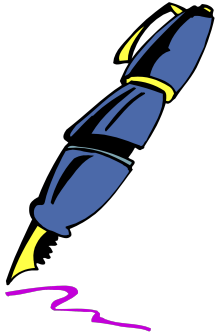
# LABBARNA

## Pentesting

Websäkerhet testas med *penetration testing*, "pentesting".

Detta är metoder för att testa möjligheten, och därmed också risken, för intrång.

Fokus för labbarna!



"Pentesting" har inget med pennor att göra.

## Labborganisation

Labbuppgifterna är obligatoriska och utförs individuellt

Du utför dem på egen tid innan deadline. Du loggar in på vår server med ditt LiU-ID.

Vi har tider då du kan få hjälp. Använd dem väl om du behöver dem.

Du får godkänt när du har klarat de obligatoriska uppgifterna.

## Server och PM

Servern är en typ som kallas "Security Shepherd", ett system för datasäkerhetsträning

Serveradressen för labbarna är *snickerboa.it.liu.se*

Lab-PM finns på kurssidan, med instruktioner, hur du loggar in mm.

## Utmaningskategorier

- CSRF
- XSS
- SQL Injection
- Osäker krypterad lagring
- Osäkta direkta objektreferenser
- Dålig datavalidering

## Lektioner och labbuppgifter

För varje kategori finns en lektion och ett antal labbuppgifter

Lektionerna introducerar ämnet

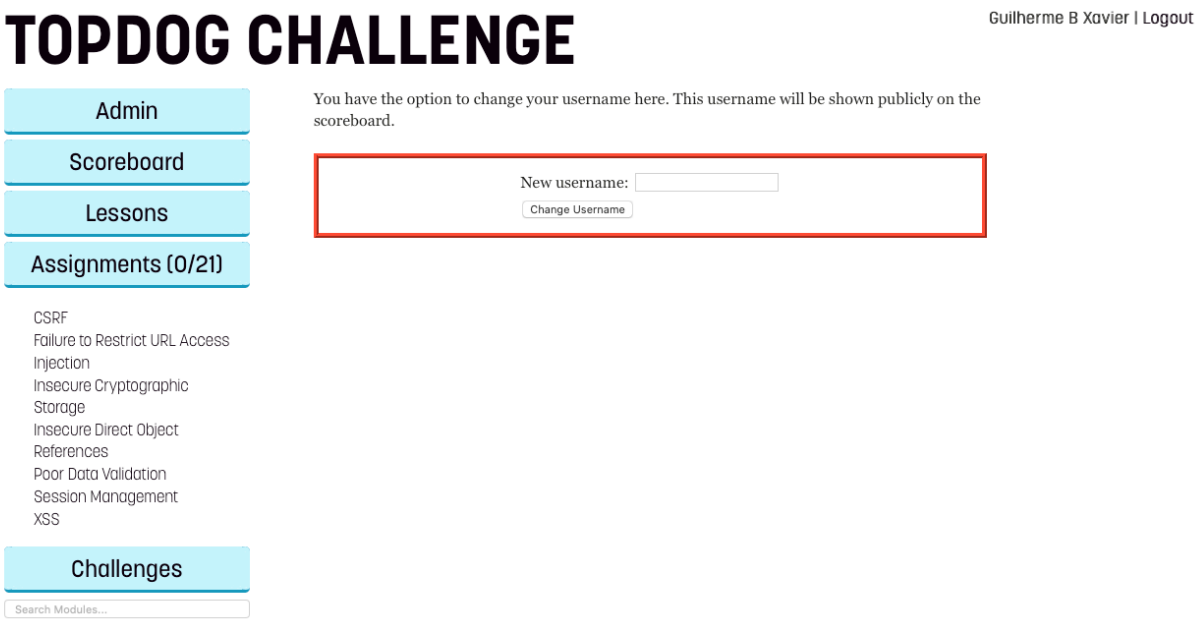
Använd lektionen för att lära dig hur just denna mekanism fungerar

