



DEPARTMENT OF COMPUTER ENGINEERING

SUBJECT: Cryptography and Network Security

Name	Vishwajit Sambhaji Sarnobat
UID no.	2023300195
Experiment No.	7

AIM:	To mitigate the vulnerabilities in DVWA.
-------------	--



DEPARTMENT OF COMPUTER ENGINEERING

SUBJECT: Cryptography and Network Security

SQL INJECTION:

```
1 2 3 4 | Monday November 17, 1:10 PM
vishwajit-vm@linuxmint-VM: ~
1 ssh -X vishwajit-vm@192.168.1.113
The authenticity of host '192.168.1.113 (192.168.1.113)' can't be established.
ED25519 key fingerprint is SHA256:spFHFAwp/b5XVXF7smCkmk8BamdlWKPEZwi6h1EY3I.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.113' (ED25519) to the list of known hosts.
vishwajit-vm@192.168.1.113's password:

vishwajit-vm@linuxmint-VM:~$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos
vishwajit-vm@linuxmint-VM:~$ cat /var/www/html/dvwa/vulnerabilities/sqli/source/low.php
<?php

if( isset( $_REQUEST[ 'Submit' ] ) ) {
    // Get input
    $id = $_REQUEST[ 'id' ];
    $id = mysqli_real_escape_string($GLOBALS["__mysqli_ston"], $id);

    switch ($_DWA1['SQLI_DB']) {
        case MySQL:
            // Check database
            $query = "SELECT first_name, last_name FROM users WHERE user_id = '$id'";
            $result = mysqli_query($GLOBALS["__mysqli_ston"], $query) or die( '<pre>' . ((is_object($GLOBALS["__mysqli_ston"])) ? mysqli_error($GLOBALS["__mysqli_ston"]) : ($__mysqli_res = mysqli_connect_error()) ? $__mysqli_res : false) . '</pre>' );
            // Get results
            while( $row = mysqli_fetch_assoc( $result ) ) {
                // Get values
                $first = $row["first_name"];
                $last = $row["last_name"];

                // Feedback for end user
                $html .= "<p>ID: {$id}<br />First name: {$first}<br />Surname: {$last}</p>";
            }
            mysqli_close($GLOBALS["__mysqli_ston"]);
            break;
        case SQLite:
            global $sqlite_db_connection;
    }
}

vishwajit-vm@linuxmint-VM:~$
```

The screenshot shows a browser window for DVWA (Damn Vulnerable Web Application) running on port 192.168.1.113. The URL is `http://192.168.1.113/dvwa/vulnerabilities/sqli/?id=%27+OR+1%3D1---+&Submit=Submit#`. The page title is "Vulnerability: SQL Injection". On the left, there is a sidebar menu with various attack types, and "SQL injection" is highlighted. The main content area has a "User ID" field containing "`OR 1=1 --`". Below the field, there is a "Submit" button. To the right of the form, under "More Information", there is a list of links related to SQL injection.

User ID: OR 1=1 --

Submit

More Information

- https://www.cs.tut.fi/~jkorpela/crypt/kb/SQL_injection
- <https://www.netspark.com/blog/web-security/sql-injection-cheat-sheet/>
- https://owasp.org/www-community/attacks/SQL_Injection
- <https://bobby-tables.com/>



DEPARTMENT OF COMPUTER ENGINEERING

SUBJECT: Cryptography and Network Security

FILE UPLOAD:

```
 1 2 3 4 Monday November 17, 1:23 PM
vishwajit-vm@linuxmint-VM:~$ sudo vim /var/www/html/dvwa/vulnerabilities/upload/source/low.php
vishwajit-vm@linuxmint-VM:~$ cat /var/www/html/dvwa/vulnerabilities/upload/source/low.php
<?php

if (isset($_POST['Upload'])) {

    $allowed_extensions = array('jpg', 'jpeg', 'png', 'gif');
    $allowed_mime_types = array('image/jpeg', 'image/png', 'image/gif');

    $file_name = $_FILES['uploaded']['name'];
    $file_tmp  = $_FILES['uploaded']['tmp_name'];
    $file_ext  = strtolower(pathinfo($file_name, PATHINFO_EXTENSION));

    // Check extension
    if (!in_array($file_ext, $allowed_extensions)) {
        die("<pre>Invalid file type. Only JPG, PNG, GIF allowed.</pre>");
    }

    // Check MIME type
    $mime = mime_content_type($file_tmp);
    if (!in_array($mime, $allowed_mime_types)) {
        die("<pre>Invalid MIME type. File is not an image.</pre>");
    }

    // Generate a safe random name
    $new_name = uniqid("img_", true) . "." . $file_ext;

    $target_path = DVWA_WEB_PAGE_TO_ROOT . "hackable/uploads/" . $new_name;

    // Upload the file
    if (!move_uploaded_file($file_tmp, $target_path)) {
        echo "<pre>Your image was not uploaded.</pre>";
    } else {
        echo "<pre>File uploaded successfully as {$new_name}</pre>";
    }
}

?>
vishwajit-vm@linuxmint-VM:~$
```





