

Forum:[Hack Forums](#)

Thread: [HTTP realm was not really that easy!](#)

pwntoken - February 28, 2014, 2:04 pm

Yes the HTTP realm might seem so easy at the first go, but however taking a look at the original RFC from 1999, I really could not pick up certain aspects to what this does. Like the HTTP-realm describes the string for the WWW-authenticate headers and does give the auth-scheme a name, but read closer at this.

Quote: The realm directive (case-insensitive) is required for all authentication schemes that issue a challenge. The realm value (case-sensitive), in combination with the canonical root URL (the absoluteURI for the server whose abs_path is empty; see section 5.1.2 of [2]) of the server being accessed, defines the protection space. These realms allow the protected resources on a server to be partitioned into a set of protection spaces, each with its own authentication scheme and/or authorization database. The realm value is a string, generally assigned by the origin server, which may have additional semantics specific to the authentication scheme. Note that there may be multiple challenges with the same auth-scheme but different realms.

First half.

Quote: The realm directive (case-insensitive) is required for all authentication schemes that issue a challenge. The realm value (case-sensitive), in combination with the canonical root URL (the absoluteURI for the server whose abs_path is empty;

realm directive could be case-insensitive, but realm value could not be? and the realm directive was supposed to be the realm header itself of the value which the web developer chooses to set?

Quote:in combination with the canonical root URL (the absoluteURI for the server whose abs_path is empty

I do not really understand what does it mean to say! what is more important about 'in combination'? what has to be combined here? Others I could get the notion of what realm does.

pwntoken - March 3, 2014, 4:16 pm

doesn't matter, got the answer... wrote papers on it too.. I wonder how hackers here go without getting to these basics and call themselves hackers. That lags the generation apart and creates a divide between the skids, anti-skids, pro and the REAL ones. Some are wannabe pro's, acting as if they know PHP and MySQL and could do SQLi at core, attains the 'hacker' position!

Eight - March 4, 2014, 10:00 am

Well you're right in saying it ain't easy.. The HTTP protocol has a lot of ramifications, I know this because I tried to write clients from scratch in the past (still do), even basic ones, but I always fail to make my code 100% compliant. This makes me appreciate tools like cURL and wget.

Kudos on managing to decipher the RFC. When you say you wrote a paper on it, was it like an academic research/school project thing ?

pwntoken - March 4, 2014, 1:37 pm

(Mar 4, 2014 11:00 AM)Eight Wrote: [\[CITE\]](#) Well you're right in saying it ain't easy.. The HTTP protocol has a lot of ramifications, I know this because I tried to write clients from scratch in the past (still do), even basic ones, but I always fail to make my code 100% compliant. This makes me appreciate tools like cURL and wget.

Kudos on managing to decipher the RFC. When you say you wrote a paper on it, was it like an academic research/school project thing ?

No, I wrote the paper from the scratch as per my personal research. I don't have to do when the university orders me! I am keeping this because I wanted to learn more.. that's all.

And currently it's not half the RFC's I had covered, because of too many ongoing changes, it keeps changing due to newer drafts. What I am keeping track of is the common ones which remains from protocol 0.9, 1.0, 1.1 to HTML5 which will be supporting 2.0

That been said, I have completely dedicated 1 month study of protocols itself. The web application level protocols is the first target I am finishing.