

Forum:[Hack Forums](#)

Thread: [\[IT - EON Engine\] Can: Auto SQL Inject | Find Admin Pages | Find Dorks | And MORE!](#)

Qub1 - October 19, 2011, 1:46 pm

[Click here to download the latest version](#)

VIRUS SCANS AT THE BOTTOM

Welcome, to the IT - EON Engine, the program that can do everything you hate to do yourself.

[\[img\]http://farm7.static.flickr.com/6100/6261813634_84eb8413aa.jpg\[/img\]](http://farm7.static.flickr.com/6100/6261813634_84eb8413aa.jpg)

I know, no begging for donations, but if you could spare something it'd be nice, use the button in the program =D.

The IT - EON Engine has these tools:

- SQL Injector:

- + - Automatically check sites for SQL Injection Vulnerability
- + - Automatically get all tables of a site
- + - Automatically get all columns of a table
- + - Automatically get all contents of a table
- + - Automatically get the database information (Name, Version, Tables, Vulnerable Table)
- + - Execute commands on page
- + - Brute Force table names when the program can't find any
- + - Manually add table names for testing (using tablelists)
- + - Use default tablelist contained within the program

- Admin Login Finder:

- + - Use pagelists (containing pages like "login/admin/index.php")
- + - Check at insanely high speed
- + - Use default pagelist contained within the program

- Mass Dork Scanner:

- + - Use enginelists containing links to search engines (can specify as many as you want, more info below)
- + - Use dorklists (containing dorks)
- + - Check at high speed
- + - Use default enginelist contained within the program
- + - Use default dorklists contained within the program

- Account Password Changer:

- + - Change passwords of other users on the same computer

- Time CP:

- + - View very detailed information about the current time

Description

A very handy program to exploit vulnerabilities.

Tested successfully with this page: www.leadacidbatteryinfo.org/newsdetail.php?id=1 Actually

thats the only page it was tested with, because of a lack of sites.

FAQ

Q: Opening a table doesn't return any results

A: Either the table is empty, the program has encountered an error or it just doesn't give a result (the site).

Q: Why is the proxy box grayed out?

A: I haven't had time to implement it yet, sorry

Q: The program crashed, what should I do?

A: Please post the crash report and error here so I can fix it.

To create a tablelist

To create a tablelist, just create a text file and enter a new possible table name on each line

To create a dorklist

To create a dorklist, just enter a new dork on each line in a text file. "inurl:" can be used, but might not work on all search engines.

To create an enginelist

This is a bit more tricky, to create an enginelist, just go to the engine you want to add and perform a search, lets say "testing 123". Each search engine has another page increase mechanism, like with google the link to the first page is:

<http://www.google.nl/search?q=testing+123&start=0>

The 0 is the important part. This is what we'll be using as the start pid later. This means the number of the page that is the first.

Now the second page is:

<http://www.google.nl/search?q=testing+123&start=10>

Here the number became 10. That means the page increase number is 10.

Now we will enter this on a new line in our enginelist:

<http://google.com/search?q=%query%&start=%pid%|0|10>

Note that the 0 is the number of the starting page, and the 10 is the increasement number.

%query% stands for the search string (in this case "testing 123") and %pid% is where the page number will be entered.

Repeat this process for each engine you would like to add to the list, and you're done.

To create a pagelist

To create a pagelist just enter a new possible pagename on each new line in a text file (like "login/admin/index.php").

Credits:

Of course I will give credit to the people of whom I have used dorklists or any other type of information here:

- Kobez (Dorklist, Tutorials)
- SideSwipe (Dorklist)
- .Newsletter (Dorklist)

I hope I've covered everything!

Now finally here is the link to the program:

[IT - EON Engine v0.0.1.2 \(includes auto-updater\)](#)

[IT - EON Engine v0.0.1.1](#)

IT - EON Engine v0.0.1.0

Does require the .NET framework 2.0

PLEASE NOTE THAT THIS PROGRAM IS STILL IN THE ALPHA STAGE, SO PLEASE REPORT ANY BUGS WHEN YOU ENCOUNTER THEM IN THIS THREAD. THANK YOU.

VirusTotal scan:

RAR:

Link:

<http://www.virustotal.com/file-scan/report.html?id=f69e7ce939f534ab06645b605c70cc8545b6ce1aba28bfb97948a8c717aeb35a-1319058082>

Screenshot:

[\[img\]http://farm7.static.flickr.com/6036/6261944224_39aba92c35.jpg\[/img\]](http://farm7.static.flickr.com/6036/6261944224_39aba92c35.jpg)

The EXE:

Link:

<http://www.virustotal.com/file-scan/report.html?id=4d9b39ab0072bba82b9e0a6b3e1936e3ac94970ced731772d7699a210bf58d40-1319058501>

Screenshot:

[\[img\]http://farm7.static.flickr.com/6053/6261427873_d7f95d6afe.jpg\[/img\]](http://farm7.static.flickr.com/6053/6261427873_d7f95d6afe.jpg)

HidingInSpace - October 19, 2011, 1:48 pm

should post a vt scan? 4 posts id be a little iffy bout this

Qub1 - October 19, 2011, 1:49 pm

Yeah sure, I'll add one now from virustotal

Power_V - October 19, 2011, 1:54 pm

Yay! Another skid tool..just what we needed. Oh, and i'm pretty sure the file is infected _

Qub1 - October 19, 2011, 1:58 pm

I just added a scan from virustotal, the file is not infected.

