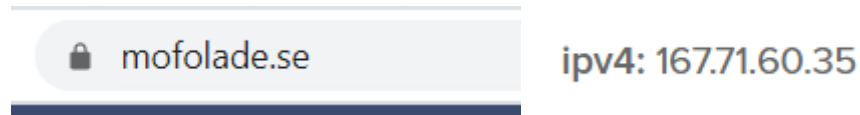


Movie Forum

Testning av säkerhet

Appen finns på adressen mofolade.se. root psw hy6het_D4Se_cYp



Jag bytte SSH port till 50896.

Ställde in välkomst text:

```
Welcome to FORUM SERVER
Last login: Wed Jan 20 18:59:52 2021 from 213.112.165.75
root@ubuntu-s-4vcpu-8gb-fra1-01:~#
```

Jag ställde in Ubuntu's inbyggda brandvägg UFW. Port 80 (http), 443 (https) och 50896 är öppen.

Jag ställde in ett SSL-certifikat. Med hjälp av Certbot installerade jag LetsEncrypt-certifikat.

Jag gjorde de nödvändiga inställningarna på reverse-proxy:

```
// Create a new secure webserver
https.createServer({
  key: certs['mofolade.se'].key,
  cert: certs['mofolade.se'].cert
}, (req, res) => {

  // Log some things
  let ip = req.connection.remoteAddress;
  console.log(`

    Date: ${new Date().toLocaleString()}
    URL: ${'http://' + req.headers.host + req.url}
    user-agent: ${req.headers['user-agent']}
    ip: ${ip}

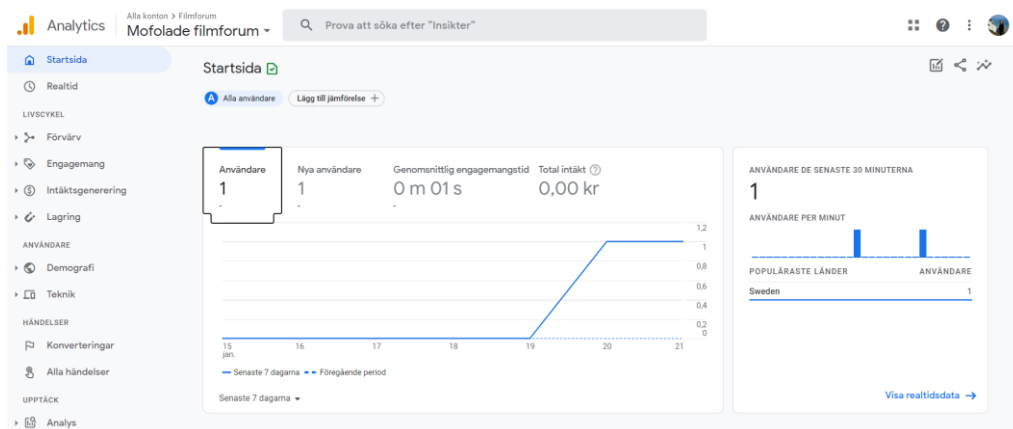
  `);
});
```

Jag använder MySQL databas.

Jag sparar inloggade användarnas IP-adresser i user_session tabell.

```
mysql> select * from emsama_comfilmforum.users_session;
+----+-----+-----+-----+-----+
| id | user_id | session_id | host | time |
+----+-----+-----+-----+-----+
| 19 | 2 | 3t86r9futu5r5t3fra260imvcg | 213.112.165.75 | 1611325984 |
+----+-----+-----+-----+-----+
1 row in set (0.00 sec)
```

Jag ställde in Google Analytics, som är ett bra verktyg för att se hur många som besökte sidan. Dessutom kan jag få en massa information om besökarna, vilka sidor de besökte, från vilka enheter, t ex mobil, dator, och vilket land



Specifikation

Klassen `classMySQL` innehåller hur man kopplar sig till databasen och `salt.json` finns med i `gitignore` filen. Jag använder förberedda sql kommando (prepare) med `bind_param` som ger över parameter.

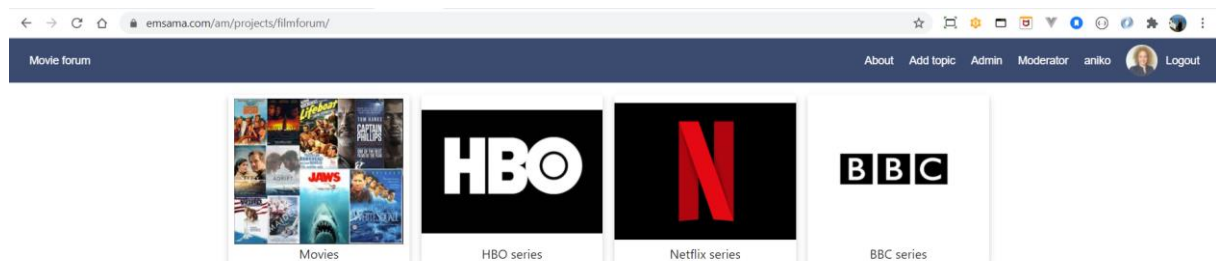
Lösenorden är krypterade. Jag använder salt som finns i `salt.json`.