Lektionerna kan också ge ledtrådar efter några misslyckade försök

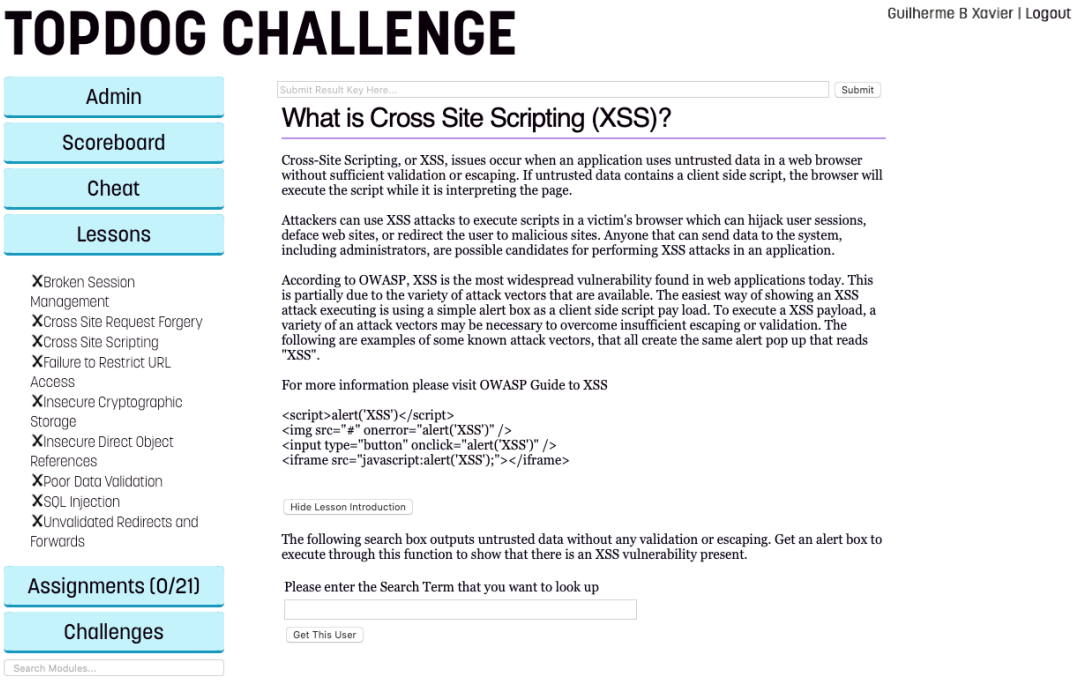
När du känner dig säker på ett ämne, fortsätt med uppgifterna

Du får godkänt efter att ha fullbordat samtliga 21 uppgifter

# Webgränssnitt för Security Shepherd



# Målet är att få ut resultatnyckeln



## Hur resultatnyckeln fungerar

När en uppgift är klar får du resultatnyckeln (result key)

Klistra in den i boxen överst och klicka på submit

Oftast (men inte alltid) ser nyckeln ut något i stil med:

```
3c17f6bf34080979e0cebda5672e90...
```

Resultatnyckeln är unik för varje användare och varje modul

Varning: Du får poängavdrag om du försöker med brute force-lösningar. Detta syns i våra adminloggar.

## Tillgängliga verktyg

Pentesting kräver ett antal verktyg

Du kan använda onlinekalkylatorer, som base64-encoders/decoders (Googla)

En sidas källkod kan avslöja mycket.

Du behöver också en attackproxy som låter dig modifiera HTTP-data skickat mellan server och klient.

