

HAAVOITTUVUUKSIEN SKANNAUS: CASE-ESIMERKKI TIETOKANNAN SKANNAUS

Johanna Hakonen

Sisällysluettelo

1	Johdanto	1
2	Aloitutus	1
3	NoSQL	2
4	Burp Suite	2
	Lähdeluettelo	4

1 Johdanto

Kyberturvariskejä hallitaan esimerkiksi skannaamalla tietokantahaavoittuvuuksia erilaisilla ohjelmilla kuten SQLmap, NoSQLmap ja Burp 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 Burp Suiteen 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 Burp Suiteella kaapattu epäonnistunut ajanvaraus.

Kuva 1. Physion ajanvarauskaavake.

The screenshot shows the Burp Suite interface. The top menu bar includes Burp, Project, Intruder, Repeater, View, and Help. Below the menu is a toolbar with various icons. The main window is divided into several panes. The top pane shows a list of HTTP history entries. The middle pane shows the details of a selected request (POST /api/bookings). The bottom pane shows the response (HTTP/1.1 400 Bad Request).

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port	Start response time
629	http://192.168.100.100:3001	GET	/api/services/workers/lauramerivirta			304	211						192.168.100.100	14:44:29 26 Mar...	8080	151	
628	http://192.168.100.100:3001	GET	/api/bookings/workers/lauramerivirta			304	212						192.168.100.100	14:44:29 26 Mar...	8080	167	
627	http://192.168.100.100:3001	GET	/api/worktimes/workers/lauramerivirta			304	211						192.168.100.100	14:44:29 26 Mar...	8080	158	
626	http://192.168.100.100:3001	POST	/api/login		✓	200	585	JSON					192.168.100.100	14:44:29 26 Mar...	8080	193	
625	http://192.168.100.100:3001	POST	/api/bookings		✓	400	358	JSON					192.168.100.100	14:42:19 26 Mar...	8080	112	
624	http://192.168.100.100:3001	GET	/api/bookings			200	5147	JSON					192.168.100.100	14:40:41 26 Mar...	8080	89	
623	http://192.168.100.100:3001	GET	/api/worktimes/workers?username=lauramerivirta		✓	200	2091	JSON					192.168.100.100	14:40:41 26 Mar...	8080	106	
622	http://192.168.100.100:3001	GET	/api/services/types/fysioterapia			200	1398	JSON					192.168.100.100	14:39:31 26 Mar...	8080	35	
621	http://192.168.100.100:3001	GET	/api/services/types			304	210						192.168.100.100	14:39:29 26 Mar...	8080	22	
620	http://192.168.100.100:3001	POST	/api/login		✓	401	317	JSON					192.168.100.100	14:38:11 26 Mar...	8080	53	
619	http://192.168.100.100:3001	GET	/api/services/workers/lauramerivirta			200	3959	JSON					192.168.100.100	14:36:55 26 Mar...	8080	122	

The detailed view of the selected request (625) shows the following details:

- Request:** POST /api/bookings HTTP/1.1. Headers include Host: 192.168.100.100:3001, User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0, Accept: application/json, text/plain, */*, Accept-Language: en-US,en;q=0.5, Accept-Encoding: gzip, deflate, br, Content-Type: application/json, Content-Length: 288, Origin: http://192.168.100.100:3001, Connection: keep-alive, Referer: http://192.168.100.100:3001/ajanvaraus, Priority: u=0.
- Response:** HTTP/1.1 400 Bad Request. Headers include X-Powered-By: Express, Access-Control-Allow-Origin: *, Content-Type: application/json; charset=utf-8, Content-Length: 82, ETag: W/"52-ddk7CjH3zccjzdyg7X2qA3v3Xg8", Date: Wed, 26 Mar 2025 18:42:20 GMT, Connection: keep-alive, Keep-Alive: timeout=5.
- Inspector:** The response body is a JSON object: {"error": "Transaction numbers are only allowed on a replica set member or mongos"}.

Kuva 2. Burp Suitella kaapattu ajanvaraus.

