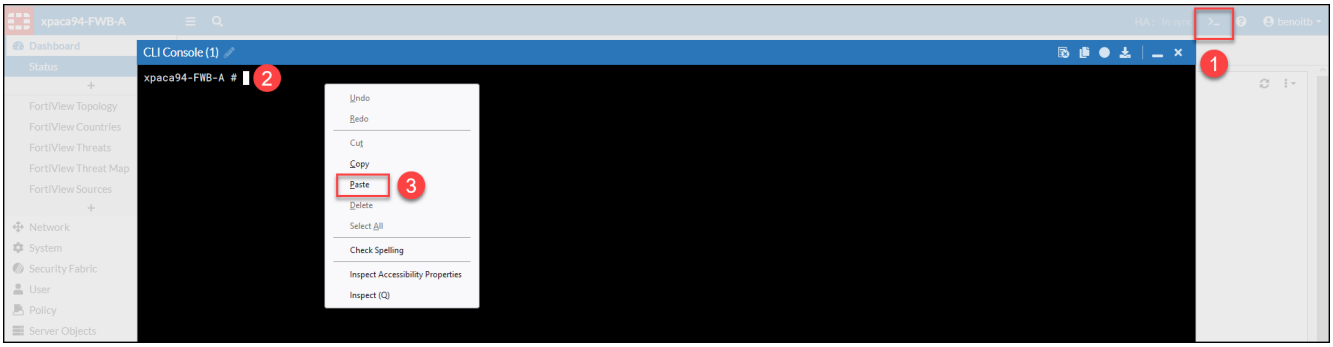
1 - Navigate to the bootstrap page

2 - Copy **Part 2** of the configuration to your clipboard

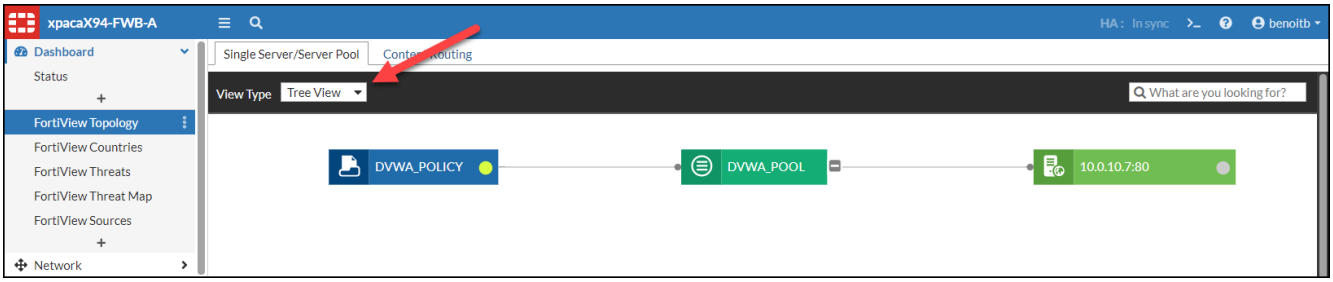


3 - Connect to your **FortiWeb** instance, and open the CLI console located in the upper left corner

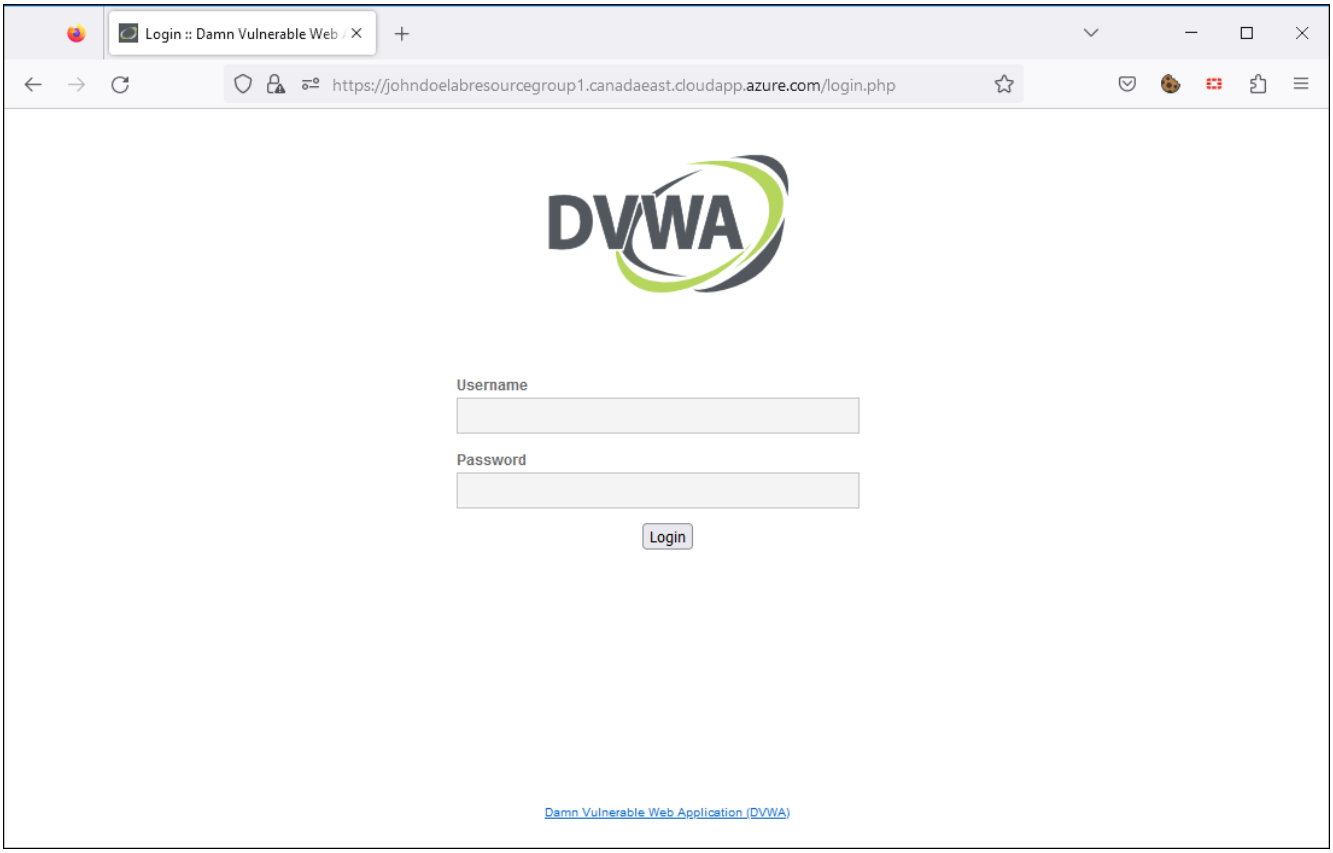
4 - Paste the copied configuration into the console



5 - Navigate to `Dashboard > FortiView Topology` and verify that the policy is now displayed



6 - You should be able to navigate to the DVWA application: https://@PREFIX.@REGION.cloudapp.azure.com

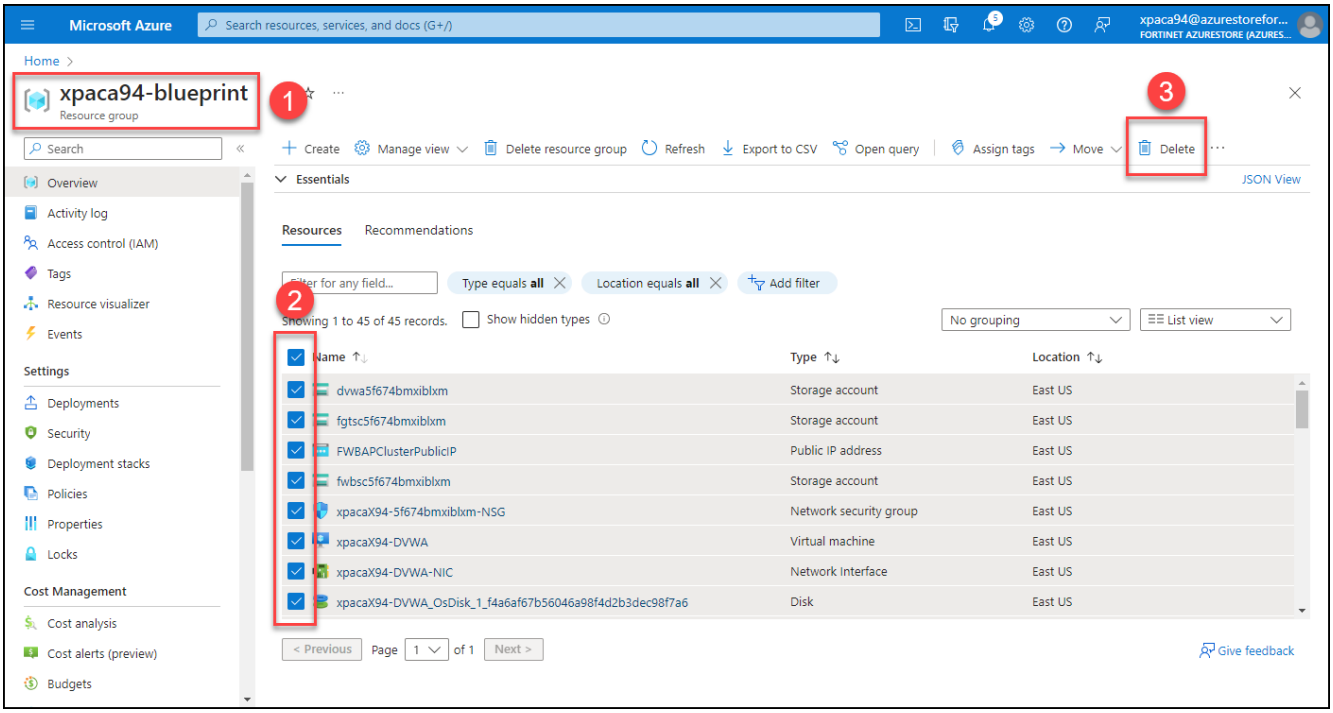


Troubleshooting - Delete and rebuild your Lab Environment

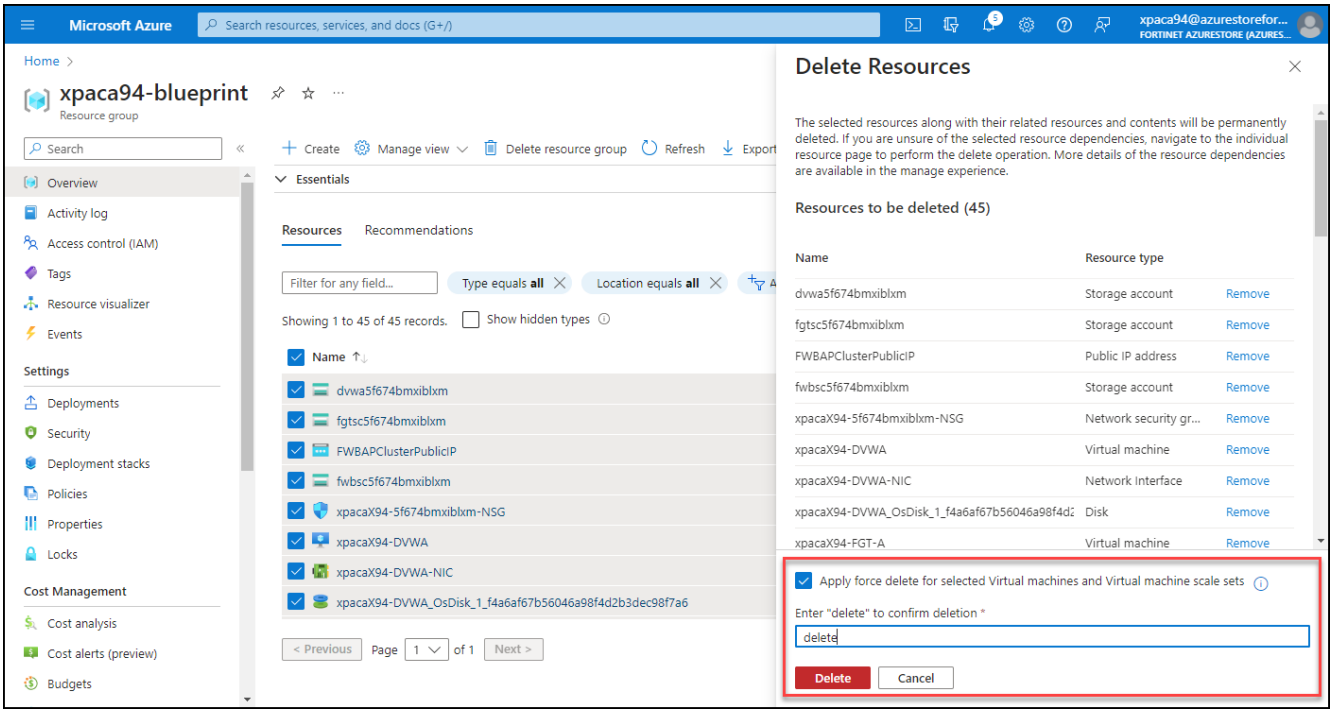
Here's the process to follow if you need to delete and rebuild your Lab environment:

Do not delete the resource group itself, as you won't be able to recreate it.

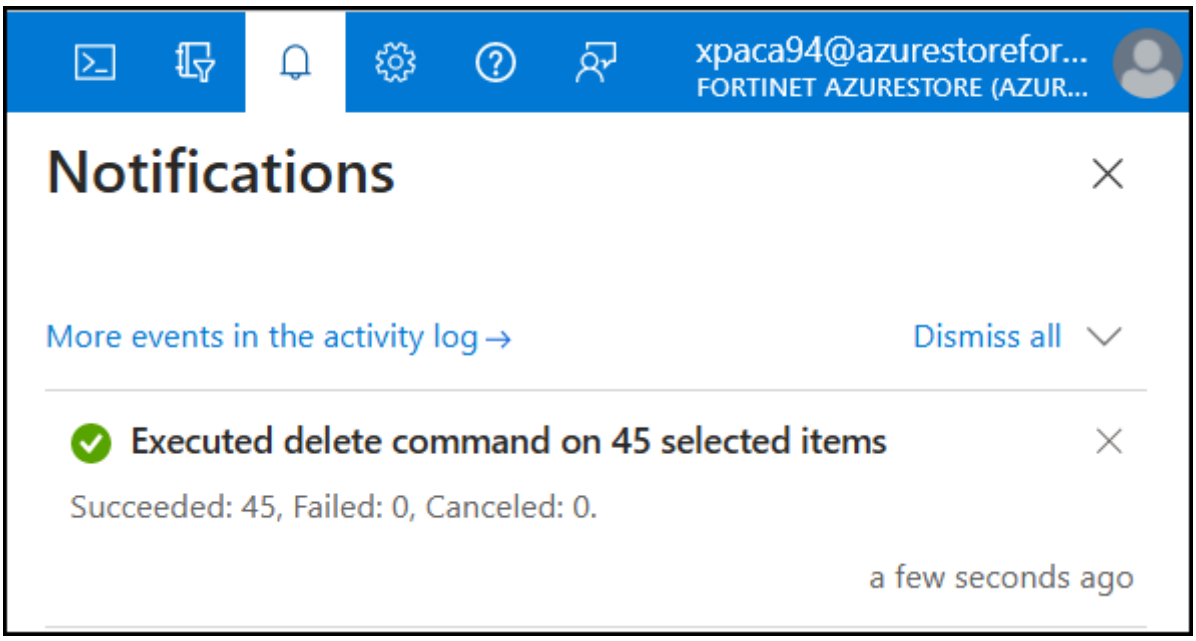
- Navigate to the Azure portal
- Choose your resource group, identified as **@RESOURCE_GROUP_NAME**
- Select all the resources within the group
- Click on **Delete**



- Opt for **Apply force delete for selected Virtual machines and Virtual machine scale sets**
- Type **delete** to confirm deletion
- Click on **Delete**



- Wait for the deletion process to complete



- Navigate to Azure Cloud Shell and make sure you are in the **fortinetCloudBlueprint** folder

```
cd fortinetCloudBlueprint
```

- Redeploy the template using the following command

```
az deployment group create --name fortinetCloudBlueprint --resource-group @RESOURCE_GROUP_NAME --template-file 000-main.bicep
```

Check your System Configuration (optional)

Once you have access to the FortiWeb GUI, those are the main menu to check your system configuration.

