

The Great “Wall of Dubai”  
Access to Flickr Hacked!!! 😊

By Simran Gambhir

tried to get to my [flickr](#) photos today, but am getting the following message:



Dubai blocks flickr!!!! Dubai blocks flickr!!!! I was astounded... i have used that site for naught but looking at some excellent photography people do... photography is an artform of beauty, a science of the heart, an untainted joy... what could possibly be wrong with flickr! Upon further investigation, i found that flickr also has some content that would be considered "objectionable", yet, i was astounded that a blanket block would be put in place!

It got me thinking on how lucky i am in the countries i reside in... there is freedom of speech, and i gotta say, i took some of it for granted, as, although i had heard of "the great firewall of china" et al, i had not myself experienced a block to the freedom to access information. Today i have!

The mentality of some "rulers" is to block exterior information that they believe might "corrupt" - but its their own hearts that are unpure. An argument of, "we are protecting you, just as a parent would protect a child" are also unsustainable! A good parent protects a child from immediate harm, but educates them so that they learn to make their own decisions in time to come, and protect themselves!

This thuggery, especially in the name of god, seems to be a common trait, particularly amongst the middle east and the within the 4 walls of the "born agains" all over the world.

I look at how to bypass this filter, and came across a solution touted by many: the "[access flickr](#)" plugin. I had a look at the code of it and tried it... it didn't work... the code showed that the names are being translated to IP's (which i presume the proxy never used to filter by; it must have been filtering by the domain name, and other stuff) and it used to fix some of the cookies then to belong to the "right domains".

I can install my own ssh tunnel one of my servers and browse anywhere i like, but i thought i would give simple things a go first... surprisingly <http://flickr.com/search/> works! but of course, you can't actually click thru to any image as that is outside the /search/ relative path.

Upon further investigation, i found that simple tricks like:

```
% telnet flickr.com 80
GET /search/./photos/c0t0c0s0/ HTTP/1.0
Host: flickr.com
```

Also did not work!

Researching further... i deduced that the proxy is allowing /search through on flickr.com, but me doing a ./ is caught by the proxy and so /search/./photos/c0t0s0d0/ is translated to /photos/c0t0s0d0 and then blocked!

I gave accessing by IP another go... and this time it worked!!!! walla!!!! My ears stood up, there are possible race conditions that can be exploited there somewhere (as an IP block is wokring \*most of the time\* but \*not all of the time\*. However, before i went down that path, i thought of simply malforming the URL and seeing what happened.

The result of:

```
% telnet flickr.com 80
GET /photos/c0t0s0d0/
```

revealed pleasing results... i got my page!!!!!! Omitting the protocol/verison as part of the GET line worked. I suspect POST would be similar!

Looking into it further, i put back the HTTP/1.0 info, but omitted the Host header... and guess what... "bob's your uncle"!!!

So, initial results... it appears that flickr at least is being filtered based on the Host header... which every current browser version under the sun will send these days! It would be simple enough to write a local proxy in perl (about a 10 line script using the modules on cpan, so even script kiddies could do it!) to omit the header the use flickr to your hearts content.

No doubt the "great "firewall of dubai" shall detect this technique and enhance the way content is filtered in time to come.. until then... enjoy!!! :) and post that... remember: a race without a finish line, is never won, but enjoyed for eternity :)

Content of <http://www.etisalat.ae/assets/document/blockcontent.pdf> below ("research" showed that they are filtering based on many different criteria, such as keywords in the domain name, etc as well... so the above technique will not work for every site... but it does work for flickr, and i dare say, there are many sites that have classified in the same category, and those sites will be possible to get to via omitting the Host header... bypassing the domain name keyword filter is left as an excercise to the reader for the moment... suffice to say, start with trying to substitute ascii for unicode, etc :) or if you are lazy, just use an open proxy or a already existing unblocked ssh tunnel! :) ... if you can get your traffic "out" of the UAE to any server encrypted, there's nothing they can do! :)

<http://www.etisalat.ae/assets/document/blockcontent.pdf>

## *Prohibited Content Categories*

### *1. Internet Content for Bypassing Blocked Content*

*This category includes Internet Content that allows or assist Users to access Blocked Content.*

### *2. Internet Content for Learning Criminal Skills*

*This category includes Internet Content that either provides instructions for or identifies methods to promote, encourage or provide the skills to commit illegal or criminal or unethical activities. These include bomb-making, phreaking (breaching phone security or phone service theft), scams and fraud, terrorism, evading law enforcement, stalking, lock picking, selling pirate material such as commercial software, music, videos or others.*

### *3. Dating Internet Content*

*This category includes Internet Content that provides online dating or matchmaking which contradicts with the ethics and morals of the UAE.*

*Exemptions: Chatting services, chatting groups, social networking and forums.*

### *4. Internet Content for Illegal Drugs*

*This category includes Internet Content that provides information on purchasing, manufacturing, promoting and using illegal drugs.*

### *5. Internet Content containing Pornography and Nudity*

*This category includes Internet Content that contains material of a pornographic nature, or relates or depicts acts of homosexuality, nudity and sexual material (including stories, jokes, animations, and video) or Internet Content that promotes sexual activity. It includes Internet Content which promote the distribution of above material (such as Peer-to-Peer websites and links).*

### *6. Gambling Internet Content*

*This category includes Internet Content that is relevant to gambling or such as gambling links, tips, sports picks, lottery results, as well as horse, car or boat racing.*

### *7. Internet Content for Hacking and Malicious Codes*

*This category includes Internet Content that distribute information and*

*tools for hacking (root kits, kiddie scripts, etc.) that help individuals gain unauthorized access to computer systems. Also include Internet Content*

*Page 1 of 2*

*Page 2 of 2*

*that distributes tools or information for producing and distributing malicious codes such as viruses, worms or Trojan horses.*

*Exemptions: Information security including ethical hacking.*

*8. Internet Content that are offensive to Religions*

*This category includes Internet Content that contains material which expresses hate to religions.*

*9. Phishing Internet Content*

*This category includes Internet Content where entities or persons falsely represent themselves as a “legitimate” businesses or enterprises for the purpose of deceiving and obtaining form Users, valuable information such as bank account or email account information including details such as usernames, passwords, credit card details or bank account details.*

*10. Internet Content that downloads Spyware*

*This category includes Internet Content that downloads Spyware which gathers private information of the users without his or her knowledge.*

*11. Internet Content providing Unlicensed Voice over Internet Protocol (VoIP) service*

*This category includes Internet Content that allows access to services which are prohibited in accordance with the TRA’s Voice over Internet Protocol Policy.*

*12. Terrorism Internet Content*

*This category includes Internet Content of terrorism groups and related Internet Content that support terrorism and publish and distribute materials for terrorism or include material for training and encouraging terrorism or help to serve terrorism groups such as funding, facilitating communication and other direct and indirect services.*

*13. Prohibited Top Level Domain (TLD)*

*This category includes Internet Content under a Top Level Domain names which offends against, is objectionable to, or is contrary to the public interest, public morality, public order, public and national security, Islam morality or is otherwise prohibited by any applicable UAE law, regulation, procedure, order or requirement.*