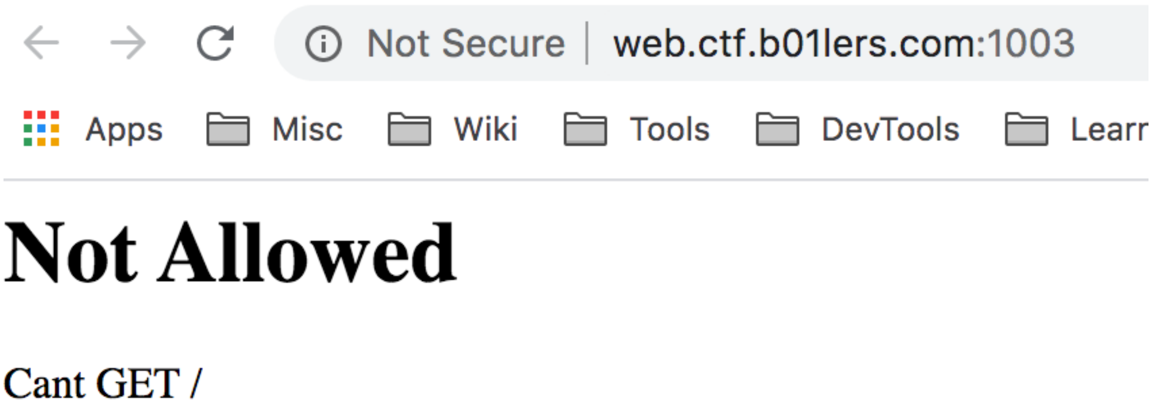
b01lers 2020 Space Noodles

Saturday, March 7, 2020 12:16 PM

Worked with Hugh on this:



Not Allowed

Cant GET /

So, try POST and get this:

```
 <html>
 </body>
     <body>
       <text><p></text>text ? pleas test teh follwing five roots<p>,</p>
 <list>
   <one>

circle</one>
   <enter>
   <enter>
   <sendkey(enter)>

two
 I'm am making an a pea eye and its grate

         PHP is the best
     <php?> printf(hello world) </php>
square<?/p>two


 :pleasequithelpwww.google.
com/seaerch

   how to exit
vim/quit
```

:wqwhy isnt it working:wq:wq:wq:qw?

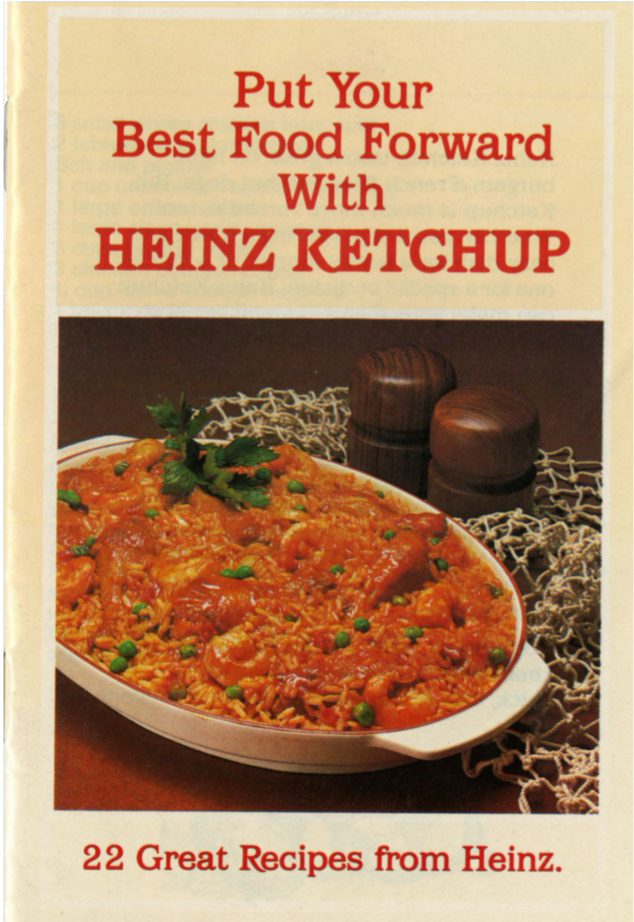
</body>

</html>

It is asking us to try five roots

circle
two
square
com/seaerch
vim/quit

Turns out each one wants a different HTTP verb.



