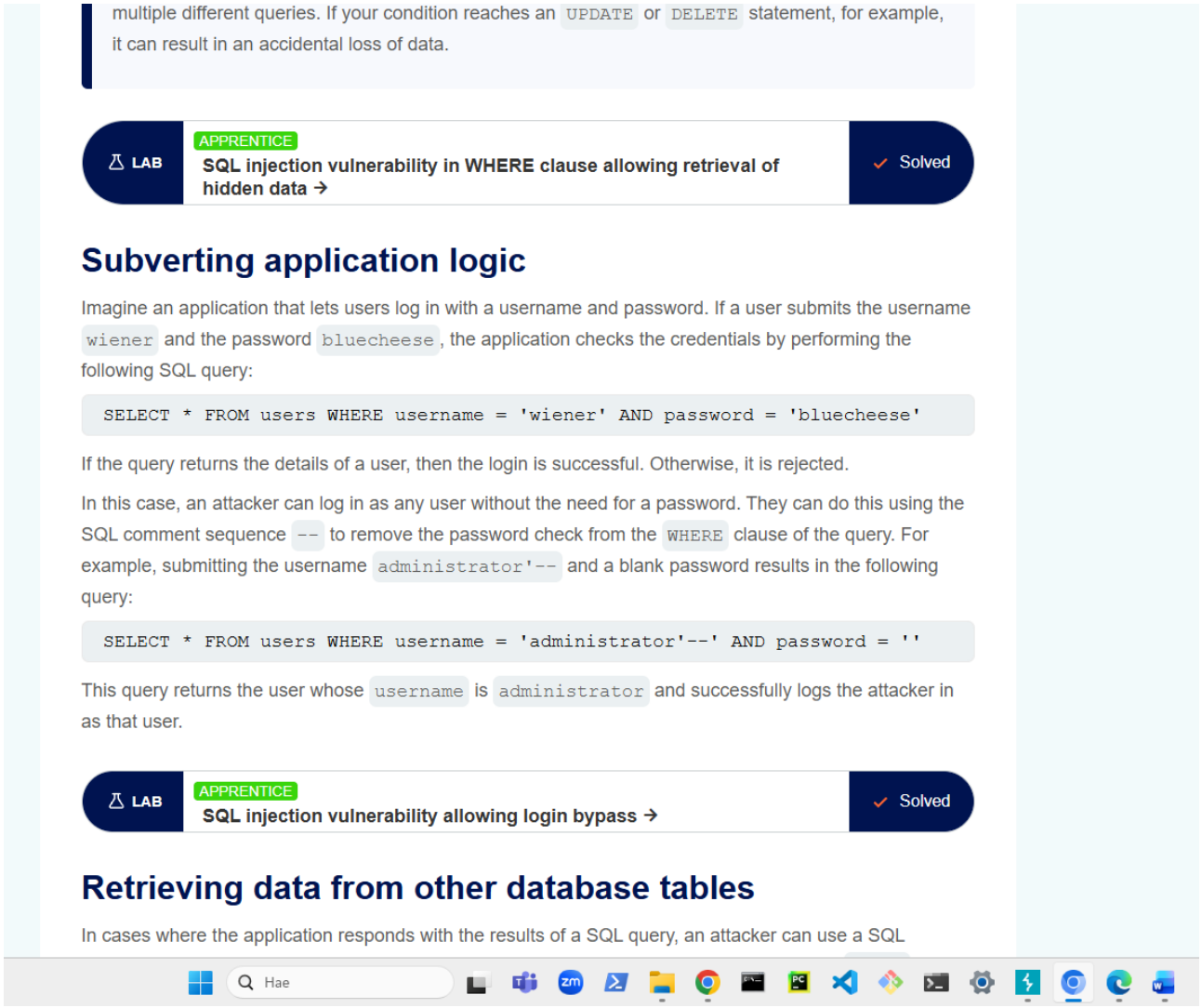


SQL injection tehtävät:

SQL injection vulnerability in WHERE clause allowing retrieval of hidden data:

Tehtävä oli mielenkiintoinen koska siinä suoraan syöttämällä URL linkin jatkoksi '+OR+1=1—koodin sai tietokannassa kyselyn SELECT * FROM products WHERE category = 'Gifts' AND released = 1 aikaiseksi. Tämä paljasti käyttäjälle piilotettua sisältöä palvelimelta. Opin kuinka SQL injektioita tehdään periaatteessa ja kuinka niitä voi tehdä myös URL kenttään syöttämällä. Olin joskus aiemmin törmännyt credentials kenttään syötettyihin arvoihin SQL injektioissa.

