Attack#3-Gain env info with hardcoded secret

Related configurations: [Attack#3.json](https://drive.google.com/open?id=1FoBL1EZx0vnKAnKAQvYw7UZf5UnmzyBI)

1. Apply all insecure configs in Attack3.json.
2. kubectl exec -it checkoutservice- -n default -- sh
3. The Attacker can directly access to the hard-coded secret (**#1**) with misconfiguration environment variable references a Secret contains that hard-coded secret (**#2**)
   1. Command: printenv

