surprise, it worked. It can't get any simpler than that when testing if features are working as intended.

I have discovered over 1,000 vulnerabilities over the last few years and each one has been from simply testing how the site works. I have not used any special tricks or any private tools. **I simply used their site as intended**. When interacting what requests are sent, what parameters are used, how is it expected to work?

Useful Resources

Below are a list of resources I have bookmarked as well as a handful of talented researchers I believe you should check out on Twitter. They are all very creative and unique when it comes to hacking and their publicly disclosed findings can help spark new ideas for you (as well as help you keep up to date & learn about new bug types such as HTTP Smuggling). I recommend you check out my following list & simply follow all of them. https://twitter.com/zseano/following

https://www.yougetsignal.com/tools/web-sites-on-web-server/
Find other sites hosted on a web server by entering a domain or IP address

https://github.com/swisskyrepo/PayloadsAllTheThings
A list of useful payloads and bypass for Web Application Security and Pentest/CTF

https://certspotter.com/api/v0/certs?domain=domain.com
For finding subdomains & domains

http://www.degraeve.com/reference/urlencoding.php
Just a quick useful list of url encoded characters you may need when hacking.

https://apkscan.nviso.be/