

Name: NIKHITHA

Date: 13.03.2023

### Task: 3

#### 1. commands execution vulnerability:


OS command injection (also known as shell injection) is a web security vulnerability that allows an attacker to execute arbitrary operating system (OS) commands on the server that is running an application, and typically fully compromise the application and all its data.



The screenshot shows the DVWA web application interface. The top header features the DVWA logo. On the left is a sidebar with navigation links: Home, Instructions, Setup, Brute Force, Command Execution (highlighted), CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security, PHP Info, About, and Logout. The main content area is titled 'Vulnerability: Command Execution'. It contains a 'Ping for FREE' section with a text input field for an IP address and a 'submit' button. Below the input field, the text 'help', 'index.php', and 'source' is displayed in red. Underneath, there is a 'More info' section with three links: <http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution>, <http://www.ss64.com/bash/>, and <http://www.ss64.com/int/>.

#### 2. file upload vulnerability:

File upload vulnerabilities are when a web server allows users to upload files to its filesystem without sufficiently validating things like their name, type, contents, or size.



- Home
- Instructions
- Setup / Reset DB
- Brute Force
- Command Injection
- CSRF
- File Inclusion
- File Upload**
- Insecure CAPTCHA
- SQL Injection
- SQL Injection (Blind)
- Weak Session IDs
- XSS (DOM)
- XSS (Reflected)
- XSS (Stored)
- CSP Bypass
- JavaScript

## Vulnerability: File Upload

Choose an image to upload:

No file selected.


../../../../hackable/uploads/pass succesfully uploaded!

### More Information

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

### 3.sql injection vulnerability:

SQL injection (SQLi) is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database. It generally allows an attacker to view data that they are not normally able to retrieve. This might include data belonging to other users, or any other data that the application itself is able to access. In many cases, an attacker can modify or delete this data, causing persistent changes to the application's content or behavior.



- 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: '%' or '' = ''  
First name: admin  
Surname: admin

ID: '%' or '' = ''  
First name: Gordon  
Surname: Brown

ID: '%' or '' = ''  
First name: Hack  
Surname: He

ID: '%' or '' = ''  
First name: Pablo  
Surname: Picasso

ID: '%' or '' = ''  
First name: Bob  
Surname: Smith

### More info

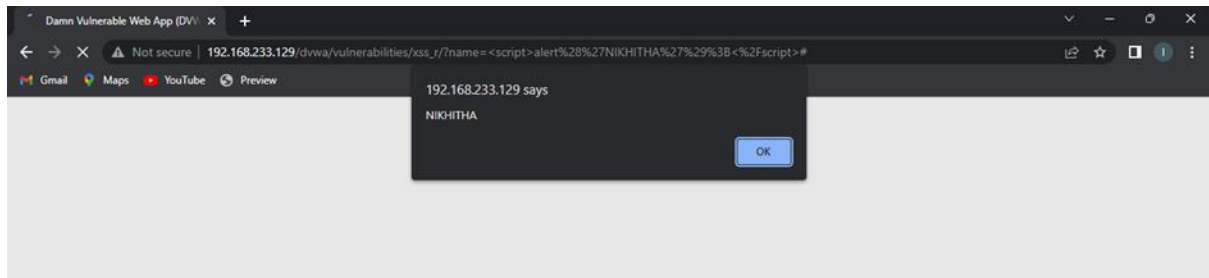
<http://www.securiteam.com/securityreviews/SDP0N1P76E.html>  
[http://en.wikipedia.org/wiki/SQL\\_injection](http://en.wikipedia.org/wiki/SQL_injection)  
<http://www.unixwiz.net/techtips/sqlinjection.html>

### 4.cross-site scripting:

**Cross site scripting (XSS)** is an attack in which an attacker injects malicious executable scripts into the code of a trusted application or website. Attackers often initiate an XSS attack by sending a malicious link to a user and enticing the user to click it.

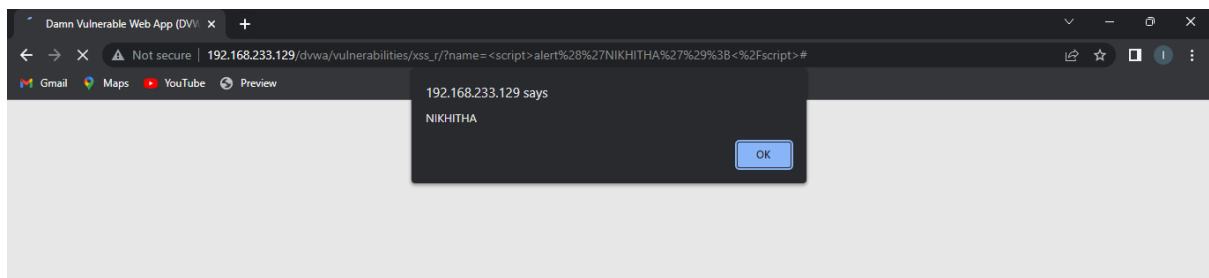
**Xss-reflected:**

**4.Cross site scripting (XSS)** is an attack in which an attacker injects malicious executable scripts into the code of a trusted application or website.



