

Forum:[Hack Forums](#)

Thread: [\[Python\] WordPress Version Fingerprinter](#)

Crypto™ - January 17, 2015, 5:00 am

Hey guys, this is just something I whipped up while waiting for some updates to install. Nothing fancy, but it will quickly attempt to discern the version of a WordPress site through two separate methods.

It requires [Python Requests](#), but it's quite easy to install.

Screenshot [\(Click to View\)](#)

Code import argparse

import requests # Requires install of Requests: <http://python-requests.org/>

import re

from urlparse import urlparse

def main():

 parser = argparse.ArgumentParser("Detects WP version from readme.html or meta tag")

 parser.add_argument("-t", "--target", action="append", dest="targets", help="Add a target to scan")

 args = parser.parse_args()

 if args.targets != None:

 scan(args.targets)

def scan(targets):

 for target in targets:

 if not target[:5] == "http:" and not target[:6] == "https:":

 target = "http://" + target

 tltarget = target

 target = target + '/readme.html'

 url = urlparse(target)

 r = requests.get(url.geturl())

 if r.status_code != 200:

 tlurl = urlparse(tltarget)

 t = requests.get(tlurl.geturl())

 w = re.compile(r'<meta name=\\"generator\\" content=\\"(WordPress \d+\.\d+\.\d+)?(\d+)?\\" V>',

re.I)

 n = w.search(t.text)

 if n:

 print "Site " + tlurl.netloc + tlurl.path + ": Running WordPress " + n.group(1)

 else:

 print "Site " + tlurl.netloc + tlurl.path + ": No version found"

 else:

 v = re.compile(r"Version (\d+\.\d+\.\d+)?(\d+)?", re.I)

```
m = v.search(r.text)
if m:
    print "Site " + url.netloc + url.path + ": Running WordPress " + m.group(1)
else:
    print "Site " + url.netloc + url.path + ": No version found"
```

```
if __name__ == "__main__":
    main()
```

[Gist](#)

Usage:

Code `python wp-fingerprinter.py -t targetblog.com -t blog.target.com -t target.com/path/to/blog -t http://blog.site.com -t https://site.com/wordpress`

Crypto™ - January 22, 2015, 8:15 pm

Just a demo on how many sites have Wordpress versions that are fingerprintable with this tool:

I tested a fairly large range of popular Wordpress powered sites, and many had their version number exposed. Some even are using some pretty outdated Wordpress versions.

kawaii - January 24, 2015, 7:02 am

Excellent tool Crypto. Really helps you narrow down what to search for on exploitdb. ;)

Crypto™ - January 29, 2015, 11:01 pm

(Jan 24, 2015 08:02 AM)Escrow Wrote: [\[CITE\]](#) Excellent tool Crypto. Really helps you narrow down what to search for on exploitdb. ;)

Glad you like it :) I'm surprised by how many sites are running seriously outdated WordPress versions. I stumbled across one with 3.5.2 running on it o_O That was released back in mid-2013.

FRANKIE - January 29, 2015, 11:05 pm

Very nicely done, this is a great tool!

Thanks Crypto!

Crypto™ - February 5, 2015, 11:14 pm

(Jan 30, 2015 12:05 AM)FRANKIE Wrote: [\[CITE\]](#) Very nicely done, this is a great tool!

Thanks Crypto!

Glad you like it ^^ I'll be trying to whip up a few other things shortly.