And drop the sarcasm, this program does what most other programs can't, it automises SQL Injection.

After a month of studying tutorials here I have finally been able to create this, with weeks of hard work, so acting like that isn't exactly going to motivate me to improve it :S.

Power_V - October 19, 2011, 2:03 pm

(Oct 19, 2011 01:58 PM)Qub1 Wrote: [\[CITE\]](#) I just added a scan from virustotal, the file is not infected.

And drop the sarcasm, this program does what most other programs can't, it automises SQL Injection.Weird, I don't know if it's just me then... but Norton detects it as a trojan.

VT finds it clean, but run in sandboxie : SBIE2331 Service start failed: [33 / 1058] The service cannot be started, either because it is disabled or because it has no enabled devices associated with it

<http://www.virustotal.com/file-scan/report.html?id=4d9b39ab0072bba82b9e0a6b3e1936e3ac94970ced731772d7699a210bf58d40-1319058033>

HidingInSpace - October 19, 2011, 2:03 pm

(Oct 19, 2011 01:58 PM)Qub1 Wrote: [\[CITE\]](#) I just added a scan from virustotal, the file is not infected.

And drop the sarcasm, this program does what most other programs can't, it automises SQL Injection.

post the actual link for the scan dude its not hard to delete the detections

also when trying to run sandboxie SBIE2331 Service start failed: [33 / 1058] The service cannot be started, either because it is disabled or because it has no enabled devices associated with it. Also scanned with anibus and it says it cannot excute file...nice try skid

Qub1 - October 19, 2011, 2:04 pm

can you just suggest a link for a good site that allows me to share the results link, I've never really generated a scan before.

Thanks

Power_V - October 19, 2011, 2:05 pm

(Oct 19, 2011 02:03 PM)iTz_H4CKED Wrote: [\[CITE\]](#) post the actual link for the scan dude its not hard to delete the detectionsNorton detected it as a trojan when i scanned it.
It's infected...

Qub1 - October 19, 2011, 2:10 pm

STOP SAYING ITS INFECTED, I just rared it. Don't beleive me? Ok, suggest a site that allows for virus scanning then, so I can scan the crap out of the file, and share it here, geez.

* There, done, added 2 screenshots and result links, happy now?!

Xch4ng3 - October 19, 2011, 2:14 pm

How about you post a virus scan of the .EXE and not the WinRAR file.

HidingInSpace - October 19, 2011, 2:15 pm

(Oct 19, 2011 02:10 PM)Qub1 Wrote: [\[CITE\]](#) STOP SAYING ITS INFECTED, I just rared it. Don't beleive me? Ok, suggest a site that allows for virus scanning then, so I can scan the crap out of the file, and share it here, geez.

unrar it and scan it on virustotal then share the result link thats how most people do it

Qub1 - October 19, 2011, 2:24 pm

I just did that, look at the first post

I included a scan of the RAR and a scan of the EXE

Power_V - October 19, 2011, 2:26 pm

(Oct 19, 2011 02:24 PM)Qub1 Wrote: [\[CITE\]](#) I just did that, look at the first post

I included a scan of the RAR and a scan of the EXE Ok, sorry about that.. You have any ideas why i'm getting that error in sandboxie though?

Qub1 - October 19, 2011, 2:30 pm

I have absolutely no idea, but then again I don't really know what sandboxie is =D, but I think it might be because of its name? Or because the program works with a lot of threads, so it might interrupt the threads sandboxie uses.

But anyway trust me, I hate viruses, I won't ever spread them, this is nothing more but a very usefull tool. If anyone gets a virus from this I would like to see proof because that's 100% impossible.

So please, try the program I guarantee you that it doesn't contain viruses.

And if you've tried it please tell me what do you think?

JoinSeventh - October 19, 2011, 2:37 pm

You should work on the WAF Bypass, what's in there atm won't bypass much.

Qub1 - October 19, 2011, 2:39 pm

I know, its still in development but I need sites that have a WAF filter so I can test it. Maybe anyone knows some good sites that are vulnerable, but protected with WAF? So I can improve the program.

