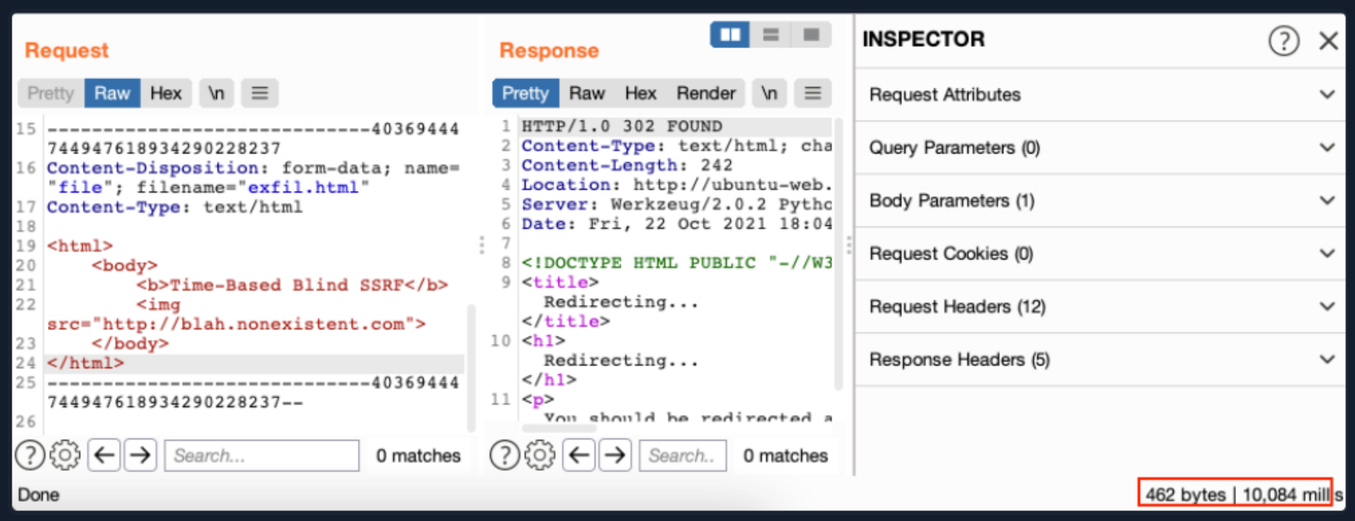
Time-Based SSRF

We can also determine the existence of an SSRF vulnerability by observing time differences in responses. This method is also helpful for discovering internal services.

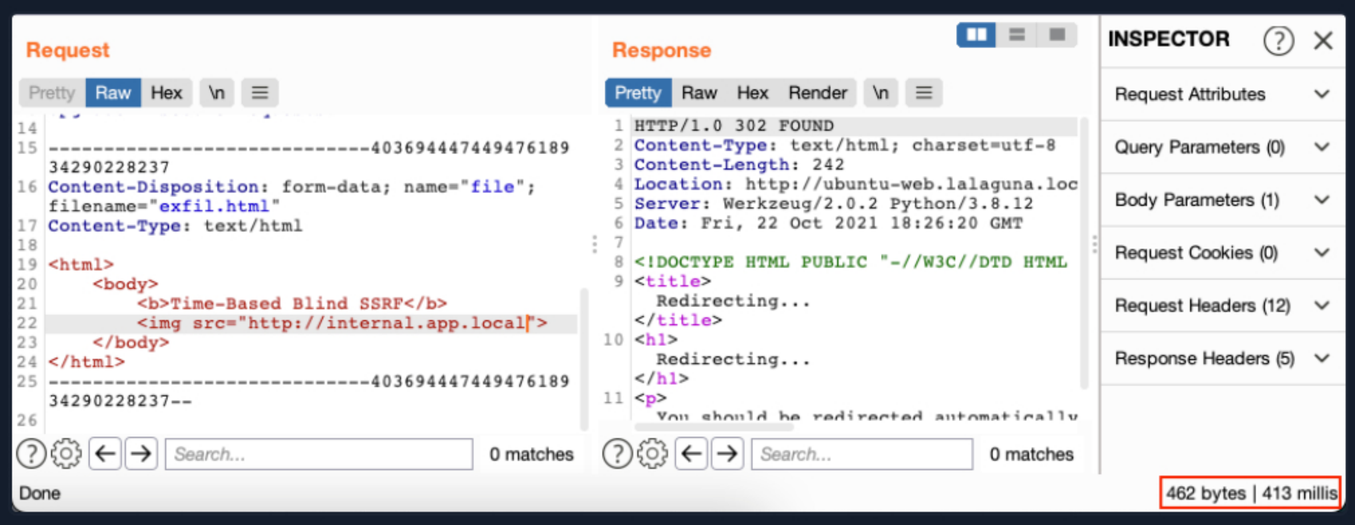
Let us submit the following document to the PDF application of the previous section and observe the response time.

Code: html

```
<html>
    <body>
        <b>Time-Based Blind SSRF</b>
        <img src="http://blah.nonexistent.com">
    </body>
</html>
```



We can see the service took 10 seconds to respond to the request. If we submit a valid URL inside the HTML document, it will take less time to respond. Remember that `internal.app.local` was a valid internal application (that we could access through SSRF in the previous section).



In some situations, the application may fail immediately instead of taking more time to respond. For this reason, we need to observe the time differences between requests carefully.

← Previous Next → Mark Complete & Next

Table of Contents

My Workstation

OFFLINE

Start Instance

∞ / 1 spawns left