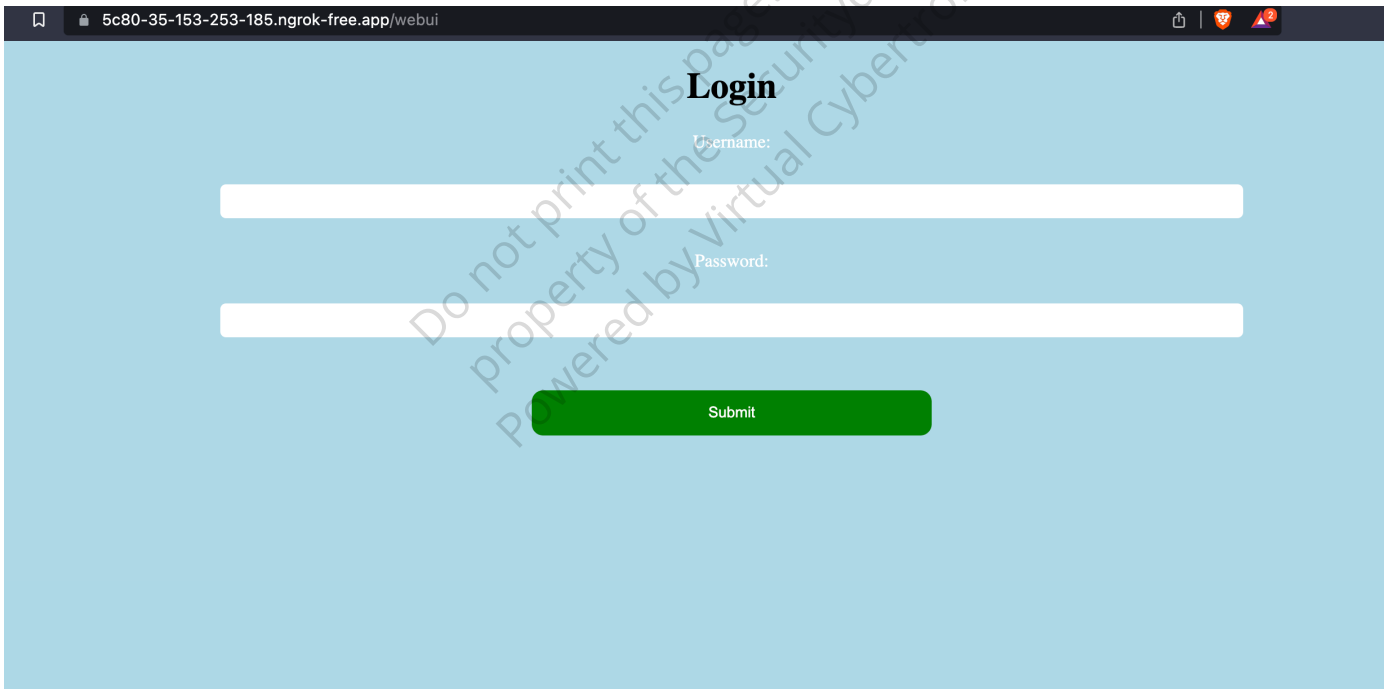
# Lab: Enumeration: From Vulnerable Cluster Web UI

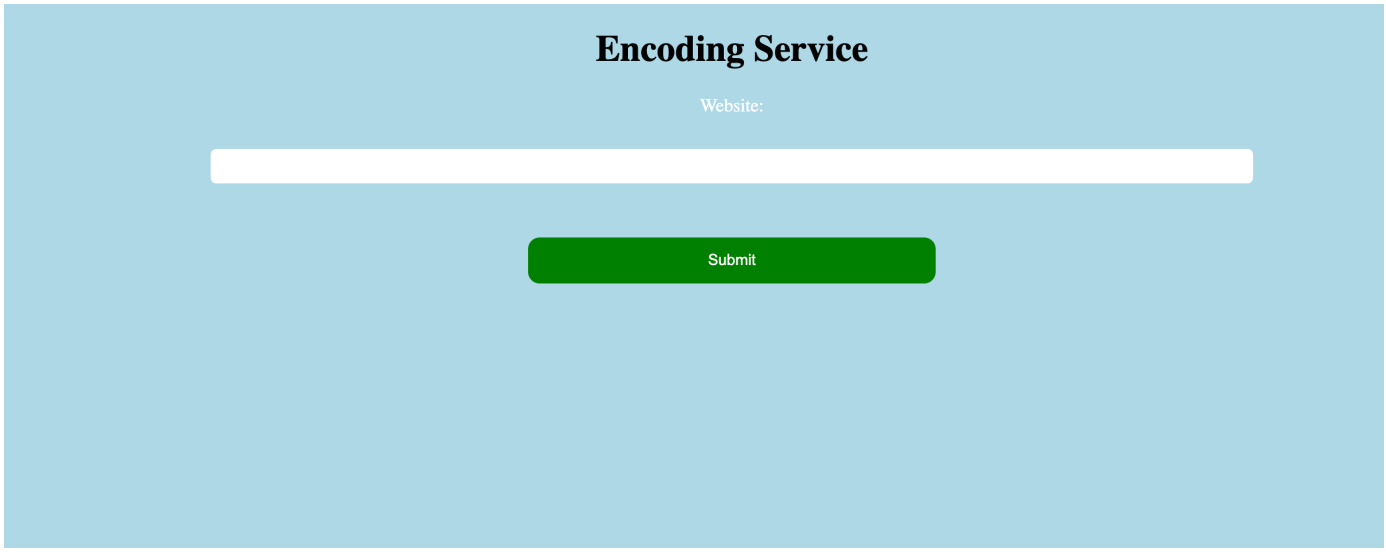
## Frontent

- Open Web URL In The Browser.
- Try signing in with the following credentials:
  - Username: `admin`
  - Password: `admin`
- You should be able to login successfully and see the flag.