## Websidans källkod

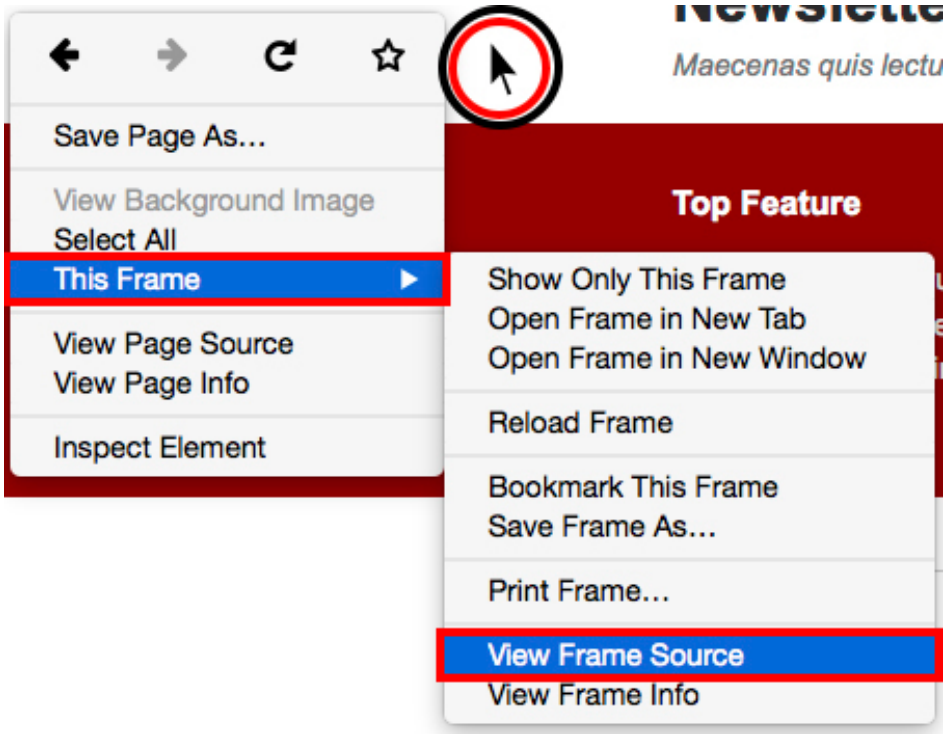
Firefox: Högerklicka/ctrl-klicka websidan och välj "View page source"

Detta visar källkoden för nuvarande sida.

I Security Shepherd behöver du se källkoden för uppgiften, dess iFrame.

Annars ser du bara källkoden för Security Shepherd.

## Visa källkod för en frame



# Exempel på källkod för websida

```
<h2 class="title">Failure To Restrict URL Access Challenge 1</h2>
<p>
    To recover the result key for this challenge you need to obtain the current server status message from an administr
    <br/>
    <br/>
    Use this form to view the status of the server <!-- from the point of view of a peasant or guest  -->
    <br/>
    <br/>
    <form id="leForm" action="javascript:;">
        <table>
        <tr><td>
            <div id="submitButton">
            <input type="submit" value="Get Server Status"/></div>
            <p style="display: none;" id="loadingSign">Loading</p>
            <div style="display: none;" id="hintButton"><input type="button" value="Would you like a hint?" id="theHint
        </td></tr>
        </table>
    </form>

    <div id="resultsDiv"></div>
</p>
```

