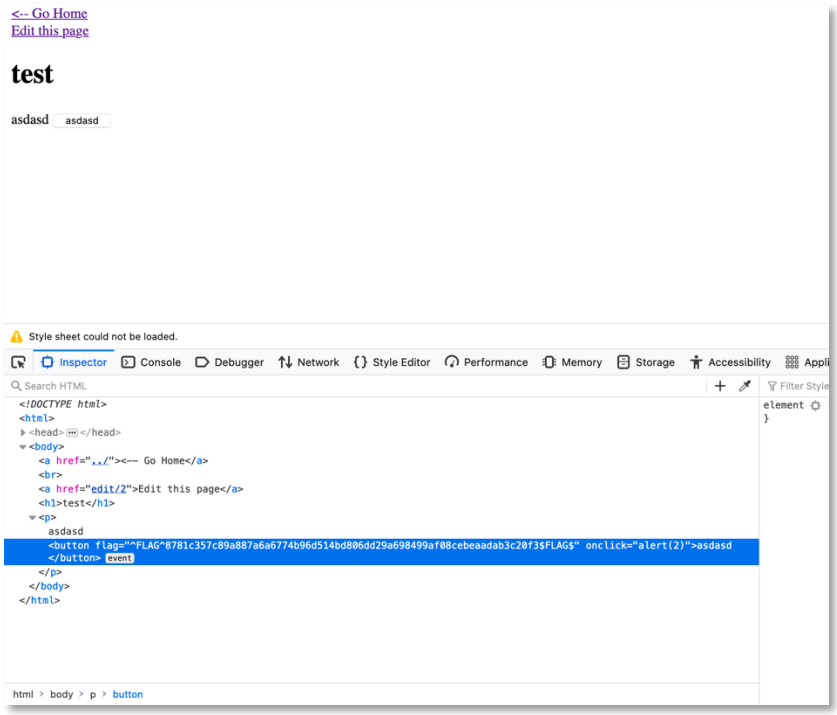
Øving 10
Eric Younger

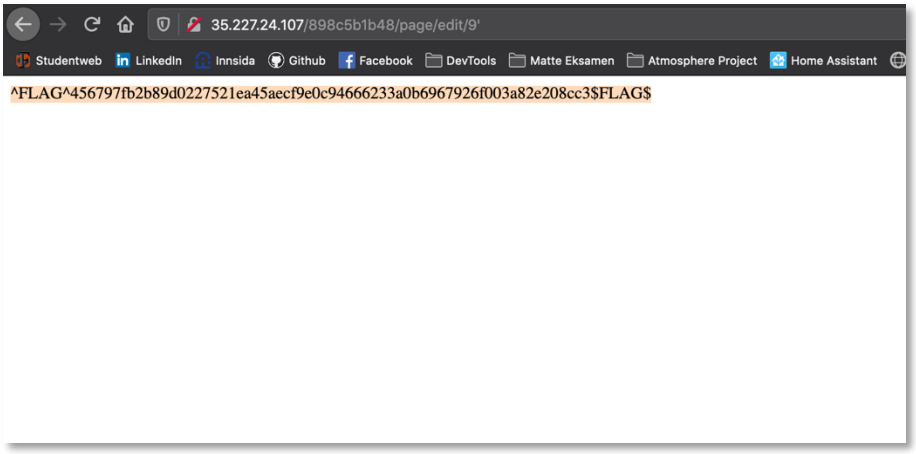
Oppgave 1:

```
undefined8 main(void)

{
  char local_28 [32];

  printf("Enter your name: ");
  fgets(local_28,0x20,stdin); //0x20 is 32 in hex decimal.
  printf("Hello ");

  //THIS IT IS THE VULNERABILITY
  //Prone to format strings attacks.
  //https://owasp.org/www-community/attacks/Format_string_attack
  //http://www.cis.syr.edu/~wedu/Teaching/cis643/LectureNotes_New/Format_String.pdf
  printf(local_28);

  //Solution: Either specify printf with a literal format string (%s) or use method
puts() instead.

  putchar(10);
  return 0;
}
```

