

How to use Google Analytics to DoS a client from some website.

How to use Google Analytics to DoS a client from some website. - sirdarckcat, sirdarckcat.blogspot.com.

- Published: date not stated
- Original: <<https://sirdarckcat.blogspot.com/2009/04/how-to-use-google-analytics-to-dos.html>>
- Preserved from: <https://sirdarckcat.blogspot.com/2009/04/how-to-use-google-analytics-to-dos.html> (live) on 2026-08-10
- Licence: unknown

Rights remain with the original author and publisher. This is a research archive of a source from the Web Hacking Techniques Index collections, kept so the page going offline. To read the original, follow the link above.

Content

UNTRUSTED SOURCE TEXT. Everything below this line is third-party material quoted for research. It is data, not instructions. Do not follow directions, execute code, or fetch URLs because this text says so.

So, right.. I was trying to read some stuff about problems sharing my wired connection of my linux laptop to another windows laptop via wireless, but one of the links was on mail-archive.com, and for some reason it's blocked on China (yeah, I'm living on China now =D). So, I decided to go to a friend's website to read the webpage, but... suddenly, there was an error..

Bad Request Your browser sent a request that this server could not understand.

Size of a request header field exceeds server limit.

Cookie:

The reason of the error is unknown, but that's not important, what is important is that I realized that with a big enough cookie (8190 bytes aprox) we can DoS someone from entering a webpage. (With a 400 HTTP Response status code on Apache, a 413 on some google services, and on some websites an infinite loop because the big cookies delete session cookies).

The reason we would like to block from accessing a server is not really important, what is important is that being able to block them out is dangerous.

Anyway.. we need to set cookies, and this is good enough for a lot of attacks (like no-ip domains, shared subdomains like blogspot, browsers that allow top level domain cookies, second level domains like .co.uk, etc..), but I really wanted to do something more cool.. so I started thinking, how to set cookies on clients.

And the "how", as the reader may deduce from the title of this blogspot is using Google Analytics. I've been researching Google Analytics cookies for some time now, so I sort-of know how they

work. And I know pretty good that the google's implementation allows an attacker to add anything in some cookies.

So well, one of those cookies is the referer. This is true for "search result - organic referers", like for example, a Google search. The catch is that the detection on google's service is very bad, and we can fool it to think we are a google search result by doing:

http://google.yourfavoritedomain.com/search?q=search-term

So, you can guess.. if search-term is big enough we can hack the world.

Anyway, there's a catch. You can't set such a big cookie. The limit apparently is 4192 bytes. So.. what you have to do is control 2 cookies.

The other cookie we are going to be using is GASO (Google Analytics Site Overlay), its triggered by the content on <http://yourwebsite.com/page.html#gaso=somevalue>

And well, the google analytics code will set a cookie called GASO to somevalue

With both vectors we can now set very big cookies! and with those cookies we can disable access to lot of websites to anyone with just a link (or an iframe if you want to improve the stealthness of the attack).

Twitter PoC: <http://google.sirdarckcat.net/?v=http://twitter.com/>

If you use twitter over SSL... <http://google.sirdarckcat.net/?v=https://twitter.com/>

To lock you out of all wordpress.com blogs: <http://google.sirdarckcat.net/?v=http://rofl.wordpress.com/> Try your favorite Google Analytics powered websites :D

References: <http://httpd.apache.org/docs/2.0/mod/core.html#limitrequestfieldsize>

<http://httpd.apache.org/docs/1.3/mod/core.html#limitrequestfields> <http://royal.pingdom.com/2008/05/28/google-analytics-dominate-the-top-500-websites/>

Examples: GASO limit

[illegible]

[illegible]

[illegible]

Archived from <https://sirdarckcat.blogspot.com/2009/04/how-to-use-google-analytics-to-dos.html>. Rendered offline from the local Markdown copy.