Configuration	Menu
FortiWeb Network Access	`Network > Interface`
Routing	`Network > Static Route`
DNS Configuration	`Network > DNS`
VM License	`Dashboard > Status > Licenses > Update VM License`
FortiGuard Status and Updates	`System > Config > FortiGuard`
Time Zone Setting	`System > Maintenance > System Time`
Timeout Setting	`System > Admin > Settings > Idle Timeout`
Firmware Version	`System > Maintenance > Firmware`

Check your Application Policy (optional)

During the Bicep deployment, we imported this bootstrap. Those are the main menus to check your Application Policy:

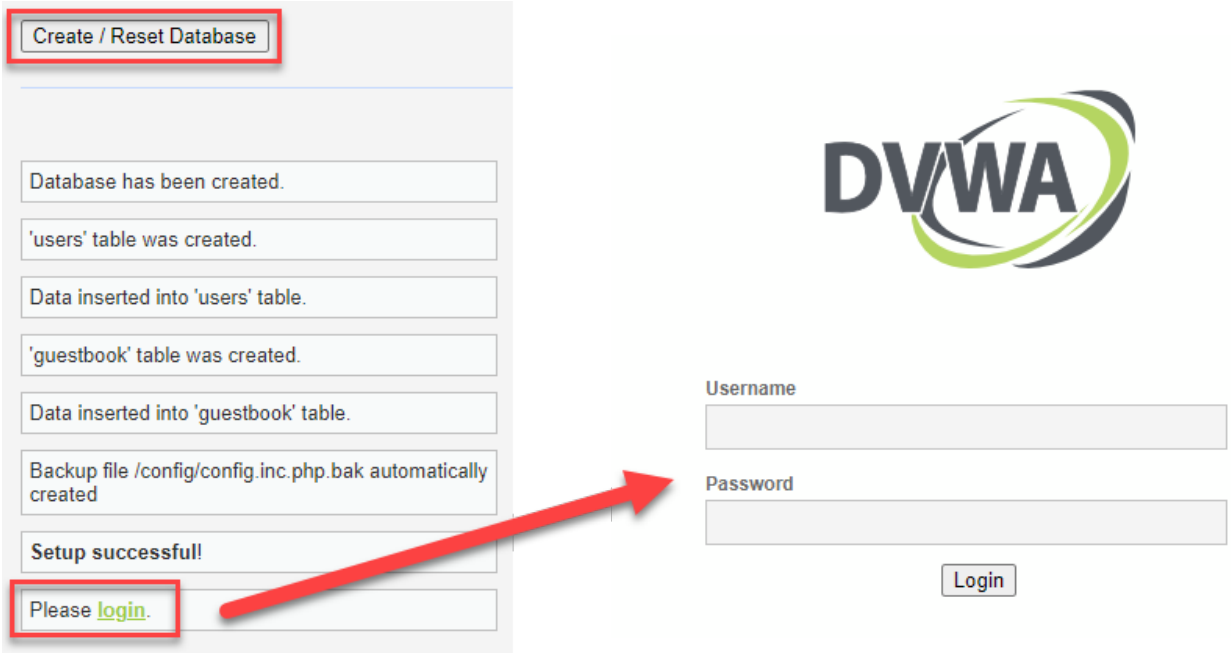
Configuration	Menu
Virtual IP	`Network > Virtual IP`
Virtual Server	`Server Objects > Virtual Server`
Server Pool	`Server Objects > Server Pool`
Signature	`Web Protection > Known Attacks > Signatures`
Web Protection Profile	`Policy > Web Protection Profile`
Policy	`Policy > Server Policy`

Initializing DVWA

Initialize DVWA database and authenticate

Connect to https://@PREFIX.@REGION.cloudapp.azure.com/setup.php

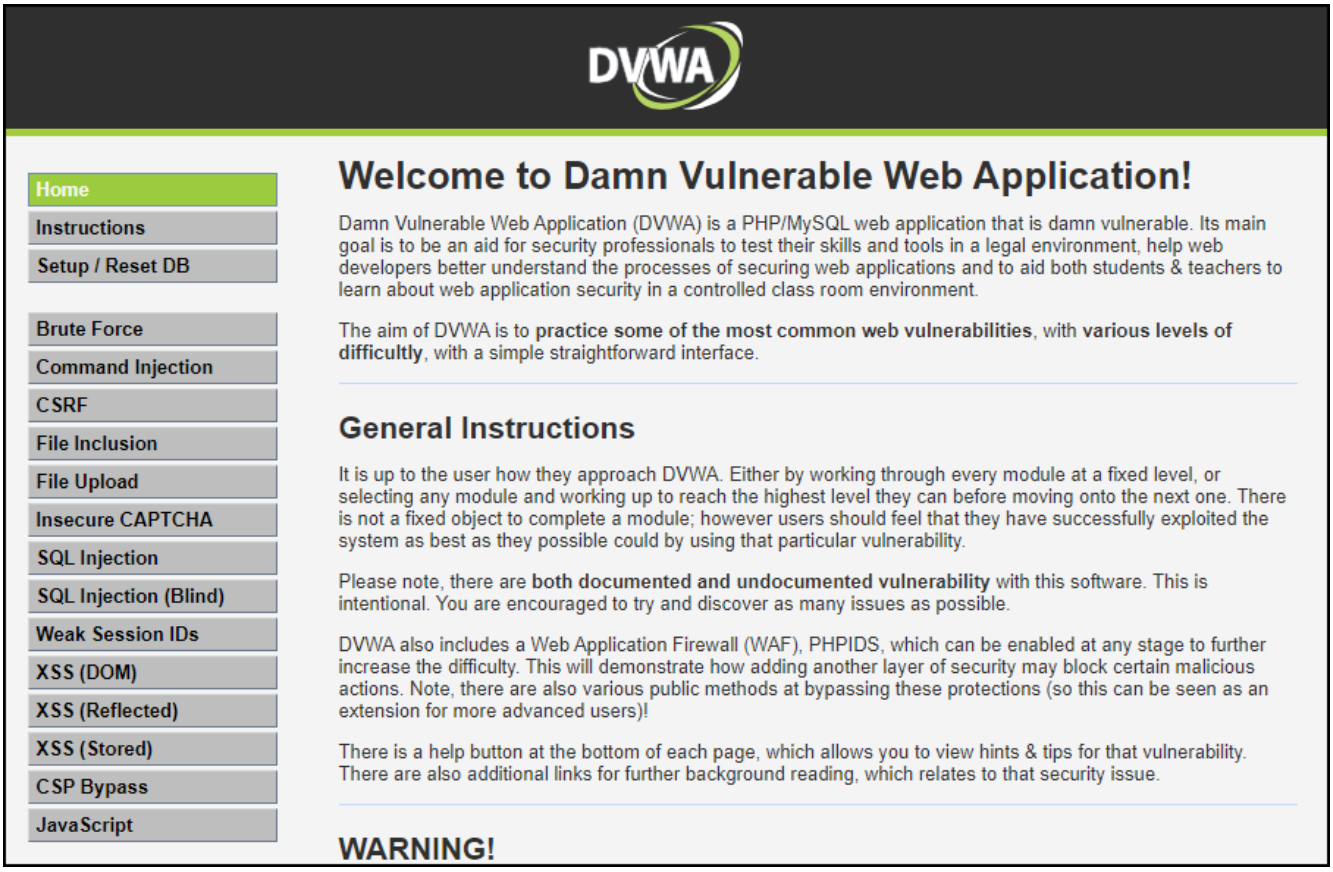
Click **Create / Reset Database**



Click **Login** and authenticate with any of these accounts:

Username	Password
admin	password
gordonb	abc123
1337	charley
pablo	letmein
smithy	password

You should be directed to the welcome page.



How to install DVWA in another Lab Environement?

If you are not using the Azure Fortinet Cloud Blueprint, you can install your own DVWA instance.

The most straightforward way to install DVWA is by utilizing Docker. Install any Linux distribution with Docker and run those 2 commands:

```
sudo docker pull vulnerables/web-dvwa
sudo docker run -d --restart unless-stopped -p 80:80 vulnerables/web-dvwa
```

You can explore additional deployment options on the official DVWA GitHub.

3. Hands on Labs

3.1 Protecting Web Application Using Azure Network Security Groups and FortiGate

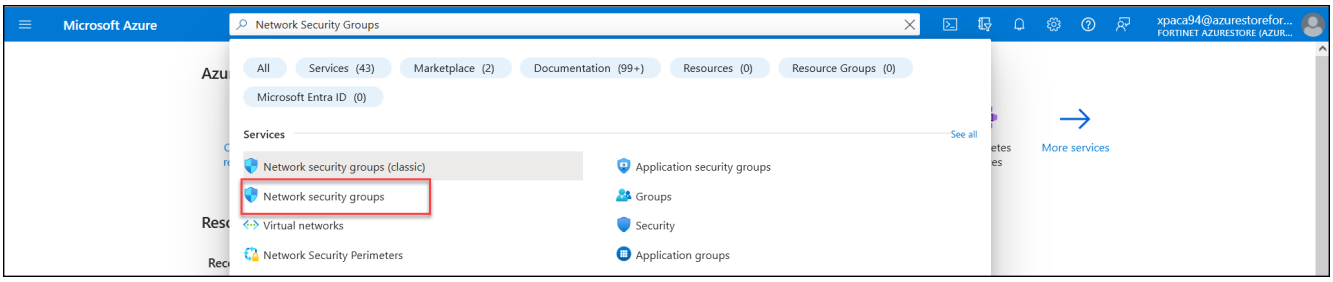
Accessing DVWA via NSG's

The first step in this exercise will be to create a Network Security Group and associate it to the subnet where the DVWA instance is deployed.

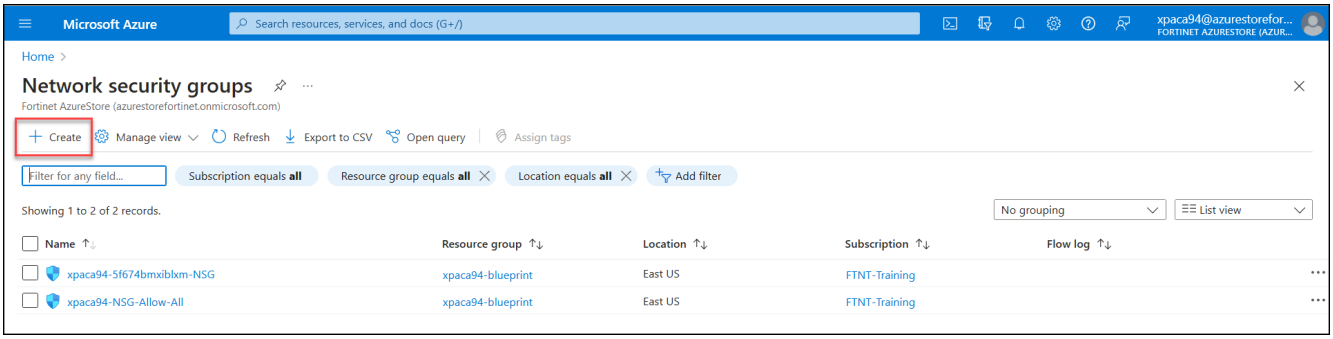
> **Tip**
>
> Click on the images to view them in a larger format.

Creating a Network Security Group

In the search bar type **Network Security Groups**, and select the non-classic option.

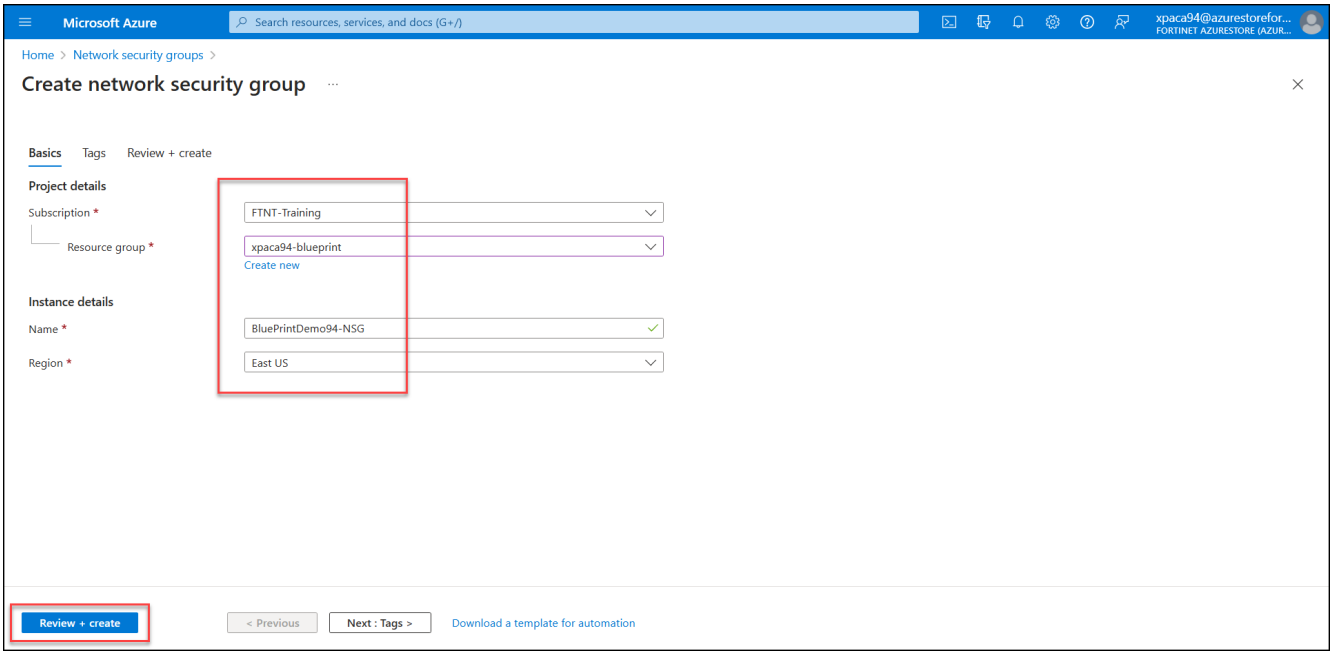


Create a new Security Group.

