Failed Attack: Traversal attack

# What is a traversal attack?

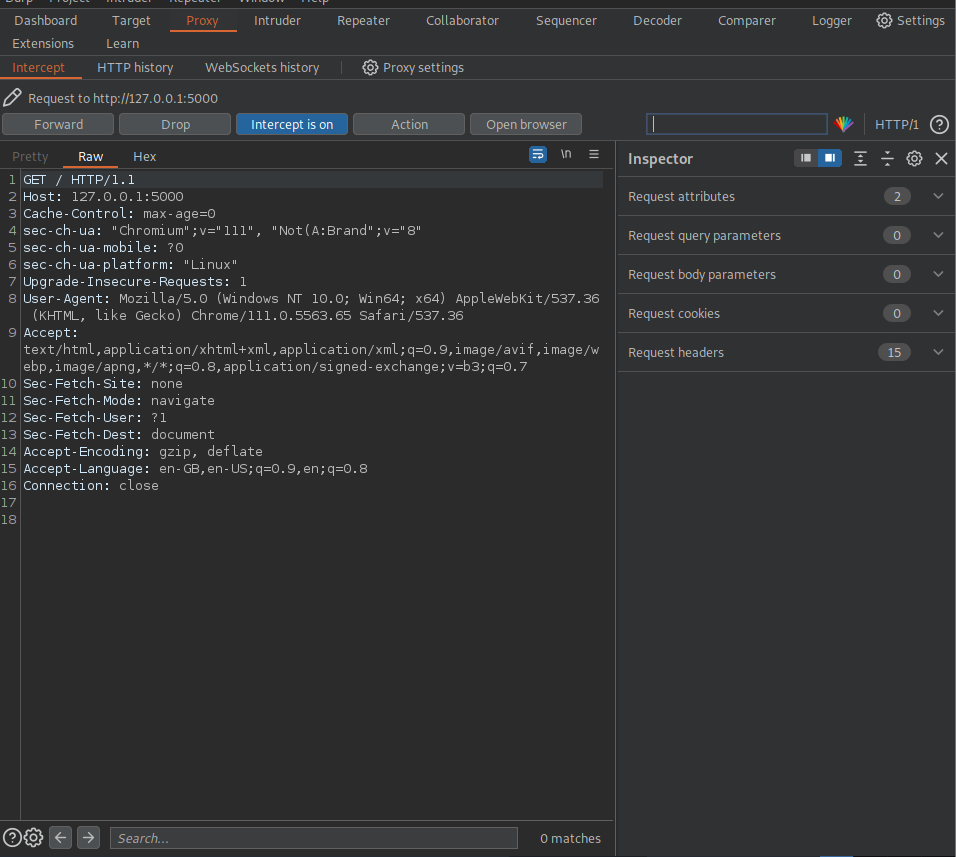
A traversal attack (also known as Directory traversal and file path traversal) which would allow for an attacker to read files that is running an application, this can lead to attackers being able to read files that may not normally be accessible. While the files that can be accessed through this attack is limited and finite there is still the possibility that there can be sensitive information stored within the directories that can be exposed to potential hackers.

# Why use a traversal attack?

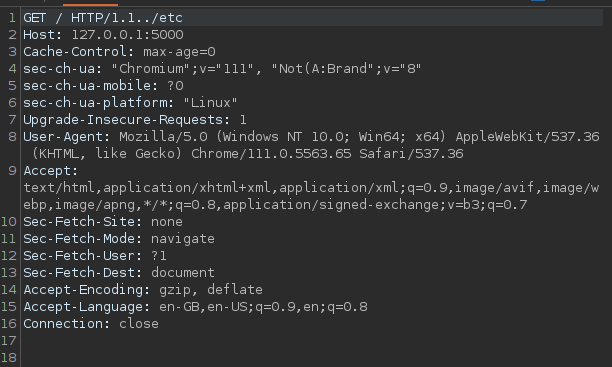
While searching for vulnerabilities any little bit helps and if an attacker can gain some files while searching for other possible methods of attacks it gives an advantage. Conducting a Traversal attack can see if there is a basic level of security and proves whether the data is being sanitized. Gaining access to files and hidden data can also allow for an attacker to gain access to any ACL if it is implemented and from there it is only a matter of time before they can mimic authorized users.