Figur:Källkoden för en av utmaningarna

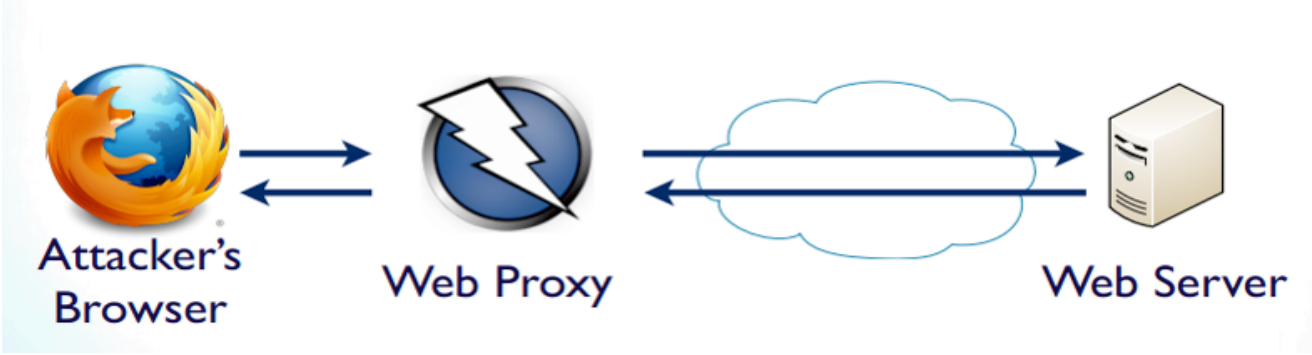
## Proxy

En proxy är ett mellanlager, en server som ligger mellan användaren och den server användaren accessar.

En proxy kan göra olika saker, anonymitet, säkerhet, konvertering av data (t.ex. översättning)...

## Använda en proxy

Viktigt verktyg för "pentesting" är en attack proxy




"Pentesting" = penetration testing

En proxy kan modifiera data som skickas genom den!

## ZAP-proxyn

Du kan använda en proxy för att "pausa" en begäran medan du ändrar det.

Vi rekommenderar ZAP-proxyn

Finns för Linux, Window och OSX

Open source

Ladda ner här:

https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project

## Att använda proxyn

När du installerar ZAP så är dess standardvärde localhost:8080

You behöver konfigurera webläsaren så den skickar alla HTTP-data genom den

Detta skickar all trafik genom proxyn, vilket är irriterande.

Vi rekommenderar att du installerar en andra webläsare som kör genom proxyn. Då kan du köra din vanliga webläsare som vanligt.

Du kan till exempel ladda ner Firefox eller Chrome, som finns för de flesta plattformar.

## Var inte vårdslös!

Attackera bara uppgifterna!

Du får inte manipulera Shepherd! Försök att göra det detekteras och rapporteras som fusk! Respektive uppgifts egen ram (iFrame) kan du dock gärna öppna och undersöka.

Din uppgift är att knäcka uppgifterna, inte att fuska dig genom labben!

Labkursen lyder under samma regler som andra kurser och vi har order att anmäla fusk till disciplinnämnden!

## Du kan jobba på egen tid

Labbarna är öppna från 14/11.

Du kan göra dem från godtycklig dator.

Det betyder, från din egen dator, kan vara hemma, eller från labbdatorer, när det passar dig.

MEN du måste vara klar senast under tentaperioden i januari!

## Fullborda labben

Inga labbrapporter

När du har klarat en uppgift så registrerar systemet detta automatiskt. Mer instruktioner kommer i PM när labbarna startar.

## Fullborda labben

Inga labbrapporter

När du har klarat en uppgift så registrerar systemet detta automatiskt. Mer instruktioner kommer i PM när labbarna startar.

Förutom detta finns en publik topplista!

## Topplista och bonuspoäng

Vi ser fortfarande vilka uppgifter du har klarat, och labben är godkänd när alla uppgifter är fullbordade

Topplistan har hittills inte varit relaterad till labbexaminationen... men jag överväger starkt att införa det nu när jag har ett poängsystem!

Topplistan är bara en kul grej, för att utmana varandra.

Alla kurser (TSIT01, TSIT02, 726G81) har gemensam topplista

Tävlingsdelen avslutas på en tid som meddelas senare (via PM och synligt i Security Shepherd).

## Bra metoder

SKRIV NER dina framsteg. När servern lagrar dina resultat så finns alltid risken att databasen kraschar på vägen.

Då kan du snabbt komma tillbaka där du var.

Jo, vi har också backuper, men ha en egen för säkerhets skull.

Dubbla system är bra för säkerheten!

# DEMO

## Slutord

Vi hoppas att detta blir en kul och intressant upplevelse.

Nej, labben är inte speciellt lätt

men du har tid på dig att förstå och klara av den i tid.