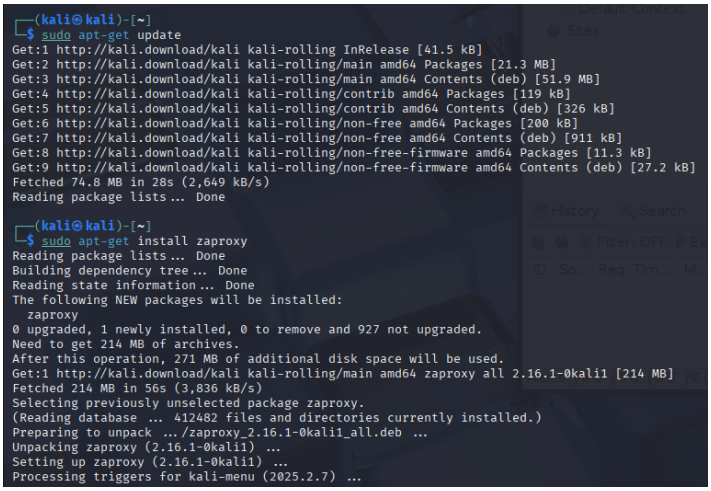
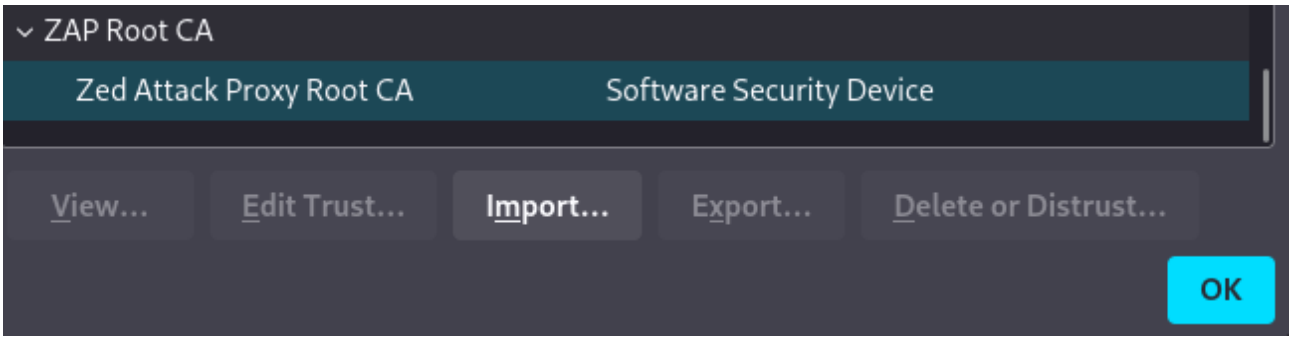
x.

- Tavallisia haavoittuvuuksia pääsyn hallinnassa
    - Jos järjestelmä ei seuraa least privilege -menetelmää
    - Pääsyn hallinnan tarkistusten ohitus
    - Jos pääsee käsiksi käyttäjään sen unique identifier:in avulla
    - API, josta puuttuu tarkistukset POST, PUT ja DELETE komennoille
    - Elevation of privilege eli, jos pystyt esittämään käyttäjää ilman kirjautumista tai adminia normaalilla käyttäjällä
    - Metadatan manipulaatio
    - CORS:in virheellinen konfiguraatio
- Hyökkäykset estetään, jos voidaan estää hyökkääjän kyky muokata pääsyn hallintaa tai metadataa
- IDOR eli insecure direct object references on pääsyn hallinnan haavoittuvuus
    - Haavoittuvuus esiintyy, kun käyttäjän hallitsemien parametrien avulla pääsee suoraan käsiksi palvelun resursseihin tai funktioihin
    - Sillä päästään ohittamaan pääsyn hallinta
- Path traversal
    - Haavoittuvuus, jossa hyökkääjä pääsee käsiksi serverin tiedostoihin, jotka voivat sisältää esim.
        - Koodia ja dataa
        - Tunnistetietoja
        - Käyttöjärjestelmän tiedostoja
    - Voidaan estää validoimalla user input ennen prosessointia
- Cross-site scripting
    - Verkko haavoittuvuus, jolla hyökkääjä voi hyväksikäyttää käyttäjän ja haavoittuneen sovelluksen vuorovaikutusta
    - Toimii manipuloimalla haavoittuva sovellus palauttamaan haitallista koodia käyttäjälle
    - Voidaan käyttää moneen tarkoitukseen, kuten
        - Toisen käyttäjän esittämiseen
        - Lukemaan käyttäjän näkemää dataa
    - Voidaan ehkäistä esim.
        - Suodattamalla saapuvaa dataa
        - CSP hyökkäyksen tapahduttua