DEPARTMENT OF COMPUTER ENGINEERING

SUBJECT: Cryptography and Network Security

**COMMAND
INJECTION:**

```
vishwajit-vm@linuxmint-VM:~$ sudo vim /var/www/html/dvwa/vulnerabilities/exec/source/low.php
vishwajit-vm@linuxmint-VM:~$ cat /var/www/html/dvwa/vulnerabilities/exec/source/low.php
<?php

if( isset( $_POST[ 'Submit' ] ) ) {
    // Get input
    $target = $_REQUEST[ 'ip' ];

    // ALLOW ONLY valid IPv4 addresses
    if (!filter_var($target, FILTER_VALIDATE_IP, FILTER_FLAG_IPV4)) {
        die("<pre>Invalid IP address</pre>");
    }

    // Determine OS and execute the ping command.
    if( strstr( php_uname( 's' ), 'Windows NT' ) ) {
        // Windows
        $cmd = shell_exec( 'ping ' . $target );
    }
    else {
        // *nix
        $cmd = shell_exec( 'ping -c 4 ' . $target );
    }

    // Feedback for the end user
    $html .= "<pre>{$cmd}</pre>";
}

?>
vishwajit-vm@linuxmint-VM:~$
```



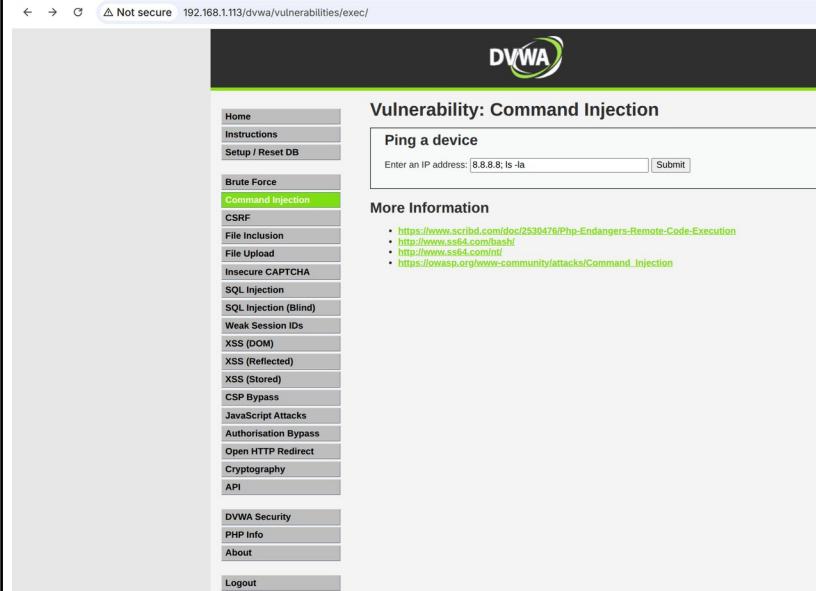


BHARATIYA VIDYA BHAVAN'S
SARDAR PATEL INSTITUTE OF TECHNOLOGY

Bhavan's Campus, Munshi Nagar, Andheri (West), Mumbai – 400058-India

DEPARTMENT OF COMPUTER ENGINEERING

SUBJECT: Cryptography and Network Security



The screenshot shows a web browser window displaying the DVWA (Damn Vulnerable Web Application) interface. The URL in the address bar is 192.168.1.113/dvwa/vulnerabilities/exec/. The main title is "Vulnerability: Command Injection". On the left, there is a vertical sidebar menu with various attack types, including Home, Instructions, Setup / Reset DB, Brute Force, Command injection (which is highlighted in green), CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection, SQL Injection (Blind), Weak Session IDs, XSS (DOM), XSS (Reflected), XSS (Stored), CSP Bypass, JavaScript Attacks, Authorisation Bypass, Open HTTP Redirect, Cryptography, and API. Below the menu is a "Ping a device" section with an input field containing "8.8.8.8; ls -la" and a "Submit" button. To the right of the input field, there is a "More Information" section with a bulleted list of links:

- <https://www.scribd.com/doc/2530476/PHP-Endangers-Remote-Code-Execution>
- <http://www.ss64.com/bash/>
- <http://www.ss64.com/nf/>
- https://owasp.org/www-community/attacks/Command_Injection