Annars skapar `php password_hash ()` ett salt för lösenord, `password_hash ()` skapar olika salt för varje lösenord. Det kommer att öka lösenords säkerhetsstyrka. Men jag vill göra alla krav till uppgiften.

På huvudsidan kan man se olika kategorier. Kategorier kommer från `categories` tabell. Alla besökare kan se kategorier och underkategorier (filmer).

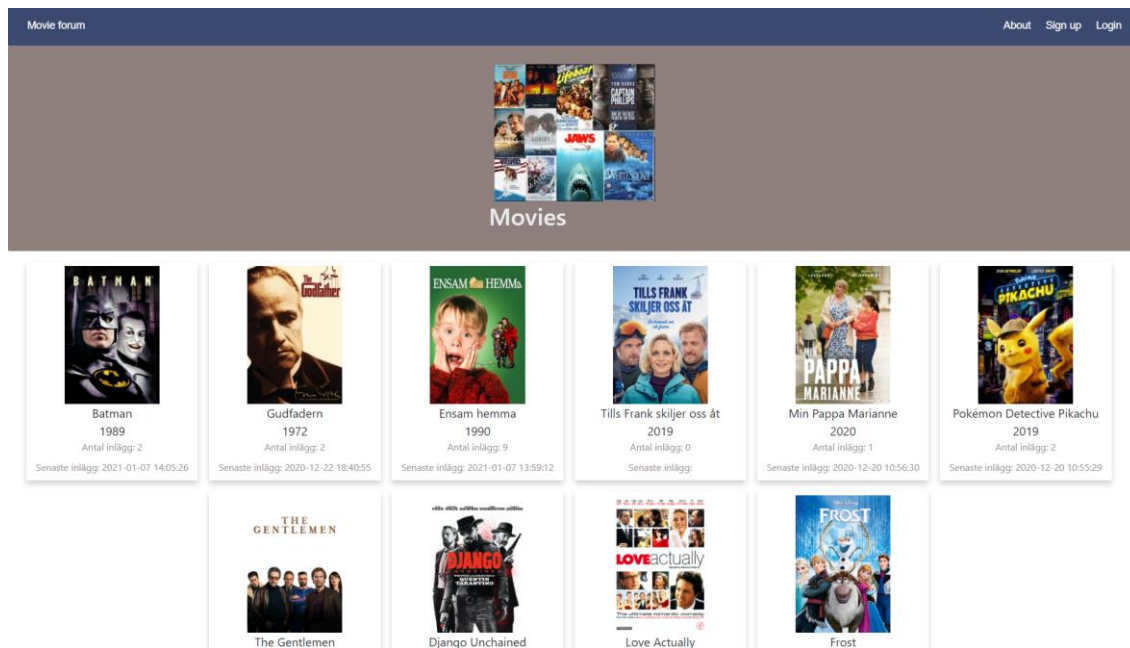
Huvudkategorier:

Man kan välja kategori genom att klicka på kategori knapp.



Just nu finns det fyra huvudkategorier och alla innehåller minst en underkategori, som är filmen själv.

Underforum:



Inom huvudkategorier finns underforum. Underforum kan skapas av alla inloggade användare genom att klicka på Add topic knappen i header. Jag beskriver det mer utförligt senare.

På url <https://mofolade.se/addTopic.php> kan man hitta formen som behövs för att skapa en underforum. Om det inte är någon inloggad användare så kommer man till inloggningssidan

Logga in

En tråd:



I input fälten bestämmer jag olika krav t ex maxlängd, minlängd, jag använder rätt datatyp för att kontrollera om datan är korrekt, t ex email typ.

I de obligatoriska inmatningsfälten finns required attribute.

```
<input type="text" name="newTopic[name]" id="name" maxlength="200" required>
```

```
echo '<input type="text" name="login[email]" id="email" name="email" placeholder="Email" required>';  
echo '<input type="password" name="login[password]" id="password" name="password" placeholder="Lösenord" required>';
```

I klassen General finns en remove_emoji funktion som jag anropar vid nytt inlägg och den tar bort alla emoji.

I databasen använder jag foreign keys där det är möjligt, t ex i tabellen topic_comments har jag user_id, topic_id. Databasen följer minst 2:a normalform i sin uppbyggnad.

