ATTACK DEFENSE

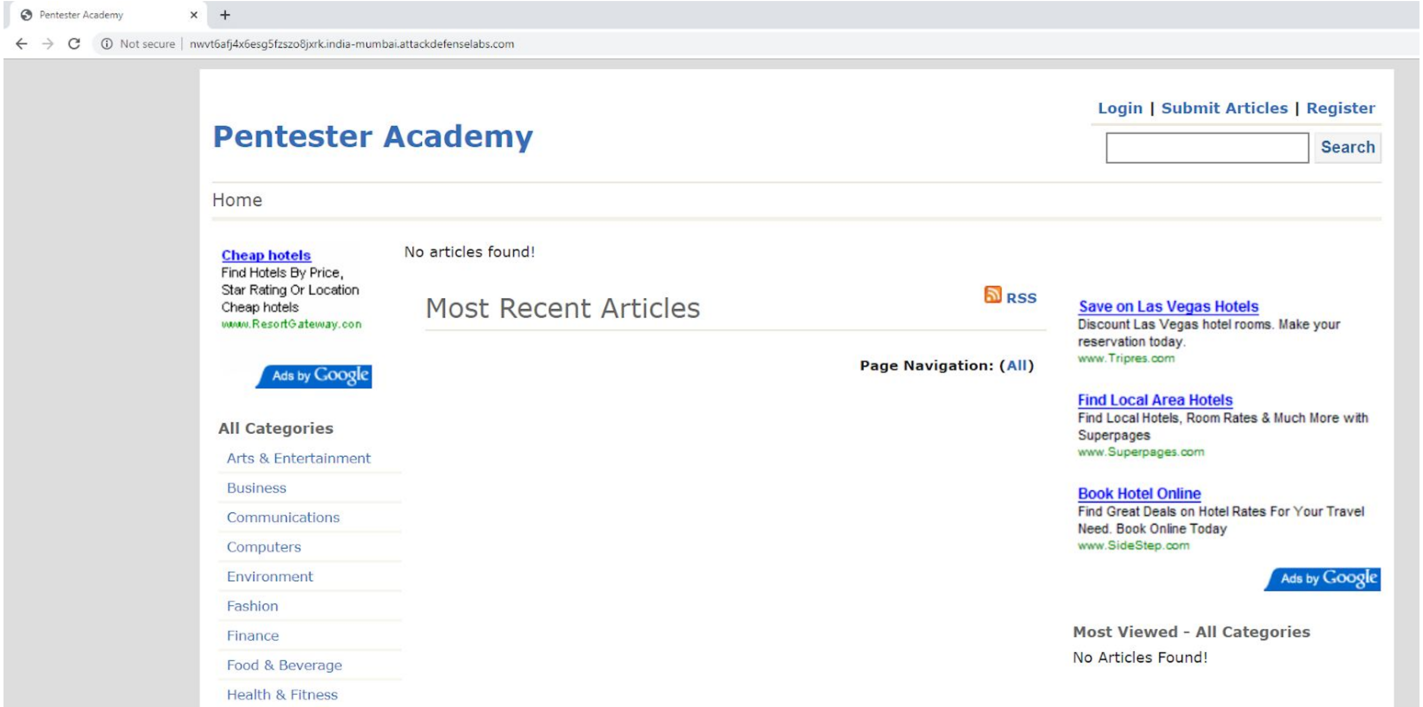
by PentesterAcademy

Name	Free Article Submissions 1.0
URL	https://www.attackdefense.com/challengedetails?cid=315
Type	Real World Webapps : Broken Authentication

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Solution:

Step 1: Inspect the web application.