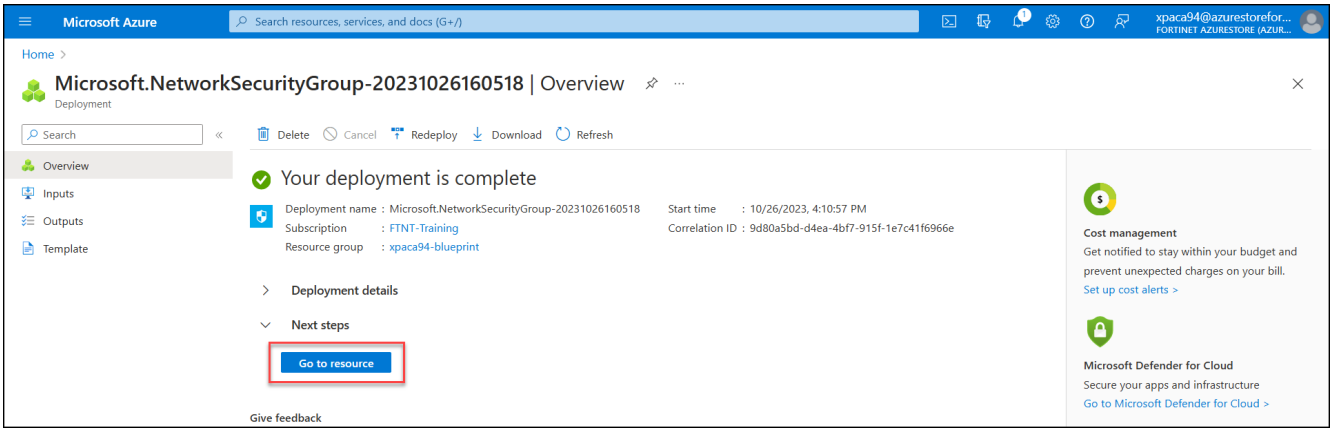


Select the Resource Group **@RESOURCE_GROUP_NAME** and give the Network Security Group a **unique name**.

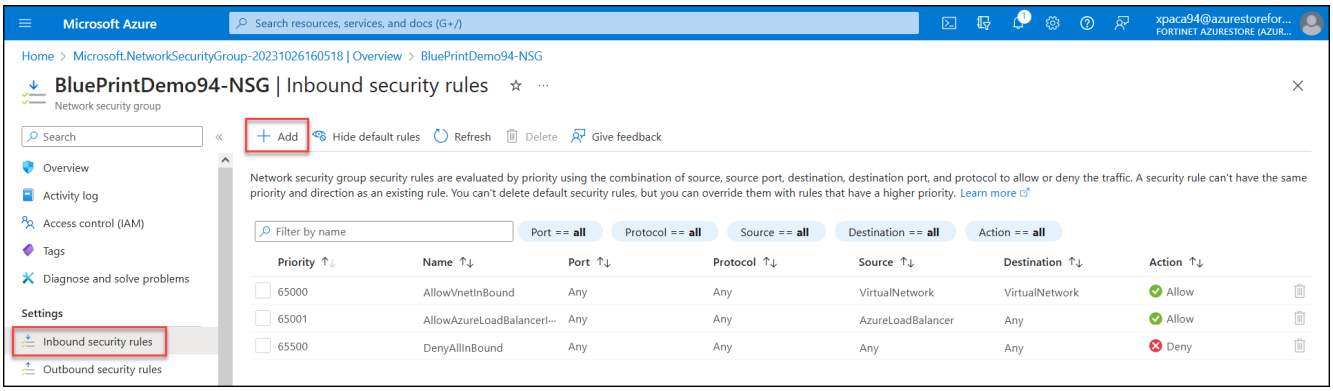
Review +Create the Resource.



Once created, Click on **Go to Resource** to be redirected to your newly created NSG.

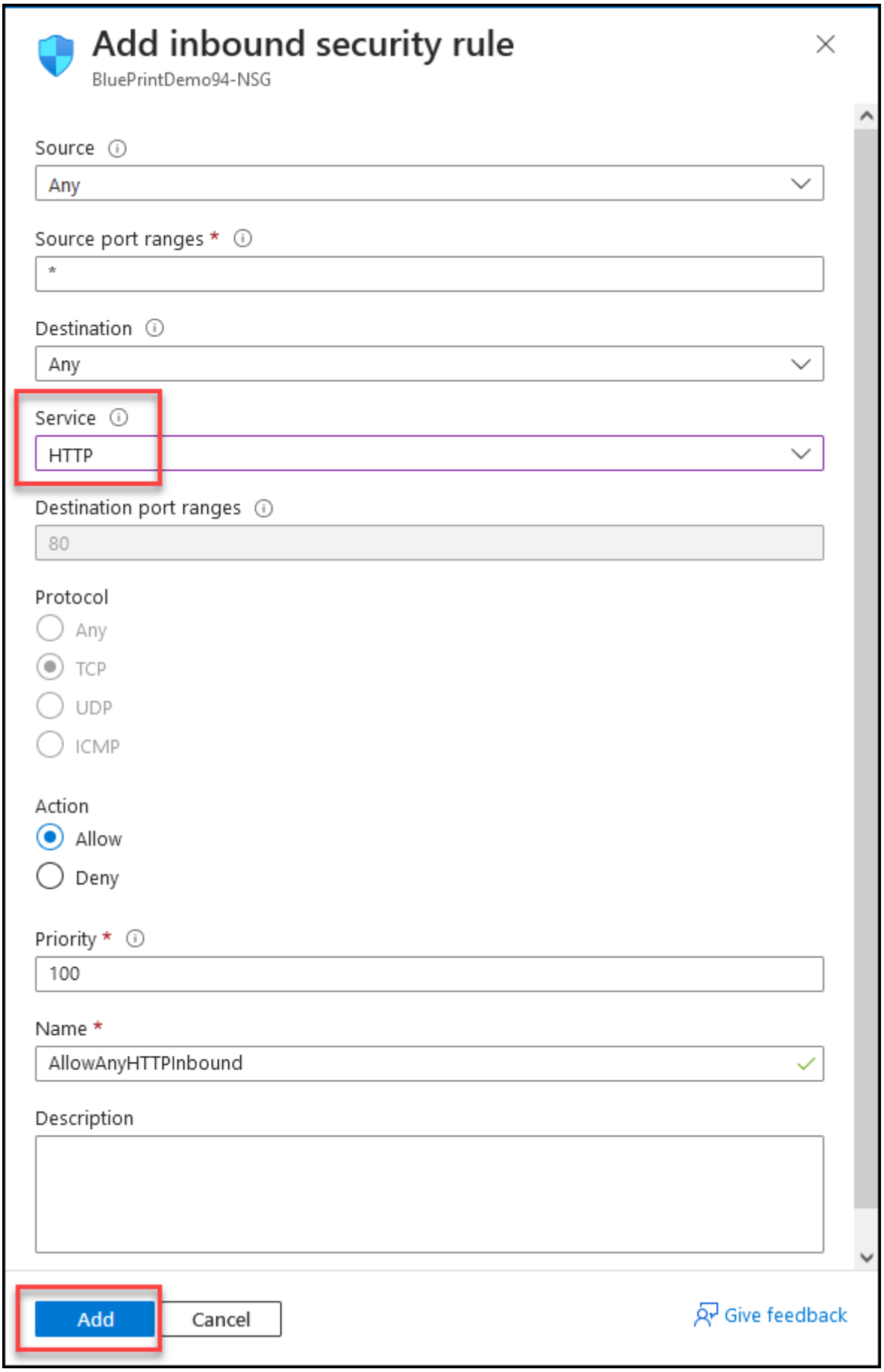


Navigate to the **Inbound Security Rules** menu Item.

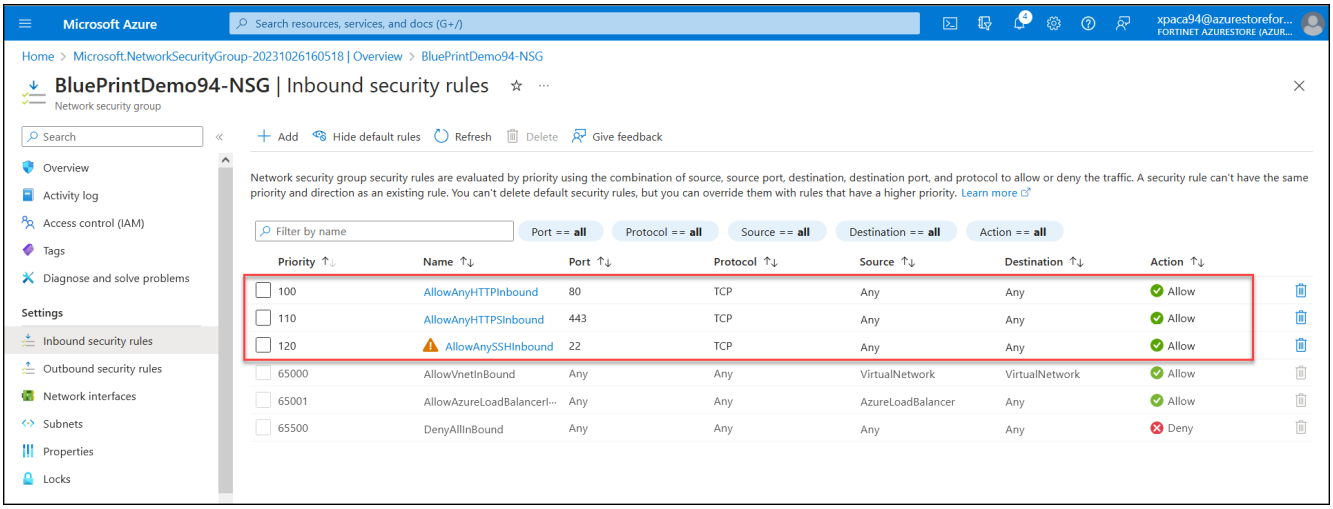


Create new entries to allow **HTTP, HTTPS, SSH** services from any sources.

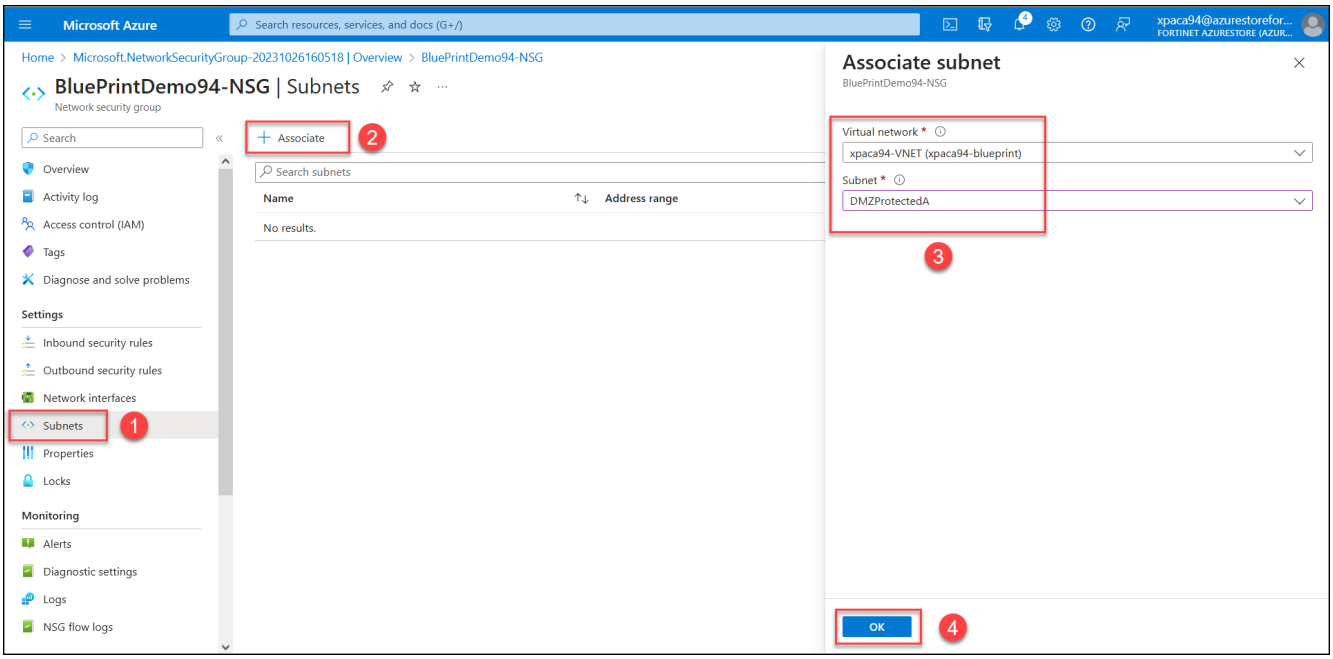
AllowAnyHTTPInbound	AllowAnyHTTPSInbound	AllowAnySSHInbound
Source = Any	**Source** = Any	**Source** = Any
Source Port = Any	**Source Port** = Any	**Source Port** = Any
Destination = Any	**Destination** = Any	**Destination** = Any
Service = HTTP	**Service** = HTTPS	**Service** = SSH
Action = Allow	**Action** = Allow	**Action** = Allow

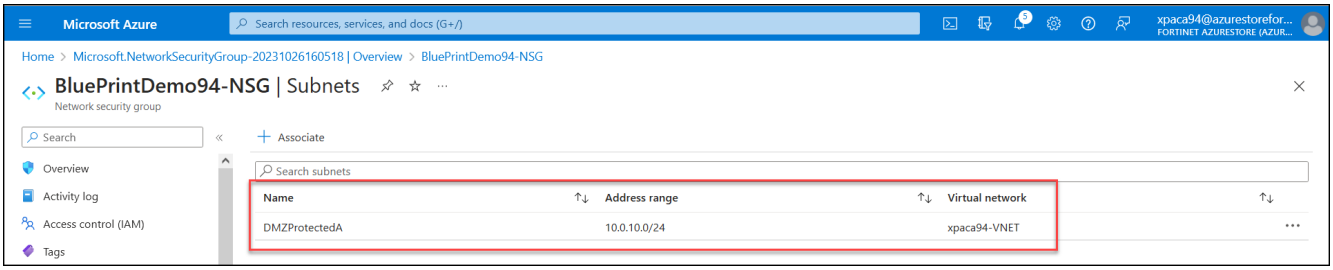

Add inbound security rule
BluePrintDemo94-NSG
Source
Any
Source port ranges *
*
Destination
Any
Service
HTTP
Destination port ranges
80
Protocol
Any
TCP
UDP
ICMP
Action
Allow
Deny
Priority *
100
Name *
AllowAnyHTTPInbound
Description
Add
Cancel
Give feedback

Once you've created the corresponding rules, you'll see your rules, in addition to the rules Azure had implicitely configured:



Navigate to the **Subnets** menu and **Associate** the Network security group to the **DMZProtectedA** Subnet.