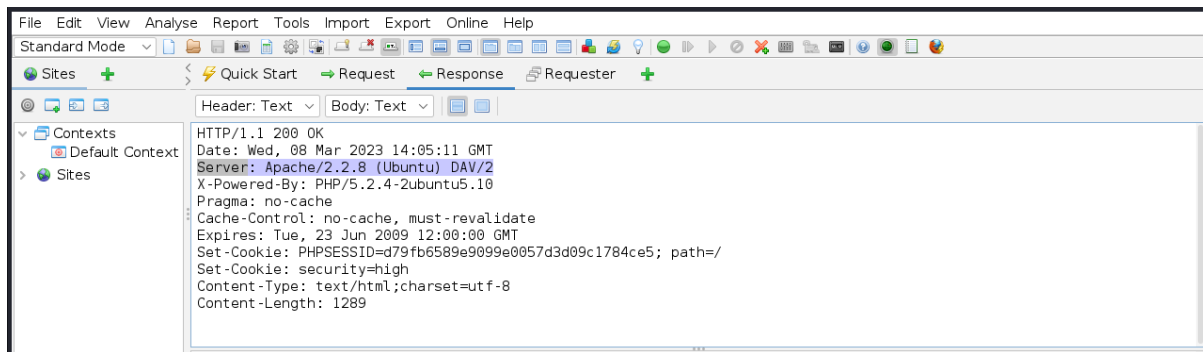
**Xss-stored:**

Attackers often initiate an XSS attack by sending a malicious link to a user and enticing the user to click it.



**5.sensitive information disclosure:**

**Sensitive Information Disclosure** (also known as **Sensitive Data Exposure**) happens when an application does not adequately protect sensitive information that may wind up being disclosed to parties that are not supposed to have access to it



## 6.local file inclusion:

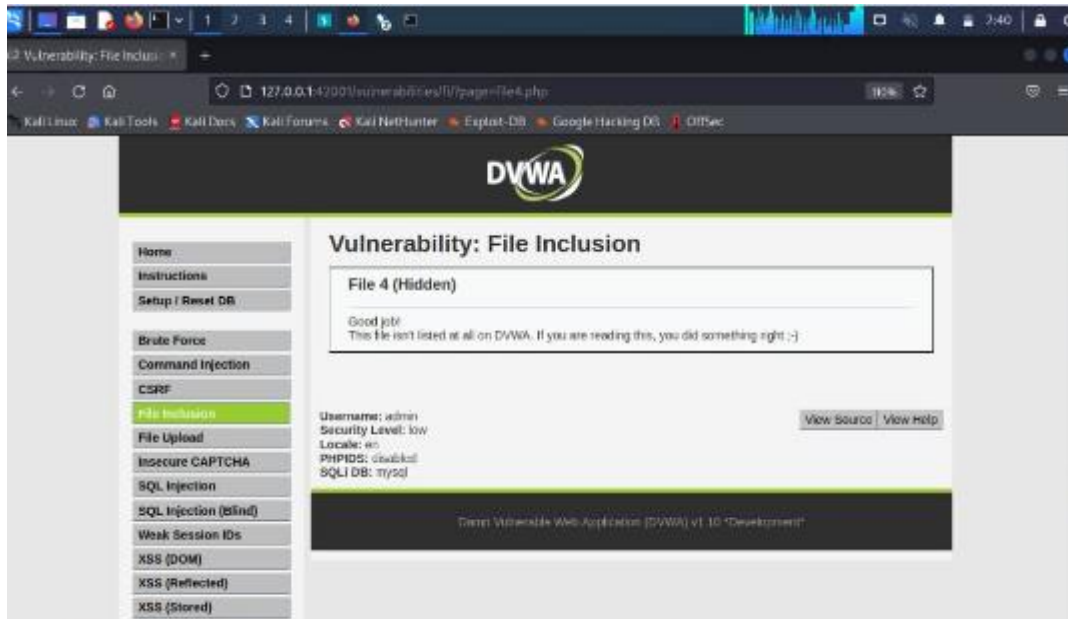
Local file injection is a type of security vulnerability that occurs when an attacker is able to inject malicious code or input into a program, web application, or operating system that allows them to access, modify, or execute local files on the targeted system.

This type of attack is also known as Local File Inclusion (LFI) or Path Traversal. It can occur in web applications that accept user input and do not properly validate or sanitize it before using it in file operations. Attackers can exploit this vulnerability to access files on the server, including sensitive data such as configuration files, database credentials, or even code files.