I tabellen roles finns tre nivåer, user, moderator och admin. När man registrerar sig får alla user nivå. I klassen ACL_settings reglerar jag tillgången enligt method och user rättigheter.

Alla inloggad user kan skapa nytt topic.

Movie forum

About Add topic Admin Moderator aniko Logout

Ny topic

Topic namn

Categories

IMDb id

År

Film beskrivning (max 500 character)

Välj en JPEG-fil att ladda upp. Max 1 MB filstorlek.

Välj fil Ingen fil har valts

Skapa ny topic

Admin kan ge moderator roll till en user.

Movie forum

About Add topic Admin Moderator aniko Logout

User id	Role	Username	Email	IsActive	Inactivation	Edit roles
1 2	user moderator admin	aniko	mofolade@gmail.com	active		Admin Moderator
2 9	user		anna@gmail.com	active		+ Admin + Moderator
3 3	user moderator	emma	emma@test.com	active		+ Admin - Moderator
4 19	user		gillarfilm@film.se	active		+ Admin + Moderator
5 20	user moderator	moderator	moderator@movieforum.com	active		+ Admin - Moderator
6 16	user		panna@gmail.com	active		+ Admin + Moderator

En moderator kan få rättigheter till olika kategorier från admin.



testuser1

Ängrar att jag inte tog mig tid att se den tidigare. Riktigt bra och välspelat! 4/5

2020-12-21 14:11:39 [Reply](#)



testuser

Bästa julfilmen som gjorts! Julkänslan och nostalgin når sin topp varje gång av denna :)

[Antecedent](#)

2020-12-20 11:44:30 [Reply](#)

Om man klickar på Antecedent knapp då kan man se tidigare kommentarer.

Bästa julfilmen som gjorts! Julkänslan och nostalgin når sin topp varje gång av denna :)

[Antecedent](#)

Den ultimate julfilmen som man bara måste se varje år runt jul. Först skrattar man, sen gråter man.

2020-12-20 11:44:30 [Reply](#)

Moderator kan skriva inlägg med en speciell utseende.



aniko

Ta det lugn! God jul!

2020-12-20 16:50:49 [Reply](#)

I html visas endast de knappar, länkar som är kopplade till olika rättigheter som har rätt rättighet för dessa. T ex i header kan endast en admin se admin länken.

Jag sparar session till user_sessions tabel.

id	user_id	session_id	host	time
12	2	5470cef0f05af688a7911295431c0724	213.112.165.75	1610109141

Man kan registrera sig Sign up sida.

Sign Up

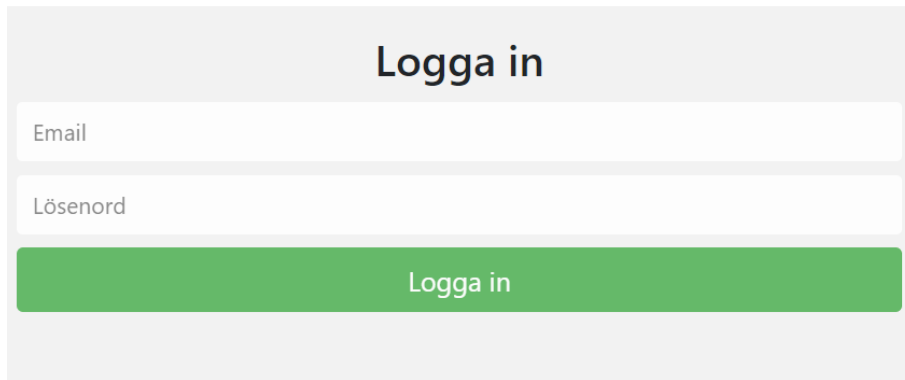
Name

Password

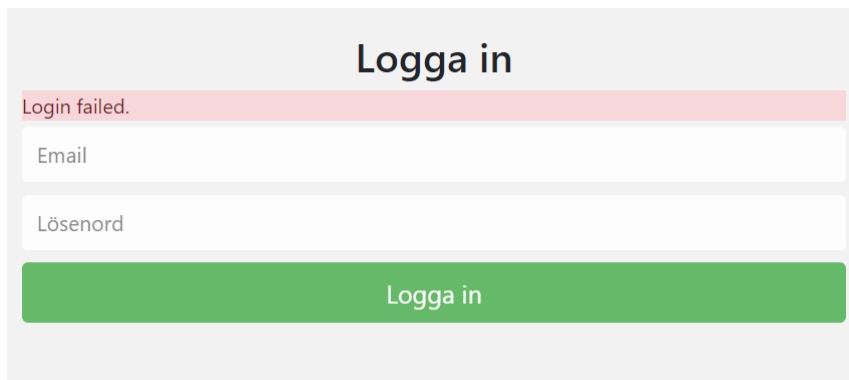
Email

[SIGN UP](#)

Man kan logga in på Login sida.