Testing your Network Security Group

In Azure CLI, print your deployment **Outputs** and click on http://@PREFIX-fgt-to-dvwa.@REGION.cloudapp.azure.com

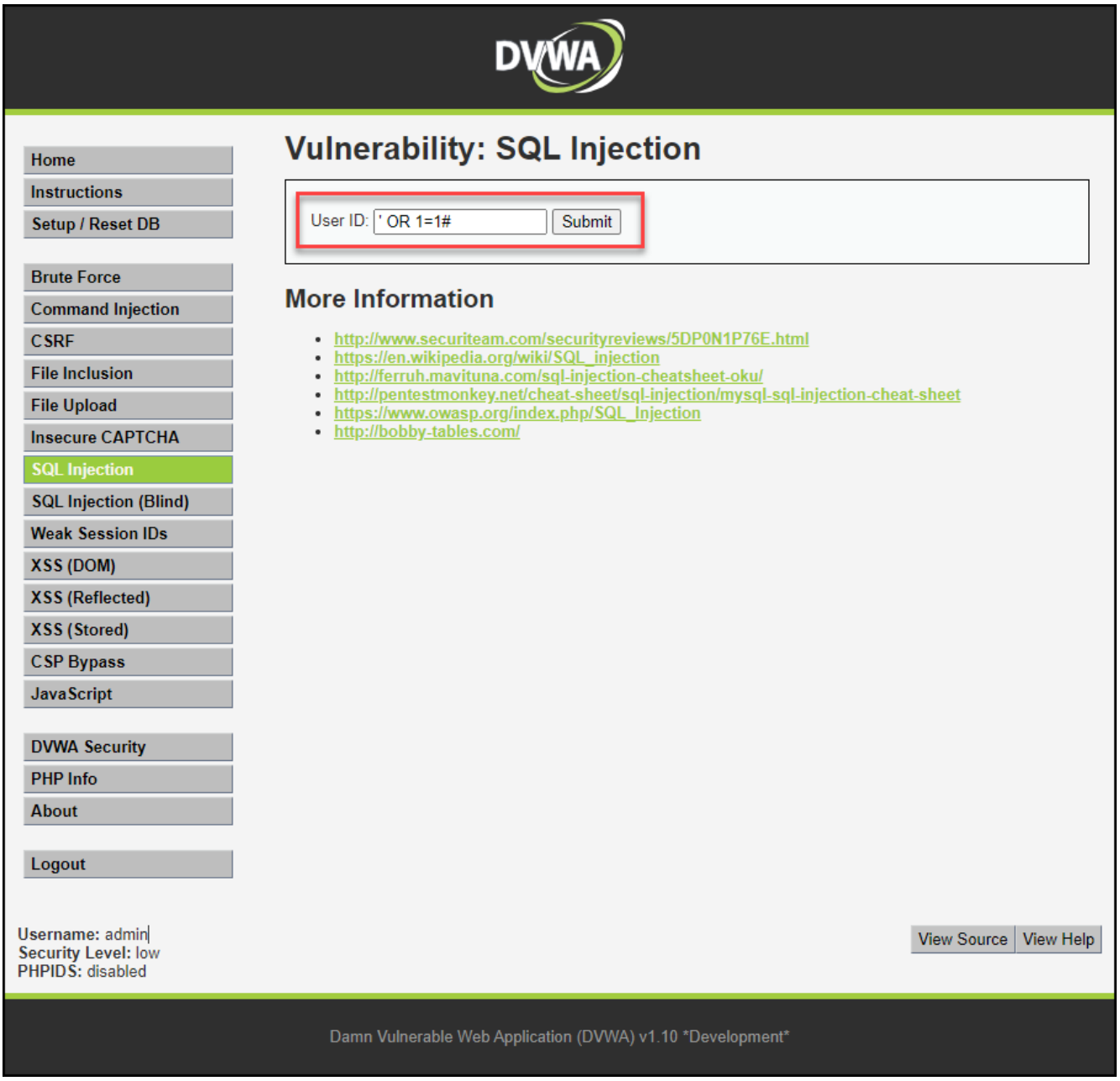
```
az deployment group show -g @RESOURCE_GROUP_NAME -n fortinetCloudBlueprint --query properties.outputs
```

```
xpaca94 [ ~ ]$ az deployment group show -g xpaca94-blueprint -n fortinetCloudBlueprint --query properties.outputs
{
  "dvwaHTTPviaFortiGate": {
    "type": "String",
    "value": "http://xpaca94-fgt-to-dvwa.eastus.cloudapp.azure.com:80"
  },
  "dvwaHTTPviaFortiWeb": {
    "type": "String",
    "value": "http://xpaca94.eastus.cloudapp.azure.com:80"
  },
  "dvwaSSHviaFortiGate": {
    "type": "String",
    "value": "4.157.173.242:22"
  },
  "fortiGateAManagementConsole": {
    "type": "String",
    "value": "https://4.157.173.231:443"
  },
  "fortiGateBManagementConsole": {
    "type": "String",
    "value": "https://4.157.173.238:443"
  },
  "fortiWebAManagementConsole": {
    "type": "String",
    "value": "https://xpaca94.eastus.cloudapp.azure.com:40030"
  },
  "fortiWebBManagementConsole": {
    "type": "String",
    "value": "https://xpaca94.eastus.cloudapp.azure.com:40031"
  }
}
```

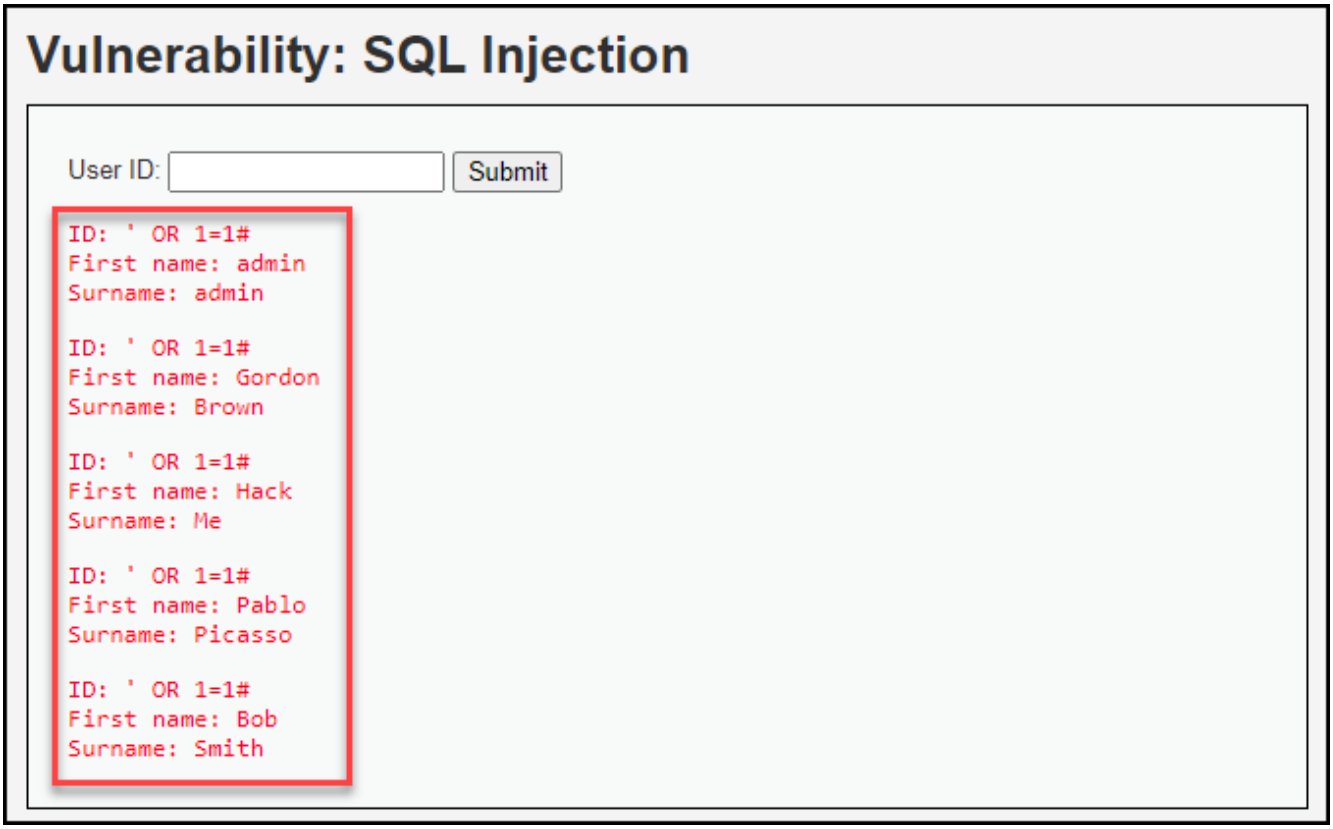
Log in to DVWA using the credentials **admin** and **password**.

Navigate to the **SQL Injection** menu item and type:

```
' OR 1=1#
```



Notice the attack was not prevented.



Why? After the NSG permitted access to the DVWA Workload on Port 80 (HTTP) no subsequent inspection occured.

Accessing DVWA via FortiGate

Now, we will execute the same attack, but this time, we will secure the DVWA Workload behind the FortiGate Firewall.

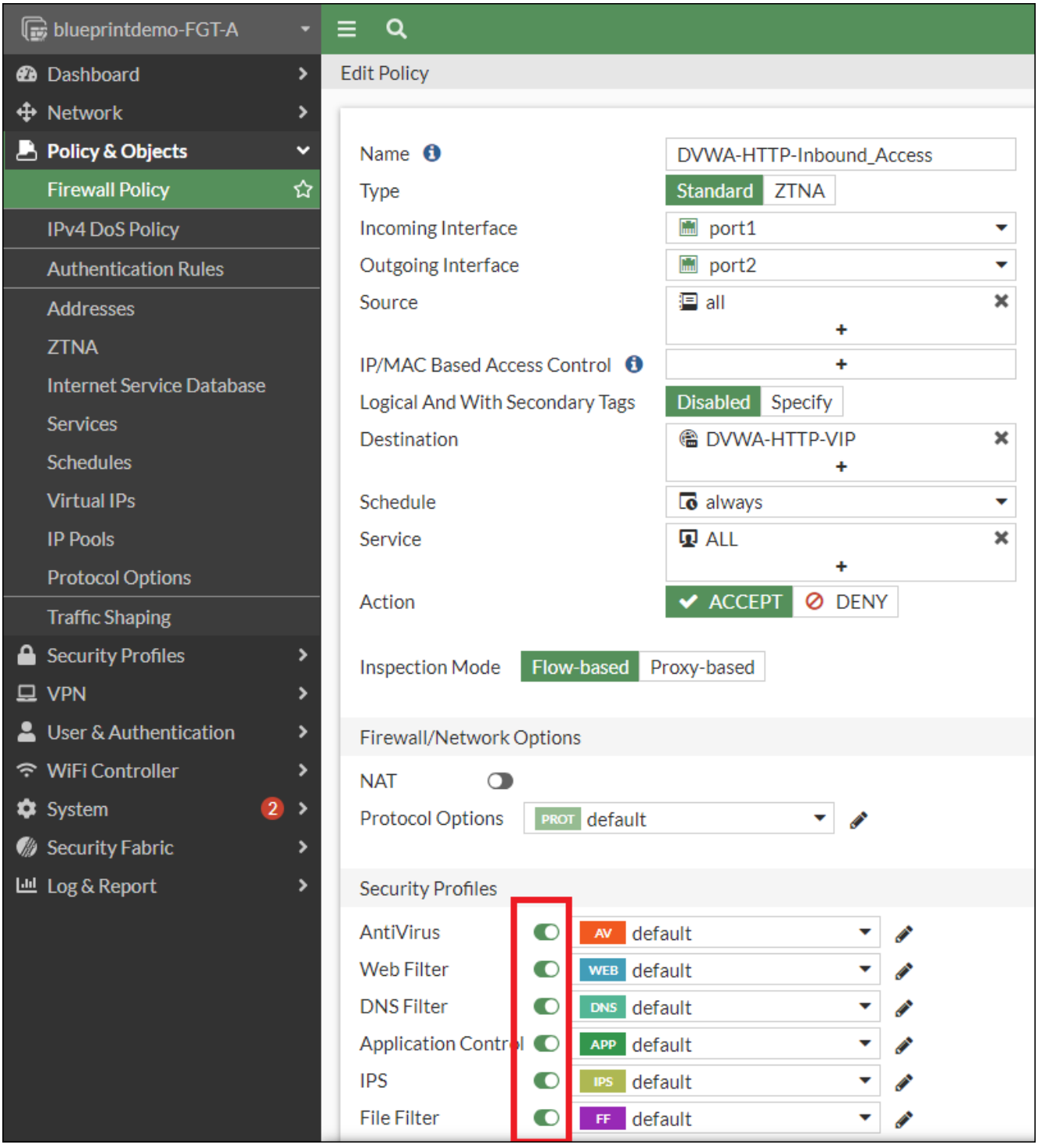
Testing SQL Injection Attack

Log in to the Primary FortiGate using the credentials you established during deployment.

```
az deployment group show -g  @RESOURCE_GROUP_NAME -n fortinetCloudBlueprint --query properties.outputs
```

```
xpaca94 [ ~ ]$ az deployment group show -g xpaca94-blueprint -n fortinetCloudBlueprint --query properties.outputs
{
  "dvwaHTTPviaFortiGate": {
    "type": "String",
    "value": "http://xpaca94-fgt-to-dvwa.eastus.cloudapp.azure.com:80"
  },
  "dvwaHTTPviaFortiWeb": {
    "type": "String",
    "value": "http://xpaca94.eastus.cloudapp.azure.com:80"
  },
  "dvwaSSHviaFortiGate": {
    "type": "String",
    "value": "4.157.173.242:22"
  },
  "fortiGateAManagementConsole": {
    "type": "String",
    "value": "https://4.157.173.231:443"
  },
  "fortiGateBManagementConsole": {
    "type": "String",
    "value": "https://4.157.173.238:443"
  },
  "fortiWebAManagementConsole": {
    "type": "String",
    "value": "https://xpaca94.eastus.cloudapp.azure.com:40030"
  },
  "fortiWebBManagementConsole": {
    "type": "String",
    "value": "https://xpaca94.eastus.cloudapp.azure.com:40031"
  }
}
```

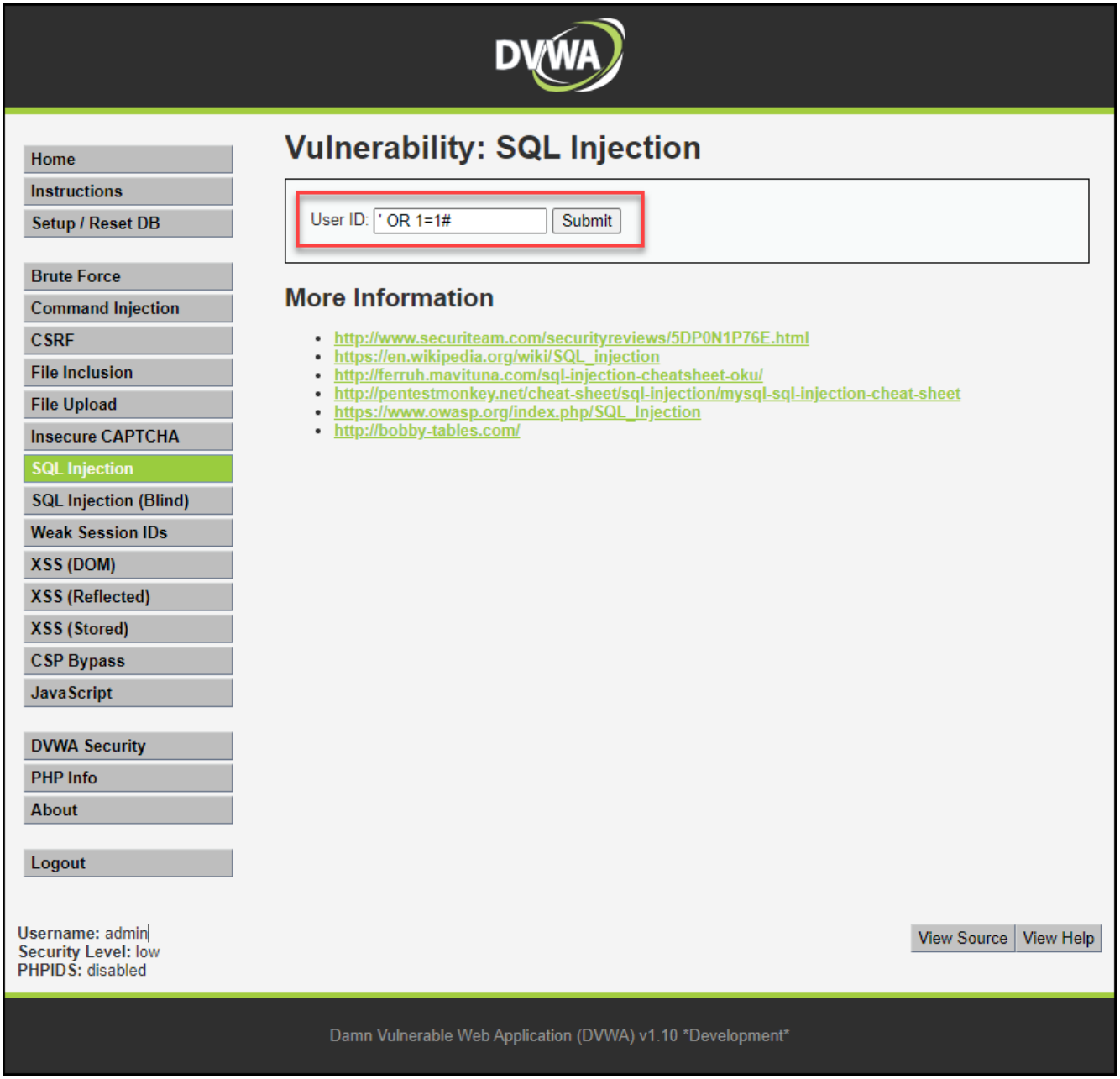
Once logged in to the FortiGate, edit the firewall policy named **DVWA-HTTP-Inbound_Access**. Enable all the security profiles with their default settings.



