

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

Insecure CAPTCHA

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

## DVWA Security

### Script Security

Security Level is currently **low**.

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

The security level changes the vulnerability level of DVWA.

low

Submit

### PHPIDS

**PHPIDS** v.0.6 (PHP-Intrusion Detection System) is a security layer for PHP bas

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

Insecure CAPTCHA

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

## 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)

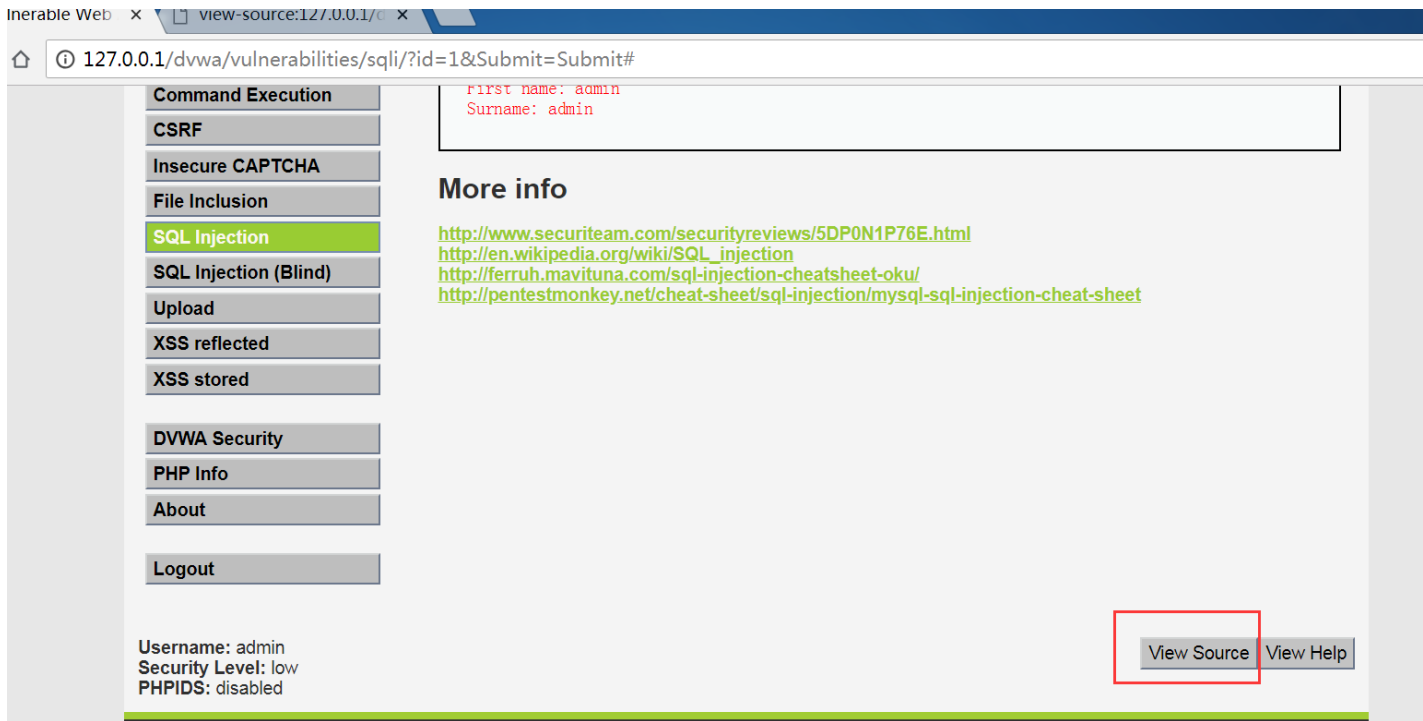
<http://ferruh.mavituna.com/sql-injection-cheatsheet-ok/>

<http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>

正常 情况下需要输入ID， 如上图；



dvwa里面提供了这么一个功能:



## SQL Injection Source

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

    $id = $_GET['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++;
    }
}
?>
```

```
1 <?php
2
3 if(isset($_GET['Submit'])) {
4
5     // Retrieve data
6
7     $id = $_GET['id'];
8
9     $getid = "SELECT first_name, last_name FROM users WHERE user_id = '$id'";
10    $result = mysql_query($getid) or die('<pre>' . mysql_error() . '</pre>');
11
12    $num = mysql_numrows($result);
13
```

```

14     $i = 0;
15
16     while ($i < $num) {
17
18         $first = mysql_result($result,$i,"first_name");
19         $last = mysql_result($result,$i,"last_name");
20
21         echo '<pre>';
22         echo 'ID: ' . $id . '<br>First name: ' . $first . '<br>Surname: ' . $last;
23         echo '</pre>';
24
25         $i++;
26     }
27 }
28 ?>
29

```

## PHP代码分析

```

if(isset($_GET['Submit'])) {           //判断Submit变量是否存在
    $id = $_GET['id'];                 //获取id变量的值并赋值给变量$id
    $getid = "SELECT first_name, last_name FROM users WHERE user_id = '$id'";
    //将select查询语句赋值给变量$getid

```

**\$\_GET**：它是获取 Submit，就是看你有没有点击提交按钮，如果点击了，这里获取的就是一个真值，如果点击了，这里就要执行大括号里面的语句，然后通过 GET 方法获取在 **id** 这个文本框里面输入的值，而后赋值给 id 变量，在下面一句就是把 select 语句赋值给了 \$getid 这个变量；

## PHP代码分析

