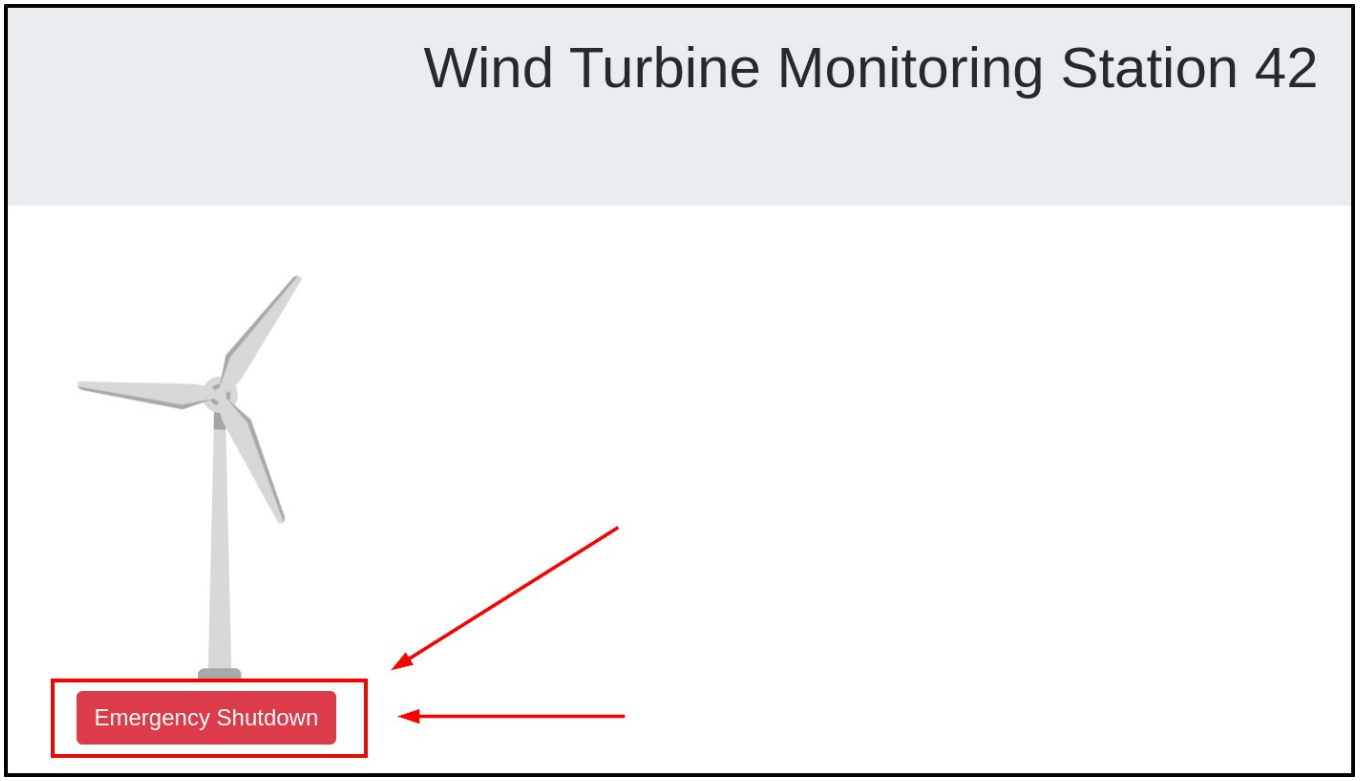
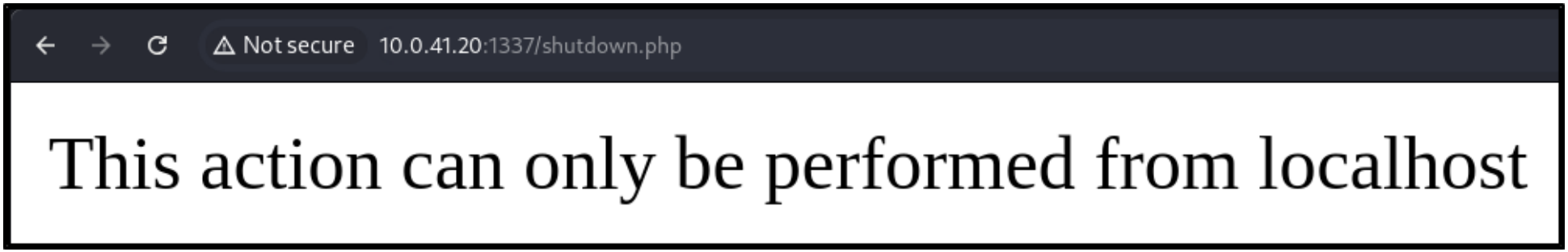
Turbine – SSRF



