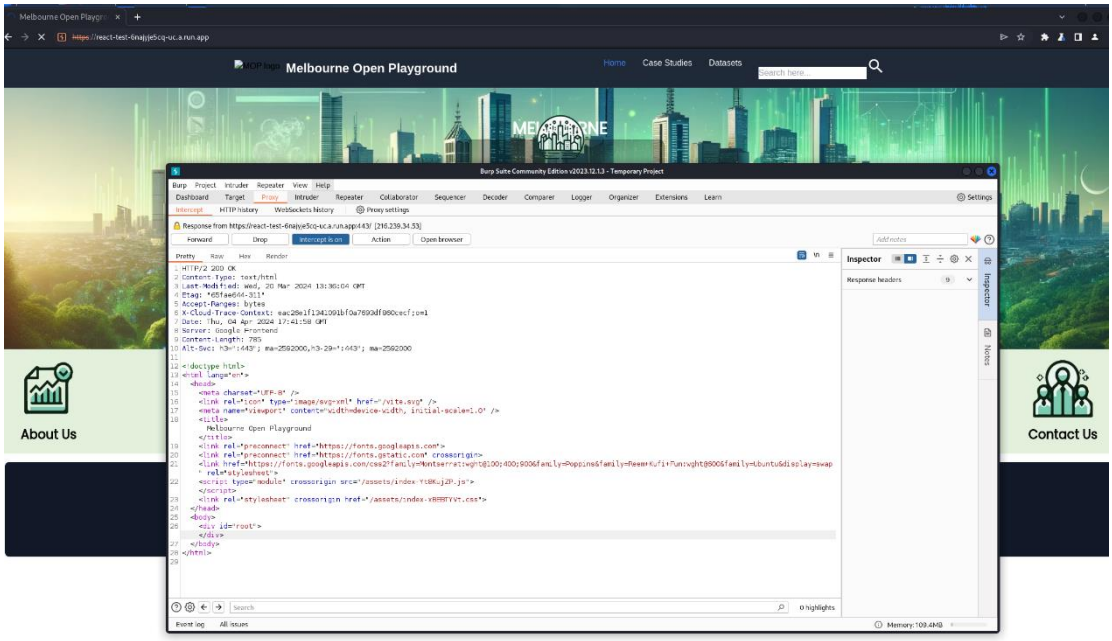
MOP TEST Done by Xing ∫𝑋

Tool: Burp Suite Firefox

1.



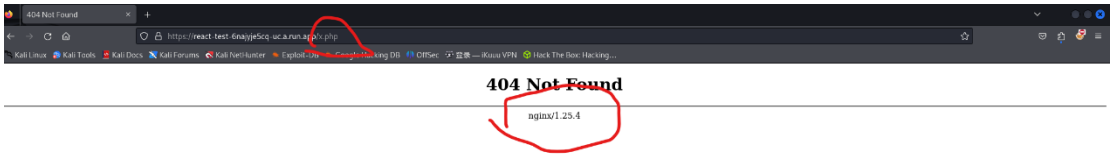
Open the URL https://react-test-6najyje5cq-uc.a.run.app/ , and at the same time open the Burp suite network packet capture tool, refresh the page and capture the packet, and obtain the response packet file of the request.

By observing the response header, it is found that the X-Frame-Options HTTP response header is not set, which may cause the website to be maliciously used in clickjacking attacks. The X-Frame-Options HTTP response header is used to indicate to the browser whether a page can be allowed. Markup displayed within <frame>, <iframe> or <object>. Websites that are not configured with X-Frame-Options may be at risk of clickjacking (the content is embedded into other people's websites and a transparent layer is added on top to induce users to click).

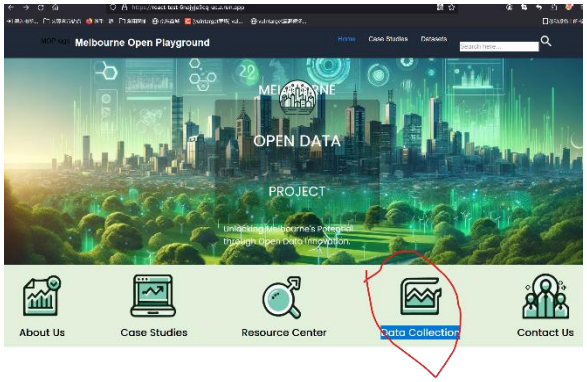
2.