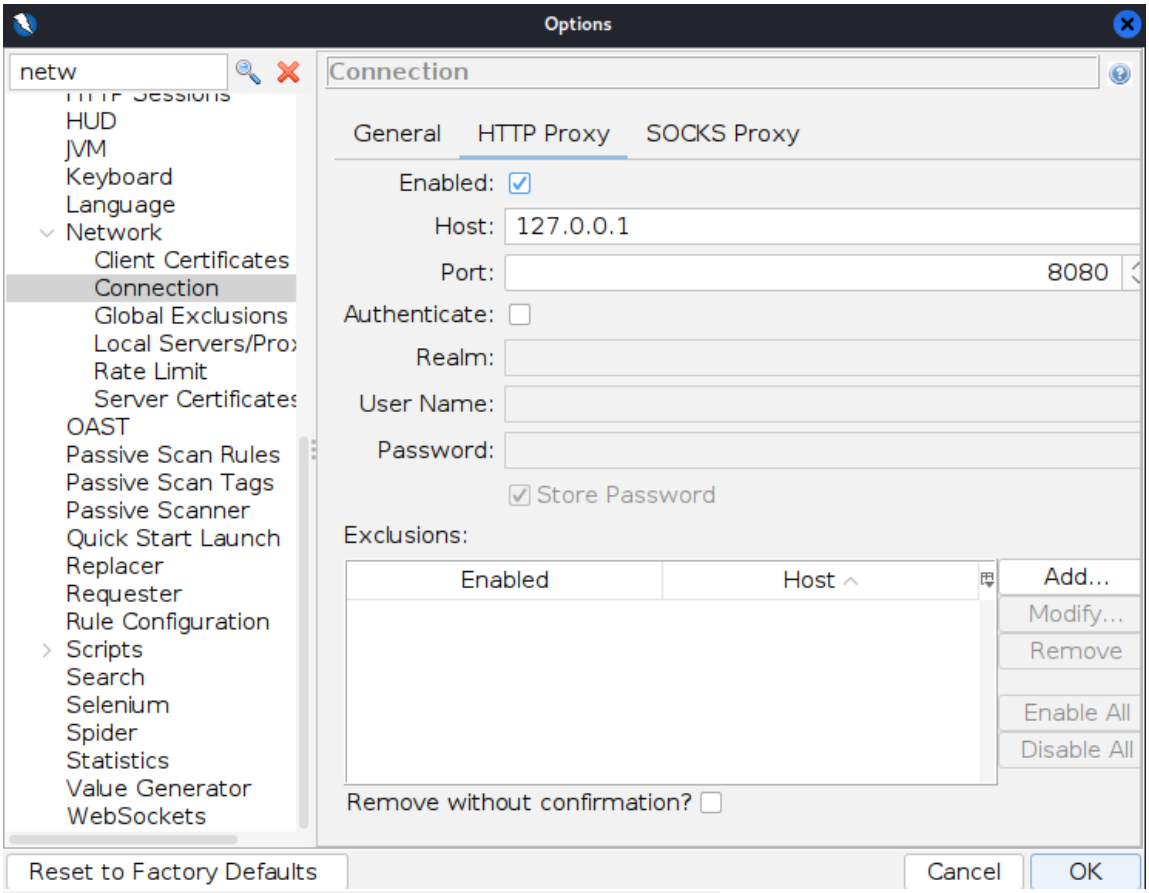
a. Minun piti päivittää apt database ennen, kuin pystyin lataamaan zaproxyn.

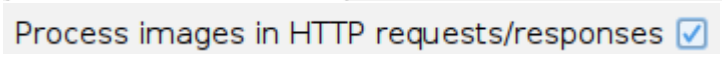


Tein sertifikaatin ja asensin sen selaimeen.



Asetin Zap:n proxyn pyörimään localhostiin ja laitoin ZAP:n kaappaamaan myös kuvat.



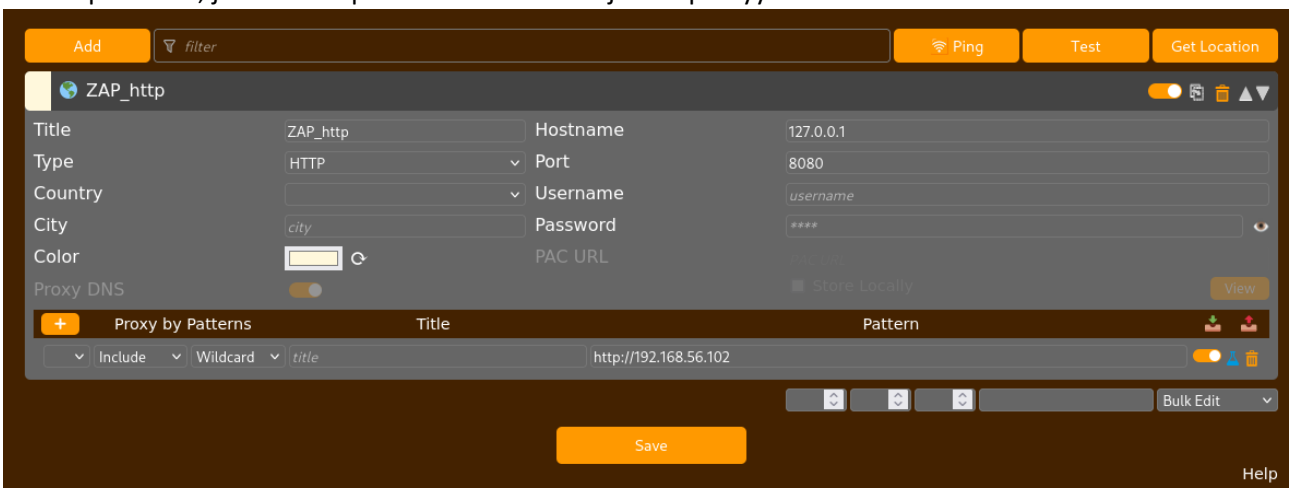


Hakupyynnöt ilmestyvät Zap:n käyttöliittymään.

