



Høyskolen
Kristiania

Det er mer å finne..

- Dagens Øving er å gjenta det som ble demonstrert og fortsette å gå gjennom og lete etter svakheter
- Gå først gjennom «normal bestilling» og tegn deg et kart.
 - Så kan du begynne å «forske».
 - Hvis serveren krasjer så må du restarte den
 - Husk at hvis du prøver på stygge ting – det er din egen PC det går utover ;-)
- Injiserer du «DROP TABLE»-utsagn, må du nok sette opp MySQL på nytt, eller kanskje du klarer å ødelegge mer...

Hvordan sette opp miljø?

- Last ned flowershop-20170315T134709Z-001.zip
- Pakk ut innholdet

feks: C:\Privat\Westerdals\flowershop\flowershop*

- Installer en web server, feks Abyss WS
- Installer PHP på serveren slik:

<http://aprelium.com/abyssws/php5win.html> [Windows instruksjoner]

<https://aprelium.com/abyssws/php.html> [Mac instruksjoner]

MEN du MÅ bruke noe som er eldre enn 5.5,

jeg anbefaler build 5.2.12, herfra <http://aprelium.com/downloads/>

Hvordan sette opp miljø?

- Obs: Hvis du har MySql installert på maskinen fra før, da skal du ikke installere på nytt (man kan kun installere en versjon av et program samtidig)
- Installer MySQL ved å laste ned (Windows brukere):
<https://dev.mysql.com/downloads/installer/>
(Velg «No thanks, just start my download» når han ber deg om konto)
Anbefales å laste ned MSI installer, og det holder med «Server Only»
Velg «Legacy password authentication»
- For Mac maskiner er linken her:
<https://dev.mysql.com/doc/mysql-osx-excerpt/5.7/en/osx-installation.html>

Hvordan sette opp miljø?

- Opprett database fra .sql fil:
 - > cd \Program Files\MySQL\MySQL Server 8.0\bin
 - > mysql.exe -u root -p
 - Mysql> source e:\privat\nith\flowershop\flowershop\sql\create_db.sql
 - Mysql> USE mysql
 - Mysql> SELECT * FROM guestbook;
 - Hvis du får «Empty set» virker det, hvis du får feilmelding har du gjort noe galt ;-)
 - Mysql> SHOW tables;
 - Får du listet ut en haug med tabeller er du ok, igjen får du feilmelding så... ;-)
- **ELLER;** Opprett en database manuelt (ikke gjør begge):
 - <http://www.wikihow.com/Create-a-Database-in-MySQL>
 - CREATE DATABASE flowershop;
 - USE flowershop;
 - CREATE TABLE guestbook (msgfrom CHAR(30) primary key, message CHAR(200));
 - (Og så videre for hele schema...)

Hvordan sette opp miljø?

- Rediger flowershop\flowershop\flowershop.conf:
 \$rootdir = "/TK2100/flowershop";
 \$siteroot = "http://127.0.0.1/flowershop/";
 \$administrator = "*minbruker@westerdals.no*";
 \$uploaddir = "/Privat/NITH/flowershop/";
 \$uploadroot = "/flowershop/uploads";
 \$host = "127.0.0.1";
 \$dbname = "*mysql*";
 \$webuser = "root";
 \$webuserpasswd = "*MITTPASSWORD*";
- For «Default Host On Port 80» utfør:
 - Velg «Configure», og så «General»
 - Under «Documents Path» velg katalogen hvor du pakket ut innholdet av zip filen
 feks: E:\Privat\NITH\flowershop
 - Trykk OK
 - Trykk RESTART (to apply the modifications)
 - På hovedsiden, velg «Start» hvis status for serveren er Stopped

Hvordan sette opp miljø?

- Du kan nå åpne en browser og velge
`http://127.0.0.1/flowershop`
Vær obs på at jeg brukte flowershop/flowershop (to kataloger), det gjør config fila mer oversiktlig...