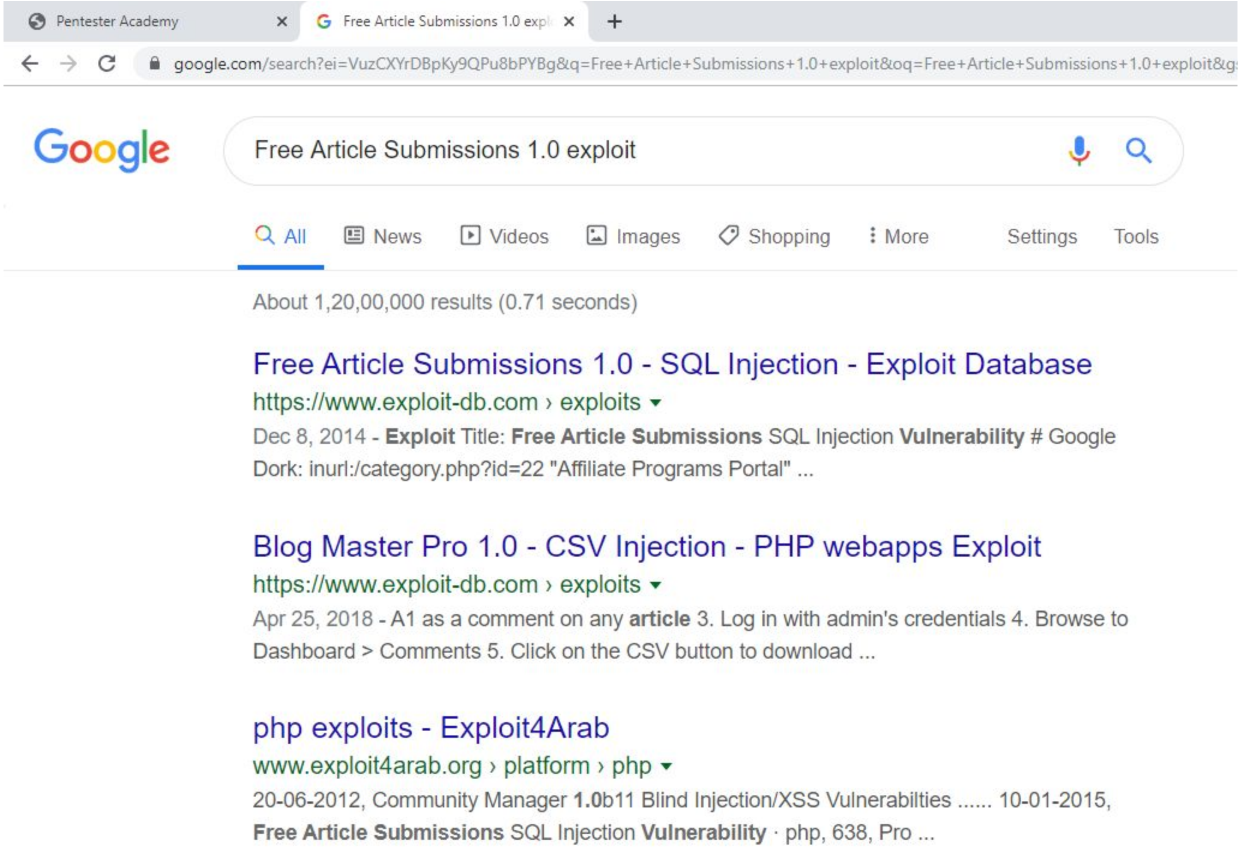


Pentester Academy
Not secure | nwvt6afj4x6esg5fzszo8jxrk.india-mumbai.attackdefenselabs.com
Pentester Academy
Login | Submit Articles | Register
Search
Home
Cheap hotels
Find Hotels By Price, Star Rating Or Location Cheap hotels
www.ResortGateway.com
Ads by Google
All Categories
Arts & Entertainment
Business
Communications
Computers
Environment
Fashion
Finance
Food & Beverage
Health & Fitness
RSS
Most Recent Articles
Page Navigation: (All)
Save on Las Vegas Hotels
Discount Las Vegas hotel rooms. Make your reservation today.
www.Tripres.com
Find Local Area Hotels
Find Local Hotels, Room Rates & Much More with Superpages
www.Superpages.com
Book Hotel Online
Find Great Deals on Hotel Rates For Your Travel Need. Book Online Today
www.SideStep.com
Ads by Google
Most Viewed - All Categories

No articles found!

No Articles Found!

Step 2: Search on google “Free Article Submissions 1.0 exploit”.