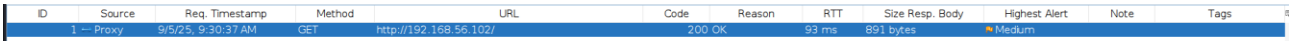
2,943	Proxy	9/5/25, 8:04:50 AM	GET	http://192.168.56.102:80/	504 Gateway Timeout 20.02 s	179 bytes
2,944	Proxy	9/5/25, 8:04:50 AM	GET	http://192.168.56.102:80/	504 Gateway Timeout 20.03 s	179 bytes
2,949	Proxy	9/5/25, 8:04:50 AM	GET	http://192.168.56.102:80/	504 Gateway Timeout 20.03 s	179 bytes
2,997	Proxy	9/5/25, 8:04:50 AM	GET	http://192.168.56.102:80/	504 Gateway Timeout 20.03 s	179 bytes
2,994	Proxy	9/5/25, 8:04:50 AM	GET	http://192.168.56.102:80/	504 Gateway Timeout 20.03 s	179 bytes
2,995	Proxy	9/5/25, 8:04:50 AM	GET	http://192.168.56.102:80/	504 Gateway Timeout 20.02 s	179 bytes
3,000	Proxy	9/5/25, 8:04:50 AM	GET	http://192.168.56.102:80/	504 Gateway Timeout 20.02 s	179 bytes
2,951	Proxy	9/5/25, 8:04:50 AM	GET	http://192.168.56.102:80/	504 Gateway Timeout 20.03 s	179 bytes
3,002	Proxy	9/5/25, 8:04:50 AM	GET	http://192.168.56.102:80/	504 Gateway Timeout 32.3 s	179 bytes
3,003	Proxy	9/5/25, 8:04:50 AM	GET	http://192.168.56.102:80/	504 Gateway Timeout 32.36 s	179 bytes
3,004	Proxy	9/5/25, 8:05:02 AM	GET	http://192.168.56.102:80/	504 Gateway Timeout 20.12 s	179 bytes
3,005	Proxy	9/5/25, 8:05:02 AM	GET	http://192.168.56.102:80/	504 Gateway Timeout 20.06 s	179 bytes
3,006	Proxy	9/5/25, 8:05:02 AM	GET	http://192.168.56.102:80/	504 Gateway Timeout 20.09 s	179 bytes
3,007	Proxy	9/5/25, 8:05:02 AM	GET	http://192.168.56.102:80/	504 Gateway Timeout 20.1 s	179 bytes

b. Asensin foxyproxyn mozilla add-on kaupasta.

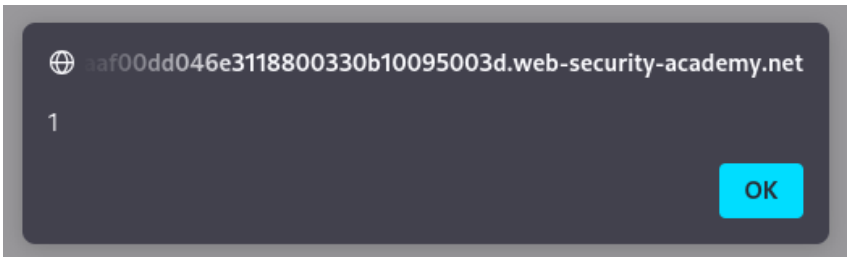
Lisäsin patternin, jossa metasploitablen liikenne ohjataan proxyyn.



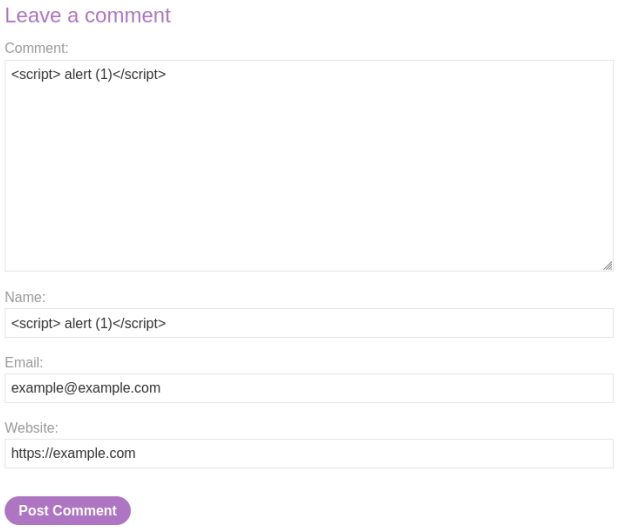
Seuraavaksi lisään ZAP:n proxyksi siihen ja laitoin sen ohjaamaan metaploitable 2 sivun liikenteen proxyyn.



c. Ratkaisin ensimmäisen PortSwigger tehtävän z3nsh3ll:n youtube videon avulla, koska en ole ennen tehnyt cross-site scriptingia. Kokeilin syöttää koodia hakukenttään. Ongelma johtuu siitä, ettei nettisivu osaa käsitellä koodia oikein vaan se palauttaa koodin syötettynä source koodiin. Palvelimen ei pitäisi suorittaa syötettyä skriptiä.



d. Toisessa kohdassa kokeilen syöttää skriptejä palautekenttään ja katsoa saanko suoritettua alert funktion jossain niistä.