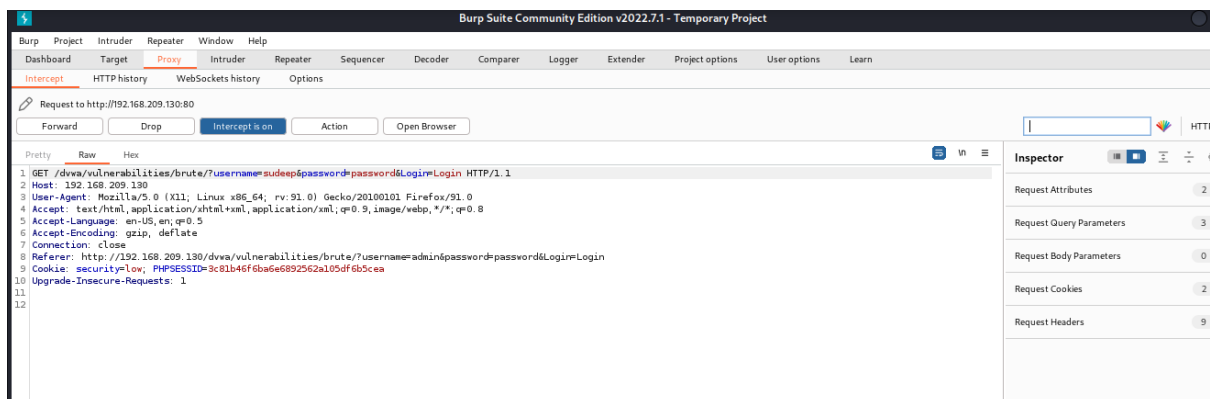
## 7.remote file inclusion:

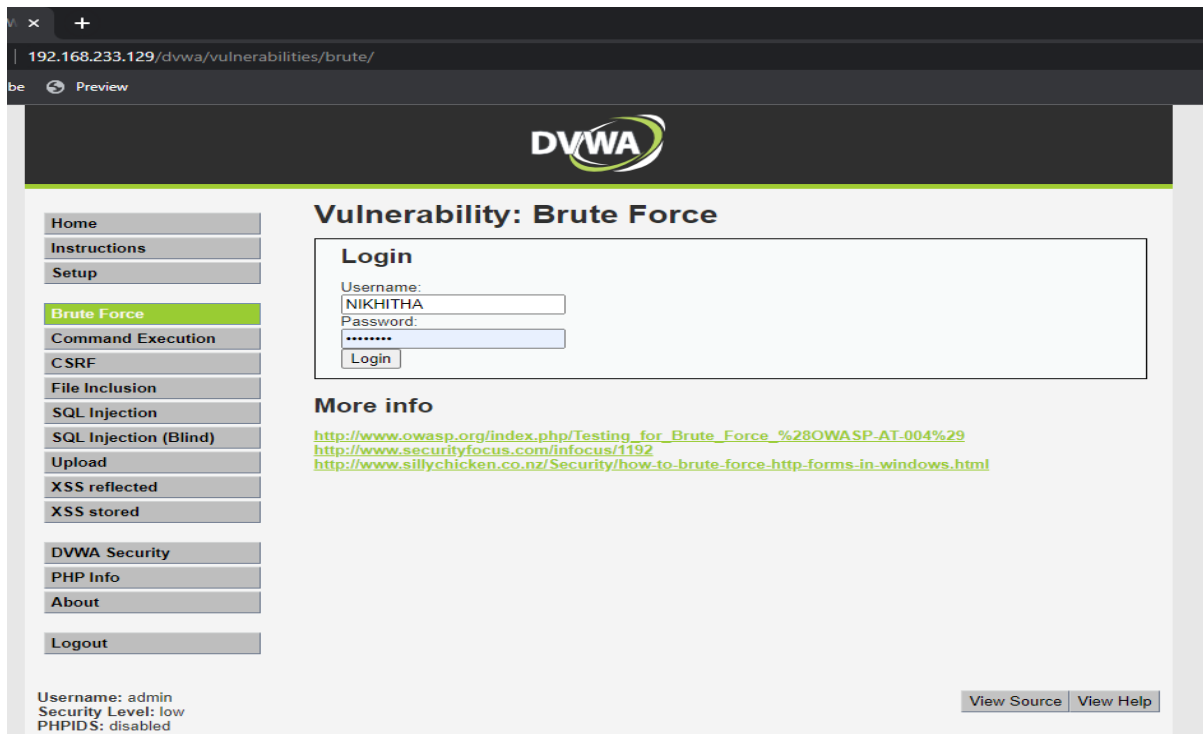
Remote file inclusion (RFI) is an attack targeting vulnerabilities in web applications that dynamically reference external scripts



## 8.bruteforce attack:

brute-force attack is a trial-and-error method used by application programs to decode login information and encryption keys to use them to gain unauthorized access to systems. Using brute force is an exhaustive effort rather than employing intellectual strategies.





### 9.forced browsing vulnerability:

Forced browsing attacks are the result of a type of security misconfiguration vulnerability. These kinds of vulnerabilities occur when insecure configuration or misconfiguration leave web application components open to attack.

### 10.components with known vulnerability:

This kind of threat occurs when the components such as libraries and frameworks used within the app almost always execute with full privileges. If a vulnerable component is exploited, it makes the hacker's job easier to cause a serious data loss or server.let us understand Threat Agents, Attack Vectors, Security Weakness, Technical Impact and Business.

### 11.html injection:

HTML Injection also known as Cross Site Scripting. It is a security vulnerability that allows an attacker to inject HTML code into web pages that are viewed by other users