Pentester Academy
Free Article Submissions 1.0 expl
google.com/search?ei=VuzCXYrDBpKy9QPu8bPYBg&q=Free+Article+Submissions+1.0+exploit&oq=Free+Article+Submissions+1.0+exploit&g
Google
All
News
Videos
Images
Shopping
More
Settings
Tools

Free Article Submissions 1.0 exploit

About 1,20,00,000 results (0.71 seconds)

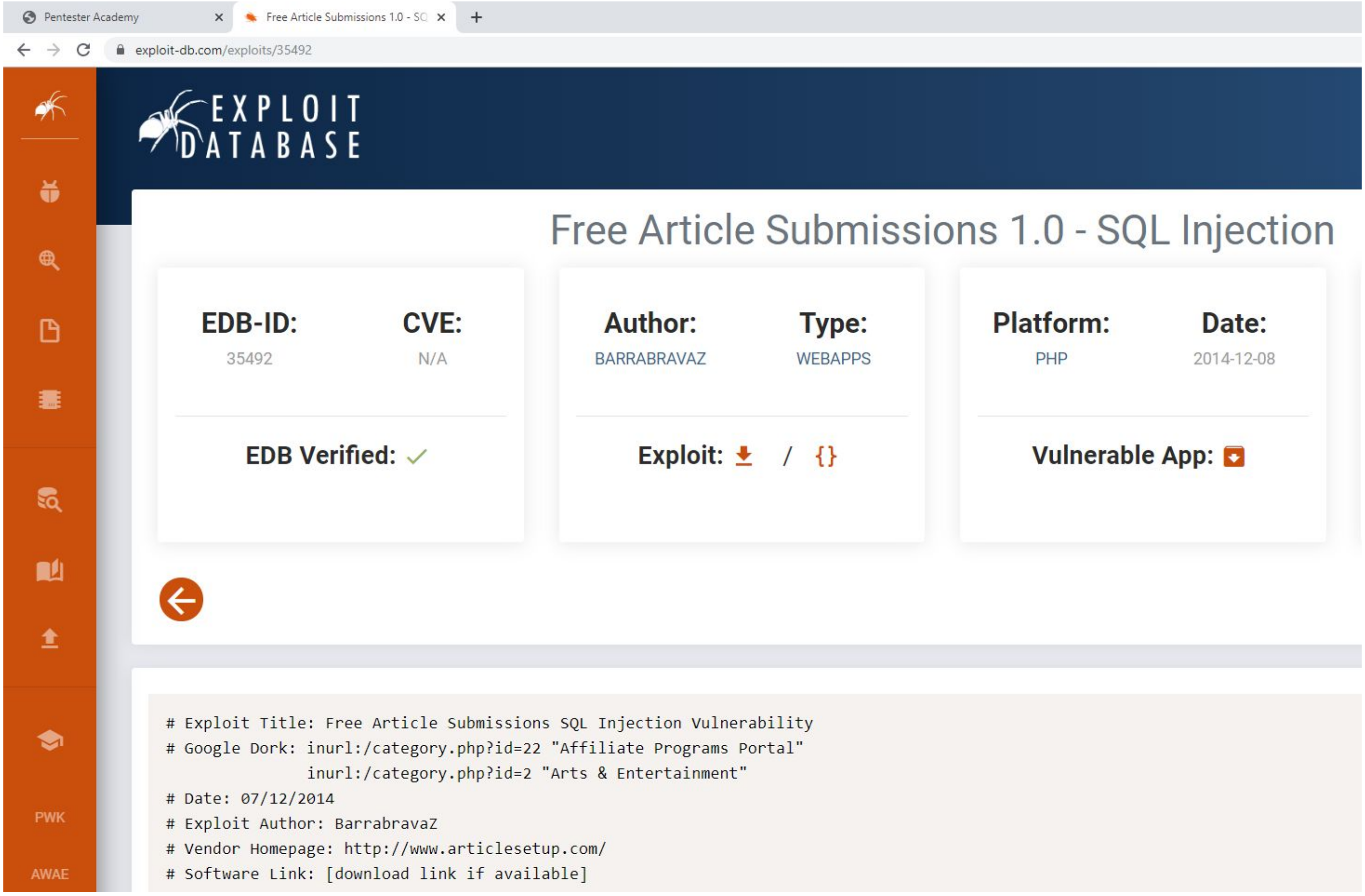
Free Article Submissions 1.0 - SQL Injection - Exploit Database
https://www.exploit-db.com › exploits ▾
Dec 8, 2014 - **Exploit** Title: **Free Article Submissions** SQL Injection **Vulnerability** # Google Dork: inurl:/category.php?id=22 "Affiliate Programs Portal" ...