Disclamer; Jeg (Bengt) har bare testet deler av denne websiden (som var utviklet av noen andre), det kan være at dere må inn å endre i SQL oppsett eller i PHP koden hvis dere finner feil. (Gjesteboken fungerer fint, så test med den først ;-)

ADVARSEL

- Hvis du googler etter exploits, ikke last exploits som modifiserer filer på serveren, er du uforsiktig sletter du ting du vil ha (for eksempel kernel32.dll) på DIN maskin
- Jeg ville ha tatt PCen av nett når du jobber, du åpner en sårbar tjeneste på port 80 + SQL server, på DIN maskin, som andre på internett kan finne og exploite!
- Etter at du er ferdig, stopp (eller avinstaller) både MySQL og Abyss WS

For viderekommende

- Ble dette for enkelt?
- Lyst til å teste «penetrasjonstesting» slik profesjonelle gjør det?
- Zenmap – portscanning og sårbarhetsscan
- OWASP ZAP – http proxy
- Nessus – sårbarhetsscan
- (Profesjonelle gjør også mye manuelt)

For MAC brukere

**Lessons learned?
+ løsning for MacOS Big Sur**

Versjonen beskrevet er 32 bit = MAC problemer 😊

- Hvis du bruker ny Mac med M1 ARM prosessor tror jeg som sagt på høst semesteret at du må installere Windows i en virtuell maskin og gjøre øvingsoppgaven der
- Det kan være det er mulig å løse øvingsoppgaven direkte på M1 chip, men jeg har ingen måte å teste det på, og erfaringsmessig er 2 timer for kort til å hjelpe studenter fra scratch da det er mange studenter som trenger hjelp, så jeg kan ikke sitte kun ett sted...
- Bruker du Intel prosessor, men av den «nye» typen som kun er 64 bit (Catalina eller Big Sur OSX) så har jeg i fjor testet på min virtuelle Mac og har dokumentert en veiledning som er mer detaljert på de neste 10 slidene 😊

Noen erfaringer fra tidligere år

- Disse rådene vil også gjelde for Windows, dette er typiske feil jeg har observert studenter gjøre på denne øvingen:
 - Hvis man velger noe annet enn port 80; <http://127.0.0.1:8000> 😊
 - Hvis man blir bedt om å «laste ned» PHP filer har man ikke fulgt instruksene på Slide 3 - <https://aprelium.com/abyssws/php.html>
 - I min eksempel konfigurasjon har jeg pakket ut filene slik at det er 2 kataloger «flowershop»; feks:
C:_Westerdals\flowershop\flowershop\index.html
 - Hvis man får opp kataloglisting har du ikke satt Index Files riktig
 - Får man 404 er en av katalogene feil (den finner ikke filen)

MAC brukere?