Click OK to apply the changes.

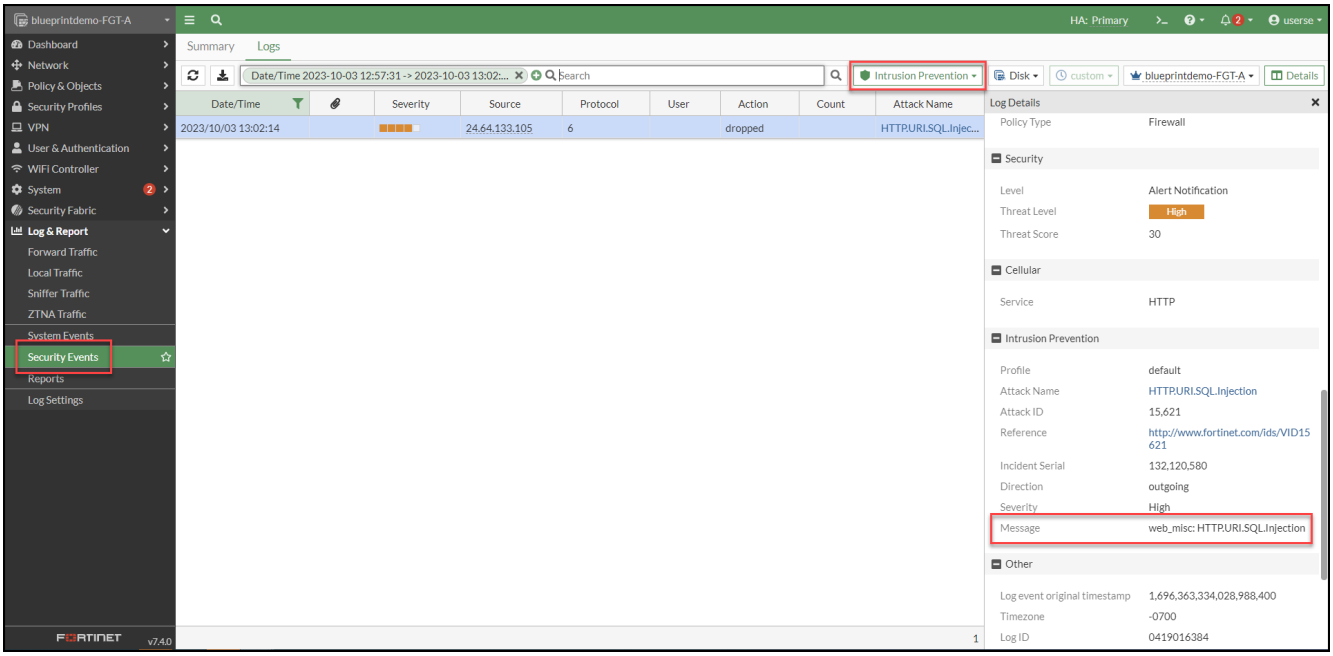
Browse again to http://@PREFIX-fgt-to-dvwa.@REGION.cloudapp.azure.com/vulnerabilities/sqli/ and enter this **SQL injection** attack into the form.

```
' OR 1=1#
```



Notice that the page is hung.

Let's dive deeper and look at the FortiGate's Log. Open the **Security Events**, select the **Logs** tab and use the **Intrusion Prevention** filter.



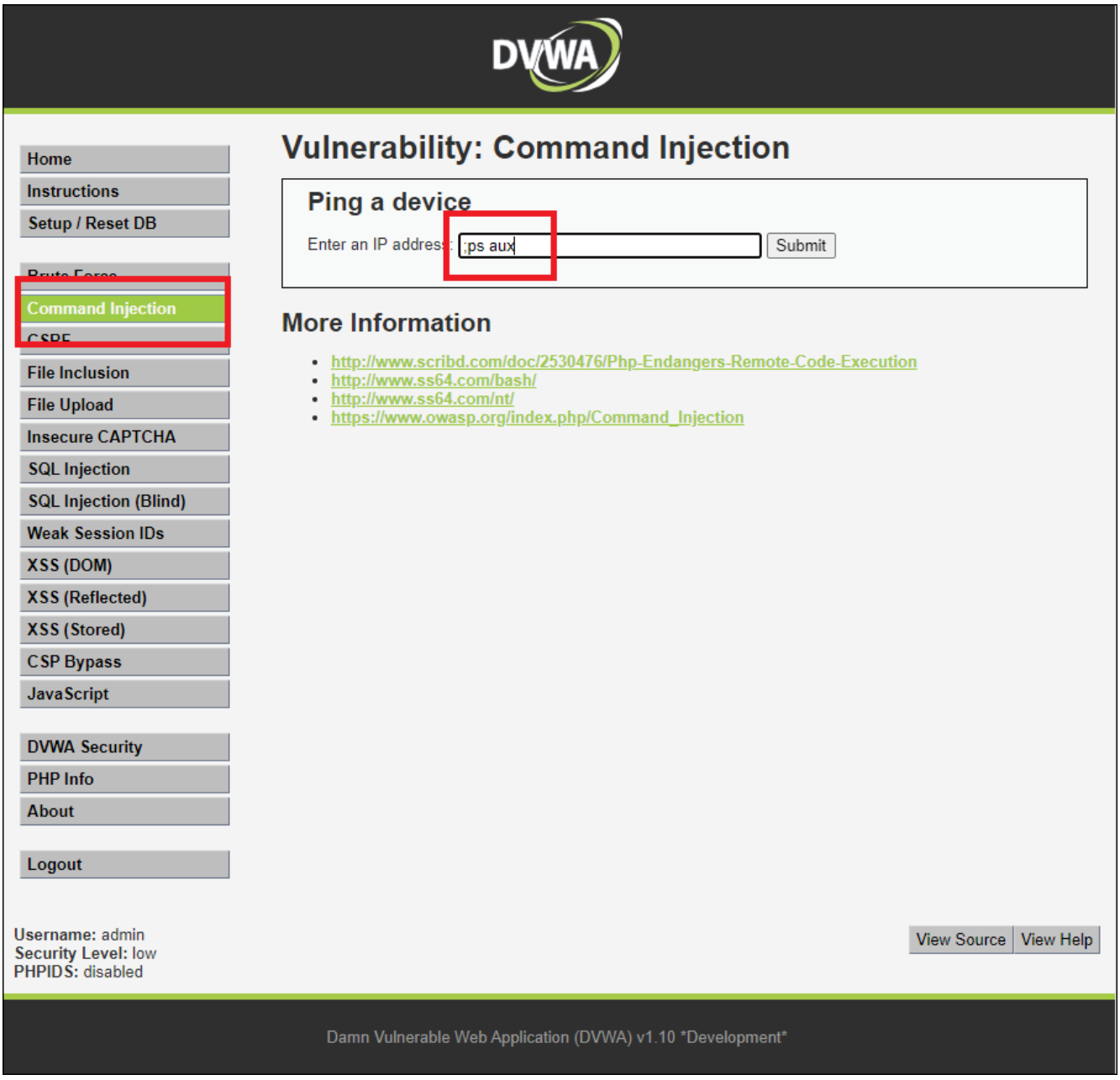
Why was this attack dropped? The attack triggered a signature set to block within the FortiGate's IPS Security Profile.

Testing Command Injection Attack

Now lets try a **Command Injection** attack.

Browse to http://@PREFIX-fgt-to-dvwa.@REGION.cloudapp.azure.com/vulnerabilities/exec/ and enter this **Command injection** attack into the form.

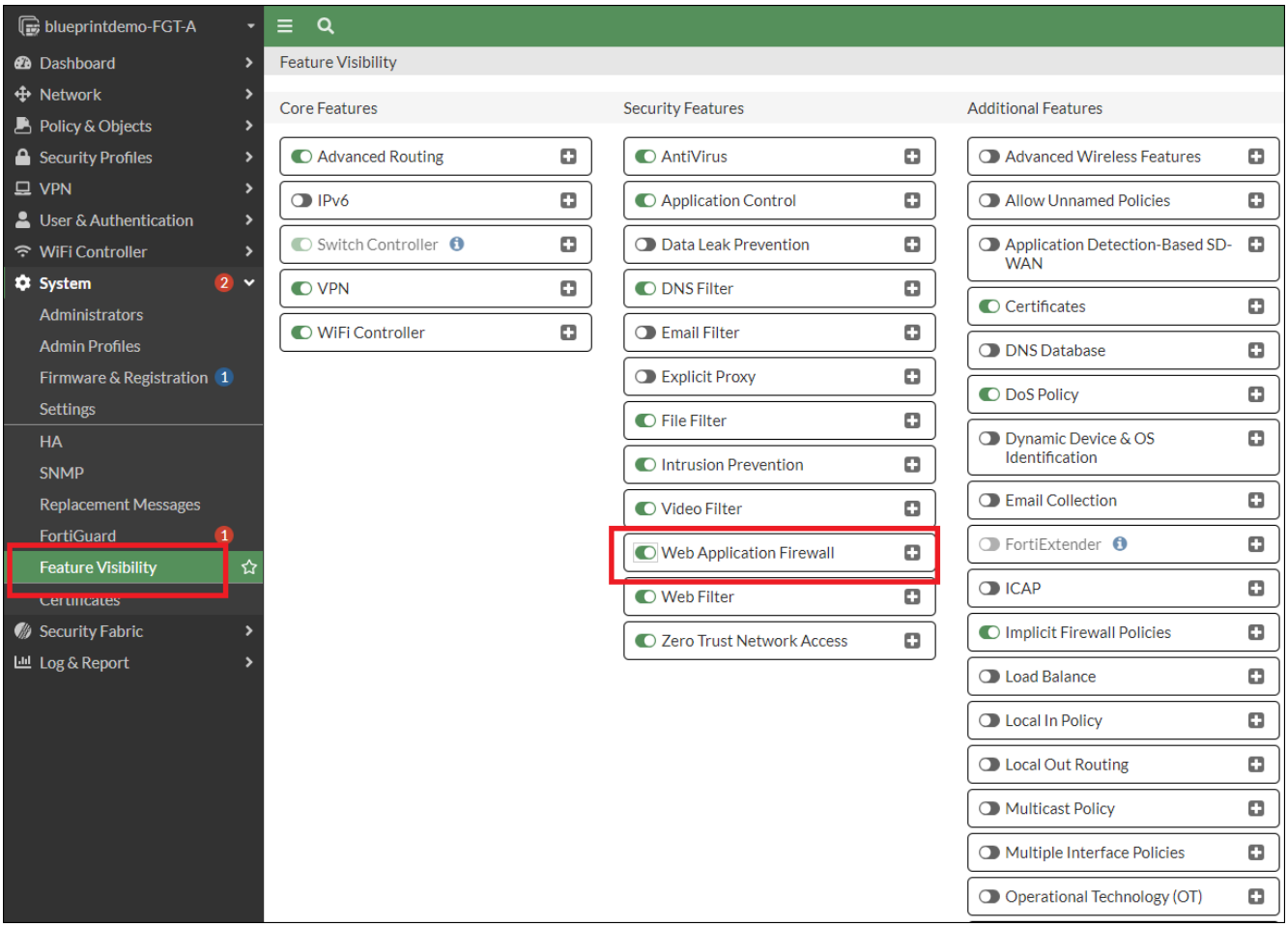
```
;ps aux
```



Why was the attack let through? The attack did not match a known IPS signature. Let's enhance the capabilities of the FortiGate by activating the **Web Application Firewall** security profile.

