NAME: KEERTHAN*

DATE: 13/03/2023

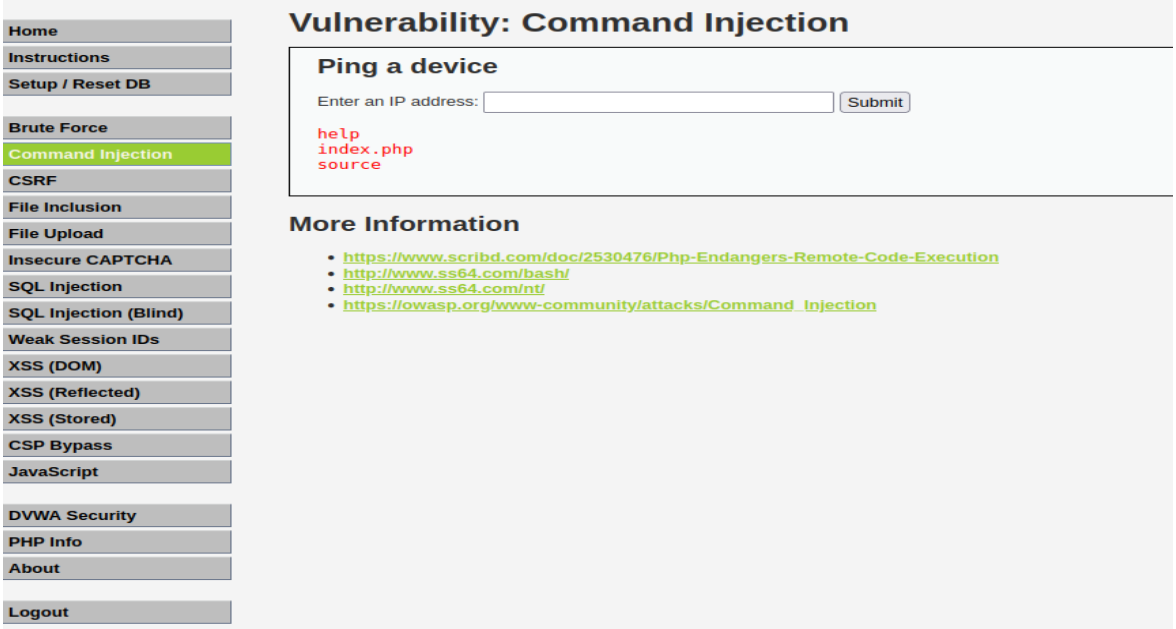
TASK-03

1)Command 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..

