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:

A screenshot of a social media post

Description automatically generated

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

A screenshot of a social media post

Description automatically generated

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

A screenshot of a social media post

Description automatically generated

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

A screenshot of a social media post

Description automatically generated

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

A screenshot of a computer

Description automatically generated

Ferdig.