HAAVOITTUVUUKSIEN SKANNAUS: CASE-ESIMERKKI TIETOKANNAN SKANNAUS

Johanna Hakonen

Sisällysluettelo

1 Johdanto

Kyberturvariskejä hallitaan esimerkiksi skannaamalla tietokantahaavoittuvuuksia erilaisilla ohjelmilla kuten SQLmap, NoSQLmap ja Burb Suite. Tässä yritettiin käyttää vanhentunutta NoSQLmap-ohjelmaa, jota ei saatu käyttöön, ja kokeiltiin vähän Burp Suitea. Apuna käytettiin ChatGPT:tä (OpenAI, 2025).

Ympäristönä toimi Windows-palvelin, wks2-työasema VMwaressa ja Kali Linux-kone, ja sen asennus on esitetty liitteissä 4a ja 5b. Physio-websovellus oli käynnissä työaseman portissa 3001.

2 Aloitus

Otetaan tietokanta käyttöön työasemalla varmuuden vuoksi MongoDB Atlas-palvelun sijaan. Asennettiin mongodump-komento (MongoDB, Inc., Download MongoDB Command LIne Database Tools, 2025) ja lisättiin C:\Program Files\MongoDB\DatabaseTools\bin ympäristömuuttujiin. Ladataan dump-kansioon tietokanta: mongodump --uri="mongodb+srv://johannahakonen:salasana@physio.efefq.mongodb.net/physioApp" --out dump/.

Ladattiin MongoDB Community Server (MongoDB, Inc., MongoDB Community Server Download, 2025). Asennus pysähtyi MongoDB Compassin kohdalle, joten asennettiin ilman sitä. Siirryttiin kansioon, jossa dump-kansio sijaitsee: ”mongorestore --drop --host localhost --port 27017 --dir dump”. Muutetaan Physio-web-sovelluksen .env-tiedostoon MongoDB:n osoite paikalliseksi:

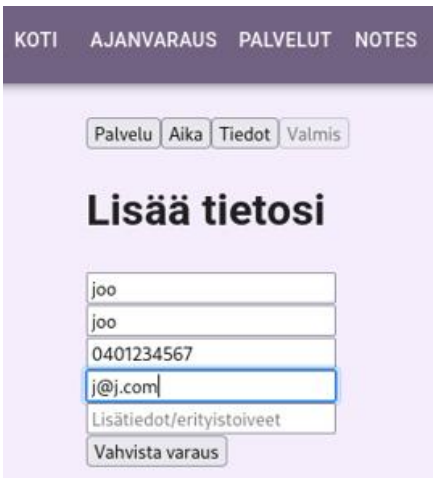
MONGO_URI=mongodb://localhost:27017/physioApp. Saatiin sivut toimimaan, mutta uusi varaus ei tule näkyviin työntekijän sivulla. Uusia työaikoja pystyttiin laittamaan sieltä, ja ne näkyivät myös kalenterissa eli tietokantaohjelma toimii ainakin osittain.