Blog Master Pro 1.0 - CSV Injection - PHP webapps Exploit
https://www.exploit-db.com › exploits ▾
Apr 25, 2018 - A1 as a comment on any **article** 3. Log in with admin's credentials 4. Browse to Dashboard > Comments 5. Click on the CSV button to download ...

php exploits - Exploit4Arab
www.exploit4arab.org › platform › php ▾
20-06-2012, Community Manager **1.0**b11 Blind Injection/XSS Vulnerabilties ...... 10-01-2015, **Free Article Submissions** SQL Injection **Vulnerability** · php, 638, Pro ...

The exploit db link contains the information regarding the vulnerable parameter and the SQLI payload required to exploit the vulnerability.

Exploit DB Link: https://www.exploit-db.com/exploits/35492


Pentester Academy
Free Article Submissions 1.0 - SQ
exploit-db.com/exploits/35492
EXPLOIT DATABASE
PWK
AWAE

Free Article Submissions 1.0 - SQL Injection

EDB-ID: 35492

CVE: N/A

Author: BARRABRAVAZ

Type: WEBAPPS

Platform: PHP

Date: 2014-12-08

EDB Verified: ✓

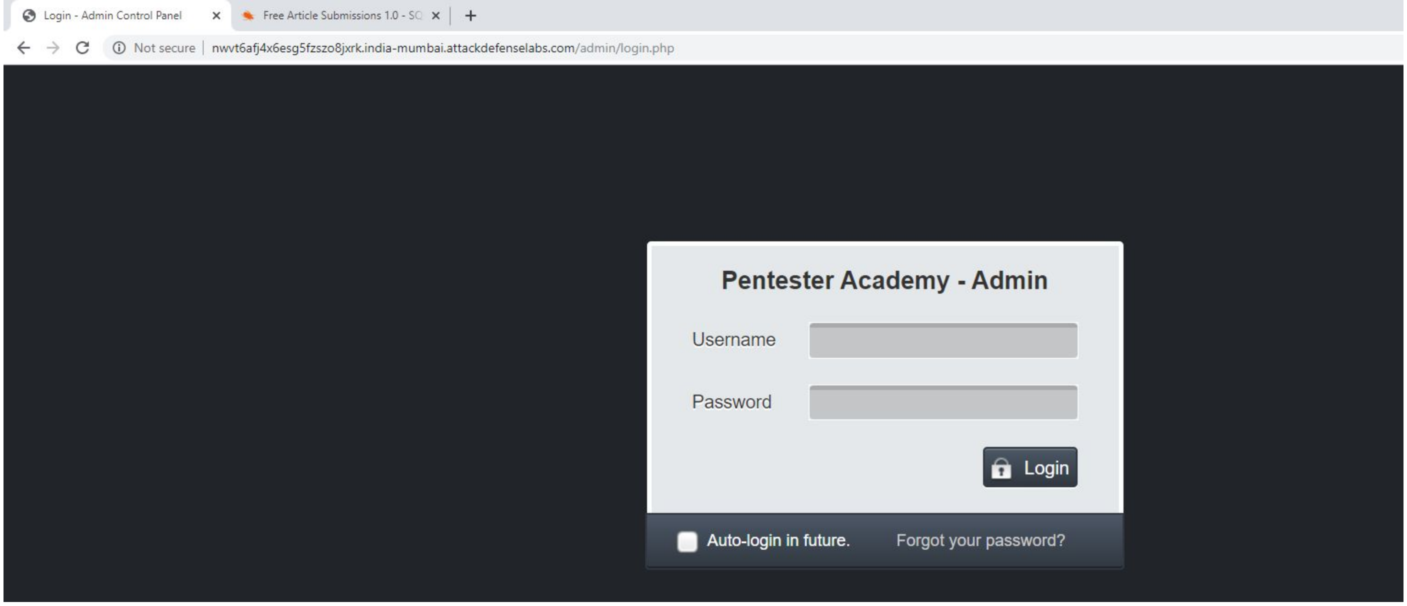
Exploit: ⬇ / {}

Vulnerable App: ⬇

```
# Exploit Title: Free Article Submissions SQL Injection Vulnerability
# Google Dork: inurl:/category.php?id=22 "Affiliate Programs Portal"
             inurl:/category.php?id=2 "Arts & Entertainment"
# Date: 07/12/2014
# Exploit Author: BarrabravaZ
# Vendor Homepage: http://www.articlesetup.com/
# Software Link: [download link if available]
```

Step 3: Navigate to the Admin panel, the admin panel is located at “/admin” panel.