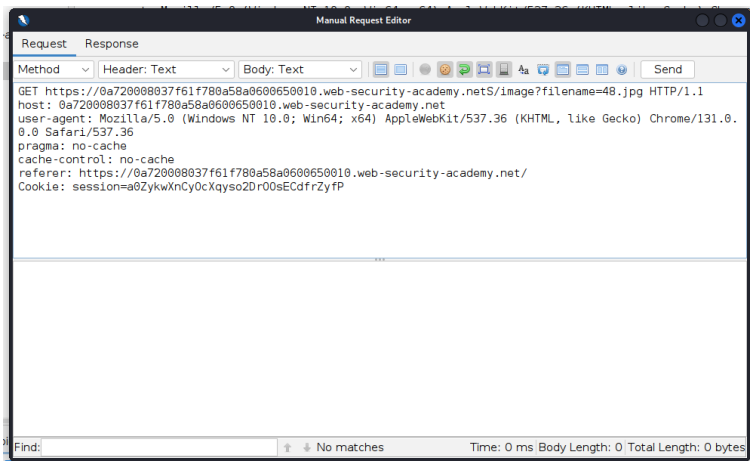


Nettisivulla tallentaa postauksen osaksi source koodia eikö encodaa sitä omaksi funktioksi.

e. Hyökkääjä pystyy syöttämään sivun source koodiin komentoja. Esim. <script>https://example.com/attack.js</script> näin hyökkääjä voi ajaa komentoja käyttäjän selaimessa.

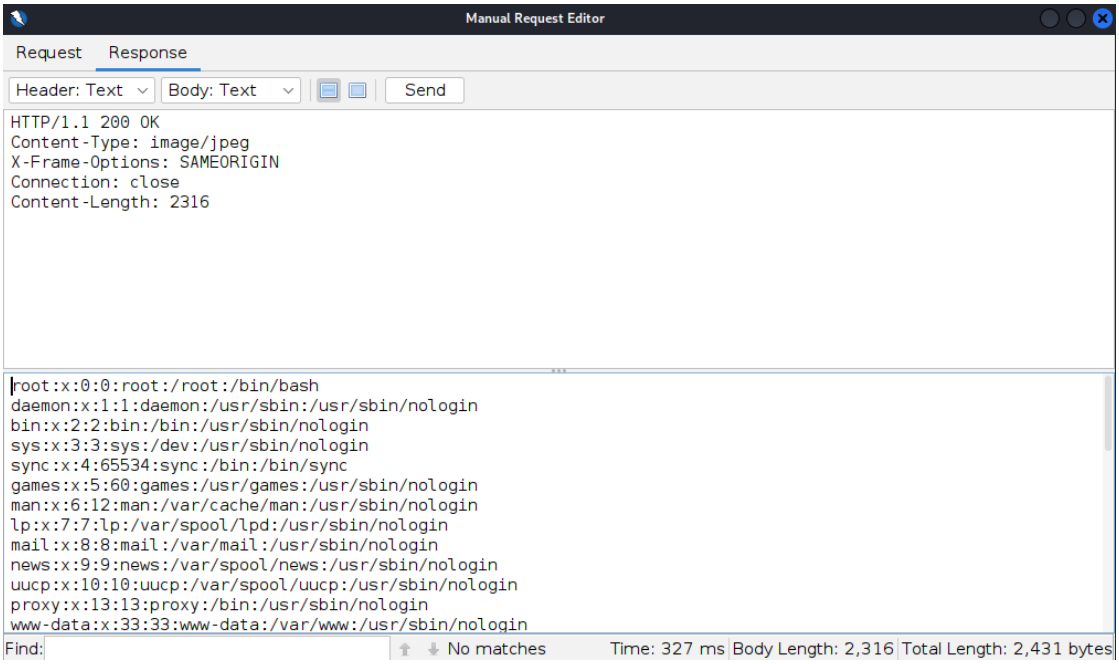
f. Käytin seuraavien tehtävien selitykseen apuna tätä sivua https://owlhacku.com/file-path-traversal-traversal-sequences-blocked-with-absolute-path-bypass/.

Tein active scannin labia vasten, josta tuli tämä kuva ja nyt muokkaan kuvan haku URL-osoitetta, niin että saan haettua passwd tiedoston. Palvelimella ei ole syötteen validointia ja se sallii kaikkien tiedostojen lukemisen. ../ kertoo montako hakemistoa pitää mennä taaksepäin, että päästään haluttuun tiedostoon.

