**Government polytechnic**

**Udupi**

**Name: Pooja**

**Register.no: 145CS20010**

**Task: 3**

**1.command execution vulnerability**

Command Execution or Command injection is anattack in which the goal is execution ofarbitrary commands on the host operating system via avulnerable application. Command injection attacks arepossible when an application passes unsafe usersupplied data (forms, cookies, HTTP headers etc.) to asystem shell.

Now open the DVWA in your pc and login with following credentials:

Username – admin

Password – password

Bypass Low Level Security

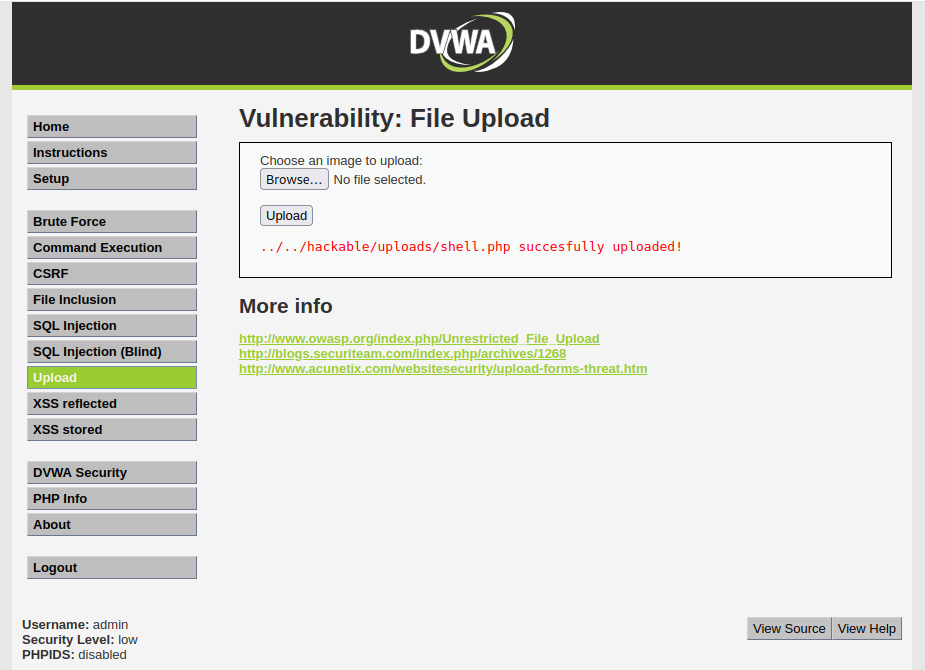
Go to the command execution page Enter an IP address and click on submit.

Now you can see the reply that tells us that we have establish a connection with the server.



**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. File upload vulnerability are a major problem with web based applications. In many web server this vulnerability depend entirely on purpose that allows an attacker to upload a file hiding malicious code inside that can then be executed on the server. An attacker might be able to put a phishing page into the website or deface the website.



**3. SQL injection vulnerability**

SQL injection is one of the most common attacks used by hackers to exploit any SQL database-driven web application. It’s a technique where SQL code/statements are inserted in the execution field with an aim of either altering the database contents, dumping useful database contents to the hacker, cause repudiation issues, spoof identity, and much more.

