# Skills Assessment – Using Web Proxies – Report

## FLAG 1:

Capturing the request in ZAP HUD we just change the button's disabled attribute to enabled.

A screenshot of a computer

AI-generated content may be incorrect.

The first time I clicked it nothing happened so I tried changing the method to GET, still nothing, started spider and found no useful sites but still went through them, then I looked at the source code and still found nothing so I looked at the hint and it stated that it won't show on the first time (guess now I know why the button says „For a chance to get the flag“. I right click the post request and sent it to repeated and spammed it until I saw a response that had a bigger file size than others, it contained the flag: HTB{d154bl3d\_bu770n5\_w0n7\_570p\_m3}

A screenshot of a computer

AI-generated content may be incorrect.

## FLAG 2:

I need to decode the cookie until I get a 31 character string and that is my flag.

A screenshot of a computer

AI-generated content may be incorrect.

I don't think this has any elegant solution so I just fiddled around and did an ASCII Hex Decode into Base64 decode and found a 31 char string: 3dac93b8cd250aa8c1a36fffc79a17a, it was the flag.

## FLAG 3:

Since it is a 31 char string it is an MD5 hash for which I need to fuzz out the last character while encoding with whatever technique I used previously. Since ZAP doesn't have an in-built HEX encode function I will use Burp Suite. I captured a request to the /admin.php site, forwarded it to Intruder. Added a wordlist of all alphanum characters, added the 31-char md5 hash as the prefix, base64 encoded it and ascii hex encoded it after that.

A screenshot of a computer

AI-generated content may be incorrect.

I looked at the length of the responses and found the ones that differed, they contained the flag: HTB{burp\_1n7rud3r\_n1nj4!}.

## FLAG 4:

To find the flag I need to find a directory in a request sent by Metasploit coldfusion\_locale\_traversal. Very easy flag to find, just setup metasploit to use our proxy and there we can see the flag.

A screenshot of a computer

AI-generated content may be incorrect.

The CFIDE directory is our flag.