



Høyskolen
Kristiania

The Black Arts of IT

ETH2100
Etisk Hacking

Arbeidskrav




Arbeidskrav

Pentest av web applikasjon

Futura Business Informatique GR x +

← → ↻ ⚠ Ikke sikker | 192.168.198.131 ☆ 📄 ⚙ ⋮

» | 📁 Andre bokmerker | 📅 Leseliste

 Futura Business Informatique

Home

Don't have an Account ? 🔑 Login

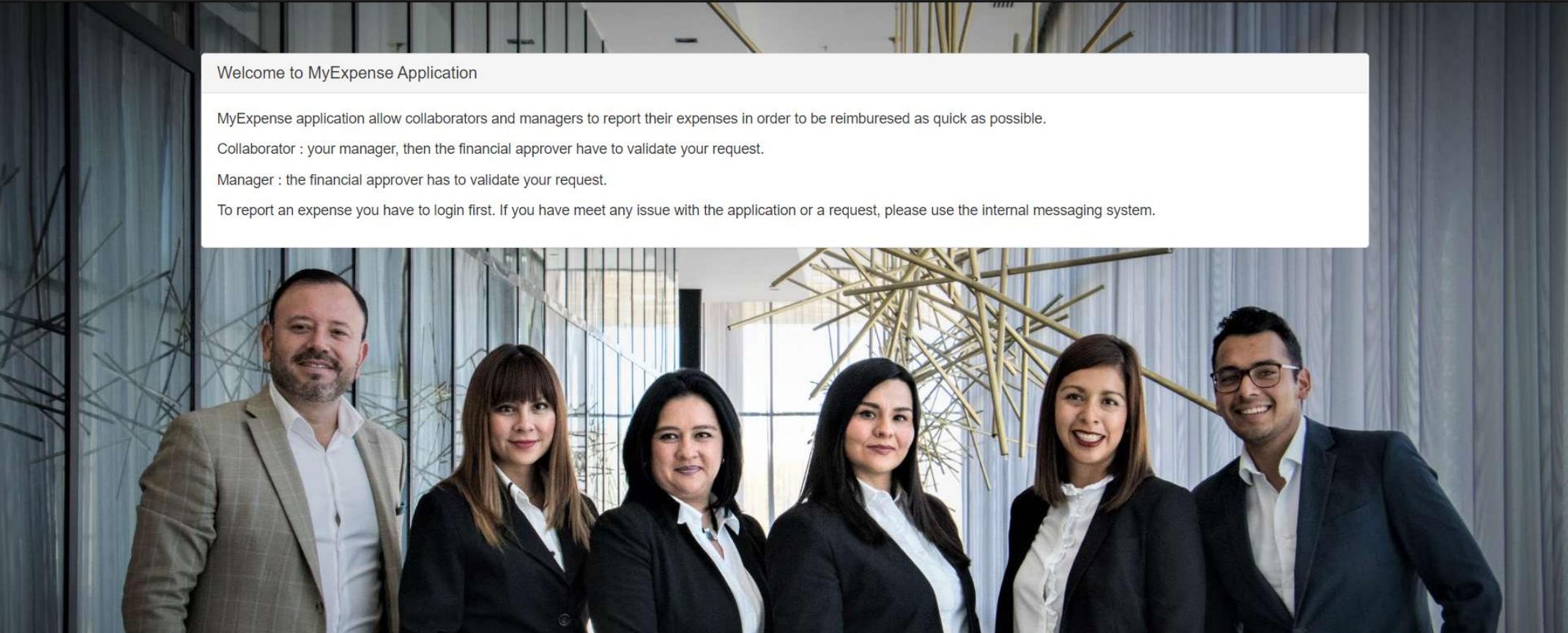
Welcome to MyExpense Application

MyExpense application allow collaborators and managers to report their expenses in order to be reimbured as quick as possible.

Collaborator : your manager, then the financial approver have to validate your request.

Manager : the financial approver has to validate your request.

To report an expense you have to login first. If you have meet any issue with the application or a request, please use the internal messaging system.



Arbeidskrav

- ***Teknisk sårbarhetsrevisjon***
- Dere skal gjennomføre en «penetrasjonstest» (teknisk sårbarhetsrevisjon) av en web applikasjon.
- Applikasjonen finner dere under ARBEIDSKRAV på Canvas, og ligger i filen ETH2100_U37_Arbeidskrav_VM_H23.zip. Filen inneholder et VmWare image dere skal starte, og som kjører en web applikasjon. Imaget er konfigurert til å kun bruke nettverksadapteret Host-Only (VmNet1).
- Filen blir tilgjengelig **etter** forelesning torsdag 14. september

Arbeidskrav

- Kunden ønsker å gjennomføre en Web Application «penetrasjonstest» av applikasjonen. Testen kan gjennomføres som en whitebox test, så dere som testere får tilgang til maskinen og kan gjennomføre statisk kodeanalyse hvis ønskelig. Dere kan logge inn lokalt på maskinen med følgende konto:
 - Brukernavn: osboxes
 - Passord: osboxes.org
- Kunden anser ikke lokal tilgang til server som en potensiell angrepsvektor og definerer derfor knekking av lokal innlogging som «out of scope».

osboxes@osboxes: ~

Edit View Search Terminal Help

osboxes@osboxes:~\$ su

word:

osboxes:/home/osboxes# hostname -I

68.198.131

osboxes:/home/osboxes# systemctl status apache2

apache2.service - The Apache HTTP Server

Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset:

State: active (running) since Fri 2021-11-05 08:54:12 EDT; 2min 17s ago

Docs: <https://httpd.apache.org/docs/2.4/>

Process: 609 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)

Main PID: 696 (apache2)

Tasks: 6 (limit: 2319)

Memory: 26.5M

Group: /system.slice/apache2.service

└─696 /usr/sbin/apache2 -k start

└─735 /usr/sbin/apache2 -k start

└─736 /usr/sbin/apache2 -k start

└─737 /usr/sbin/apache2 -k start

└─738 /usr/sbin/apache2 -k start

└─739 /usr/sbin/apache2 -k start

5 08:54:11 osboxes systemd[1]: Starting The Apache HTTP Server...

5 08:54:12 osboxes apachectl[609]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.0.1 as fallback

5 08:54:12 osboxes systemd[1]: Started The Apache HTTP Server.

Starte VM

Leveranser

1. Pentest rapport i PDF format
 2. Powerpoint for «kunden»
- Leveres inn i WiseFlow eller Canvas (avklaring kommer i uke 39)
 - Innleveringsfrist fredag 29. september klokken 12.00

Arbeidskravet blir Bestått / Ikke Bestått

OBS: Tilsvarende (men en annen) pentest inngår i mappevurderingen i faget!



Høyskolen
Kristiania