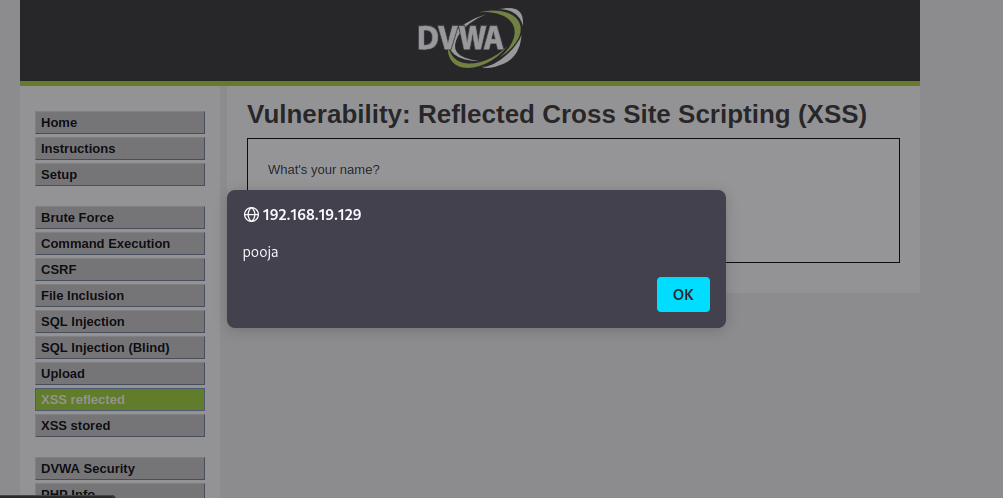


**4. cross site scripting**

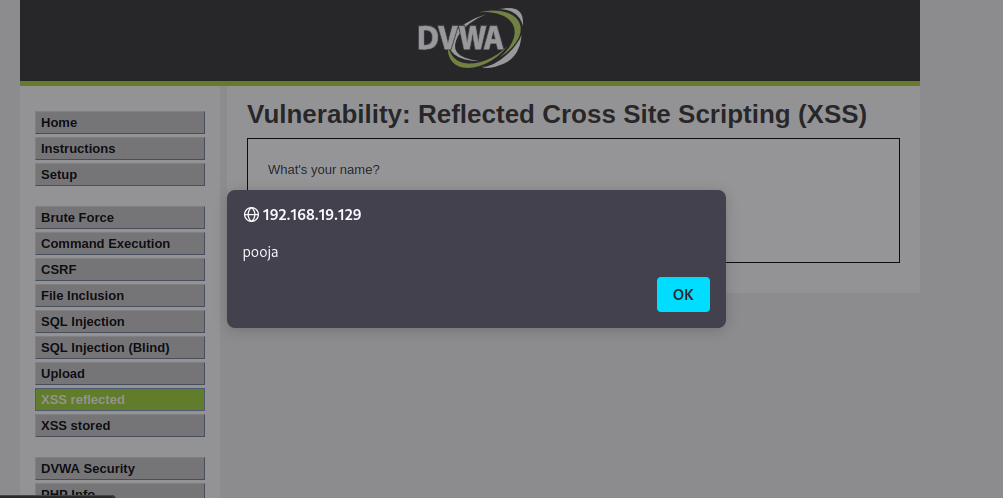
XSS is a technique in which attackers inject malicious Scripts into a target website and may allow them to gain access control of the website. If a website allows users to input data like comment, username field and email address field without controls then attacker can insert malicious code script as well.

Cross site scripting is a type of web security vulnerability where an attacker is able to inject malicious code, usually in the form of scripts, into a web page viewed by other users. This can allow the attacker to steal sensitive information, such as login credentials or personal data, or to modify the content of the page in a way that can harm users.

**Xss-reflected:**



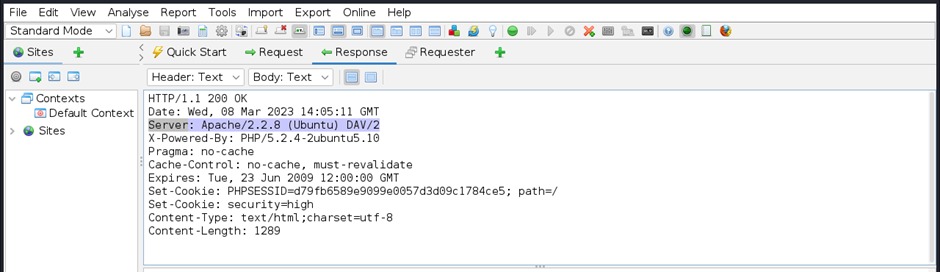
**Xss-stored:**



**5. Sensitive information disclosure**

Information disclosure, also known as information leakage, is when a website unintentionally reveals sensitive information to its users. Depending on the context, websites may leak all kinds of information to a potential attacker.

Sensitive data can include application-related information, such as session tokens, file names, stack traces, or confidential information, such as passwords, credit card data, sensitive health data, private communications, intellectual property, metadata, the product’s source code, etc.



**6. Local file inclusion**

Local file inclusion vulnerabilities allow an attacker to read (and sometimes execute) files on the victim machine. This can be very dangerous because if the web server is misconfigured and running with high privileges, the attacker may gain access to sensitive information. If the attacker is able to place code on the web server through other means, then they may be able to execute arbitrary commands.



**7. Remote file inclusion**

Remote file inclusion vulnerabilities are easier to exploit but less common. Instead of accessing a file on the local machine, the attacker is able to execute code hosted on their own machine.