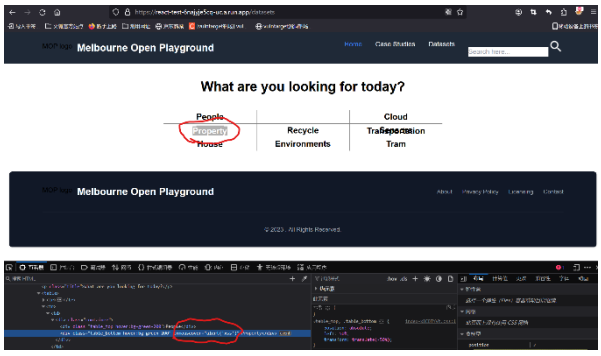
At the same time, by observing the response header, it was found that the X-Content-Type-Options parameter setting was missing. The web server's response header to the HTTP request is missing the X-Content-Type-Options, which means the website is more vulnerable to cross-site scripting attacks (XSS). The X-Content-Type-Options response header is equivalent to a prompt flag. It is used by the server to prompt the client to follow the MIME type setting in the Content-Type header and not to modify it. This disables the client. End-to-end MIME type sniffing behavior. Browsers usually identify resource types based on the Content-Type field of the response header. The Content-Type of some resources is wrong or undefined. In this case, the browser will enable MIME-sniffing to guess the type of the resource and parse the execution content. Using this feature, an attacker can cause requests that should be parsed as images to be parsed as JavaScript code.

3.



Try to report an error by adding a non-existent directory after the domain name, https://react-test-6najyje5cq-uc.a.run.app/x.php, as shown in the figure, the website successfully reports an error and displays nginx. The error page indicates that the nginx version number is 1.25.4. Sensitive server information such as this middleware version detected through such an error may be used by hackers in network attacks.





Nginx 1.25.4 vulnerability: https://www.tenable.com/plugins/was/114207

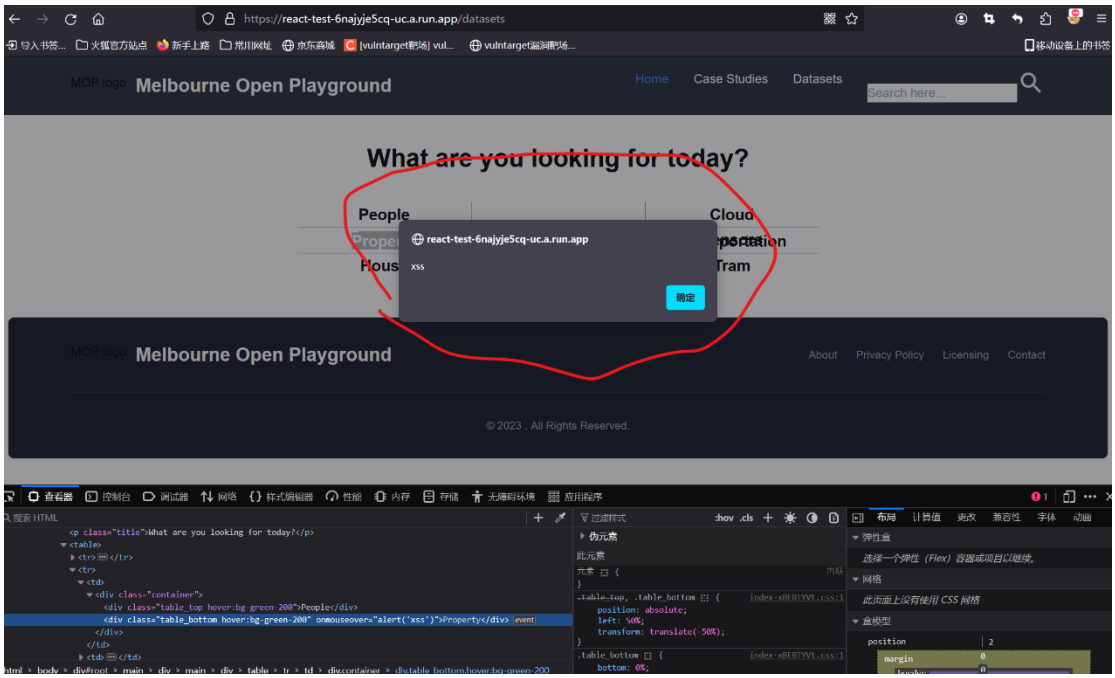
4.

Click the page Data Collection button to enter a new page.

I found that if you hover the mouse over the PeopleProperty in the new page, the text will turn green. Here we try reflective XSS, open the developer tools, and add onmouseover="alert('xss')" attributes.

5.

When the mouse passes over the PeopleProperty, a JS pop-up window pops up successfully, indicating that there is a reflected XSS vulnerability here.



Solution to fix:

(1) For the repair of the missing X-Content-Type-Options response header, since nginx is used, the following code can be added to the nginx configuration:

“add_header X-Content-Type-Options "nosniff" always;”

(2) To fix the missing X-Frame-Options HTTP response header, you can add the following code to the nginx configuration file:

“add_header X-Frame-Options "ALLOW-FROM https://example.com";”

(3) For repairing XSS cross-site scripting attacks on websites, there are several avoidance ideas:

A. Input validation: Ensure that all inputs are validated to be of the correct type and format, and match expected values.

B. Clean input: Clean up all HTML tags and special characters before storing or outputting.

C. Use prepared statements: Use prepared statements in database queries to prevent SQL injection attacks.

D. Output encoding: Encode the output appropriately, such as using HTML entity encoding to escape special characters.

E. Content Security Policy (CSP): Configure Content Security Policy (CSP) to restrict the origin of executable scripts.