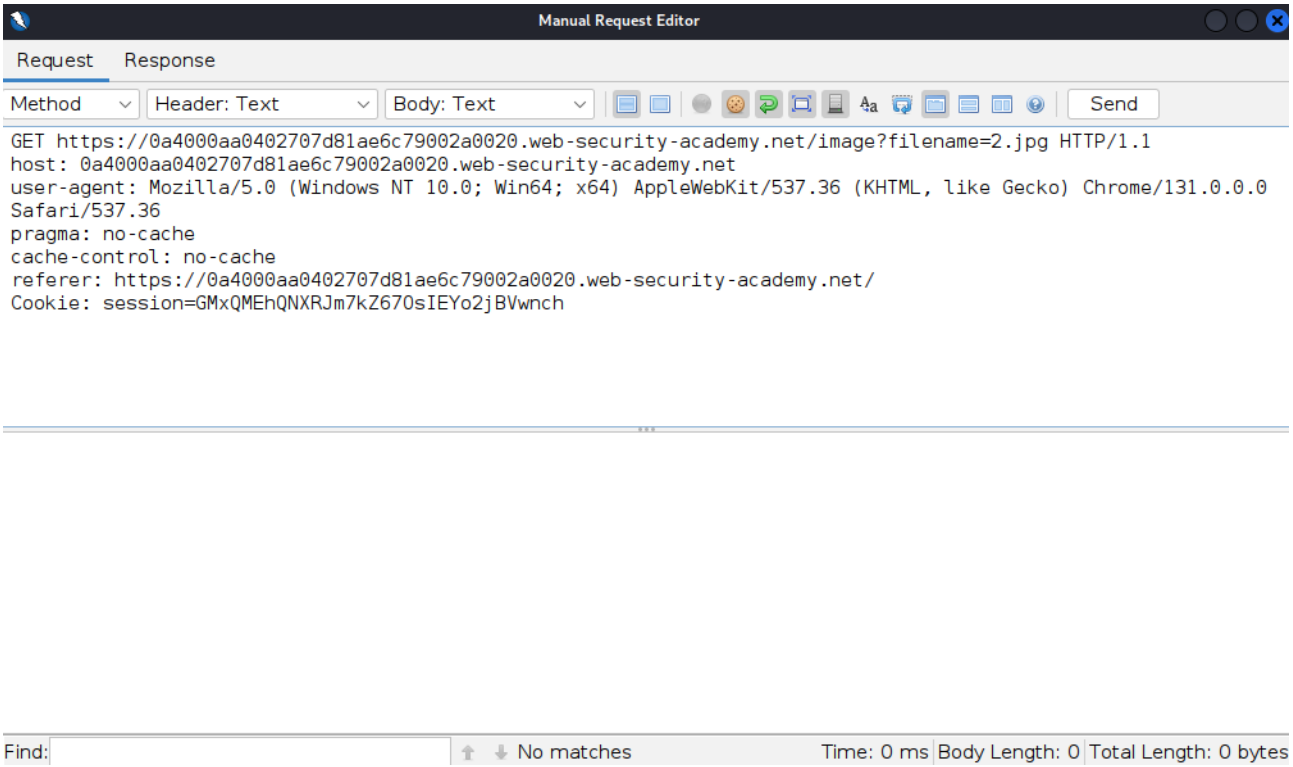


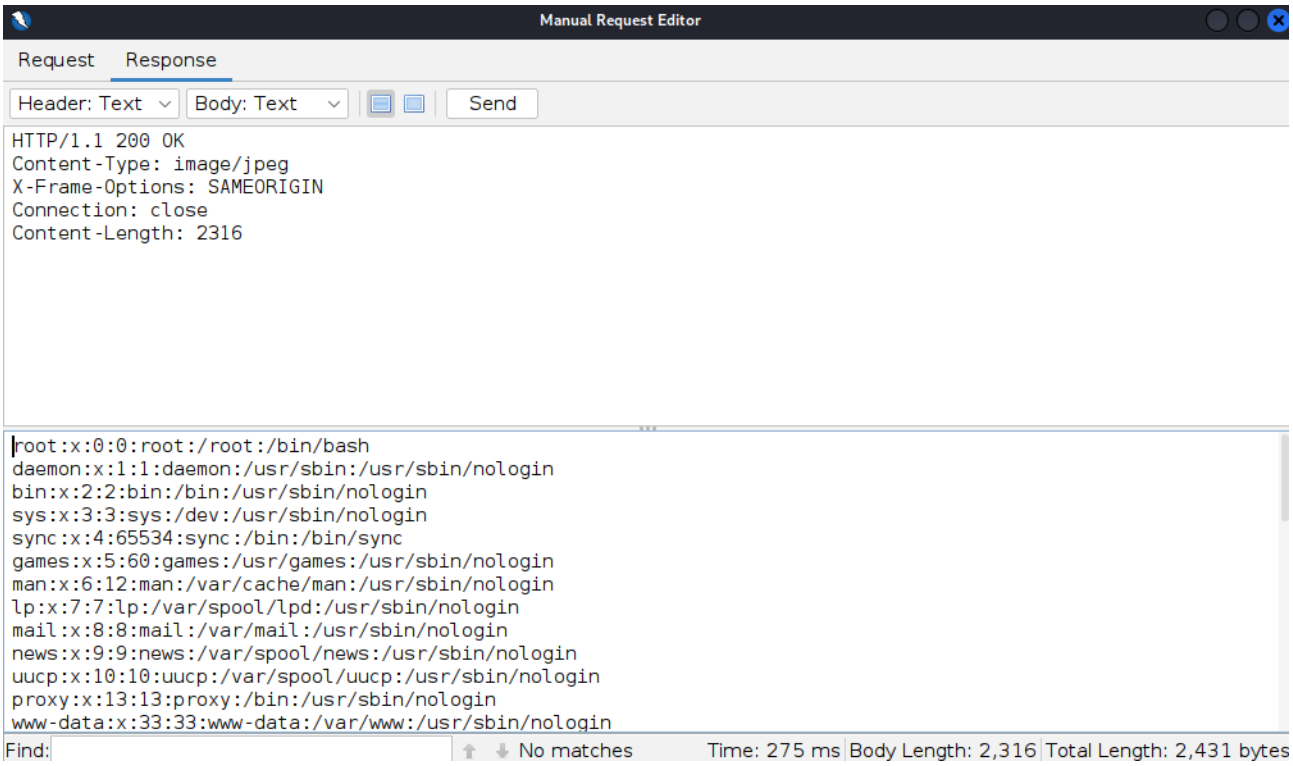
Tässä muokattu haku:

```
GET https://0a720008037f61f780a58a0600650010.web-security-academy.net/image?filename=../../../../etc/passwd
HTTP/1.1
```