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

The screenshot shows the Burp Suite interface. The top menu bar includes Burp, Project, Intruder, Repeater, View, and Help. Below the menu is a toolbar with various icons. The main window is divided into several panes. The top pane shows a list of HTTP history entries. The middle pane shows the details of a selected request (GET /api/worktimes/workers?username=lauramerivirta). The bottom pane shows the response (HTTP/1.1 200 OK).

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port	Start response time
629	http://192.168.100.100:3001	GET	/api/services/workers/lauramerivirta			304	211						192.168.100.100	14:44:29 26 Mar...	8080	151	
628	http://192.168.100.100:3001	GET	/api/bookings/workers/lauramerivirta			304	212						192.168.100.100	14:44:29 26 Mar...	8080	167	
627	http://192.168.100.100:3001	GET	/api/worktimes/workers/lauramerivirta			304	211						192.168.100.100	14:44:29 26 Mar...	8080	158	
626	http://192.168.100.100:3001	POST	/api/login		✓	200	585	JSON					192.168.100.100	14:44:29 26 Mar...	8080	193	
625	http://192.168.100.100:3001	POST	/api/bookings		✓	400	358	JSON					192.168.100.100	14:42:19 26 Mar...	8080	112	
624	http://192.168.100.100:3001	GET	/api/bookings			200	5147	JSON					192.168.100.100	14:40:41 26 Mar...	8080	89	
623	http://192.168.100.100:3001	GET	/api/worktimes/workers?username=lauramerivirta		✓	200	2091	JSON					192.168.100.100	14:40:41 26 Mar...	8080	106	
622	http://192.168.100.100:3001	GET	/api/services/types/fysioterapia			200	1398	JSON					192.168.100.100	14:39:31 26 Mar...	8080	35	
621	http://192.168.100.100:3001	GET	/api/services/types			304	210						192.168.100.100	14:39:29 26 Mar...	8080	22	
620	http://192.168.100.100:3001	POST	/api/login		✓	401	317	JSON					192.168.100.100	14:38:11 26 Mar...	8080	53	
619	http://192.168.100.100:3001	GET	/api/services/workers/lauramerivirta			200	3959	JSON					192.168.100.100	14:36:55 26 Mar...	8080	122	
618	http://192.168.100.100:3001	GET	/api/bookings/workers/lauramerivirta			200	5189	JSON					192.168.100.100	14:36:55 26 Mar...	8080	135	
617	http://192.168.100.100:3001	GET	/api/worktimes/workers/lauramerivirta			200	2091	JSON					192.168.100.100	14:36:55 26 Mar...	8080	129	
616	http://192.168.100.100:3001	POST	/api/login		✓	200	585	JSON					192.168.100.100	14:36:54 26 Mar...	8080	164	
613	http://192.168.100.100:3001	GET	/static/js/main.37168ee9.js			304	299	script	js				192.168.100.100	14:36:32 26 Mar...	8080	3	
612	http://192.168.100.100:3001	GET	/			304	297						192.168.100.100	14:36:32 26 Mar...	8080	2	

The detailed view of the selected request (617) shows the following details:

- Request:** GET /api/worktimes/workers?username=lauramerivirta HTTP/1.1. Headers include Host: 192.168.100.100:3001, User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0, Accept: application/json, text/plain, */*, Accept-Language: en-US,en;q=0.5, Accept-Encoding: gzip, deflate, br, Connection: keep-alive, Referer: http://192.168.100.100:3001/ajanvaraus, Priority: u=0.
- Response:** HTTP/1.1 200 OK. Headers include X-Powered-By: Express, Access-Control-Allow-Origin: *, Content-Type: application/json; charset=utf-8, Content-Length: 1821, ETag: W/"71d-XhtNVBoa40E7+0LIWosVb1Dt3T8", Date: Wed, 26 Mar 2025 18:40:41 GMT, Connection: keep-alive, Keep-Alive: timeout=5.
- Inspector:** The response body is a JSON object: {"id": "65d75f14d6ef8f29c3e516f6", "start": "2024-11-28T10:00:00.000Z", "end": "2024-11-28T16:45:00.000Z", "worker": {"username": "lauramerivirta", "id": "65eaff6db22b4f0a35a744d8"}, "v": 0}.

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