

Forum:[Hack Forums](#)

Thread: [A few simple scripts for pentest with Python](#)

sam021 - December 11, 2018, 10:08 am

This project includes a number of simple, useful, and informative scripts that you can use. For those who want to learn how to test penetration with Python, it can be very useful. see it in github:

github.com/Naategh/PyCk/

4ground_daemon - December 16, 2018, 9:22 am

Hey man nice scripts just a few tips id suggest if you wanted to improve them.

some scripts have "file.read().splitlines()" when instead it could just be file.readlines()

Some scripts like the admin finder say get(link) which is fine but if the page holds(which iv had before) your script will just get stuck and wait. i would add timeout=2 for safety. this way the max it will hold is 2 seconds.

I would also look into using threads as this will speed things up a lot more. instead of testing one admin page at a time you could use 20 threads and do 20 at once. Only really useful on networking tools though because you are waiting on the network delay.

But in general nice stuff man!

sam021 - December 17, 2018, 2:07 am

(Dec 16, 2018 10:22 AM)4ground_daemon Wrote: [\[CITE\]](#) Hey man nice scripts just a few tips id suggest if you wanted to improve them.

some scripts have "file.read().splitlines()" when instead it could just be file.readlines()

Some scripts like the admin finder say get(link) which is fine but if the page holds(which iv had before) your script will just get stuck and wait. i would add timeout=2 for safety. this way the max it will hold is 2 seconds.

I would also look into using threads as this will speed things up a lot more. instead of testing one admin page at a time you could use 20 threads and do 20 at once. Only really useful on networking tools though because you are waiting on the network delay.

But in general nice stuff man!

Thank's alot, bro.

I will certainly apply these changes in the next version.

notjapanese - December 22, 2018, 5:51 pm

(Dec 17, 2018 03:07 AM)sam021 Wrote: [\[CITE\]](#) Thank's alot, bro.

I will certainly apply these changes in the next version.

really liked the email bomber, had to configure my gmail to allow it access but otherwise rllly good. thanks!

sam021 - December 23, 2018, 12:29 am

(Dec 22, 2018 06:51 PM)notjapanese Wrote: [\[CITE\]](#) really liked the email bomber, had to configure my gmail to allow it access but otherwise rily good. thanks!

I'm glad to be useful to you ?

Nomad.Null - December 24, 2018, 6:45 am

(Dec 16, 2018 10:22 AM)4ground_daemon Wrote: [\[CITE\]](#) Hey man nice scripts just a few tips id suggest if you wanted to improve them.

some scripts have "file.read().splitlines()" when instead it could just be file.readlines()

Some scripts like the admin finder say get(link) which is fine but if the page holds(which iv had before) your script will just get stuck and wait. i would add timeout=2 for safety. this way the max it will hold is 2 seconds.

I would also look into using threads as this will speed things up a lot more. instead of testing one admin page at a time you could use 20 threads and do 20 at once. Only really useful on networking tools though because you are waiting on the network delay.

But in general nice stuff man!

The method he is using with file.read().splitlines() actually has a very good use case when you need to omit newline and carriage return characters. readlines() will leave them in by default and tends to leave them as trailing characters that can screw stuff up. Just thought you'd find that worth knowing. :)

4ground_daemon - December 24, 2018, 10:43 am

oh thanks for letting me know that, i use to always use line.strip() instead. Nice that everyone is sharing knowledge for once rather in being abusive haha