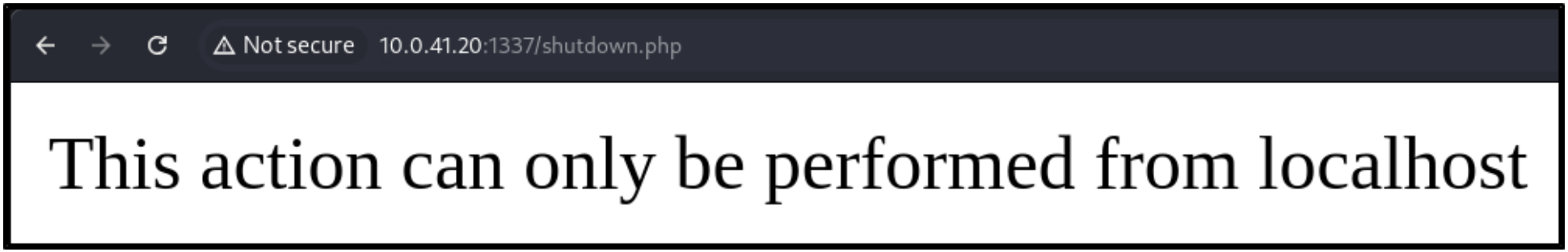
This application has a button which is supposed to “shut down” the turbine

Turbine – Localhost Restricted



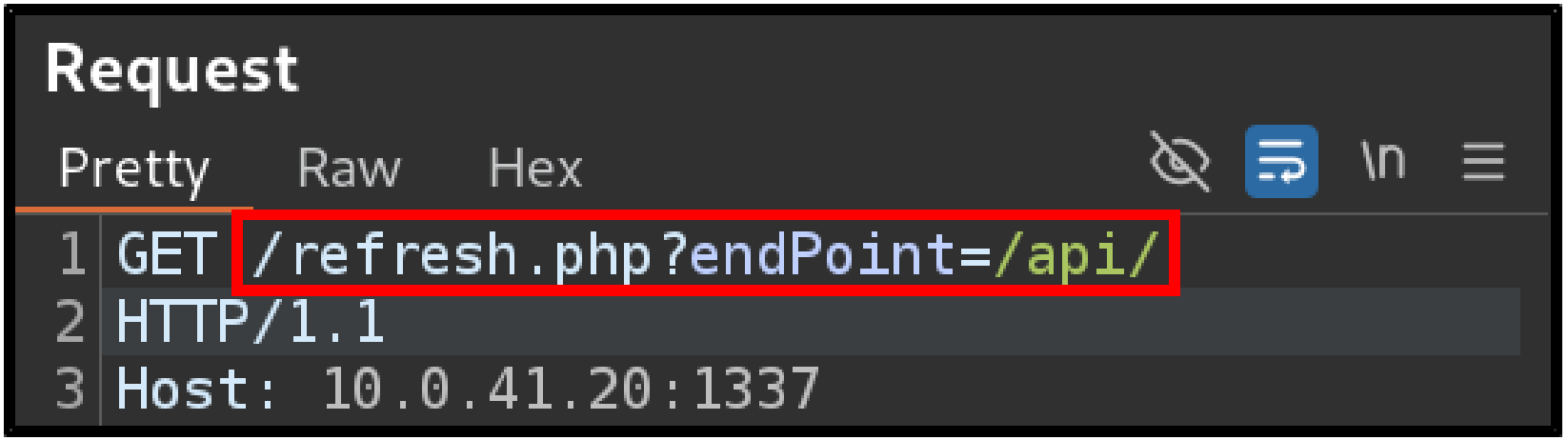
But we can't access the page, and we get an error message indicating that this page can only be accessed from the localhost