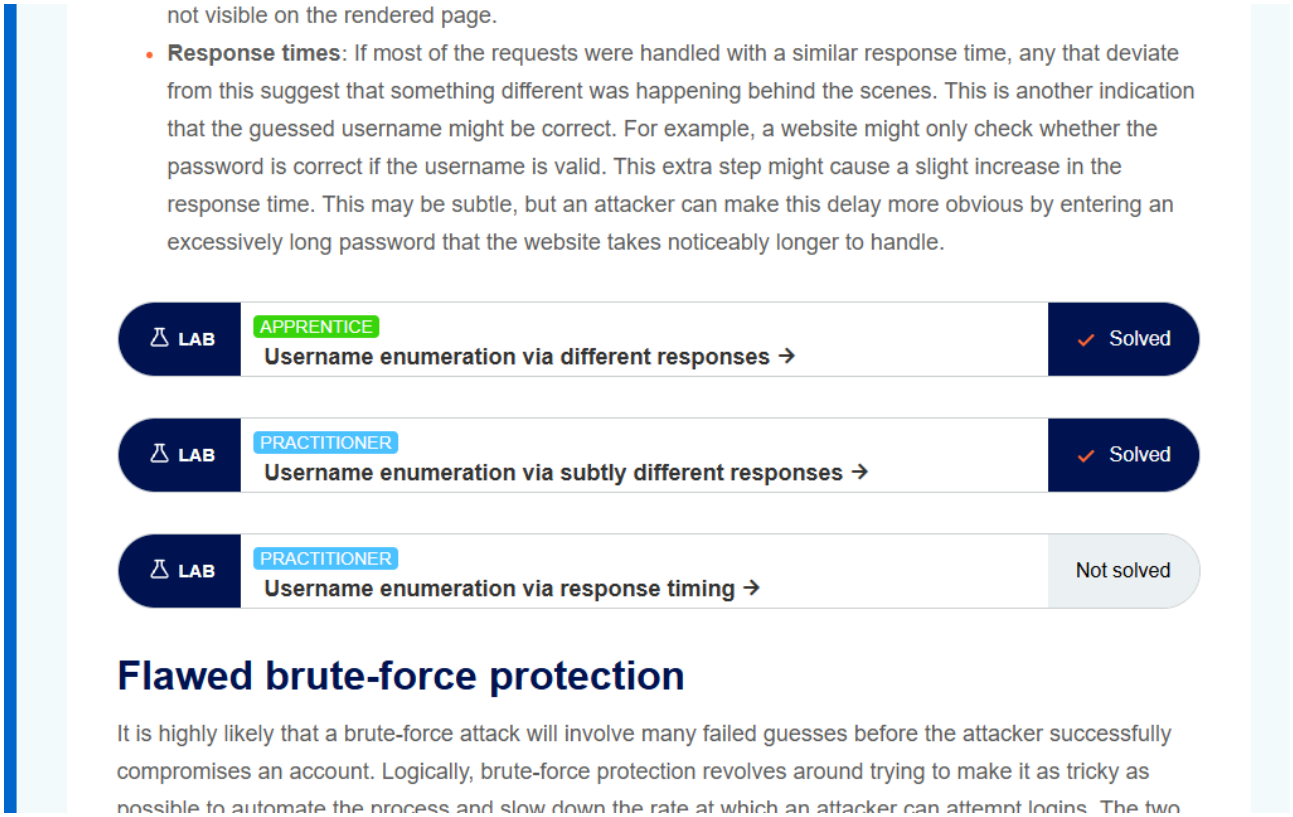
Tehtävä oli haastava ilman apua, koska minulla ei ollut aiempaa kokemusta SQL injektioiden tekemisestä. Käytin ohjetta avuksi, mutta en tarvinnut ohjevideota avuksi.

SQL injection vulnerability allowing login bypass:

Tehtävässä opin Kuinka tietyn komennon syöttämällä login credentialseihin on mahdollista saada tietokannassa kysely, joka ohittaa salasanan varmistuksen. Kun tehtävässä syötti ” ’ ” merkin niin se saa aikaiseksi selaimella SQL kyselyn. Kun antoi usernameksi ”administratorin” niin sai admin

oikeudet, joilla voi esim. poistaa käyttäjiä. Kun laittoi ”--” kyselyn loppuun niin se ohittaa salasanan tarkistuksen. Opin siis tehtävässä paljon tuon haavoittuvuuden moniuloitteisuudesta ja logiikasta.

Tehtävä sujui toisena SQL injektiona ihan hyvin ja turvauduin vain ohjeen apuun. Minun ei tarvinnut katsoa apuvideoita.



Passwd based login tehtävät:

Username enumeration via different responses:

Opin käyttämään paljon kurssin työkaluja kuten Burpia. Tämä tehtävä oli ensimmäinen ”hakkerointi” minulle, joten se oli hyvin mielenkiintoista. Termi brute force on minulle hyvin tuttu, mutta nyt oli hauskaa päästä käyttämään ihan työkalua sitä varten. Opin tehtävässä tosiaan Burp käyttöä, proxyn käyttöä, http pyyntöjen tarkastelua Burpin avulla vs. devtools ja sniper attackin toteuttamisen Burpin avulla. Myös periaate ensin username ja sitten salasana selkeni tehtävässä hyvin eri pyyntöjen koodien takia. Tehtävässä tärkeintä oli huomata kuinka oikean usernamen sattuessa kohdalle, virheilmoitus muuttui merkittävästi.