- There is another hidden encoding service, try to find the encoding service and exploit the vulnerability.
- Get the Kubernetes Secret details.




# Backend.



## Demo By Trainer

- Change directory to `/Users/securitydojo/Desktop/training/Course/training/kubernetes/insecure-python-microservice`.

```
cd /Users/securitydojo/Desktop/training/Course/training/kubernetes/insecure-python-microservice
```

- Ssh into the bastion host.

```
ssh -i infrastructure/terraform/6zif0-bastion_key.pem ubuntu@54.158.240.88
```

- SSH into the worker-node-2

```
ssh -i ec2_key.pem ubuntu@10.0.1.76
```

- Switch to root user.

```
sudo su
```

## Kyverno Live Demo

- Try exec into the microservice pod.

```
kubectl get pods
```

```
kubectl exec microservice2-b5f4f694d-jjkcm -- cat /etc/passwd
```

- Check the error `resource PodExecOptions/default/ was blocked due to the following policies` due to gatekeeper

```
root@ip-10-0-1-76:/home/ubuntu# kubectl exec microservice2-b5f4f694d-jjkcm -- cat /etc/passwd
Error from server: admission webhook "validate.kyverno.svc-fail" denied the request:

resource PodExecOptions/default/ was blocked due to the following policies

deny-exec-by-namespace-name:
  deny-exec-ns-pci: Pods in this namespace may not be exec'd into.
```

- Delete the kyverno policy as we are root user.

---

Do not run the application as root & do not allow users to perform ssh into node via `default` user like ec2, ubuntu & root user.

---

```
delete -f insecure-python-microservice/kyverno/
```

- Try exec into the microservice pod & run command as malicious user.

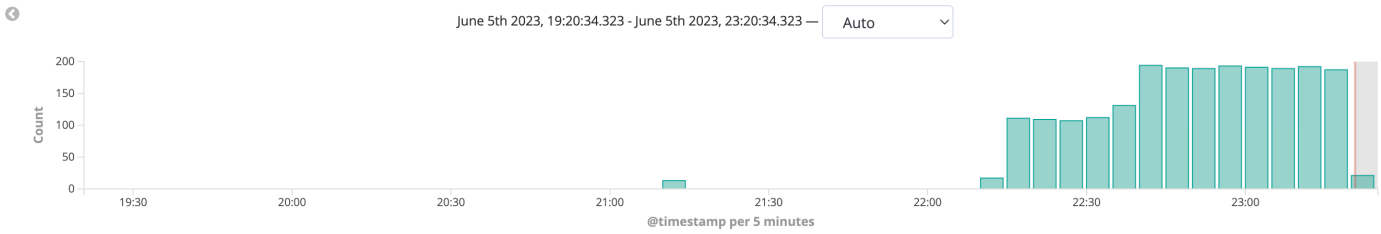
```
kubectl exec microservice2-b5f4f694d-jjkcm -- cat /etc/shadow
```

- Check the falco ELK UI to validate the results.

---

Explore the EFK stack.

---




| Time | _source |
|---|---|
| June 5th 2023, 23:20:27.392 | log: Reading /etc/shadow... stream: stdout docker.container_id: 087b6dd28302128da70636a5adfc9054550854c6a157b46c653ee3baffb50270 kubernetes.container_name: falco-event-generator kubernetes.namespace_name: default kubernetes.pod_name: falco-event-generator-deployment-ff5c77455-6mvmb kubernetes.pod_id: 0949ebec-1ba0-4aa4-8404-6f39edc1dd0a kubernetes.labels.app: falco-event-generator kubernetes.labels.pod-template-hash: ff5c77455 kubernetes.labels.security_istio_io/tlsMode: istio kubernetes.labels.service_istio_io/canonical-name: falco-event-generator kubernetes.labels.service_istio_io/canonical-revision: latest kubernetes.host: ip-10-0-1-76 |
| June 5th 2023, 23:20:25.412 | output: 17:50:23.390212232: Warning Sensitive file opened for reading by non-trusted program (user=root program=event_generator command=event_generator file=/etc/shadow parent=docker-entrypoi gparent=containerd-shim ggparent=systemd gggparent=<NA> container_id=087b6dd28302 image=justmorpheu5/falco-event-generator) k8s.ns=default k8s.pod=falco-event-generator-deployment-ff5c77455-6mvmb container=087b6dd28302 output_fields.fd.name: /etc/shadow log: {"hostname":"falco-daemonset-bbg2v","output":"17:50:23.390212232: Warning Sensitive file opened for reading by non-trusted program (user=root program=event_generator command=event_generator file=/etc/shadow parent=docker-entrypoi |
| June 5th 2023, 23:20:24.317 | log: Reading /etc/shadow... stream: stdout docker.container_id: 2c55c98a02cf489704669f985f7fe5fe7483ea2a5f46c2ee5cc264f79bab7aa8 kubernetes.container_name: falco-event-generator kubernetes.namespace_name: default kubernetes.pod_name: falco-event-generator-deployment-ff5c77455-dfpxz kubernetes.pod_id: 5375c439-ddcd-4e9a-b44a-2069d3371e4d kubernetes.labels.app: falco-event-generator kubernetes.labels.pod-template-hash: ff5c77455 kubernetes.labels.security_istio_io/tlsMode: istio kubernetes.labels.service_istio_io/canonical-name: falco-event-generator kubernetes.labels.service_istio_io/canonical-revision: latest kubernetes.host: ip-10-0-1-162 |

- Run `exit` to exit the lab.