

RE: Website search engine is a hacking tool..

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2004-07/0092.html>

From: Amal Mohammad Al Hajeri (amal_at_nis.etisalat.ae)

Date: 07/24/04

To: charles.gillman@ethertech.com.au
Date: Sat, 24 Jul 2004 08:46:48 +0400

Hello List,

Thank you all for the valuable inputs. Am aware of the subject of using Google as a hacking tool, However, how is it different than using a local website search engine? will it give the same results? is it possible that a local engine may give extra juicy stuff? and how can we mitigate the risk of using such techniques? did anyone succeed in using the local search engine as a proxy to attack other targets?

Have a good day :)

On Sat, 2004-07-24 at 07:16, Charles Gillman wrote:

> *The folks at Foundstone have already created a tool to do exactly as Amal*
> *suggests using the Google API's. It's called SiteDigger*
> <http://www.foundstone.com/index.htm?subnav=resources/navigation.htm&subconten.html>
> *nt=/resources/information_gathering_tools.htm*

>
> *I have found it to be a bit buggy, returning results to an unrelated site*
> *occasionally but that could also be the Google API's.*

>
> CG

>> -----Original Message-----
>> *From: Drew Copley [mailto:dcopley@eEye.com]*
>> *Sent: Friday, 23 July 2004 8:01 AM*
>> *To: Gerry Eisenhour; Amal Mohammad Al Hajeri*
>> *Cc: pen-test@securityfocus.com*
>> *Subject: RE: Website search engine is a hacking tool..*

>>> -----Original Message-----
>>> *From: Gerry Eisenhour [mailto:GEisenhour@cisco.com]*
>>> *Sent: Wednesday, July 21, 2004 12:54 PM*
>>> *To: Amal Mohammad Al Hajeri*
>>> *Cc: pen-test@securityfocus.com*

RE: Website search engine is a hacking tool..

SecurityFocus Penetration: RE: Website search engine is a hacking tool..

> > > *Subject: Re: Website search engine is a hacking tool..*
> > >
> > > *There have been many articles written about using google as a hacking
> > > tool. All you really though need is an imagination.*
> > >
> > > *Here are some google modifiers that you might not know of:*
> > > <http://www.google.com/help/operators.html>
> > >
> > > *and here are some ideas to get you started:*
> > > <http://johnny.ihackstuff.com/index.php?module=prodreviews>
> > >
> > > *You would be amazed at whats out there, I've found everything
> > > from VNC
> > > passwords for entire domains, WEP keys, to pictures of peoples family.*
> > >
> > > *Not sure how "pictures of people's family" is relevant.*
> > >
> > > *I have had to track back some people sometimes through the years, and
> > > at least once found "pictures of their family".*
> > >
> > > *The most successful examples have been for tracking back entirely
> > > "anonymous" people through their fingerprint of writing to their
> > > real identities. Identity in the plural, because often the only
> > > identity online is multiple psuedo-anonymous ones that give real
> > > details in various forums.*
> > >
> > > *In one example we thought a troll was a pedophile because he was
> > > found trying to pick up fifteen year old girls. Turns out, surprise
> > > surprise, he was fifteen. His terrified mom told us when we called
> > > her up.*
> > >
> > > *In another case, a neo-nazi troll was caught because of his unusual
> > > fascination with a certain vulgar phrase he had the unfortunate luck
> > > to coin.*
> > >
> > > *This trace back gave his home address and the highly vulnerable
> > > information that he actually kept gold bars under his baseboards.*
> > >
> > > *Being confronted with this information he promptly repented and never
> > > returned.*
> > >
> > > *Their "fingerprint" is derived by breaking up their sentences and
> > > finding specific phrases and misspellings. Then, these are put into
> > > search engines and return counts and possible identities are put
> > > against these. If lucky, one can whittle down the suspect list
> > > to some positive proof. I am not aware of this method being used
> > > or documented anywhere, though it works on basic forensic science
> > > principles used in physical criminology and utilizes well known
> > > linguistic forensics...*
> > >
> > > *So that is a more unusual example of "google hacking" [sic]..*

RE: Website search engine is a hacking tool..

SecurityFocus Penetration: RE: Website search engine is a hacking tool..

>>
>> *While the methods I specified are useful for tracking back
>> scum bags they also could be used to find hackable targets in
>> a weak link target scenario.*
>>
>> *There are few corporate or governmental targets better then
>> an "executive" at home on his take home laptop. Search engines
>> are instrumental in finding that kind of identity. FYI.*
>>
>>
>>>
>>> --gerry
>>>
>>>
>>> *Amal Mohammad Al Hajeri wrote:*
>>>> *Hi List,*
>>>>
>>>> *Did you ever thought of the website search engine as a hacking tool?*
>>>> *During one of the pen-tests, The website search engine, was
>>>> a valuable
>>>> tool to discover interesting directories within the website itself,
>>>> these directories were not detected by famous website scanners like
>>>> nikto or SPI dynamics,i managed to get documentation pages
>>>> about the API
>>>> application implemented, management login pages, backup
>>>> files and much
>>>> more.*
>>>> *I leave it to your imagination to search for words like:*
>>>> *password,login,oracle,database,administrator, backup...etc*
>>>>
>>>> *Best Regards,*
>>>>
>>>>
>>>> -----
>>>> *Amal M. Al-Hajeri*
>>>> *E/Network & Information Security*
>>>> *Etisalat*
>>>>
>>>>
>>>>
>>>>
>>>>
>>>>
>>>>
>>>>
>>>> --
>>> *Gerald Eisenhour*
>>> *Cisco Systems, Inc.*
>>> *1414 Massachusetts Ave.*
>>> *Boxborough, MASSACHUSETTS 01719*
>>> *tel: 978.936.0465*
>>> *geisenhour@cisco.com*
>>>

SecurityFocus Penetration: RE: Website search engine is a hacking tool..

>>
>>
>>

--

Amal M. Al-Hajeri
E/Network & Information Security
HO-B 12th Floor
Etisalat
P.O.Box:3838
Tel(office):00971206182584
Tel(cel):00971506677061