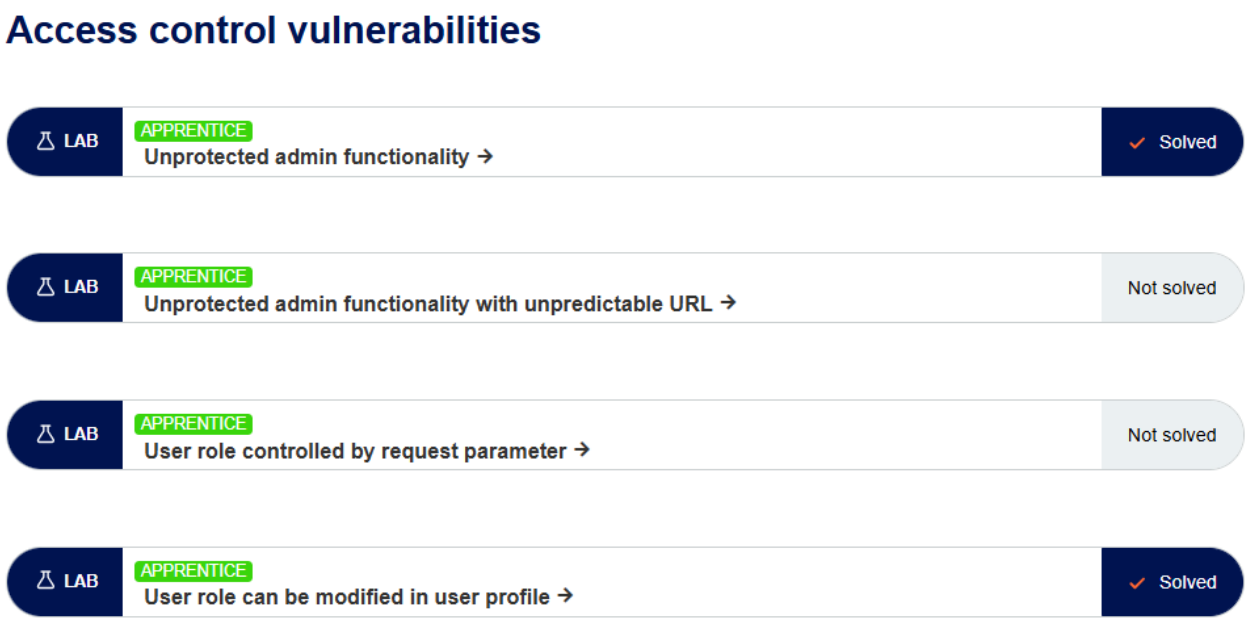
Tehtävässä haastavinta oli siihen pystyminen täysin itse, vaan seurasin opettajan luentotallennetta, kun tein kyseisen tehtävän alusta loppuun.

Username enumeration via subtly different responses

Opin taas lisää burpin käyttöä ja brute force tekniikkaa. Tehtävässä oli hienoa huomata, kuinka oikean usernamen sattuessa virheilmoituksessa oli vain hyvin pieni virhe ”Invalid username or password.” vs.

”Invalid username or password”, jossa pisteen puuttuminen paljasti usernamen olevan oikea. Pyynnöissä ei ollut muuten eroa niiden numeroinnissa.

Tehtävä oli haastava tehdä, koska minulla ei ole aiempaa kokemusta penetraatiotestauksesta. Jouduin turvautumaan apuvideoihin tehtävää tehdessäni. Pidin kovasti toisesta hakkeroinnistani.



Access contol vulnerabilities tehtävät:

User role can be modified in user profile: Opin kuinka käyttäjän roolia voi muuttaa, kun on lähettänyt serverille post pyynnön sähköpostiosoitteen tallentamisesta. Samanlaisella, mutta uudella post pyynnöllä kykeni muuttamaan Wiener:peter käyttäjän roleid 1 to roleid 2 =adminiksi ja kykenin poistamaan Carloksen.

Haastavinta oli keksiä miten se email pyynnön avulla saa ujutettua myös roolin muutoksen. Tarvitsin ohjevideon apua. Myös jouduin käynnistämään kaikki prosessini ja tietokoneeni uudestaan, koska en kyennyt kirjautumaan enää wiener:peter tunnuksilla, vaan hakkasin niissä päätäni seinään pitkän aikaa.

Unprotected admin functionality:

Opin että, kirjoittamalla domain kenttään tiettyjä parametereja, kuten admin-panel, on mahdollista päästä kirjautumatta muuttamaan käyttäjätietoja palvelusta. Myös robots.txt tekstitiedoston sisältöä pääsi tarkastelemaan kirjautumatta palveluun. Sieltä näki, että polku admin paneeliin loppuu:

User-agent: *

Disallow: /administrator-panel.

Tehtävä ei ollut kovin haastava vaan onnistuin tekemään sen ilman apuvideota. Tehtävässä ei tarvinnut tarkastella ollenkaan koodia.

Jatkan PortSwigger tehtävien tekemistä myöhemmin korottaakseni arvosanaani. 😉