

## 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>
    
  </body>
</html>
```

The screenshot shows a browser developer tools interface with three panels: Request, Response, and Inspector. The Request panel shows a POST request with a large body containing the provided HTML code. The Response panel shows a 302 FOUND status with a Location header pointing to a local file 'exfil.html'. The Inspector panel shows the response headers and body, which includes a redirect message.

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).

The screenshot shows a browser developer tools interface with three panels: Request, Response, and Inspector. The Request panel shows a POST request with a large body containing the provided HTML code with a different URL. The Response panel shows a 302 FOUND status with a Location header pointing to the new URL. The Inspector panel shows the response headers and body, which includes a redirect message.

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

Introduction to Server-Side Attacks	✓
Abusing Intermediary Applications	
AJP Proxy	✓
Nginx Reverse Proxy & AJP	✓
Apache Reverse Proxy & AJP	✓
Server-Side Request Forgery (SSRF)	
Server-Side Request Forgery (SSRF) Overview	✓
SSRF Exploitation Example	✓
Blind SSRF	✓
Blind SSRF Exploitation Example	✓
Time-Based SSRF	✓
Server-Side Includes (SSI) Injection	
Server-Side Includes Overview	✓
SSI Injection Exploitation Example	✓
Edge-Side Includes (ESI) Injection	
Edge-Side Includes (ESI)	✓
Server-Side Template Injections	
Introduction to Template Engines	✓
SSTI Identification	✓
SSTI Exploitation Example 1	✓
SSTI Exploitation Example 2	✓
SSTI Exploitation Example 3	✓
Extensible Stylesheet Language Transformations Server-Side Injections	
Attacking XSLT	✓
Skills Assessment	
Server-Side Attacks - Skills Assessment	✓

### My Workstation

OFFLINE

Start Instance

00 / 1 spawns left