DeafCon - October 19, 2011, 3:09 pm

Didn't work for me on the test site: <http://testphp.vulnweb.com/listproducts.php?cat=1> it managed to get the tables but opening them up produced no results. I couldn't select the "Proxy" option that was grayed out all the time. The Dork scanner also crashed the program for me so far it's been pretty unusable. I am running Windows XP SP3.

Qub1 - October 19, 2011, 3:19 pm

Please state what errors you encounter with the dork scanner. So copy the contents of the error you get here, please.

And the proxy is grayed out because I haven't had time to implement it yet.

And empty tables mean that the site just doesn't return a result, sorry, but it means it is unhackable. You can check manually if the table returns a result. If it does, please reply, so I can look into it. Also keep in mind that the program is still in the Alpha stage, so you are very likely to run into errors.

* I also just added these questions to a FAQ within the first post.

DeafCon - October 19, 2011, 4:30 pm

(Oct 19, 2011 03:19 PM)Qub1 Wrote: [\[CITE\]](#) Please state what errors you encounter with the dork scanner. So copy the contents of the error you get here, please.

And the proxy is grayed out because I haven't had time to implement it yet.

And empty tables mean that the site just doesn't return a result, sorry, but it means it is unhackable. You can check manually if the table returns a result. If it does, please reply, so I can look into it. Also keep in mind that the program is still in the Alpha stage, so you are very likely to run into errors.

* I also just added these questions to a FAQ within the first post.

The site is fully hack-able and it has been made for testing... I hacked it manually and via SQLmap and it was very simple. When using the mass dork scanner the error box does not give any technical error information as to why it needs to shut down, it just says "IT -EON Engine has encountered a problem and needs to close. We are sorry for the inconvenience" and underneath "If you were in the middle of something, the information you were working on might be lost" you have no option but to click on the "close" button. The same error also occurred when I tried to use the admin pagefinder on the leadbattery site however it did find the column information from the tables on that site.

Qub1 - October 19, 2011, 4:32 pm

Hmm, what did you do to reproduce the problem with the mass dork scanner, what checkboxes did you check etc...

So basically did you use any default lists, and if so which?

And for the test site, I'll look into its format and add it to the next version of the program.

Thanks!

* Also just released a new update that fixes some small bugs within the Admin Login Finder.

DeafCon - October 19, 2011, 4:49 pm

I just selected the Kobez dork list and the default search engines, I selected one Dork from that list and then "start" and it crashed. I don't know if I'm doing that correctly... when I removed all dorks from the list but the one I wanted to use then it appeared to work fine. The Admin page-finder now also seems to work after the mini-update.

Qub1 - October 20, 2011, 2:13 am

Ok, I'm going to implement an error reporting system in the program, and then I'll release a new version, give me 20 minutes.

* Might take a bit longer, also fixing some other things

EDIT:

Ok, I've made a new version with an auto-updater and it has error handling for the Mass Dork Scanner. Please report the error you get when using it.

The new version also has support for the site you entered now, it is tested and works correctly. This means it has a wider site compatability range.

DeafCon - October 21, 2011, 3:11 am

Ok downloaded the new version and when I load in the Kobez dork list (2459 dorks) I select (highlight) one from the list (say trainers.php) but it scans from the top of the list (index.php) and I am now getting an "Index was outside the bounds of the array" error box, however the program does not crash now and I am able to close down the dork scanner. When I chose the same list (default search engines) and then delete all but one dork in the list (say trainers.php) I am now getting another error "Invalid URI: The Format of the URI could not be determined", again I am able to close down the box. The test site now works fine now and the admin-pagefinder seems to be working fine although 203 imo is a small amount of admin-logins to check for.

Qub1 - October 21, 2011, 6:08 am

Ahh, Ok, I get the error of the index now too, I'll try to fix it. Watch this post for updates.

However, I wasn't able to get the error of the Invalid URI, but they might be related so I'll fix the first error first.

EDIT:

Fixed, your auto-updater should now prompt you to download the latest version, containing the fixes.

ConSext - October 21, 2011, 6:45 am

can you post a mediafire link ?

tnx you

Qub1 - October 21, 2011, 7:10 am

Yeah sure.

But may I ask why? It'll be exactly the same as the current link...

* Link: http://it-eon.no-ip.info/it-eon_engine/latest_mediafire.php
It redirects to the latest version on mediafire.

Sleepyz0r - December 27, 2011, 4:50 am

Hey there ppl!

I have a question... I tried many links on SQL Injector or Admin Login Finder..
I allways get the error:

Quote:Invalid URL:
Sorry, but the website is incorrect!
<http://postimage.org/image/dtw7hz00n/>

I even tried with ur Vuln test.

PS: Im inside a proxy @ work.

Cumps!

pwntoken - December 27, 2011, 5:22 am

There is a problem up with that tool. See below, whenever i try to inject, it tries to find the tables and this shit happens all the time :/

wtf?

gizmodo - December 28, 2011, 8:12 am

thanks i will check it out. downloading now