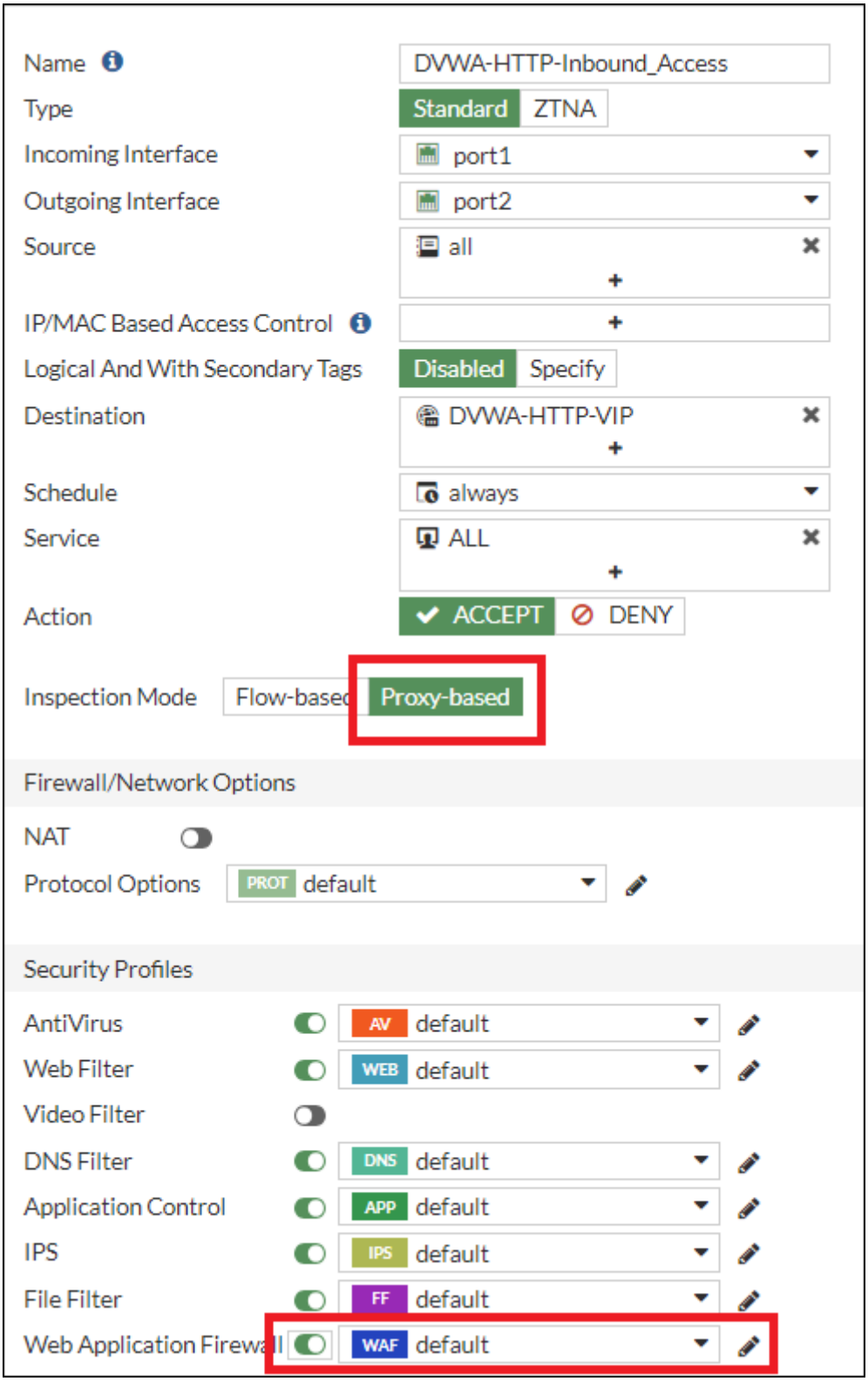
Enable WAF on FortiGate

Enable the **Web Application Firewall** Security Profile from `System -> Feature Visibility`



Once enabled, go back to the **Firewall Policy** and edit the **DVWA-HTTP-Inbound_Access** Firewall Policy.

Toggle the **Inspection Mode** to **Proxy-Based** and enable the default **Web Application Firewall** Security Profile.



Browse to http://@PREFIX-fgt-to-dvwa.@REGION.cloudapp.azure.com/vulnerabilities/exec/ and enter the **Command injection** attack again.

```
;ps aux
```

The **Command Injection** should now be prevented.

The attack is blocked because WAF signatures have been activated.

Conclusion

Did you notice that all of the attacks stopped by the FortiGate were all stopped based on existing signatures?

Demonstrating non-signature based attacks via FortiGate

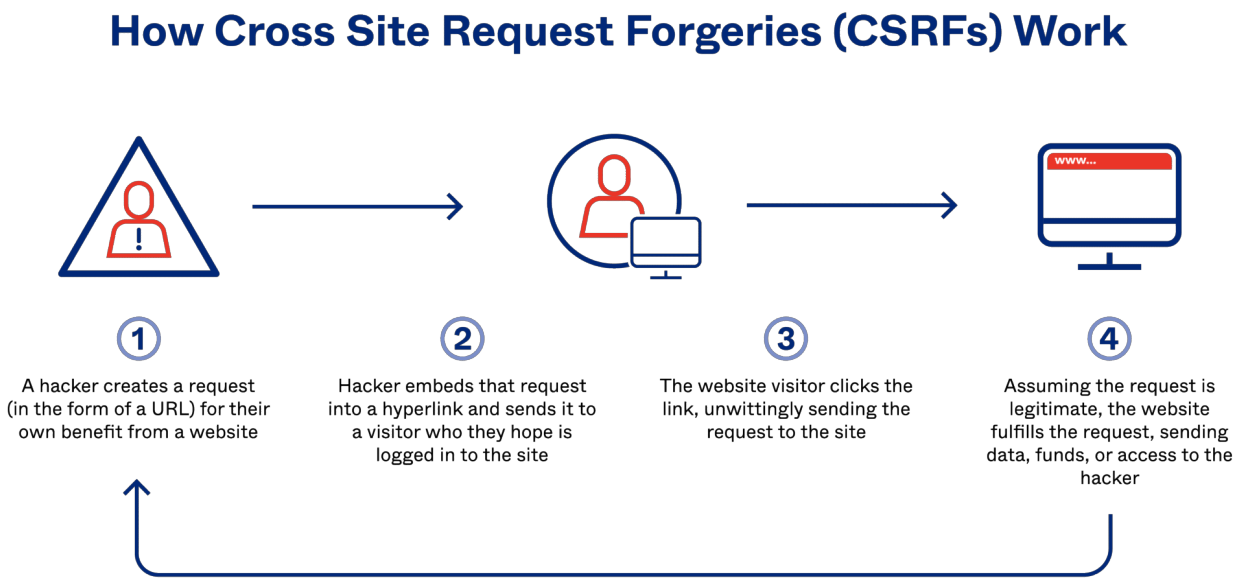
In this section, we will demonstrate various web application attacks to showcase and highlight the significance of the protections the Fortiweb will bring when compared to it's Next Generation Firewall counterpart.

CSRF Attack via FortiGate

What is Cross site request forgery (CSRF) attack?

Cross-Site Request Forgery (CSRF) is a type of security vulnerability that dupes a web browser into executing an undesired action within an authenticated application.

The attack usually involves deceptive social engineering tactics, such as sending a misleading email or link to the victim. Because the user is already authenticated within the application when the attack occurs, it becomes challenging to differentiate between legitimate and fraudulent requests.



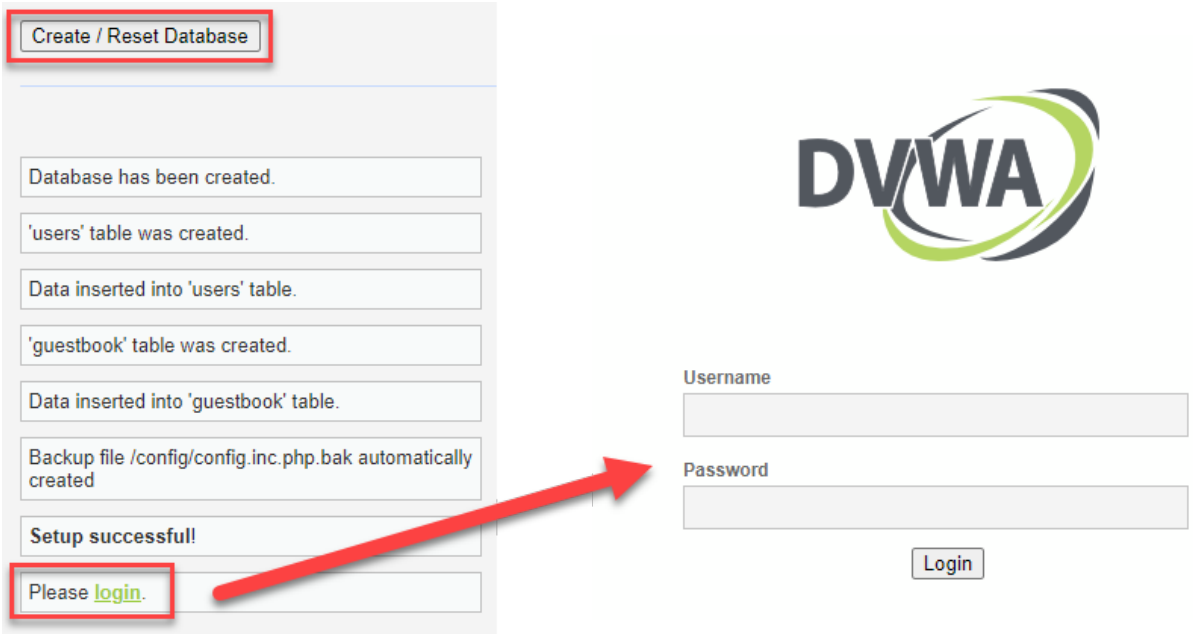
Authenticating to the Web Application

To successfully run the CSRF Attack, you must first authenticate yourself within the application.

Browse to http://@PREFIX-fgt-to-dvwa.@REGION.cloudapp.azure.com and log in using the username **admin** and password **password**.

Troubleshooting - If you encounter any authentication issues

- Browse to http://@PREFIX-fgt-to-dvwa.@REGION.cloudapp.azure.com/setup.php
- Click on **Create / Reset Database**



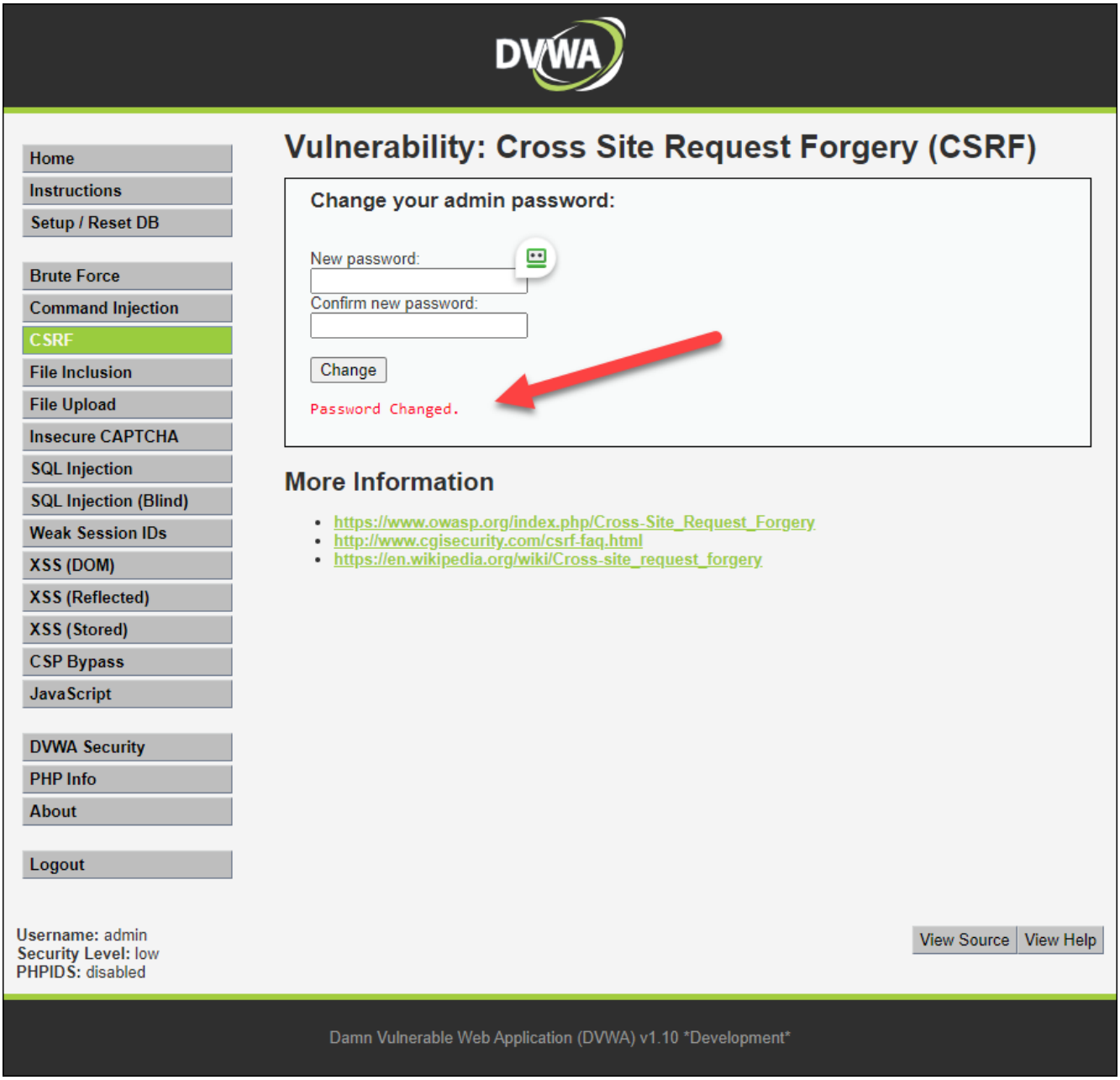
Executing CSRF Attack

Once authenticated to DVWA, click on the **LINK** bellow to generate the attack.

Outlook

Dear user,
All Hotmail customers have been upgraded to Outlook.com. Your Hotmail Account services has expired.
Due to our new system upgrade to Outlook. In order for it to remain active
follow the **LINK** Sign in Re-activate your account to Outlook.
Thanks,
The Microsoft account team

The link employs **Cross-Site Request Forgery** to exploit your authenticated session in order to initiate a password change.

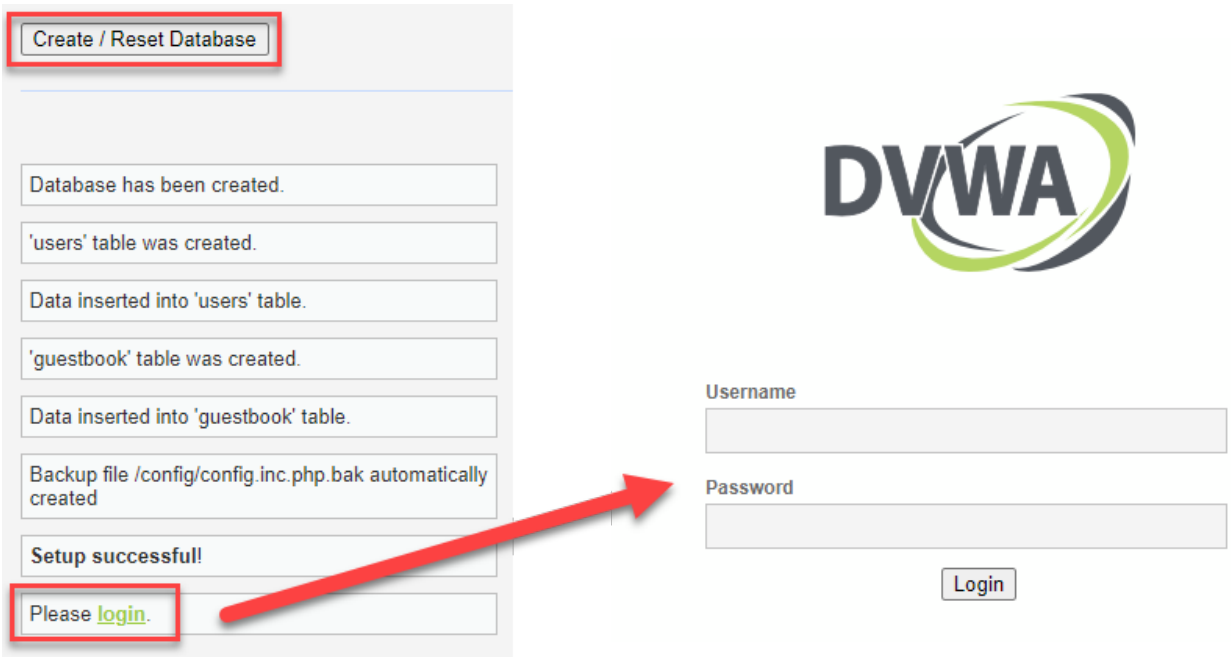


Your password has been changed without your knowledge.