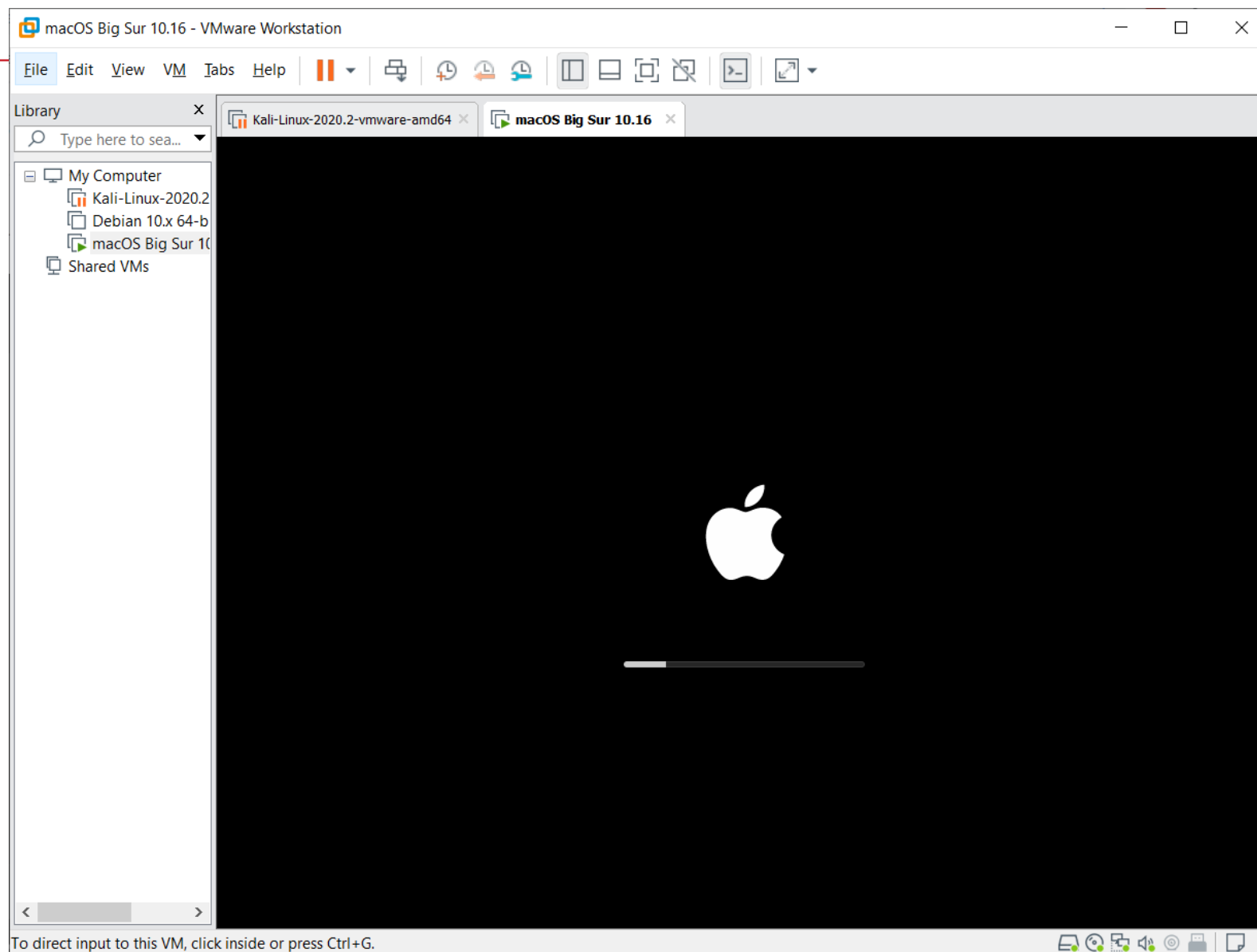
- Mange studenter på Mac kom i fjor så langt at når de trykker på Guestbook får de en 500 feil?
- Da er webserveren nesten satt opp, siste som feiler er at PHP interpreteren ikke virker
- For en Windows bruker var ofte “siste feil” at man ikke brukte “Fast CGI Local Pipes”, men vanskelig for veiledere og meg å forstå om a) det virker, b) det virker fortsatt ikke så studenten ga opp

<https://www.theverge.com/2019/10/12/20908567/apple-macos-catalina-breaking-apps-32-bit-support-how-to-prepare-avoid-update>

<https://www.houstonchronicle.com/techburger/article/Some-of-your-favorite-Mac-apps-will-be-casualties-14088505.php>

Catalina og Big Sur

- Catalina og Big Sur er KUN 64 bit
- Det betyr at for de som kjøpte seg en ny Mac i 2020 eller senere så virker ikke 32 bits applikasjoner, og det inkluderer PHP
- Studentene i fjor hadde gleden av å være det første kullet med dette spesifikke Mac problemet 😊
- Jeg valgte derfor å sette opp en Mac i VmWare – og jobbet med å finne en løsning for Big Sur (og som takk for det valgte Apple i 2021 å gå over til ARM prosessor... ;-)



Precompiles for 64 bit MAC

- Problemet med Flowershop koden er at funksjonen `mysql_connect` brukes, denne ble deprecated i versjon 5.5.0, og ble fjernet i 7.0.0