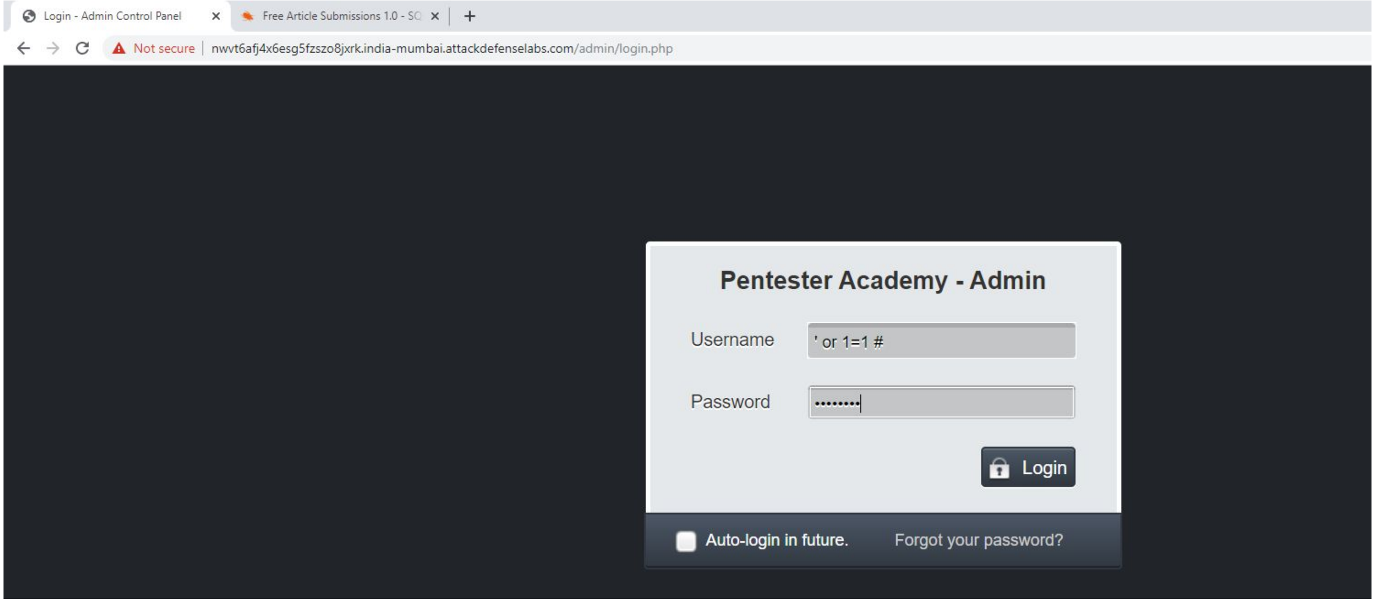
URL: http://shqcopsqovqbz033xt2091ztm.hidenseek-1.attackdefenselabs.com/install


Login - Admin Control Panel
Free Article Submissions 1.0 - SQ
Not secure
nwvt6afj4x6esg5fzszo8jxrk.india-mumbai.attackdefenselabs.com/admin/login.php
Pentester Academy - Admin
Username
Password
Login
Auto-login in future.
Forgot your password?

Step 4: Inject the SQLI payload in the username field and enter any value in the password field to bypass the authentication.