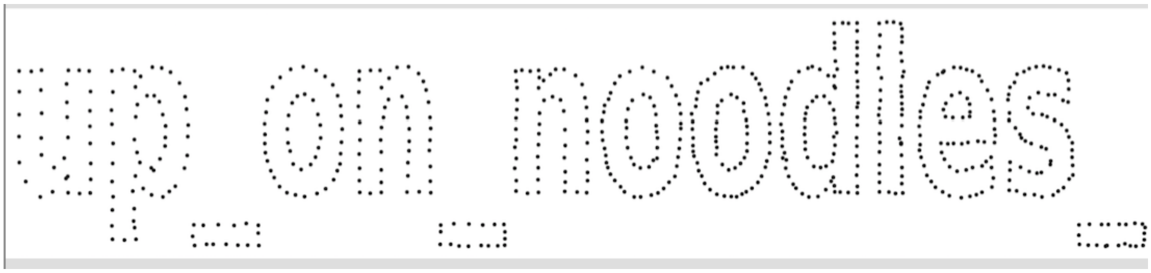
two ended up needing PUT two/

which returned:

Put the dots???

ZAP won't let me use the CONNECT verb for reasons I don't understand but this will:

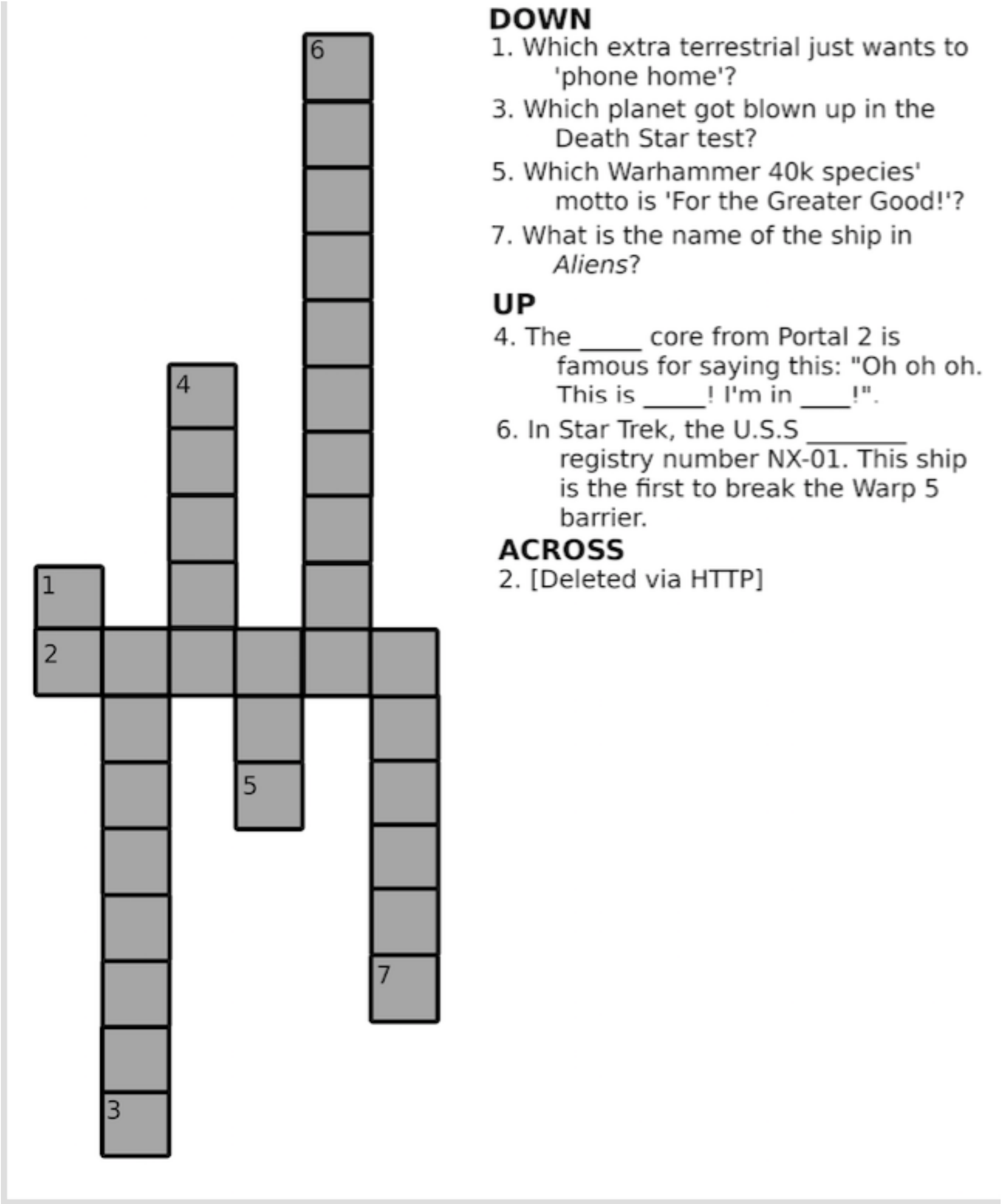
```
curl -X CONNECT http://web.ctf.b01lers.com:1003/two/ > junk.jpg
```



