1. ESP registration:

The application needs to be registered in ESP and ESP link shared. <https://wiki.cisco.com/display/INFOSEC/Registering+%28Creating%29+an+Application>

2. SSO: There must be authentication in place for the application. INtegration with SSO is one option. SSO team's wiki link is: <https://wiki.cisco.com/display/GISIAM/PingFederate+Portal>

3. SSL: The application must be over HTTPS/SSL enabled. Trusted SSL certificates can be obtained from here: <https://sslcerts.cisco.com/sslrequest/>

4. The application's source code needs to be checked for vulnerabilities. This can be done using a tool for python "bandit": <https://pypi.org/project/bandit/>

Results must be shared with appsec team for review.

5. The openstack host/source host must be scanned for vulnerabilities through a tool called "qualys". The self-service link is "<https://ndcs-workflow.cisco.com/QualysSelfScan>". Results must be shared with appsec team for review. (helpdesk: <https://infosec-jira.cisco.com/jira/servicedesk/customer/portal/6/group/42?groupId=42>)

Solutions

Vulnarabilities - TLS1.0

<https://www.digitalocean.com/community/questions/disable-old-tls-versions-1-0-1-1-for-apache-nginx-on-ubuntu-18-04-or-centos-7>

sudo vim /etc/apache2/mods-available/ssl.conf

Change:

SSLCipherSuite  
SSLProtocol

To:

SSLCipherSuite "ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384"  
SSLProtocol TLSv1.2

Directory traversal:

sudo vim /etc/apache2/sites-available/default-ssl.conf

Add below under <Lcoation>

<Location "/">

RedirectMatch 400 etc|passwd

</Location>

HTTP Security Header Not Detected

sudo vim /etc/apache2/sites-available/default-ssl.conf

Add below:

Header always append X-Frame-Options SAMEORIGIN  
Header set X-XSS-Protection "1; mode=block"  
Header set X-Content-Type-Options nosniff

Remove Apache default page

<https://serverfault.com/questions/790337/cannot-remove-apache2-ubuntu-default-page>

sudo vim /etc/apache2/apache2.conf

Remove below:

<Directory /var/www>…

</Directory>