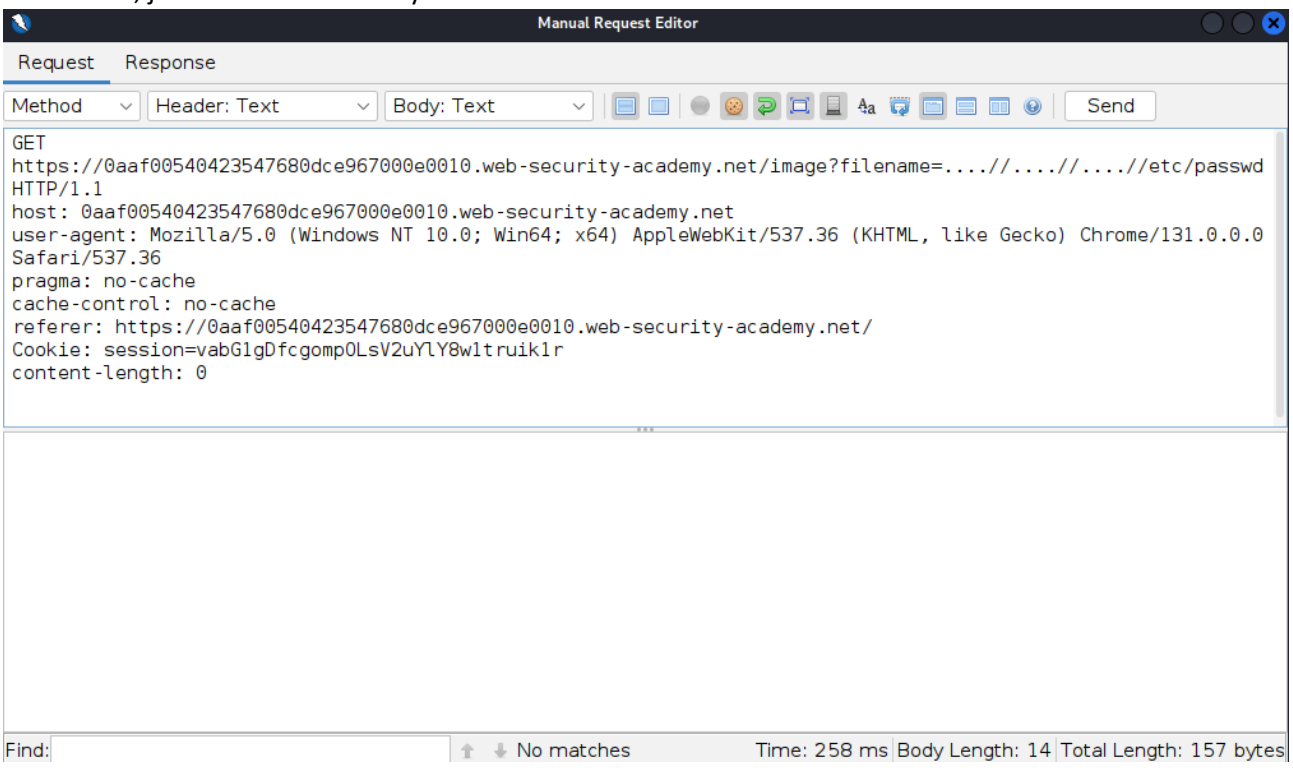


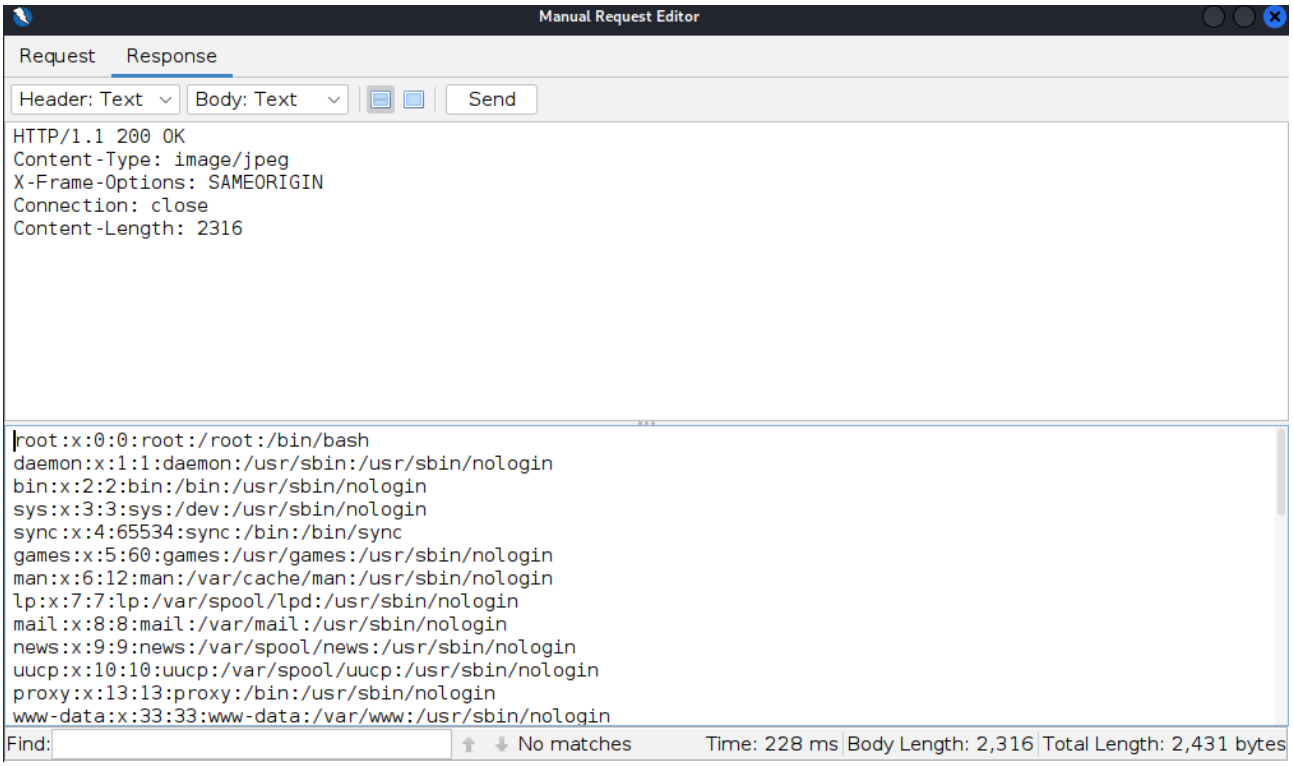
g. Tässä tehtävässä teen lähes saman mitä viime tehtävässä, mutta palvelimella on blokattu ../ käyttö, mutta voin yhä hakea suoraan tiedostoa.