<https://www.php.net/manual/en/function.mysql-connect.php>

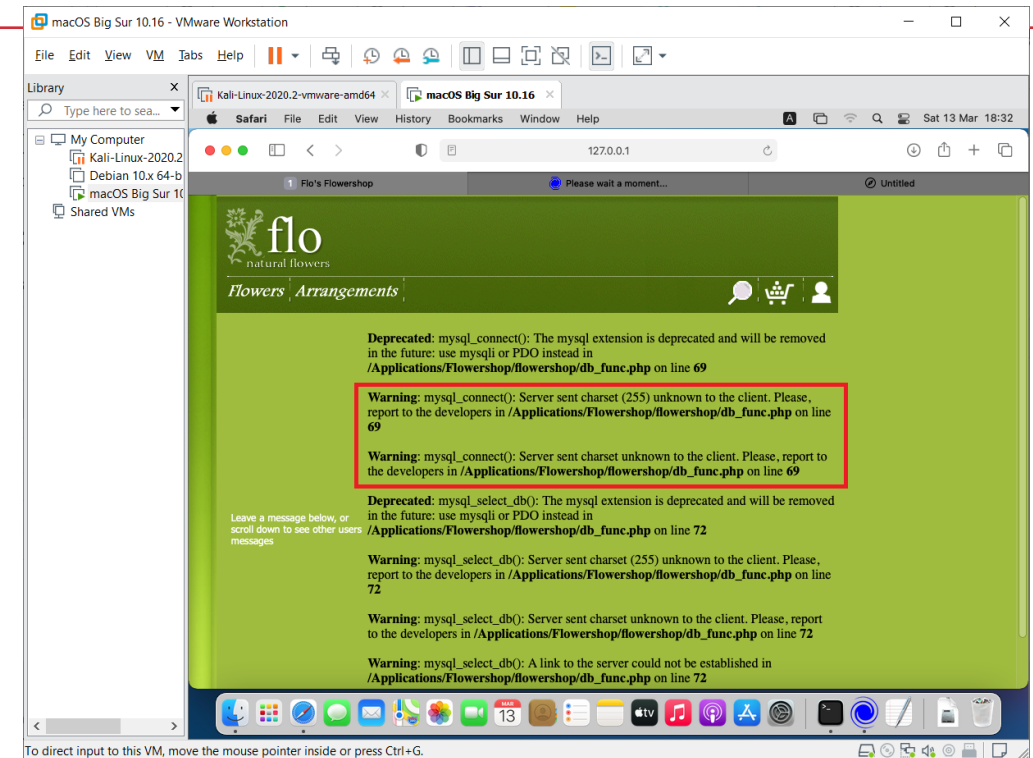
- Her er liste over alt som er precompiled fra Aprelium (5.6.40 er eneste 64 bit build for MAC hvor `mysql_connect` kun vil være deprecated og ikke fjernet)

<https://aprelum.com/downloads/php.html>

- PHP5 bygget er ikke “notarized” av Apple, så det må legges inn unntak for den

<https://macresearch.org/macos-cannot-verify-that-this-app-is-free-from-malware/>

Nytt problem: UTFMB4



- Viser seg at ny MySql (i alle fall på Mac, kanskje Windows også) bruker UTF8MB4 istedefor UTF8 som tegnsett, dette må derfor endres:


<https://thisinterestsme.com/charset-255-unknown-mysql/>

https://www.codegrepper.com/code-examples/sql/MAC+mysql_connect%28%29%3A+Server+sent+charset+%28255%29+unknown+to+the+client.

Løsning for PHP på Catalina / Big Sur

1. Last ned <https://aprelum.com/data/PHP5640.dmg>
2. Åpne DMG filen, høyreklikk på PHP5 mappen og vel Copy
3. Gå til Applications, og velg Paste Item
4. Gå inn i PHP5, gå inn i bin, høyreklikk på php-cgi og velg Open
5. Trykk Open for at den skal bli godkjent av OSet
6. Gå inn i PHP5/lib og åpne php.ini, rediger error_reporting linjen til:
`error_reporting = E_ALL & ~E_DEPRECATED & ~E_NOTICE & ~E_STRICT`
7. Rediger my.ini i MySQL som forklart på forrige slide for å fikse UTF8MB4
8. Restart mysql.server (eller restart hele maskinen)

Fikk jeg ikke til å virke, men er ikke en kritisk fiks...



Scripting parameters skal se slik ut:

Scripting Parameters

Abyss Web Server Console :: Hosts - Edit - Default Host On Port 80 :: Scripting Parameters



[Help](#)

☒ Enable Scripts Execution ?

CGI Parameters ? : **Edit...**

ISAPI Parameters ? : **Edit...**

FastCGI Parameters ? : **Edit...**

Interface	Interpreter	Associated Extensions	
FastCGI (Local - Pipes)	/Applications/PHP5/bin/php-cgi	php	 
Add			

Virtual Path
/*.php
Add

Name	Value
Empty	
Add	

OK

Håper denne guiden hjelper dere med MAC

