

## Re: cs-host, host header and destination

**Source:**

<http://www.tech-archive.net/Archive/Internet-Server/microsoft.public.inetserver.iis/2004-03/0825.html>

---

**From:** Paul (*nobody\_at\_devnull.spamcop.net*)

**Date:** 03/06/04

Date: Sat, 6 Mar 2004 15:32:16 -0500

Hi Kristofer,

This reflects what I am seeing in the logs, thanks for showing me how it could be done. I can understand why someone would want to cloak their sending information, I just can't imagine why anyone would want to cloak the destination. The resources they where after where questionable, so it raised my concerns as to what was happening. Just so I can try to understand how it actually does get routed, could you provide me with some keywords, like what the area and/or field is called so I can do a search and find out how it does work. You can explain it here if you would like, I seem to be able to understand the way you explain things.

Thanks,

Paul Coleman

"Kristofer Gafvert" <kgafvert@NEWSilopia.com> wrote in message news:O1dEShuAEHA.576@TK2MSFTNGP11.phx.gbl...

> *Okay, let me explain this a bit, and this might be why you see this.*

>

> *The CS-Host field is sent by the client. It is possible for the client to fake this (for privacy for example, not that this is dangerous to give out...). If the server is configured with host headers only, i dont think that this is possible (but not completely sure).*

>

> *So, let's try this with telnet. server.com is any way to make a connection to the server (domain name, or IP)*

>

> *telnet server.com 80 <enter>*

> *GET /default.html HTTP/1.1 <enter>*

> *Host: fakeHost.com <enter>*

> *<enter><enter>*

>

> *Now, if you look in the log file (wait until this is logged), you will see someone "accessing the site" using fakeHost.com. This is not really true, the client just sended the Host fakeHost.com*

>

> *Everything in the logfile starting with CS is something sent from the client, to the server. This information can be faked, and the referer is the*

microsoft.public.inetserver.iis: Re: cs-host, host header and destination

> *most common faked header. If you see these strange Host together with a  
> strange referer, then it is almost for sure that an add-in for the client  
> did this.*  
>  
> *If the client did not send a Host, nothing is logged (except for the dash  
> (-)) in the logfile.*  
>  
> *Does this explain what you are seeing? It sounds that this doesn't happen  
> too often, so i do not think that something is wrong with IIS.*  
>  
> *So, to sum up:*  
>  
> *CS-Host does not necessary have to have something to do with the actual  
> host. It is just the Host field sent by the client, to the server (and  
there  
> were already a connection to the server when this information was sent).*  
>  
>  
> --  
> *Regards,*  
> *Kristofer Gafvert – IIS MVP*  
> *Reply to newsgroup only. Remove NEWS if you must reply by email, but  
please  
> do not.*  
> *www.ilopia.com – FAQ and Tutorials for Windows Server 2003*  
>  
>  
> *"Paul" <nobody@devnull.spamcop.net> wrote in message  
> news:nfGdnSA6Udmo\_trdRVn-vw@adelphia.com...*  
> > *Hi,*  
> > *I have always thought that the destination for a request was determined  
by  
> > the contents of the host header and thus the cs-host field in the logs.*  
I  
> > *expected to see either my websites IP address or a domain name that  
> resolved*  
> > *to my IP address. I have been seeing both domain names that do not  
> resolve*  
> > *to my IP address as well as NULL values in this field a small percentage  
> of*  
> > *the time. If this means that this field does not determine the  
> destination,*  
> > *how is a request routed to my website? What is this called so I can do  
a  
> > search and find out more about how requests get routed to my website?  
> > I do not own the web server, I use a web presents provider. They either  
> do*  
> > *not understand the question, don't know the answer or are deliberately  
not  
> > telling me for some reason.*  
> > *If I am using the wrong terminology or if there is a better terminology*

Re: cs-host, host header and destination

I

> > *should be using, I would be grateful if you would provide that as well.*

> > *Thanks,*

> > *Paul Coleman*

> >

> >

>

>