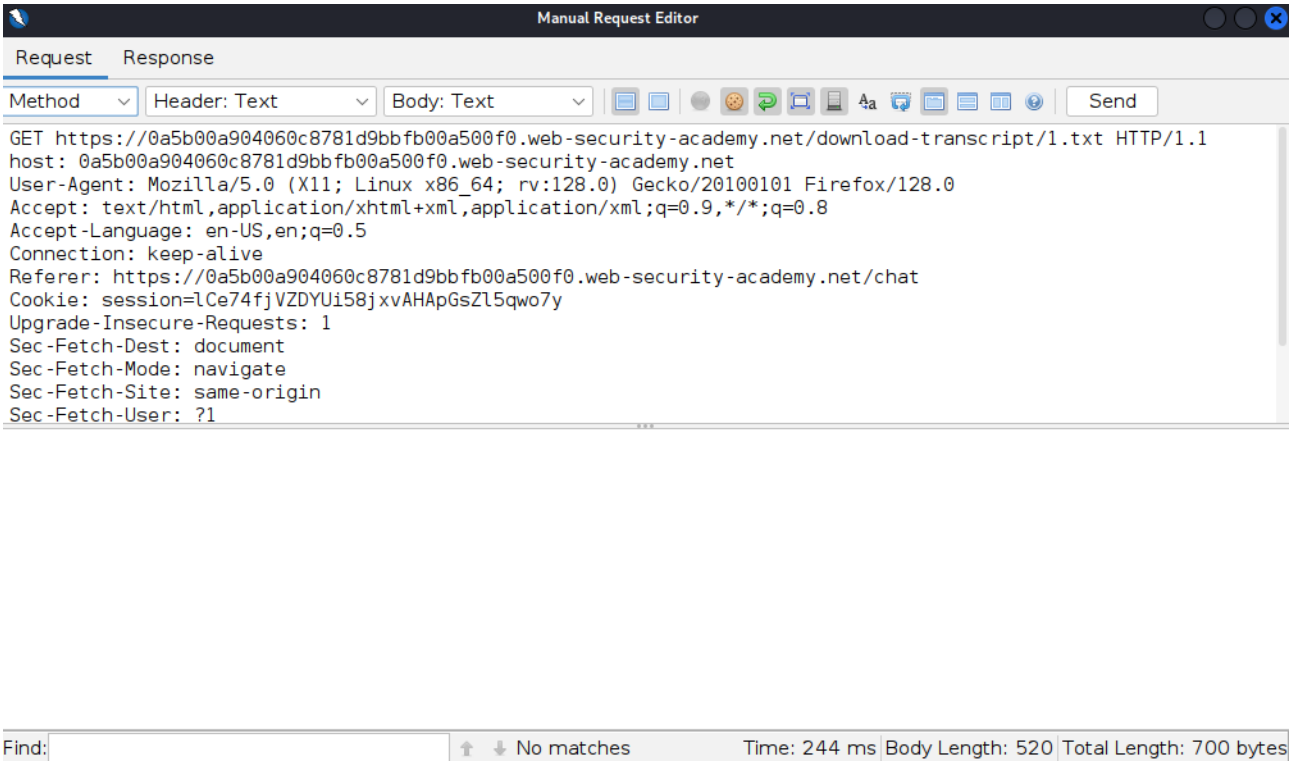


h. Lähdin tekemään tätäkin samalla tavalla, mutta hain taas tiedostoa eri tavalla. Palvelin poistaa ../ syötteet, mutta jos syötän ….// se poistaa sisimmäisen, mutta jättää jäljelle ensimmäiset 2 pistettä ja viimeinen kenoviiva. Palvelin siis tekee vain yhden input validaation, mutta pitäisi tehdä output validaation, joka tarkistaisi lähetetyn tiedon.





i. Sivulta pystyy lataamaan transcriptin chatista, jotka on numeroitu. Lähetän siis pyynnön, jossa pyydetään transcript 1.



Request Response

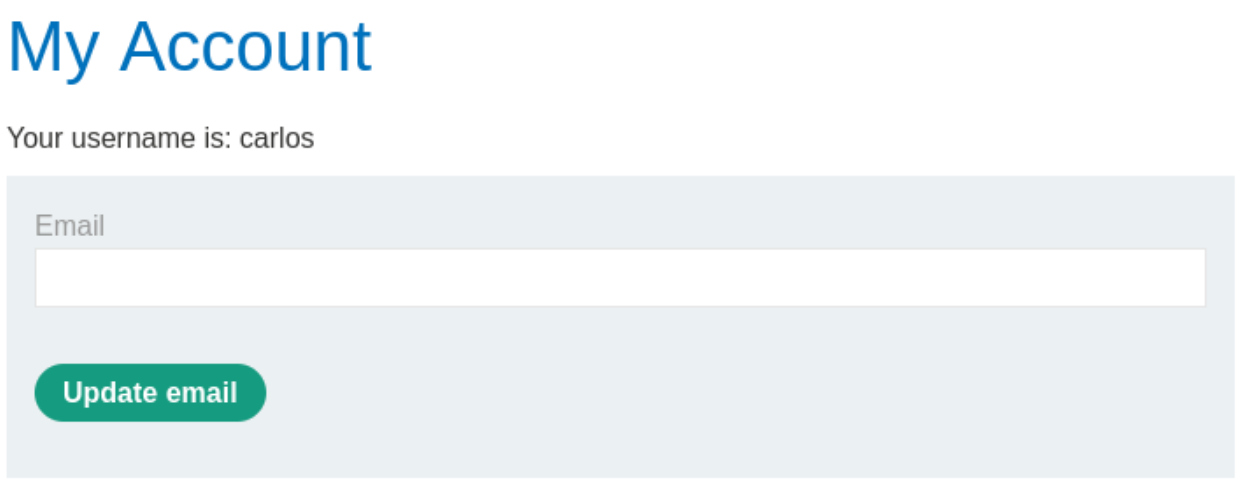
Header: Text Body: Text Send

```
HTTP/1.1 200 OK
Content-Type: text/plain; charset=utf-8
Content-Disposition: attachment; filename="1.txt"
X-Frame-Options: SAMEORIGIN
Connection: close
Content-Length: 520
```

```
CONNECTED: -- Now chatting with Hal Pline --
You: Hi Hal, I think I've forgotten my password and need confirmation that I've got the right one
Hal Pline: Sure, no problem, you seem like a nice guy. Just tell me your password and I'll confirm whether it'
s correct or not.
You: Wow you're so nice, thanks. I've heard from other people that you can be a right ****
Hal Pline: Takes one to know one