up_on_noodles_

square ended up needing DELETE:

```
curl -X DELETE http://web.ctf.b01lers.com:1003/square/ > junk.jpg
```



DOWN

1. Which extra terrestrial just wants to 'phone home'?
3. Which planet got blown up in the Death Star test?
5. Which Warhammer 40k species' motto is 'For the Greater Good!'?
7. What is the name of the ship in *Aliens*?

UP

4. The _____ core from Portal 2 is famous for saying this: "Oh oh oh. This is _____! I'm in ____!".
6. In Star Trek, the U.S.S ________ registry number NX-01. This ship is the first to break the Warp 5 barrier.

ACROSS

2. [Deleted via HTTP]

solution is

tastes

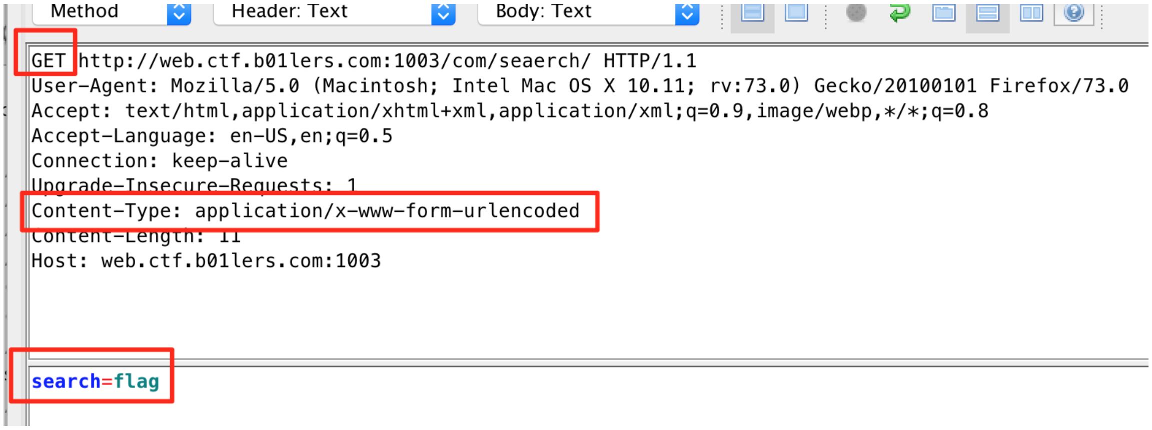
com/seaerch needed GET:

```
curl -X GET http://web.ctf.b01lers.com:1003/com/seaerch/
<htlm>

,,,,,,,,<search> <-- comment for search --!>:

  ERROR </> search=null</end>
```

This was the weirdest one. You then had to include a request body that simulated a form submission.



```
GET http://web.ctf.b01lers.com:1003/com/seaerch/ HTTP/1.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11; rv:73.0) Gecko/20100101 Firefox/73.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 11
Host: web.ctf.b01lers.com:1003


search=flag
```

At first I tried search=fun and it said:

fun is not a good search, please use this one instead: 'flag'

but flag returns:

<htlm>

,,,,,,,,,<search> <-- comment for search --!>:

  <query> good search</query>
  results: <p>**_good_in_s**</p>:w

</html>

vim/quit/ needed TRACE:

curl -X TRACE http://web.ctf.b01lers.com:1003/vim/quit/
   <hteeemel<body>>

                  <wrong>uh oh
                ?exit=null
          </wrong>

Since the original page had :wq I tried:

curl -X TRACE http://web.ctf.b01lers.com:1003/vim/quit/?exit=:wq
   <hteeemel<body>>

      <flag> well done wait </flag>

<text> this one/> <flag>**pace_too}**</flag>

Putting it all together required guessing whether heinz or ketchup or both were relevant.

Winning combination is:

pctf{ketchup_on_noodles_is_good_in_space_too}