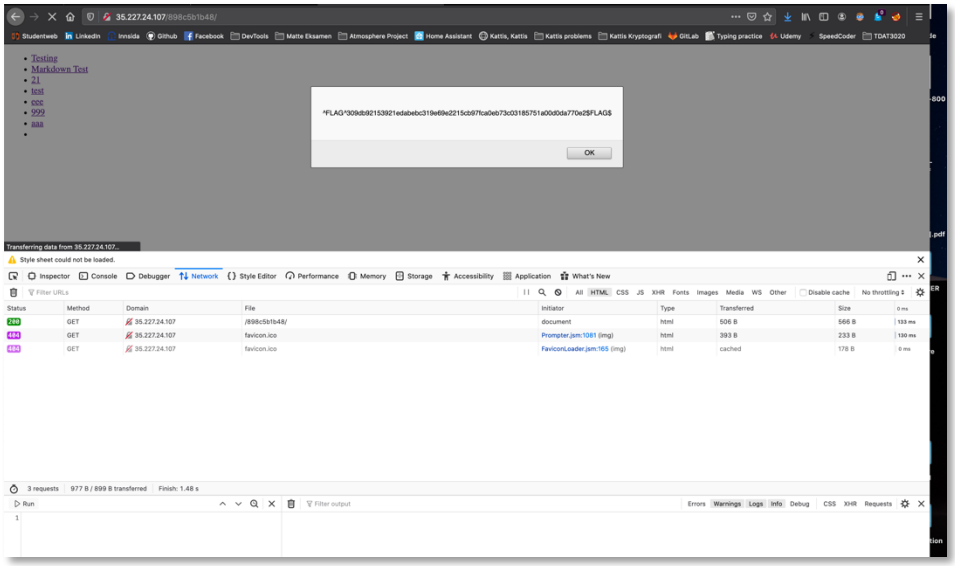
Oppgave 2:



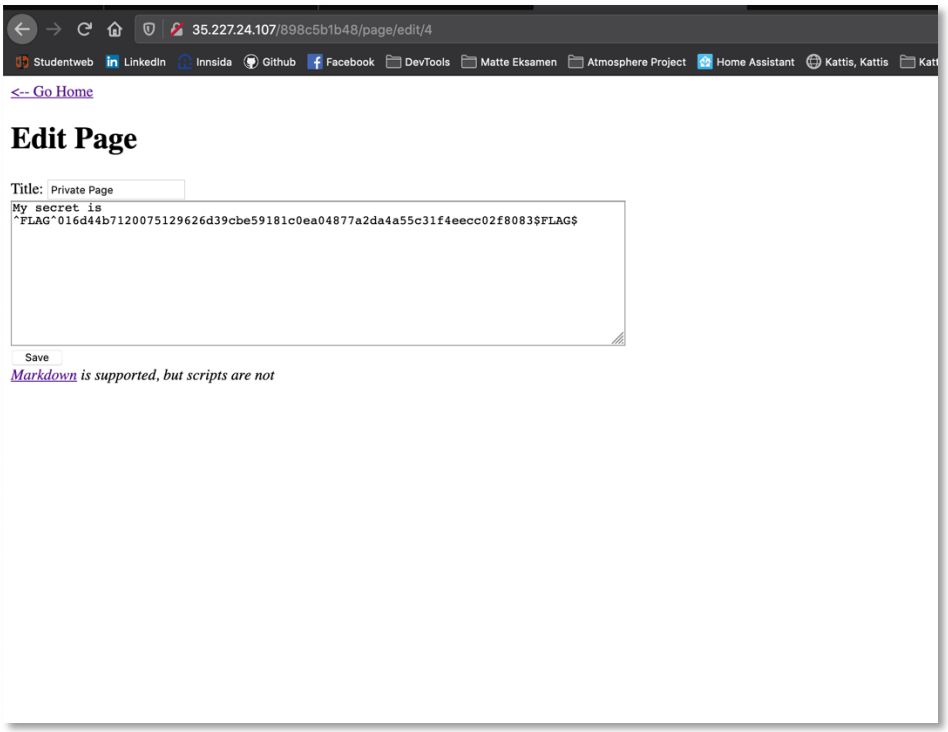
Flagget finner jeg ved å sette inn en knapp inn i body input-feltet med et script knyttet til seg.