3 NoSQL

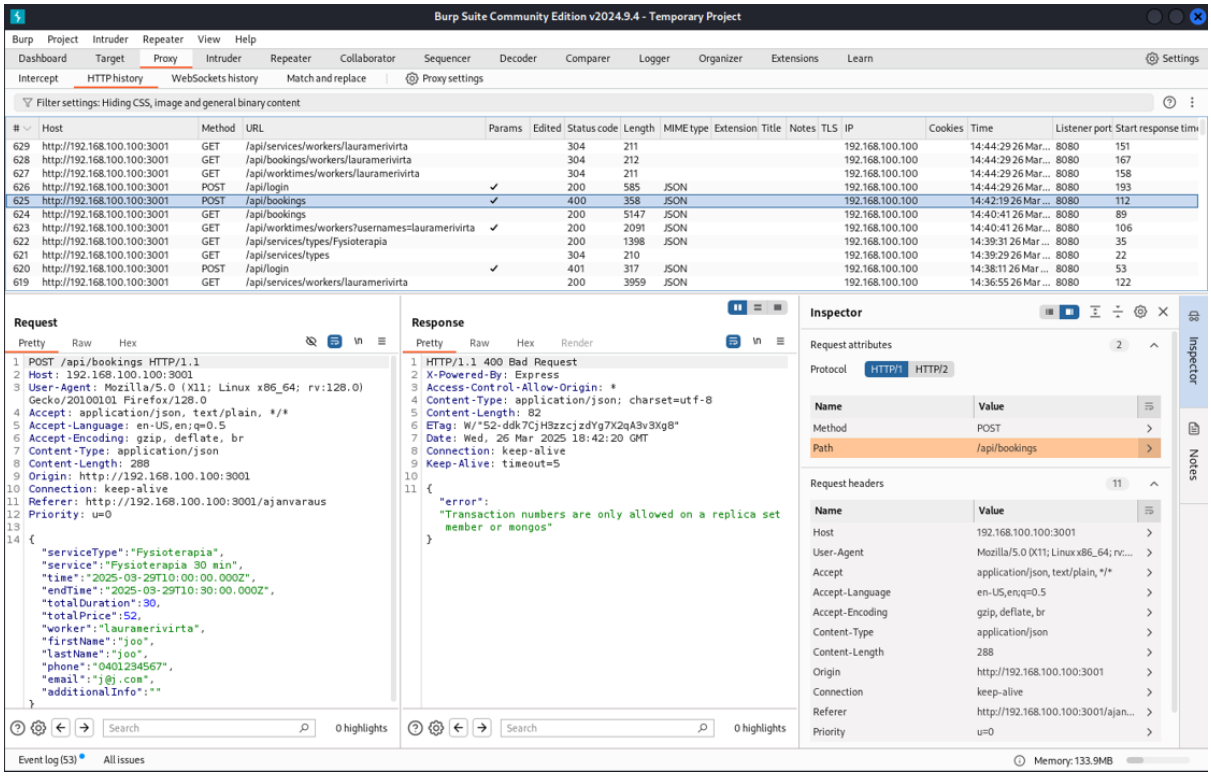
Yritettiin asentaa NoSQLMap mutta se on vanha ja perustuu Python2:een, eikä onnistunut ChatGPT:n ohjeilla. Komennot olivat seuraavat: git clone https://github.com/codingo/NoSQLMap.git, cd NoSQLMap, python setup.py install (Intigriti, 2025), sudo apt update, curl -O https://bootstrap.pypa.io/pip/2.7/get-pip.py, python2 get-pip.py, python2 -m pip install couchdb pymongo, python2 -m pip install nsmcouch, python2 -m pip install pbkdf2, wget https://github.com/dlitz/python-pbkdf2/archive/master.zip, unzip master.zip, cd python-pbkdf2-master, python2 setup.py install –user, python2 nosqlmap.py, pip2 install ipcalc –user, sudo apt update, sudo apt install python2-pip -y: Error: Unable to locate package python2-pip. Luovutettiin tässä kohtaa.

4 Burp Suite

Kali Linuxin Firefoxin Manual proxy configuration -asetus oli 127.0.0.1:8080 ja Burb Suitessa Proxy settings sama. Saatiin näkyviin tietoja Physio-web-sovelluksesta. Uudet varaukset eivät mene läpi paikalliseen MongoDB-tietokantaan ("error":"Transaction numbers are only allowed on a replica set member or mongos"), mutta jos sen saisi korjattua, voisi kokeilla injektioita varauskaavakkeen kautta. Kuva 1 on esitetty ajanvarauskaavake ja Kuva 2 Burb Suitella kaapattu epäonnistunut ajanvaraus.