A screenshot of a login form titled "Logga in". It features two input fields: "Email" and "Lösenord". Below these fields is a green button labeled "Logga in".

Jag skriver ut felmeddelandet om någon gitt fel text fel vid login

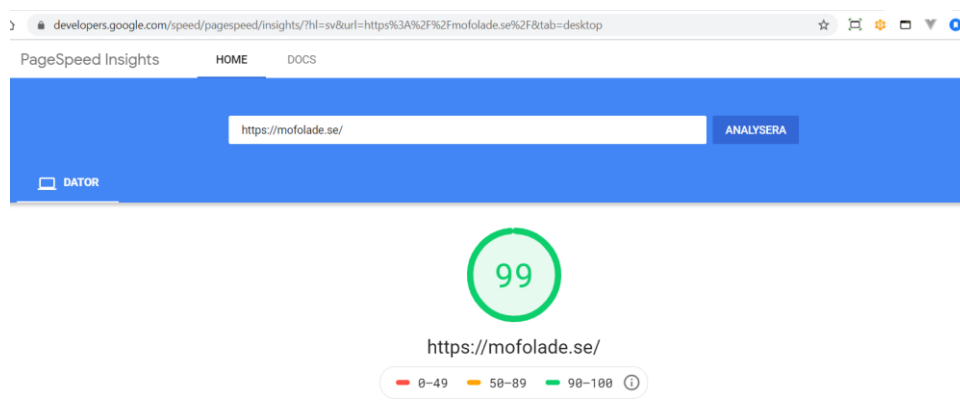
A screenshot of the login form titled "Logga in" showing an error state. A red message "Login failed." is displayed above the "Email" and "Lösenord" input fields. The green "Logga in" button remains at the bottom.

Testning vidare:

Jag testade även vad händer om jag loggar in på användargränssnittet och i bakgrunden jag startat om servern med hjälp av putty.

Sidan var inte nårbart i några sekunder, men efter omladdning fungerade den och användaren var fortfarande inloggad.

Hastigheten på sidans laddning testade jag med hjälp av google PageSpeed Insights.



Att ladda sidan går mycket snabbt

Jag märkte aldrig någon långsamhet under användningen av appen, de olika inställningarna så som ändringar i moderator/admin rättigheter slog genom direkt.

Jag kollade HTML kodens rätta syntax med hjälp av validator.w3.org. Inga fel hittades.

Nu Html Checker

This tool is an ongoing experiment in better HTML checking, and its behavior remains subject to change

Showing results for <https://mofolade.se/>

Checker Input

Show ☐ source ☐ outline ☐ image report [Options...](#)

Check by [address](#)

<https://mofolade.se/>

[Check](#)

Document checking completed. No errors or warnings to show.

Used the HTML parser. Externally specified character encoding was UTF-8.

Total execution time 286 milliseconds.

IP adress information:

IP Address Lookup

IP: 167.71.60.35 [Lookup](#)

IP Address	167.71.60.35	IP Address	167.71.60.35
ASN	14061	ASN	14061
City	Frankfurt am Main	City	Frankfurt am Main
State/Region	Hessen	State/Region	Hesse
Country Code	Germany	Country Code	DE
Postal Code	65931	Postal Code	60313
ISP	DigitalOcean LLC	ISP	DigitalOcean, LLC
Time Zone	+01:00	Time Zone	Europe/Berlin

[IP2Location.com](#) Results [ipdata.co](#) Results

[Update This Info](#) [Report IP Abuse](#) [Is This IP Blacklisted](#)

Testing med Postman:

forum

GET <https://mofolade.se/category.php?id=1>

Send Save

Params Authorization Headers (8) Body Pre-request Script Tests Settings

Query Params

KEY	VALUE	DESCRIPTION
☒ id	1	
Key	Value	Description

Body Cookies (1) Headers (9) Test Results

Status: 200 OK Time: 33 ms Size: 13.16 KB [Save Response](#)

Pretty Raw Preview Visualize

[Movie forum](#) [AboutSign upLogin](#)

Movies

Batman1989Antal inlägg: 25Senaste inlägg: 2021-01-07 14:05:26

Guðfadern1972Antal inlägg: 25Senaste inlägg: 2020-12-22 18:40:55

Ensam hemma1990Antal inlägg: 10Senaste inlägg: 2021-01-19 20:10:03

route	roller	metod	request body	testresultat	planerad respons	verklig respons
/category.php/:id	alla	get	{id:1}	Perfect	Status: 200	Status: 200
/topic.php/:id	alla	get	{id:3}	Perfect	Status: 200	Status: 200

Aniko Magyar