Logout of DVWA and Log back in using `admin:pwned`

Reseting the database for the next Lab

- Browse to http://@PREFIX-fgt-to-dvwa.@REGION.cloudapp.azure.com/setup.php
- Click on **Create / Reset Database**
- You can now login with the original password



Conclusion

We have observed that FortiGate provides an additional layer of protection compared to NSGs, thanks to its WAF signatures. However, we can see that more advanced attacks like CSRF are not addressed by FortiGate.

Cookie Poisoning via FortiGate

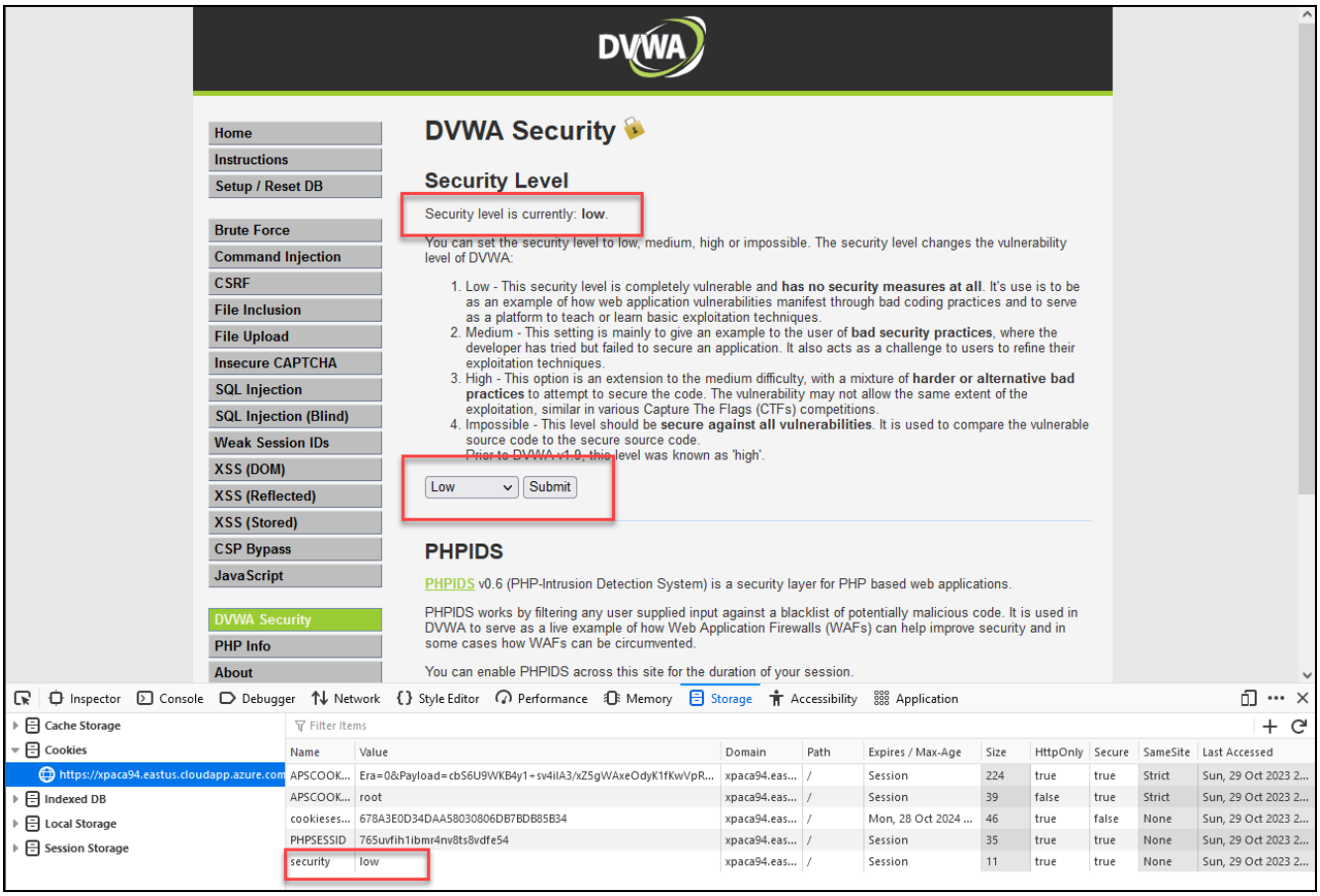
What is Cookie Poisoning?

In this lab, we will delve into the world of cookies - data stored in a user's browser that is specific to a website and session. These cookies serve a variety of purposes, from tracking user behavior to personalizing the online experience. However, they are also susceptible to cookie poisoning, a form of unauthorized manipulation by attackers aiming to gain access to sensitive information or services. This is particularly concerning because cookies often contain authentication data and other sensitive details, making them a prime target for hackers.

Changing Security Level Through Legitimate Web App Interactions

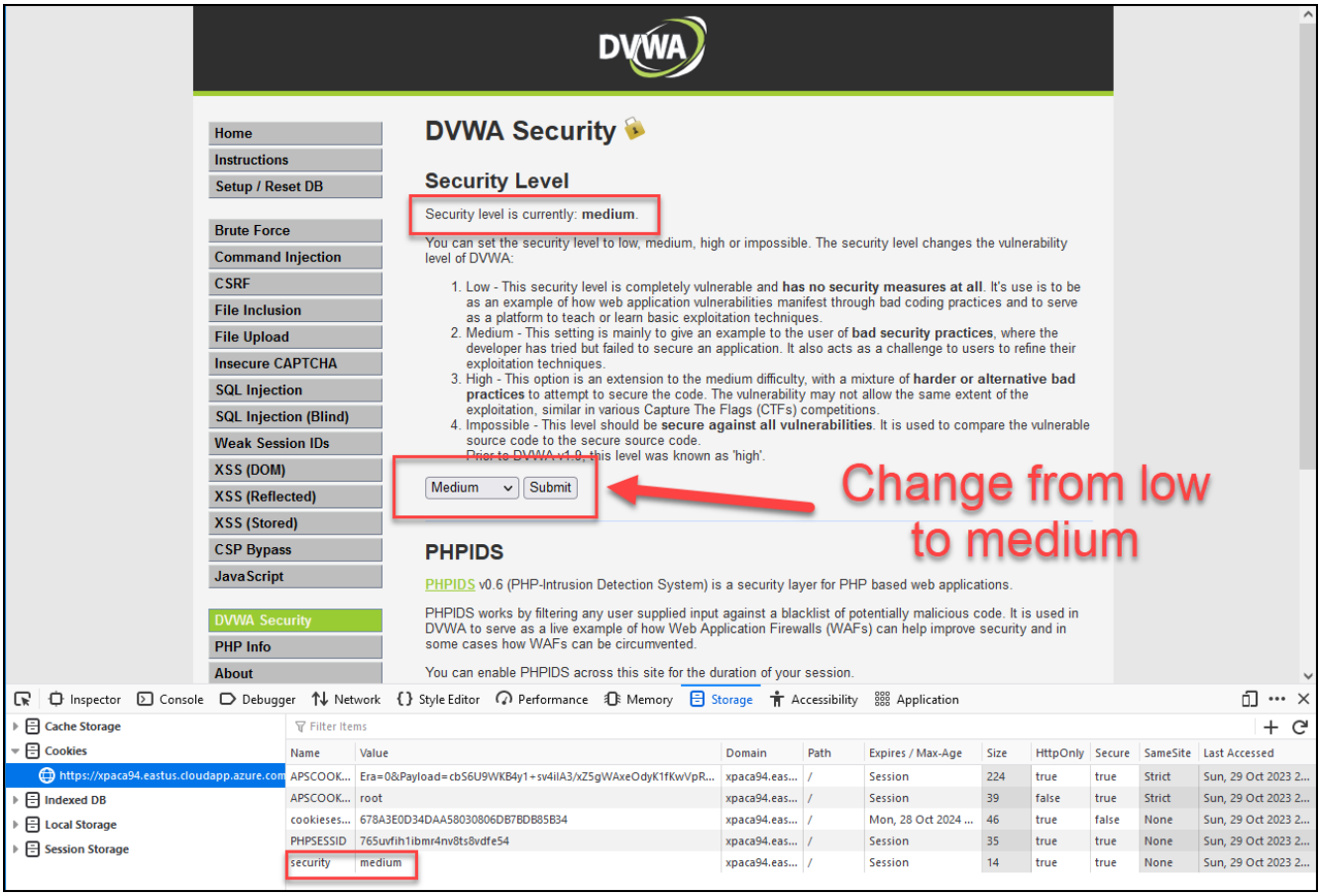
Browse to @PREFIX-fgt-to-dvwa.@REGION.cloudapp.azure.com/security.php

Right click the page and select **Inspect**, go to **Storage** (Firefox) or **Application** (Chrome, Edge) and select **Cookies**.



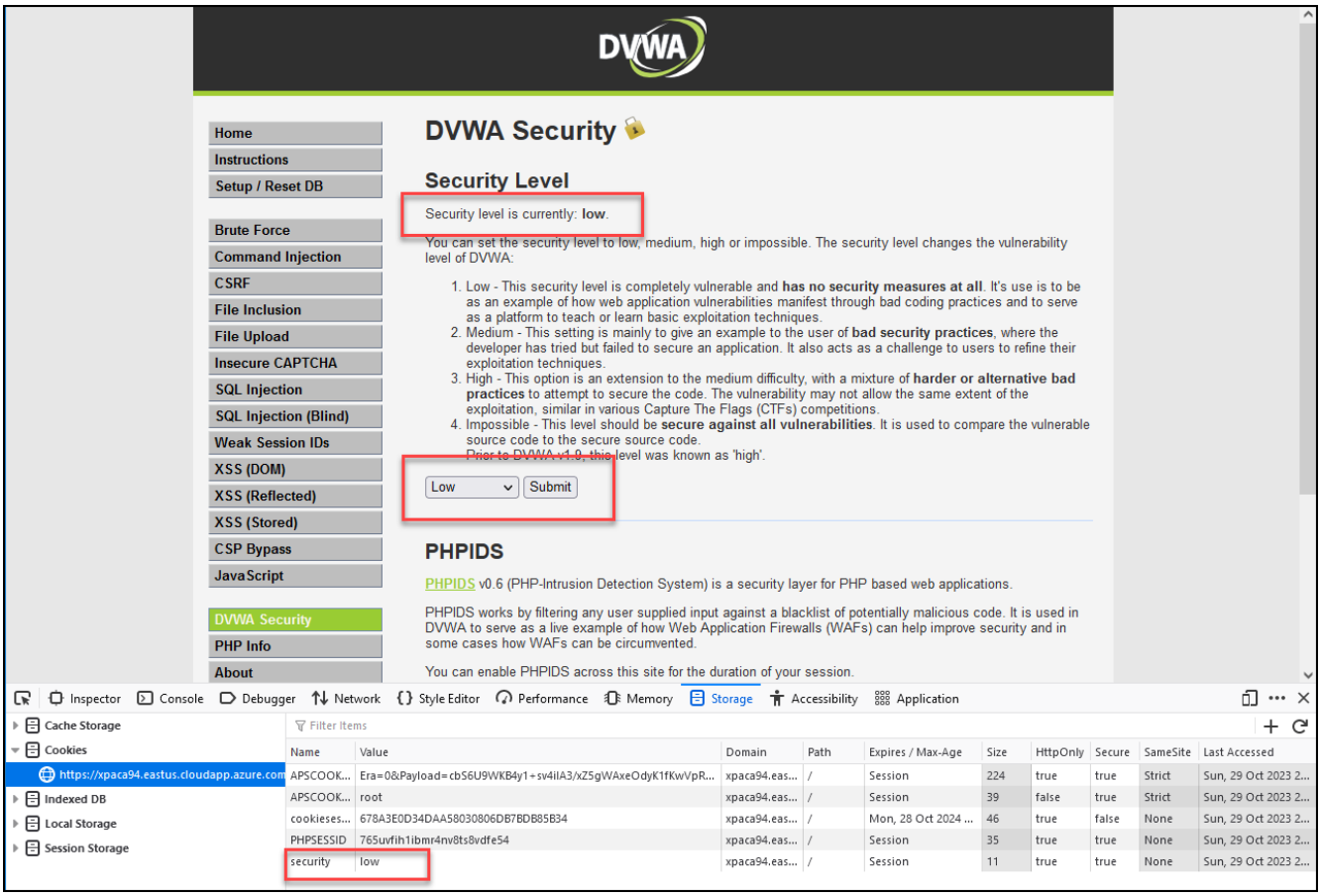
The security level granted to the user is stored in the cookie.

From the **Web page**, select **Medium** and click **submit**. This is a legitimate action, and your security level has changed.


DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
DVWA Security
PHP Info
About
DVWA Security
Security Level
Security level is currently: medium.
You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:
1. Low - This security level is completely vulnerable and has no security measures at all. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of bad security practices, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of harder or alternative bad practices to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be secure against all vulnerabilities. It is used to compare the vulnerable source code to the secure source code.
Prior to DVWA v1.9, this level was known as 'high'.
Medium
Submit
Change from low to medium
PHPIDS
PHPIDS v0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.
PHPIDS works by filtering any user supplied input against a blacklist of potentially malicious code. It is used in DVWA to serve as a live example of how Web Application Firewalls (WAFs) can help improve security and in some cases how WAFs can be circumvented.
You can enable PHPIDS across this site for the duration of your session.
Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Storage
Accessibility
Application
Cache Storage
Cookies
https://xpaca94.eastus.cloudapp.azure.com
Indexed DB
Local Storage
Session Storage
Filter Items
Name
Value
Domain
Path
Expires / Max-Age
Size
HttpOnly
Secure
SameSite
Last Accessed
APSCOOK...
Era=0&Payload=cbS6U9WKB4y1+sv4ilA3/xZ5gWAxeOdyK1fKwVpR...
xpaca94.eas...
/
Session
224
true
true
Strict
Sun, 29 Oct 2023 2...
APSCOOK...
root
xpaca94.eas...
/
Session
39
false
true
Strict
Sun, 29 Oct 2023 2...
cookieses...
678A3E0D34DAA58030806DB7BDB85B34
xpaca94.eas...
/
Mon, 28 Oct 2024 ...
46
true
false
None
Sun, 29 Oct 2023 2...
PHPSESSID
765uvfih1ibmr4nv8ts8vdfe54
xpaca94.eas...
/
Session
35
true
true
None
Sun, 29 Oct 2023 2...
security
medium
xpaca94.eas...
/
Session
14
true
true
None
Sun, 29 Oct 2023 2...

Overriding Security Level with Malicious Cookie Manipulation

Instead, now change the **security cookie** value manually to **low** and **reload** the page.



Notice we were able change the DVWA's security setting by tampering with the value of the **security cookie**.

Hidden Fields Manipulation via FortiGate

What is Hidden Fields

Hidden form inputs are often written into an HTML page by the web server when it serves that page to the client and are not visible on the rendered web page. Because HTTP is essentially stateless, like cookies, hidden form inputs are one way that web applications can use to remember session data from one page request to the next (called “persistence”).