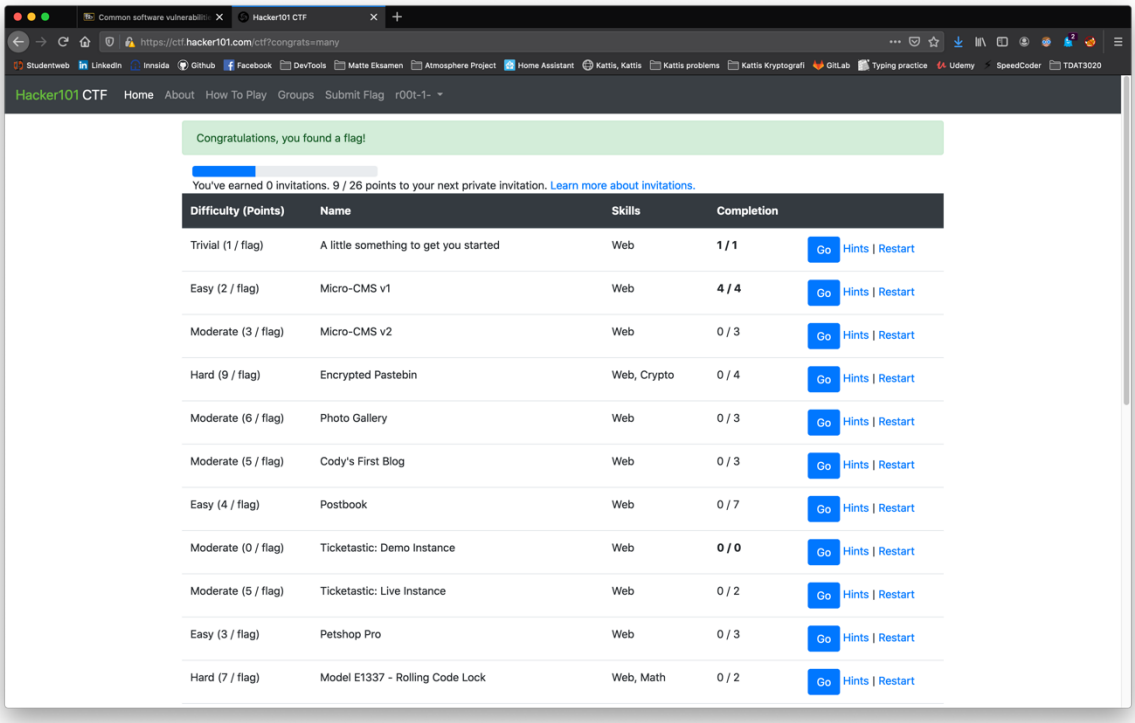
Flagget finner jeg ved å escape en string character i url feltet.



Flagget finner jeg ved å legge til <script>alert(2);</script> istede for tittel.



Såg at en artikkel ga forbidden status, fant flagget ved å gå via edit for å se innholdet i page/4.


Common software vulnerabilities
Hacker101 CTF
https://ctf.hacker101.com/ctf?congrats=many
Studentweb
LinkedIn
Innsida
Github
Facebook
DevTools
Matte Eksamen
Atmosphere Project
Home Assistant
Kattis, Kattis
Kattis problems
Kattis Kryptografi
GitLab
Typing practice
Udemy
SpeedCoder
TDAT3020
Hacker101 CTF
Home
About
How To Play
Groups
Submit Flag
r00t-1-
Congratulations, you found a flag!
You've earned 0 invitations. 9 / 26 points to your next private invitation. Learn more about invitations.
Difficulty (Points)
Name
Skills
Completion
Trivial (1 / flag)
A little something to get you started
Web
1 / 1
Go
Hints | Restart
Easy (2 / flag)
Micro-CMS v1
Web
4 / 4
Go
Hints | Restart
Moderate (3 / flag)
Micro-CMS v2
Web
0 / 3
Go
Hints | Restart
Hard (9 / flag)
Encrypted Pastebin
Web, Crypto
0 / 4
Go
Hints | Restart
Moderate (6 / flag)
Photo Gallery
Web
0 / 3
Go
Hints | Restart
Moderate (5 / flag)
Cody's First Blog
Web
0 / 3
Go
Hints | Restart
Easy (4 / flag)
Postbook
Web
0 / 7
Go
Hints | Restart
Moderate (0 / flag)
Ticketastic: Demo Instance
Web
0 / 0
Go
Hints | Restart
Moderate (5 / flag)
Ticketastic: Live Instance
Web
0 / 2
Go
Hints | Restart
Easy (3 / flag)
Petshop Pro
Web
0 / 3
Go
Hints | Restart
Hard (7 / flag)
Model E1337 - Rolling Code Lock
Web, Math
0 / 2
Go
Hints | Restart

Ferdig.