# Evidence

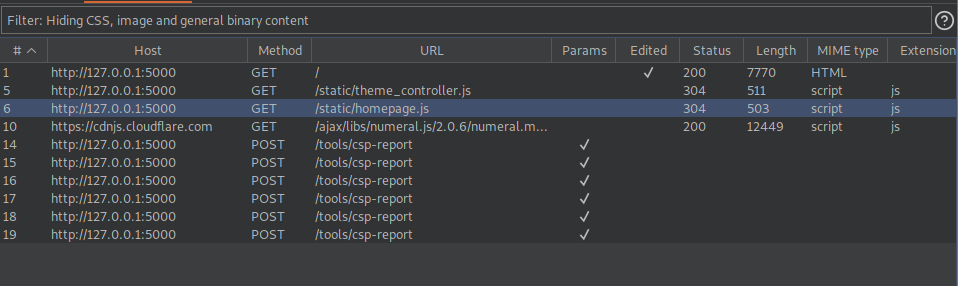
Using burpsuite (shown below) we can intercept any traffic to and from the website, this allows you to attack before a packet gets forwarded onwards, you can choose to drop packets as well however that doesn’t accomplish anything apart from getting the page to not load, we can edit the get request while it is intercepted to try and



This screenshot shows that the packet I sent was edited however the results were that the data gets sanitized and anything that doesn’t belong either gets rejected or simply redirected to the homepage. I am not able to see any directories or any folders I shouldn’t



Above is a screenshot showing a modified version of the packet im about to send, typically if the data doesn’t get sanitized doing something as simple as this would allow me to see the directories.

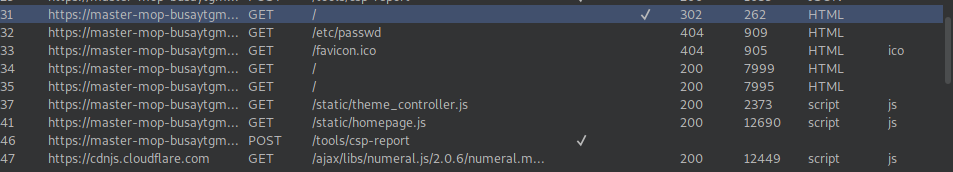


As shown in this screenshot below editing the get request will often refuse connection in this case which means there are already methods in place to prevent traversal attacks.