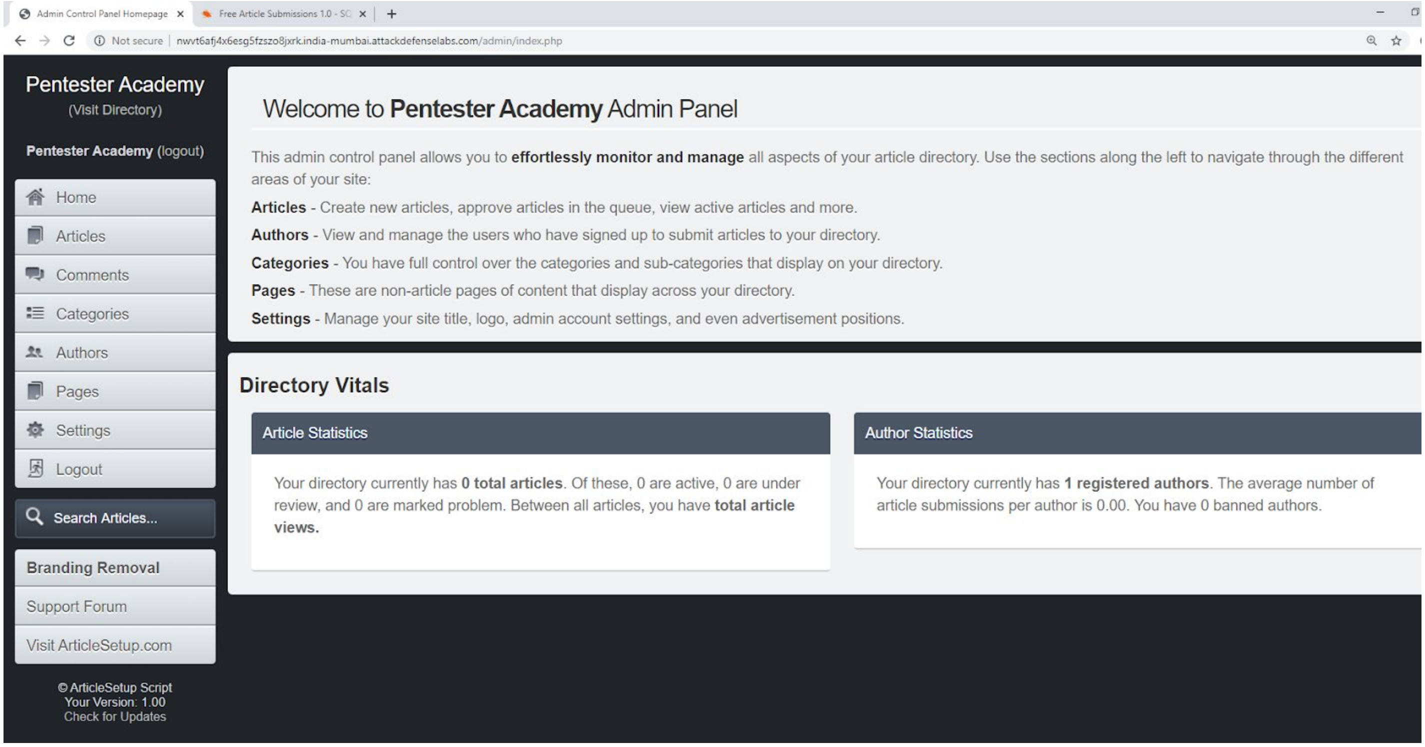
Payload: ' or 1=1 #

Username: ' or 1=1 #
Password: password


Login - Admin Control Panel
Free Article Submissions 1.0 - SQ
Not secure
nwvt6afj4x6esg5fzszo8jxrk.india-mumbai.attackdefenselabs.com/admin/login.php
Pentester Academy - Admin
Username
Password
Login
Auto-login in future.
Forgot your password?

Username ' or 1=1 #
Password ••••••••

Admin Dashboard:



Welcome to **Pentester Academy** Admin Panel

This admin control panel allows you to **effortlessly monitor and manage** all aspects of your article directory. Use the sections along the left to navigate through the different areas of your site:

Articles - Create new articles, approve articles in the queue, view active articles and more.

Authors - View and manage the users who have signed up to submit articles to your directory.

Categories - You have full control over the categories and sub-categories that display on your directory.

Pages - These are non-article pages of content that display across your directory.

Settings - Manage your site title, logo, admin account settings, and even advertisement positions.

Directory Vitals

Article Statistics

Your directory currently has **0 total articles**. Of these, 0 are active, 0 are under review, and 0 are marked problem. Between all articles, you have **total article views.**

Author Statistics

Your directory currently has **1 registered authors**. The average number of article submissions per author is 0.00. You have 0 banned authors.

© ArticleSetup Script
Your Version: 1.00
Check for Updates

The authentication was bypassed successfully.

References:

1. Free Article Submissions (http://www.articlesetup.com/)
2. Free Article Submissions 1.0 - SQL Injection (https://www.exploit-db.com/exploits/35492)