Turbine – Localhost Restricted



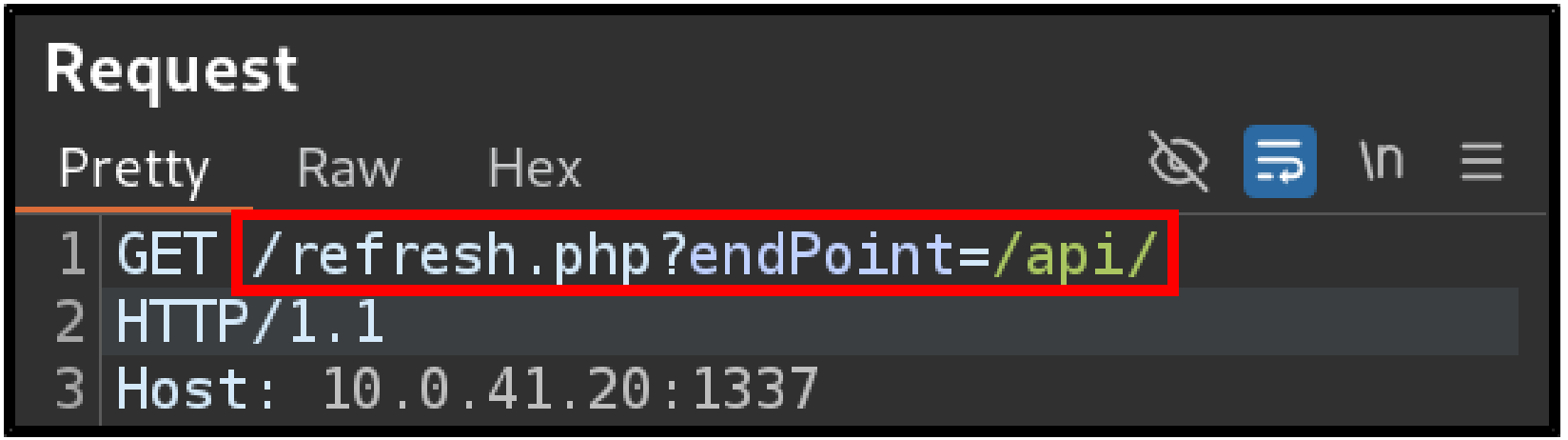
To solve the challenge, we'll need to force the app to return local-access content, which would be an example of Server-Side Request Forgery (SSRF)

