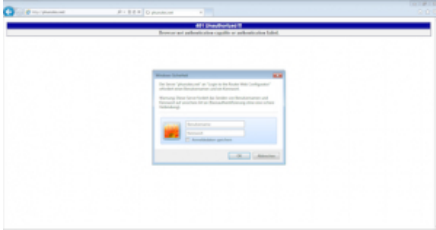


## DrayTek Vigor 2600v does some DNS spoofing

I always wondered about an obscure behaviour observed in my home network.

Whenever I access my website using it's plain domain name (<http://phunsites.net>), I'd end up with a password prompt from my DSL router.



Thinking about DNS it would be an easy assumption that there was likely to be a wrong resource record like this in my DNS zone:

```
@ IN A 192.0.2.1
```

But it turned there wasn't - why should it anyway?

Looking further into this, I did a DNS trace. It was striking that querying for **www.phunsites.net** would yield another result ...

```
$ dig A www.phunsites.net.
```

```
; DiG 9.6.0-APPLE-P2 A www.phunsites.net.  
;; global options: +cmd  
;; Got answer:  
;; ->>HEADERHEADERHEADERHEADER
```