Parameth

Information Security Inc.

Contents

- About Parameth
- Testing Environment
- Required packages
- Installing Parameth
- Using Parameth
- References

About Parameth

- Parameth can be used to brute discover GET and POST parameters

parameth - Tool to brute discover GET and POST parameters

Testing Environment

- Kali Linux 2017

```
root@kali2017:~# cat /etc/*rel*
DISTRIB_ID=Kali
DISTRIB_RELEASE=kali-rolling
DISTRIB_CODENAME=kali-rolling
DISTRIB_DESCRIPTION="Kali GNU/Linux Rolling"
PRETTY_NAME="Kali GNU/Linux Rolling"
NAME="Kali GNU/Linux"
ID=kali
VERSION="2017.2"
VERSION_ID="2017.2"
ID_LIKE=debian
ANSI_COLOR="1;31"
HOME_URL="http://www.kali.org/"
SUPPORT_URL="http://forums.kali.org/"
BUG_REPORT_URL="http://bugs.kali.org/"
```

Required packages

- numpy==1.9.1
- requests==2.5.1
- fuzzywuzzy
- python-Levenshtein

```
root@kali2017:~# pip install python-Levenshtein  numpy requests fuzzywuzzy
Requirement already satisfied: python-Levenshtein in /usr/lib/python2.7/dist-packages
Requirement already satisfied: numpy in /usr/lib/python2.7/dist-packages
Requirement already satisfied: requests in /usr/lib/python2.7/dist-packages
Collecting fuzzywuzzy
  Downloading fuzzywuzzy-0.15.1-py2.py3-none-any.whl
Installing collected packages: fuzzywuzzy
Successfully installed fuzzywuzzy-0.15.1
```

Installing Parameth

- Download GitHub repository

```
root@kali2017:~# git clone https://github.com/maK-/parameth.git
Cloning into 'parameth'...
remote: Counting objects: 160, done.
remote: Total 160 (delta 0), reused 0 (delta 0), pack-reused 160
Receiving objects: 100% (160/160), 55.58 KiB | 211.00 KiB/s, done.
Resolving deltas: 100% (79/79), done.
```

Using Parameth

- Running parameth

```
root@kali2017:~# cd parameth/
root@kali2017:~/parameth# ls
dumbParamsGrabFromURL.sh  lists  parameth.py  README.md  requirements.txt  simpletest.php
root@kali2017:~/parameth# ./parameth.py
usage: parameth.py [-h] [-v] [-u URL] [-p PARAMS] [-H HEADER] [-a AGENT]
                   [-t THREADS] [-off VARIANCE] [-diff DIFFERENCE] [-o OUT]
                   [-P PROXY] [-x IGNORE] [-s SIZEIGNORE] [-d DATA]
                   [-i IGMETH] [-c COOKIE] [-T TIMEOUT]

optional arguments:
  -h, --help            show this help message and exit
  -v, --version         Version Information
  -u URL, --url URL     Target URL
  -p PARAMS, --params PARAMS
                        Provide a list of parameters to scan for
  -H HEADER, --header HEADER
                        Add a custom header to the requests
  -a AGENT, --agent AGENT
                        Specify a user agent
  -t THREADS, --threads THREADS
                        Specify the number of threads.
  -off VARIANCE, --variance VARIANCE
                        The offset in difference to ignore (if dynamic pages)
  -diff DIFFERENCE, --difference DIFFERENCE
                        Percentage difference in response (recommended 95)
  -o OUT, --out OUT     Specify output file
  -P PROXY, --proxy PROXY
                        Specify a proxy in the form http|s://[IP]:[PORT]
  -x IGNORE, --ignore IGNORE
                        Specify a status to ignore eg. 404,302...
  -s SIZEIGNORE, --sizeignore SIZEIGNORE
                        Ignore responses of specified size
  -d DATA, --data DATA  Provide default post data (also taken from provided
                        url after ?)
  -i IGMETH, --igmeth IGMETH
                        Ignore GET or POST method. Specify g or p
  -c COOKIE, --cookie COOKIE
                        Specify Cookies
  -T TIMEOUT, --timeout TIMEOUT
                        Specify a timeout in seconds to wait between each
                        request
```

Using Parameth

- Simple Test -> simpletest.php, contains unknown php parameters

```
root@kali2017:/var/www/html# cat simpletest.php
<?php

if(isset($_GET['redirect'])){
        $redir = $_GET['redirect'];
        header("HTTP/1.1 301 Moved Permanently");
        header("Location: ".$redir);
}

if(isset($_GET['m'])){
        echo ' ikemnolmnlkfe';
}

if(isset($_POST['r'])){
        echo 'kdnelnfjkenfjfnelkfn';
}


?>


efnsefknlslelknself
```

Using Parameth

- Simple Test -> using elinks to access simpletest.php

Using Parameth

- Simple Test -> Discover the unknown php parameters

```
root@kali2017:~/parameth# ./parameth.py -u http://192.168.10.12/simpletest.php
parameth v1.337 - find parameters and craic rocks
Author: Ciaran McNally - https://securit.ie/

Establishing base figures...
POST data:
Offset value: 0
GET: content-length-> 22  status-> 200
POST: content-length-> 22  status-> 200
Scanning it like you own it...
POST(size): r | 22 ->42 ( http://192.168.10.12/simpletest.php )
GET(status): redirect | 200-> 301 ( http://192.168.10.12/simpletest.php?redirect=discobiscuits )
GET(size): m | 22 ->36 ( http://192.168.10.12/simpletest.php?m=discobiscuits )
```

References

- Kitploit
http://www.kitploit.com/2017/10/parameth-tool-to-brute-discover-get-and.html

- Kali Linux
https://www.kali.org/downloads/

- w3schools
https://www.w3schools.com/php/php_superglobals.asp