

OT: question about HTTP headers

Source: <http://linux.derkeiler.com/Mailing-Lists/Debian/2003-08/2565.html>

From: Roberto Sanchez (*rcsanchez97_at_yahoo.es*)

Date: 08/14/03

Date: Thu, 14 Aug 2003 04:12:44 +0200 (CEST)
To: debian-user <debian-user@lists.debian.org>

Warning: this will probably be a long message by the time I am done typing it.

Greetings list.

Several months ago I posted here about a problem with a website that wouldn't let me in because I (thought at the time) I was running Mozilla. I tried the standard angle of attack by changing my user agent string. That did not work. I also tried installing the Win32 Mozilla in WINE, but that didn't work either (install wouldn't finish). I managed to figure out that Firebird would work in WINE and the site would actually believe that it was a Win32-base browser. However, the most recent (in unstable) WINE packages are b0rked and Firebird doesn't seem to want to run anymore.

I had contacted a supervisor in the tech support department who seemed very sympathetic to my situation. But after the first email I sent her describing the problem and the error I was getting, I have heard nothing back and I have been unable to get in touch with her again.

I decided I would roll up my sleeves and get this problem figured out.

I booted my desktop machine over to WinXP (yuck!) and installed Firebird and LiveHTTPHeaders. I also installed mozilla-livehttpheaders (via apt) on my laptop (running unstable).

After examining the headers, it seems that the site uses some esoteric method of identifying my browser/OS and then hides it in some POST data.

Here is the header request/response from Firebird 0.6 in WindowsXP (where I am able to log in to the site):

<https://mypay.dfas.mil/mypay.asp>

```
POST /mypay.asp HTTP/1.1
Host: mypay.dfas.mil
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.4b)
Gecko/20030516 MozillaFirebird/0.6
Accept:
```

Debian-User: OT: question about HTTP headers

text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,video/x-mng,image/png,image/jpeg,
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate,compress;q=0.9
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: <https://mypay.dfas.mil/>
Content-Type: application/x-www-form-urlencoded
Content-Length: 44
|-HiddenVal=Netscape5.0+%28Windows%3B+en-US%29

HTTP/1.x 200 OK
Server: Microsoft-IIS/5.0
Date: Thu, 14 Aug 2003 01:13:01 GMT
Connection: close
Content-Length: 92319
Content-Type: text/html
Set-Cookie: ASPSESSIONIDQQBQDDDC=PJMACPLDBECNEBCAJMLGOILG; path=
Cache-Control: private

Here is the header request/response from Mozilla 1.3 in Sid (where I can't log in to the site):

<https://mypay.dfas.mil/mypay.asp>

POST /mypay.asp HTTP/1.1
Host: mypay.dfas.mil
User-Agent: Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.3) Gecko/20030430
Debian/1.3-5
Accept:
text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,video/x-mng,image/png,image/jpeg,
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: <https://mypay.dfas.mil/index.htm>
Cookie: ASPSESSIONIDCQBTDCDC=HEFFLNNANGKAACEBKJOCPNLP;
ASPSESSIONIDCSCSACAD=GKOMLMLDGNJLLGPIEDOMINMO
Content-Type: application/x-www-form-urlencoded
Content-Length: 40
|-HiddenVal=Netscape5.0+%28X11%3B+en-US%29

HTTP/1.x 200 OK
Server: Microsoft-IIS/5.0
Date: Thu, 14 Aug 2003 01:22:01 GMT
Connection: close
Content-Length: 92298
Content-Type: text/html
Set-Cookie: ASPSESSIONIDAATRCCAB=BIBNHPLDMDIOLLOOLIDGLIIMP; path=
Cache-Control: private

OT: question about HTTP headers

Debian-User: OT: question about HTTP headers

The problem is in the HiddenVal in the form data. The error message I get when I try to log in is this:

Your browser has been identified as indicated below:

Netscape 5.0 (X11; en-US)

I used wget to download the two .asp scripts that run when you first bring up the page, but I could not find in the browser identification code where this particular information was pulled from.

I am determined to get around this, but I can't figure out how. Is there a way to spoof ASP or IIS into believing that I am running on windows? I checked about:config in Mozilla and was unable to find anything that specifically identified the host OS. That makes me think that there is some specific ASP or IIS functionality that they are using to make the determination.

I searched Google for many hours but could not find anything on the facilities available in ASP and IIS to do browser identification that indicated how it might also be possible to identify the host OS.

I know this is way OT for the list, but there are lots of folks here with expertise. I am hoping someone either knows how to get past this or can at least point me in the right direction.

-Roberto

Yahoo! Messenger – Nueva versión GRATIS
Super Webcam, voz, caritas animadas, y más...
<http://messenger.yahoo.es>

--

To UNSUBSCRIBE, email to debian-user-request@lists.debian.org
with a subject of "unsubscribe". Trouble? Contact listmaster@lists.debian.org