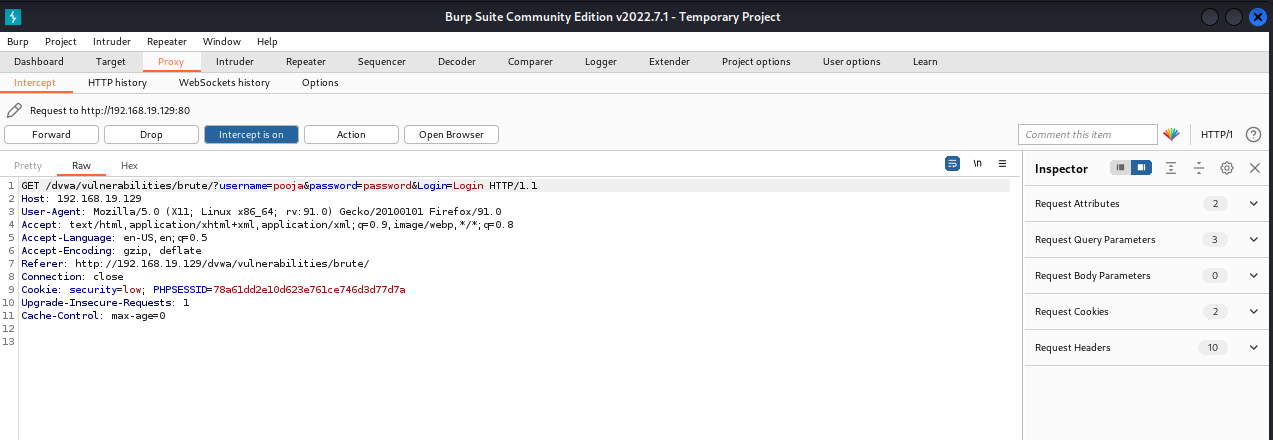
Remote file inclusion (RFI) is an attack targeting [vulnerabilities](https://www.imperva.com/learn/application-security/vulnerability-management/) in web applications that dynamically reference external scripts. The perpetrator’s goal is to exploit the referencing function in an application to upload malware (e.g., [backdoor shells](https://www.imperva.com/learn/application-security/backdoor-shell-attack/)) from a remote URL located within a different domain.

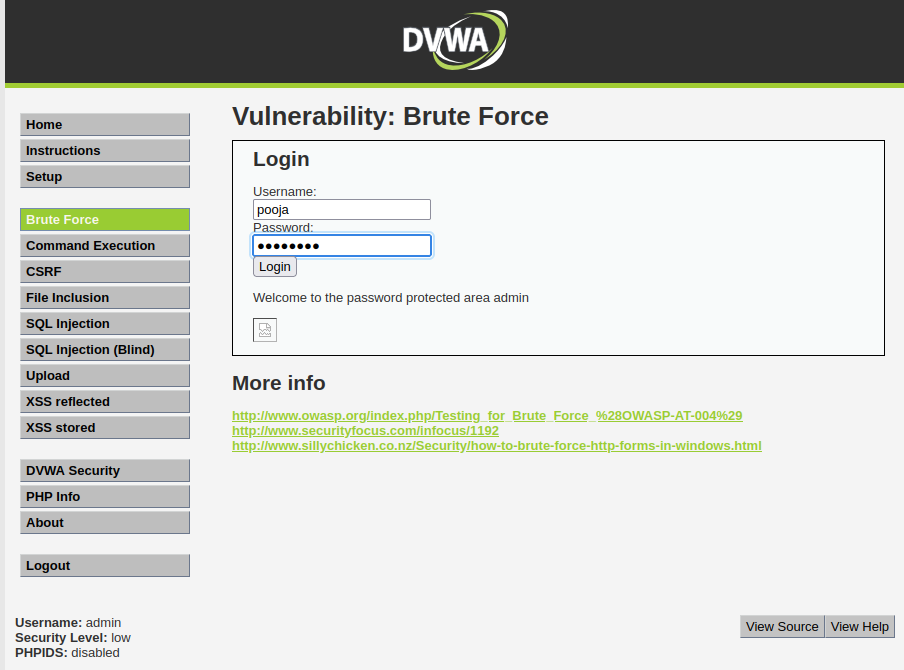


**8. Brute force attack**

A brute force attack is uses a trial-and-error approach to systematically guess login info, credentials, and encryption keys. The attacker submits combinations of usernames and passwords until they finally guess correctly.

A brute force attack is a hacking method that uses trial and error to crack passwords, [login credentials](https://www.fortinet.com/resources/cyberglossary/login-credentials), and encryption keys. It is a simple yet reliable tactic for gaining unauthorized access to individual accounts and organizations’ systems and networks. The hacker tries multiple usernames and passwords, often using a computer to test a wide range of combinations, until they find the correct login information.





**9. Forced browsing vulnerability**

Forced browsing is an attack where the aim is to enumerate and access resources that are not referenced by the application, but are still accessible. Forced browsing attack are the result of a type of security misconfiguration vulnerability. These kind of vulnerabilities occur when insecure configuration or misconfiguration leave web application components open to attack.

**10. Components with known vulnerability**

Using Components with Known Vulnerabilities According to OWASP: Using Components with Known Vulnerabilities Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate server data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine the app.

**11. Html injection**

Hypertext Markup Language (HTML) injection is a technique used to take advantage of non-validated input to modify a web page presented by a web application to its users. Attackers take advantage of the fact that the content of web page is often related to a previous interaction with users. When applications fail to validate user data, an attacker can send HTML- fomatted text to modify site content that gets presented to other users.

