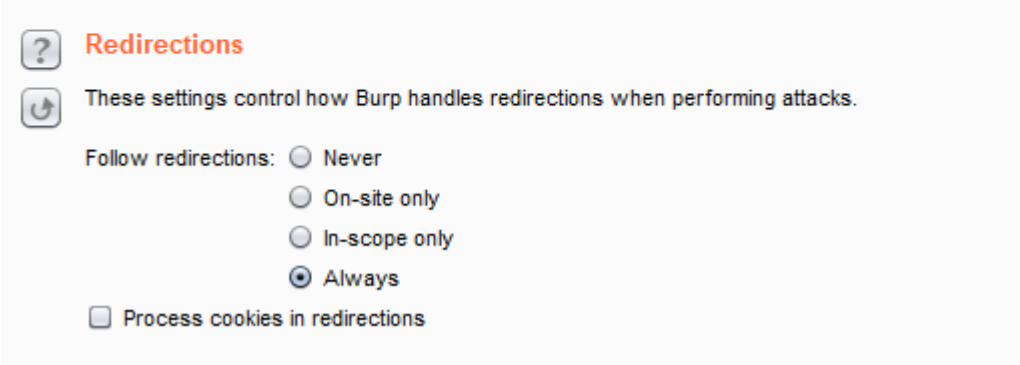
contains a list of endpoints the website owner does & does NOT want indexed by google so for example if the subdomain is using some type of third-party software then this may reveal information about what's on the subdomain. I personally find /robots.txt a great starting indicator to determine whether a subdomain is worth scanning for further directories/files. This is for me personally as I like to find subdomains which have functionality to play with, rather than relying on a wordlist to discover content.

You can use Burp Intruder to quickly scan for robots.txt by simply setting the position as:

```
GET /redirect.php?url=§https://www.target.com/§robots.txt HTTP/1.1
Host: www.zs.eano
Connection: close
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537
Accept: */*
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: tasty=yes
```



Run XAMPP locally, host a basic PHP script:
<?php header("Location: ".$_GET['url']; ?> and don't forget to set it to follow redirects in options, then load your domains to scan for. After running it will give you an indication as to which domains are alive and respond and potentially information about content on the subdomain. From here I will pick and choose domains that simply look interesting to me. Does it contain certain keywords such as "dev", "prod", "qa"? Is it a third-party controlled domain such as careers.target.com? **I am primarily looking for subdomains which contain areas for me to play with**. I