You: Ok so my password is mvin1e1nubbkm1t0oges. Is that right?
Hal Pline: Yes it is!
You: Ok thanks, bye!
Hal Pline: Do one!
```

Find: No matches Time: 244 ms Body Length: 520 Total Length: 700 bytes

Pääsin kirjautumaan käyttäjällä carlos.



Tämä on mahdollista, koska tiedostot ovat numerosarjassa 1, 2, 3 jne. eikä randomisoitu ja kuka tahansa pystyy ladata transcriptit.

Lähteet:

Tero Karvinen. Tunkeutumistestaus. https://terokarvinen.com/tunkeutumistestaus/#h3-taysin-laillinen-sertifikaatti.

OWASP. A01:2021 – Broken Access Control. https://owasp.org/Top10/A01_2021-Broken_Access_Control/.

PortSwigger. IDOR. https://portswigger.net/web-security/access-control/idor.

PortSwigger. What is path traversal? https://portswigger.net/web-security/file-path-traversal.

PortSwigger. Cross-site scripting. https://portswigger.net/web-security/cross-site-scripting.

How To Install zaproxy on Kali Linux. https://installati.one/install-zaproxy-kalilinux/.

Z3nsh3ll. WHat is Reflected XSS? (Cross Site Scripting). https://youtu.be/P8YOuAYW8es.

Owlhacku. File path traversal, traversal sequences blocked with absolute bypass. https://owlhacku.com/file-path-traversal-traversal-sequences-blocked-with-absolute-path-bypass/.