```

$result = mysql_query($getid) or die('<pre>' . mysql_error() . '</pre>');
//mysql_query() 函数执行mysql查询
//die() 函数输出一条消息，并退出当前脚本。
//mysql_error() 函数返回上一个MySQL操作产生的文本错误信息。
//or之前的语句执行不成功时，才会执行后面的语句。
//and之前的语句执行成功时，才会执行后面的语句。

```

利用 mysql\_query 执行 sql 的增删改查语句，而后把执行的结果发送给了 result 这个变量，**' '** 是原样输出，**.** 是连接的意思，mysql\_error 的意思是如果前面一句 Mysql\_query 的执行结果是错误的，那么这里就会把错误的信

息打印出来;

or之前的语句执行不成功,后面的语句才会执行;

and之前的语句执行成功的时候,才会执行后面的语句;

即: or : 1 or \* =1(前面执行成功了,后面可以不用看了)

and : 1 and 1 =1

mysql\_query():

如果是执行查询之类的语句(select), 那么会返回一个资源标识符,也就是我们要查找的 数据结果集;

如果执行的是增删 改之类的语句,返回的 就是true或者false了;

UC 浏览器

PHP代码分析

```
$num = mysql_numrows($result);           //返回结果集中行的数目
$i = 0;
while ($i < $num) {
    $first = mysql_result($result,$i,"first_name"); //返回结果集中first_name字段的值
    $last = mysql_result($result,$i,"last_name");  //返回结果集中last_name字段的值
    echo '<pre>';
    echo 'ID: ' . $id . '<br>First name: ' . $first . '<br>Surname: ' . $last;
    echo '</pre>';
    $i++;
}
```

在学习

edu.51cto.com

就第一句 `mysql_numrows` 而言, 你可能查找到符合条件的有好几条记录,一条记录是一行,你通过 `mysql_numrows`这个函数可以查到现在`$result`这个变量里面到底 有几行数据;

具体函数你可以看下面这里:

[http://www.w3school.com.cn/php/php\\_ref\\_mysql.asp](http://www.w3school.com.cn/php/php_ref_mysql.asp)

应用

好玩的网站

百度文库财富值

健康养生之类

编程相关以及算法视

英语口语

电脑硬件相关

机器学习 等学习视屏

模糊数学 统计学等 视

算

AJAX RSS Reader

AJAX Poll

PHP 参考手册

PHP Array

PHP Calendar

PHP Date

PHP Directory

PHP Error

PHP Filesystem

PHP Filter

PHP FTP

PHP HTTP

PHP LibXML

PHP Mail

PHP Math

PHP MySQL

PHP MySQLi

PHP SimpleXML

PHP String

PHP XML

PHP Zip

PHP 杂项

## PHP MySQL 函数

**PHP:** 指示支持该函数的最早的 PHP 版本。

函数	描述	PHP
<a href="#">mysql_affected_rows()</a>	取得前一次 MySQL 操作所影响的记录行数。	3
<a href="#">mysql_change_user()</a>	不赞成。改变活动连接中登录的用户	3
<a href="#">mysql_client_encoding()</a>	返回当前连接的字符集的名称	4
<a href="#">mysql_close()</a>	关闭非持久的 MySQL 连接。	3
<a href="#">mysql_connect()</a>	打开非持久的 MySQL 连接。	3
<a href="#">mysql_create_db()</a>	不赞成。新建 MySQL 数据库。使用 <a href="#">mysql_query()</a> 代替。	3
<a href="#">mysql_data_seek()</a>	移动记录指针。	3
<a href="#">mysql_db_name()</a>	从对 <a href="#">mysql_list_dbs()</a> 的调用返回数据库名称。	3
<a href="#">mysql_db_query()</a>	不赞成。发送一条 MySQL 查询。 使用 <a href="#">mysql_select_db()</a> 和 <a href="#">mysql_query()</a> 代替。	3
<a href="#">mysql_drop_db()</a>	不赞成。丢弃 (删除) 一个 MySQL 数据库。 使用 <a href="#">mysql_query()</a> 代替。	3
<a href="#">mysql_errno()</a>	返回上一个 MySQL 操作中的错误信息的数字编码。	3
<a href="#">mysql_error()</a>	返回上一个 MySQL 操作产生的文本错误信息。	3

## PHP代码分析

```
$num = mysql_numrows($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++;  
}
```

//返回结果集中行的数目

//返回结果集中first\_name字段的值

//返回结果集中last\_name字段的值

edu.51cto.com

mysql\_result这个是从`result`这个变量里面取某个字段的值,来取哪一行呢,这里用*i*表示,一开始*i* = 0,就要取第1行的数据, `$first = mysql_result($result,$i,"first_name");` 这句话取得是first\_name这个字段的值,并赋值给first变量,下面一句取得还是第一行里面last\_name字段的值,