Turbine – Additional Requests



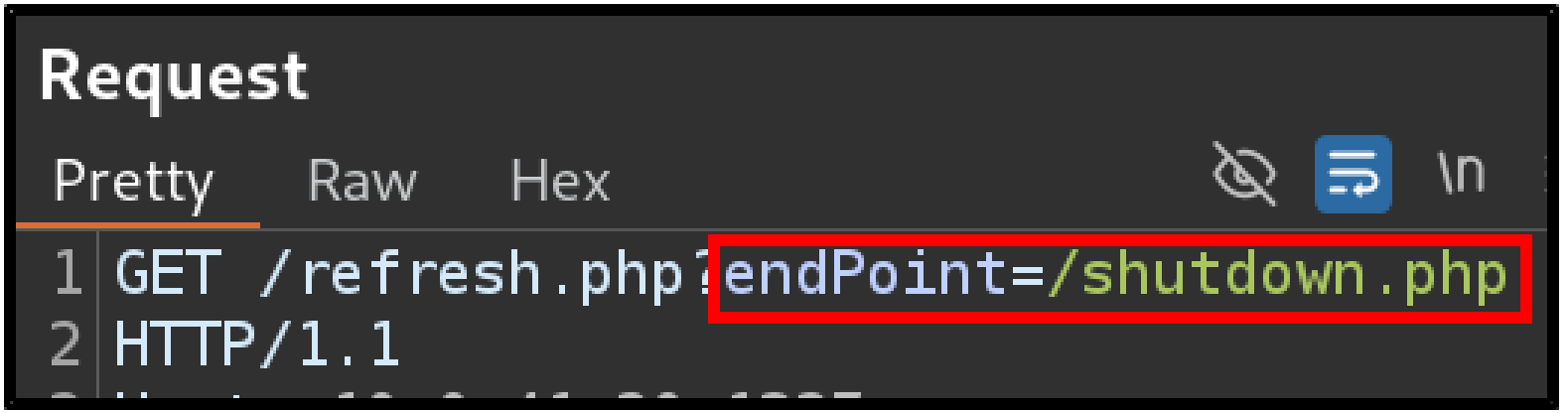
If we take a look at the requests in Burp Suite, we see that after each request we make the server, we make a request to the `/refresh.php` page

Turbine – Resource Access via Parameter



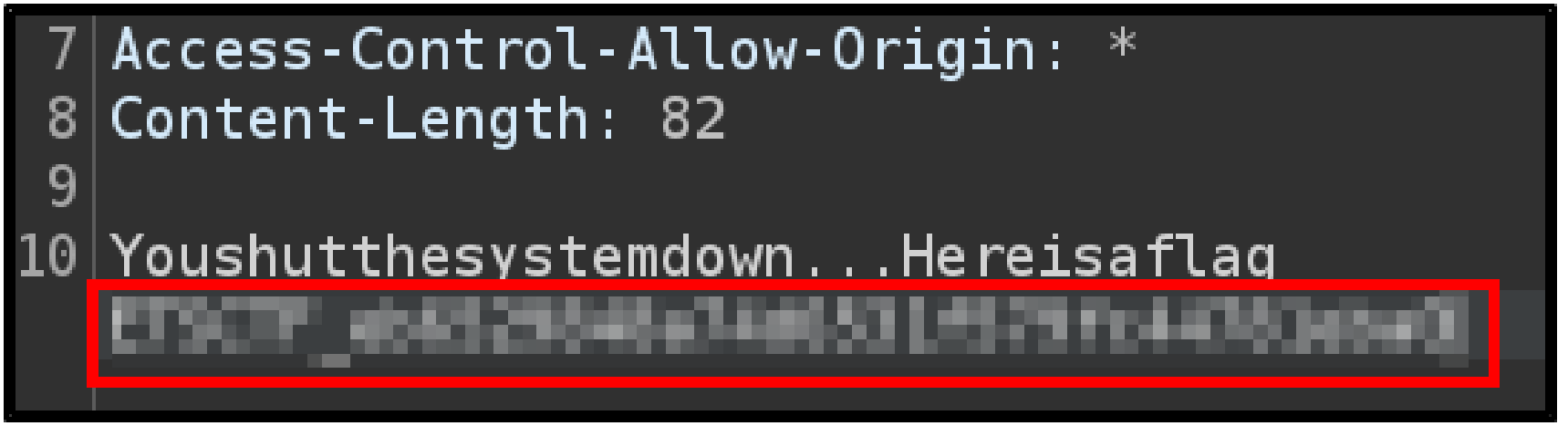
The most important part of this request is the URL parameter `endPoint`, which implies the parameter is used to load in other resources

Turbine – Resource Access via Parameter



We know we need to access the `shutdown.php` endpoint to finish the challenge, so we can try accessing it through the `refresh.php` page's `endPoint` parameter

Turbine – SSRF Confirmed



And we're able to use the Sever-Side Request Forgery to access the local-only endpoint `shutdown.php`