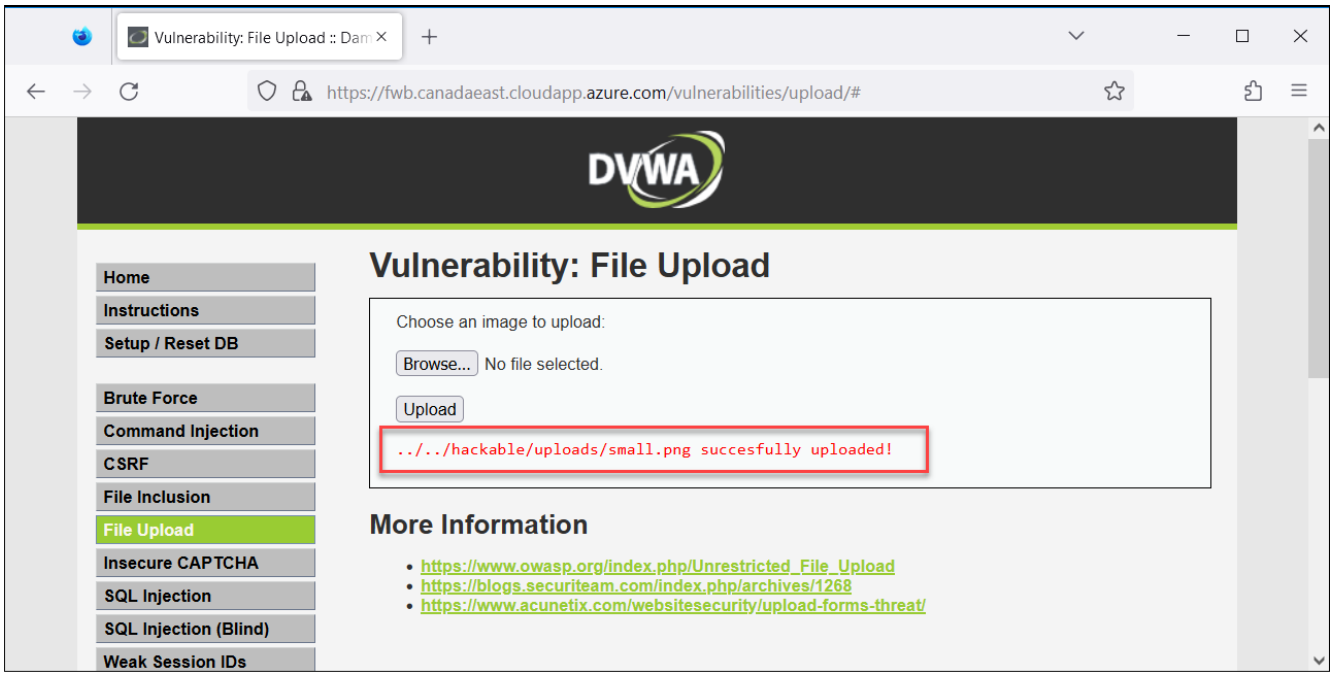
Since they are not rendered visible, hidden inputs are sometimes erroneously perceived as safe. But like session cookies, hidden form inputs store the software’s state information client-side, instead of server-side. This makes it vulnerable.

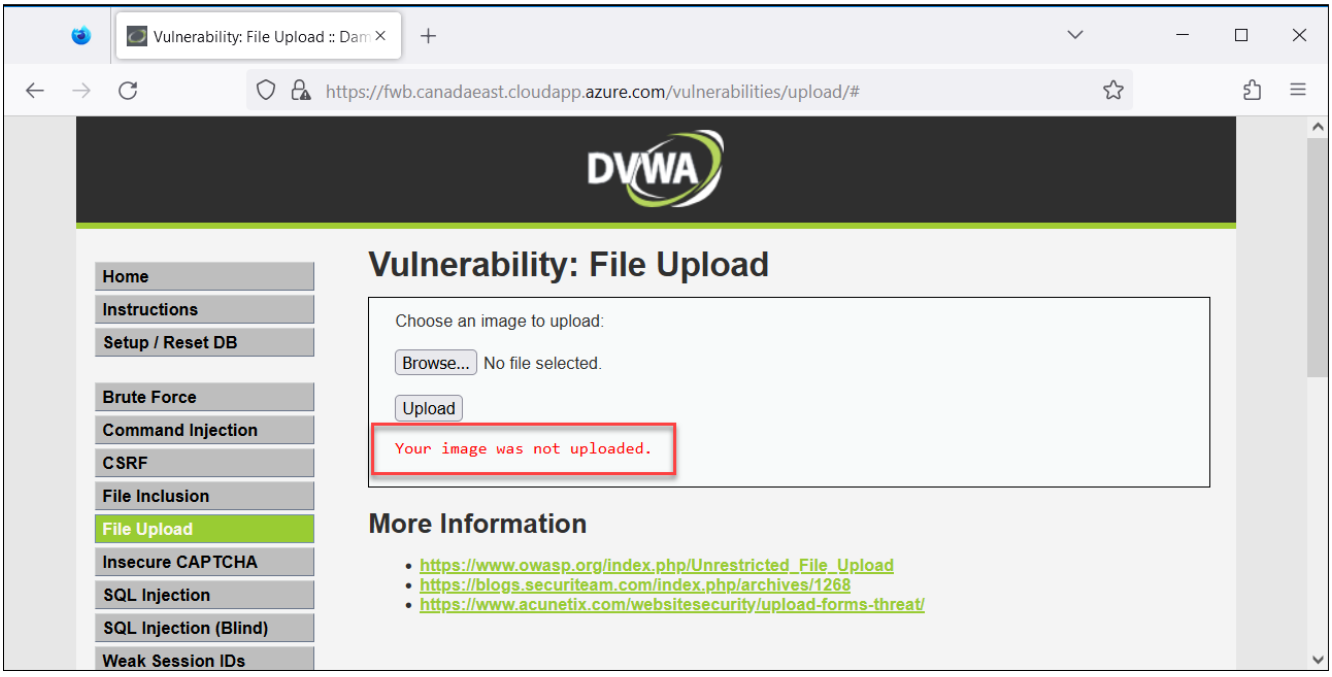
Enforcing File Size Limitations – Successfully Blocking a Large File Upload

Download those 2 images to your computer:

- Small Image (14Ko)
- Large Image (433Ko)

Go to @PREFIX-fgt-to-dvwa.@REGION.cloudapp.azure.com/vulnerabilities/upload and upload the two images one at a time.

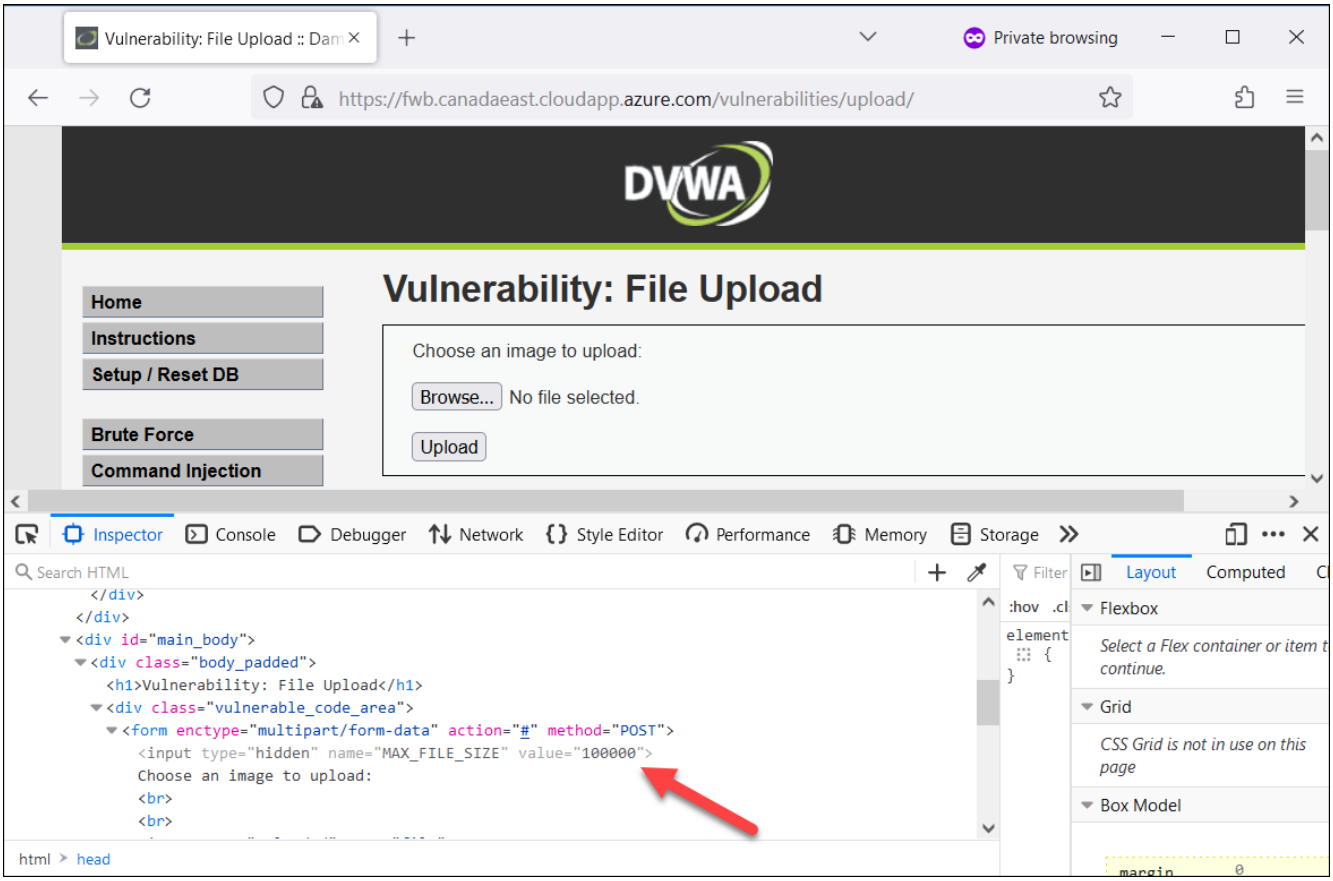




The website enforces a policy that prohibits the uploading of images larger than 100 KB. Let's see how we can bypass the policy restrictions.

Bypassing Policy Restrictions to Upload a Large File

Right click the page, select **Inspect**, go to **Inspector** tab (Firefox) or **Element** tab (Chrome, Edge) and find the **MAX_FILE_SIZE** hidden form.



Change the value to **500,000** and try to upload the large image again. Notice you were now able to successfully upload the larger file.

Conclusion

In summary, though the FortiGate is not inherently bound to the use of signatures, many functionalities revolving around Web Applications, IPS and AV are. This means, for attacks that do not have a corresponding signature, the FortiGate will be vulnerable to many unknown attacks.

In the next lab, we will evaluate FortiWeb and explore how to comprehensively protect a web application.

Info

To view the WAF Feature Comparison between FortiWeb and FortiGate, navigate to the Reference Architecture section.

3.2 Protecting Web Application Using FortiWeb

To begin, we will connect to the DVWA Web Application through FortiWeb.

Connecting to DVWA

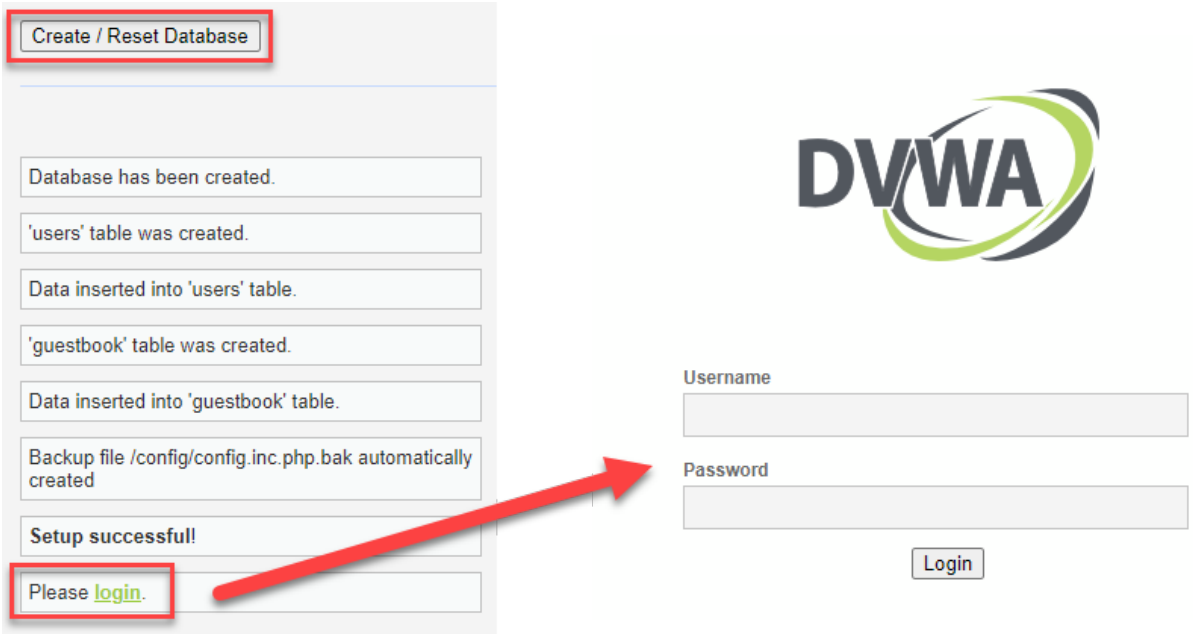
Connecting to DVWA

Connect to https://@PREFIX.@REGION.cloudapp.azure.com and authenticate with one of these accounts:

Username	Password
admin	password
gordonb	abc123
1337	charley
pablo	letmein
smithy	password

Troubleshooting - If you encounter any authentication issues

- Browse to https://@PREFIX.@REGION.cloudapp.azure.com/setup.php
- Click on **Create / Reset Database**



This Hands-on Lab allows us to demonstrate 25+ FortiWeb protections. Let's take a closer look at FortiWeb's sequence of scans.

Sequence of Scans

Sequence of Scans

FortiWeb applies protection rules and performs protection profile scans in the order of execution according to the following list. The second tab highlights the security features that will be demonstrated in this Hands-On Lab.

Protections **Highlights**

1. TCP Connection Number Limit (TCP Flood Prevention)
2. Add X-Forwarded-For
3. Client Management
4. IP List
5. IP Reputation
6. Quarantined source IP addresses
7. Known Bots
8. Geo IP
9. WebSocket protocol
10. Add HSTS Header
11. Protected Server Check
12. Allow Method
13. Mobile Application Identification
14. HTTP Request Limit/sec (HTTP Flood Prevention)
15. TCP Connection Number Limit (Malicious IP)
16. HTTP Request Limit/sec (Shared IP) (HTTP Access Limit)
17. HTTP Authentication
18. Global Object Allow List
19. ADFS Proxy
20. URL Access
21. Mobile API Protection
22. Padding Oracle Protection
23. HTTP Protocol Constraints
24. File Parse
25. File Security
26. Web Shell Protection
27. Parameter Validation
28. Bot Deception
29. ML based Bot Detection
30. Cross-site request forgery (CSRF) attacks
31. Protection for Man-in-the-Browser (MiTB) attacks
32. Biometrics Based Detection
33. XML Protection
34. JSON Protection
35. Signatures
36. SQL/XSS Syntax Based Detection
37. Site Publish
38. Hidden Fields Protection
39. Custom Policy
40. Threshold Based Detection
41. User Tracking
42. API Gateway
43. OpenAPI Validation
44. CORS Protection
45. URL Rewriting (rewriting & redirection)
46. ML based API Protection
47. File Compress
48. Cookie Security Policy
49. ML based Anomaly Detection