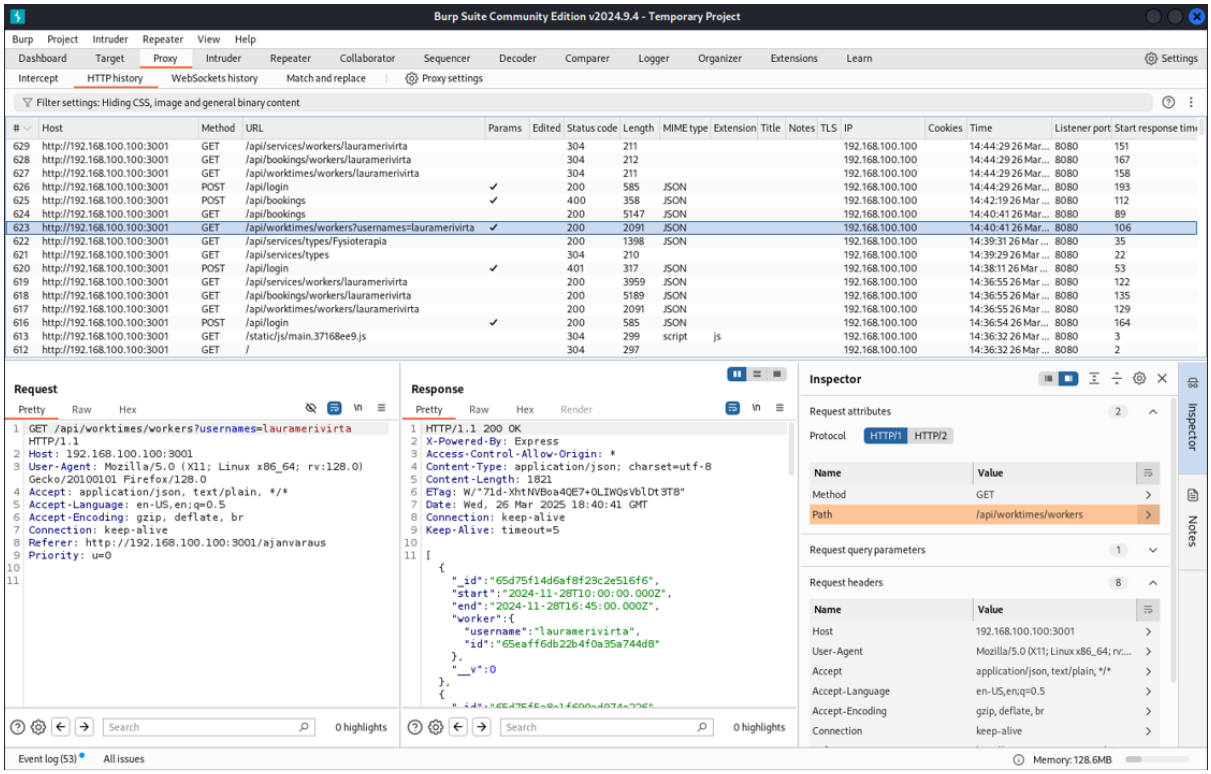


Kuva 1. Physion ajanvarauskaavake.



Kuva 2. Burp Suitella kaapattu ajanvaraus.

Tietokannan rakennetta ja esimerkiksi työntekijän id saatiin näkyviin liikkuessa sivustolla (Kuva 3).



Kuva 3. Burp Suitella kaapattua tietoa.

Lähdeluettelo

Intigriti. (14. Maaliskuu 2025). *Hacker Tools: NoSQLMap – No SQL, Yes exploitation*. Noudettu osoitteesta https://www.intigriti.com/researchers/blog/hacking-tools/hacker-tools-nosqlmap

MongoDB, Inc. (14. Maaliskuu 2025). *Download MongoDB Command LIne Database Tools*. Noudettu osoitteesta https://www.mongodb.com/try/download/database-tools

MongoDB, Inc. (26. Maaliskuu 2025). *MongoDB Community Server Download*. Noudettu osoitteesta https://www.mongodb.com/try/download/community

OpenAI. (17. Maaliskuu 2025). *ChatGPT*. Noudettu osoitteesta chatgpt.com