Visit <https://pipedream.com/sources/dc_8Pu4AW7>

we can create public “bins” that log all incoming request which we can use to see If a target is attempting to request the page.

This does work confirmed!! -> <img src=requestbinURL.com> will reach out and send a get request to our request bin. (if we have working xss) great way to spot blind vulns. Once found find this will show proof of concept but once discovered we should try to make some sort of exploit to show more. For example we can attempt to hook a browser with beef

To hook with beef all we need to do is open up 1 tunnel (ssh localhost.run thing) on port 3000, of course add it to the config.ymal thing and then start beef.

Copy the public link to the hook and add it as the src to a payload and win!!

* Note for hooking with beef it seems to only work as script src=hook.js
* For just doing a GET request to the request bin url it will work with any payload such as img or iframe

Also note we can easily view the logs of an apache server!

* Make sure to tunnel the port its running on using the ssh localhost.run functionality basically just how we did it for beef.
* Send this link into user input and see if it is requested!

We can see requests made to our server by navigating to localhost/server-status. This is probably the best way of doing it as we can see a lot more information as opposed to having to choose separate links for http requests dns lookups etc. Here we essentially have everything in 1 nice package!

Interactsh is also very good CLI available on linux (haven’t looked into it yet but seems awesome) and have a web based version <https://app.interactsh.com/#/> which is great and records all traffic.