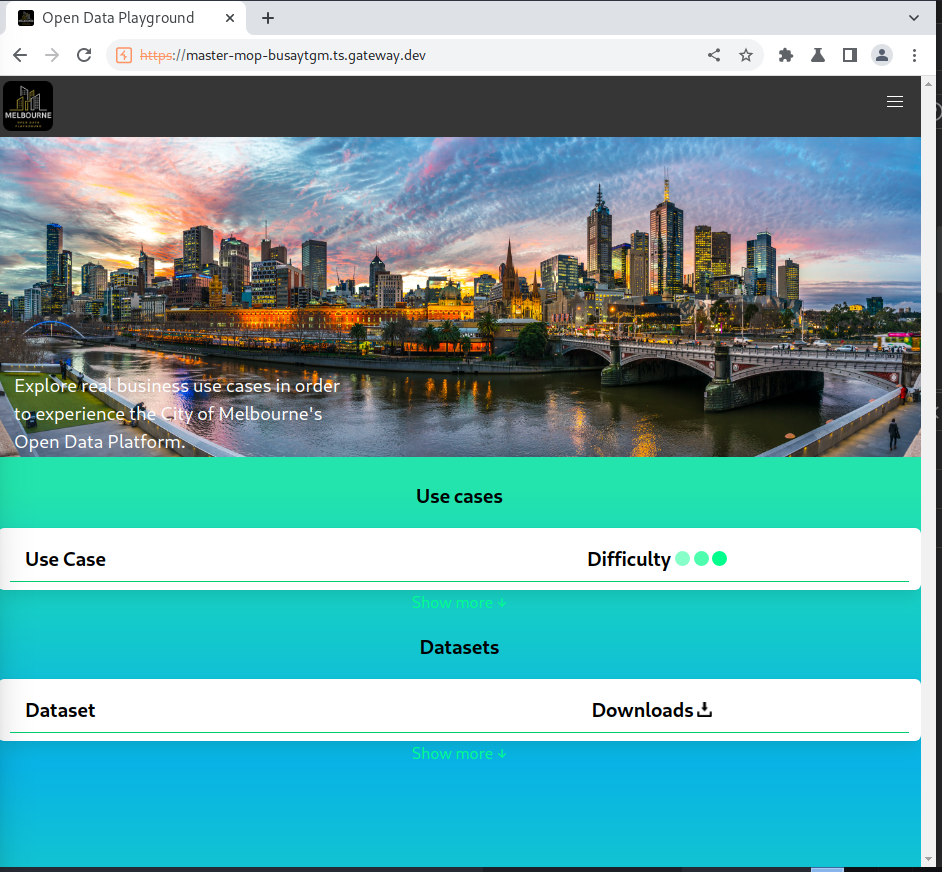
# Prevention methods

Although further investigation will be required for me to see what measures have been implemented into this code the way methods to prevent this type of attack can include sanitizing filename parameters and not allowing user supplied data as filenames, if a file needs to be accessed by a user accessing the webapp then whitelists can come in handy. And ensuring that there are the correct privileges set up for different users, accessing the files is one thing but if they are denied read and execute rights then that is one method to deter attackers.

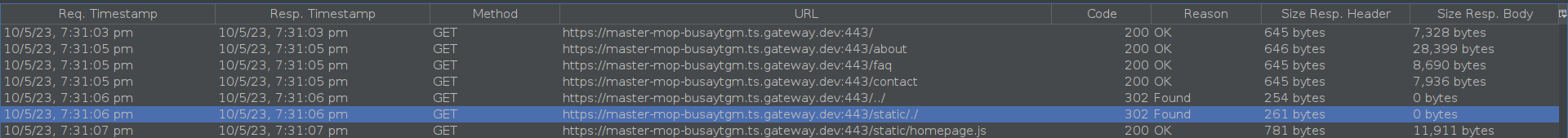
# Traversal Attacks on HTTPS



As shown in the screenshot above editing the packet to try and navigate further in the potential directory where the files are shown results in the website ignoring it and just loading the page as normal (below)



# Further Findings

I decided to look further into this type of attack and see what exactly is happening. Although the directory does exist (see below)  


It is giving a redirection error, which in this case is a good thing because it shows the data is being sanitized properly and it isn’t letting anyone who doesn’t have access to the directories gain access by manually inputting the address. The error 302 code is saying that the directory does indeed exist but putting this into the browser will ensure that the user entering this will get redirected.

Although the fact this directory can be found isn’t a vulnerability the server can be further configured so that this page cannot be found

# Reference list

Dahan, M. (2022). *What are Path Traversal Attacks? (+ how to prevent them)*. [online] Comparitech. Available at: https://www.comparitech.com/blog/information-security/path-traversal-attacks/.

Luktevich, B. (n.d.). *What is a Directory Traversal Attack? - TechTarget*. [online] Security. Available at: https://www.techtarget.com/searchsecurity/definition/directory-traversal.

OWASP (n.d.). *Path Traversal | OWASP*. [online] owasp.org. Available at: https://owasp.org/www-community/attacks/Path\_Traversal.

PortSwigger (2019). *What is directory traversal, and how to prevent it?* [online] Portswigger.net. Available at: https://portswigger.net/web-security/file-path-traversal.