Security level: low

Security level: medium

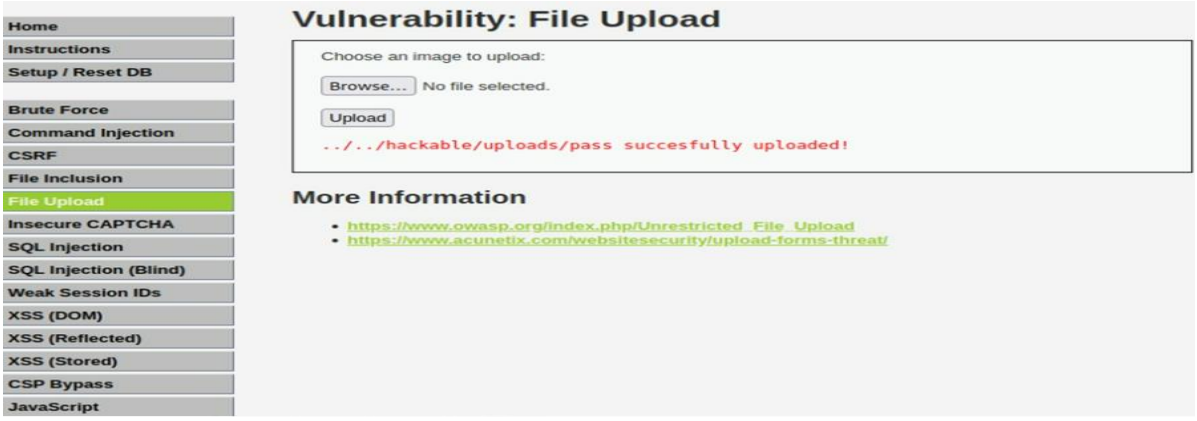
Security level: high

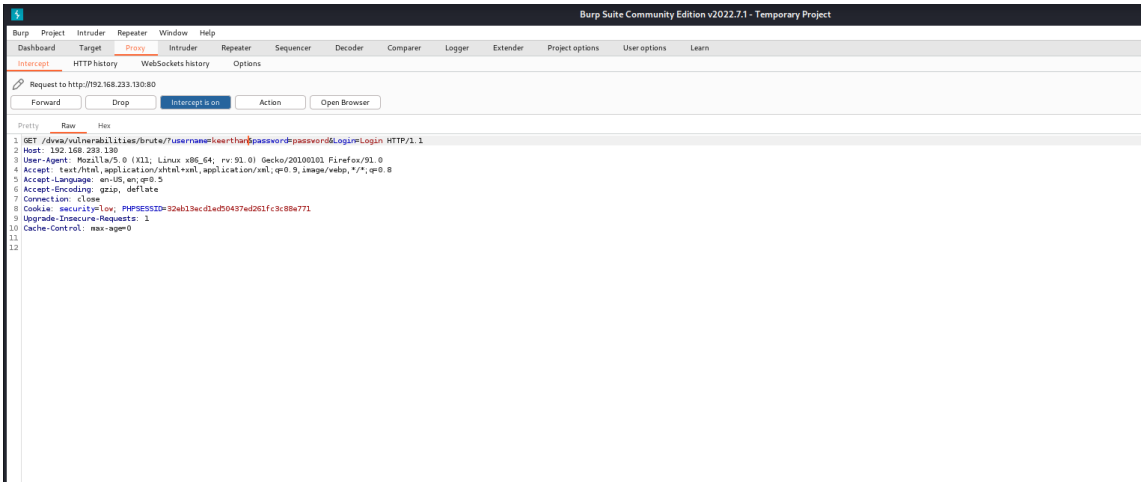


2) File upload vulnerability :

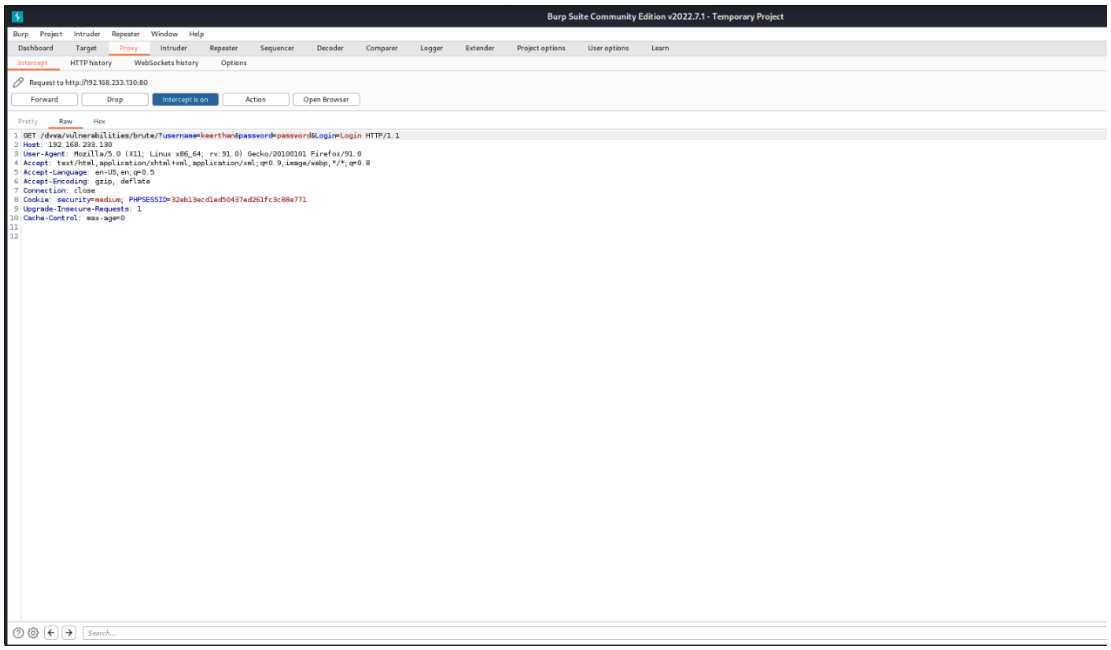
File upload vulnerability refers to a security flaw in web applications that allows attackers to upload and execute malicious files on the server. This type of vulnerability occurs when a web application does not properly validate the file being uploaded, allowing an attacker to upload a file with malicious code.

Security level: low

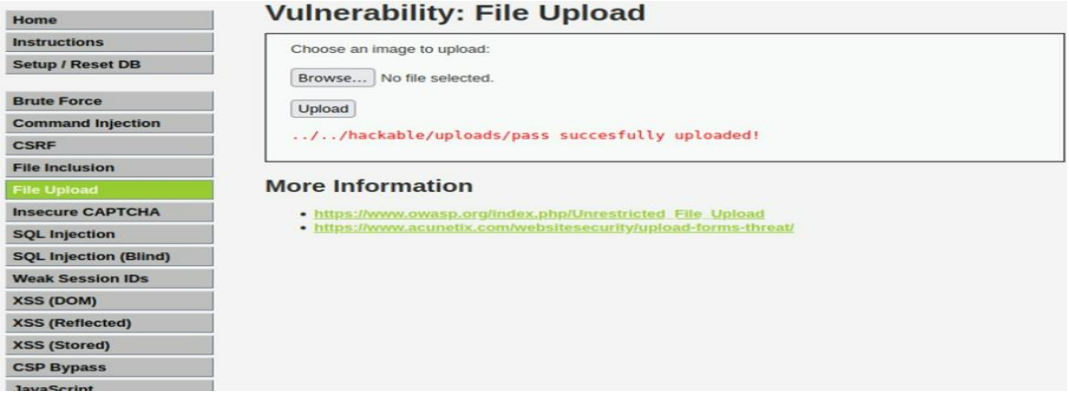


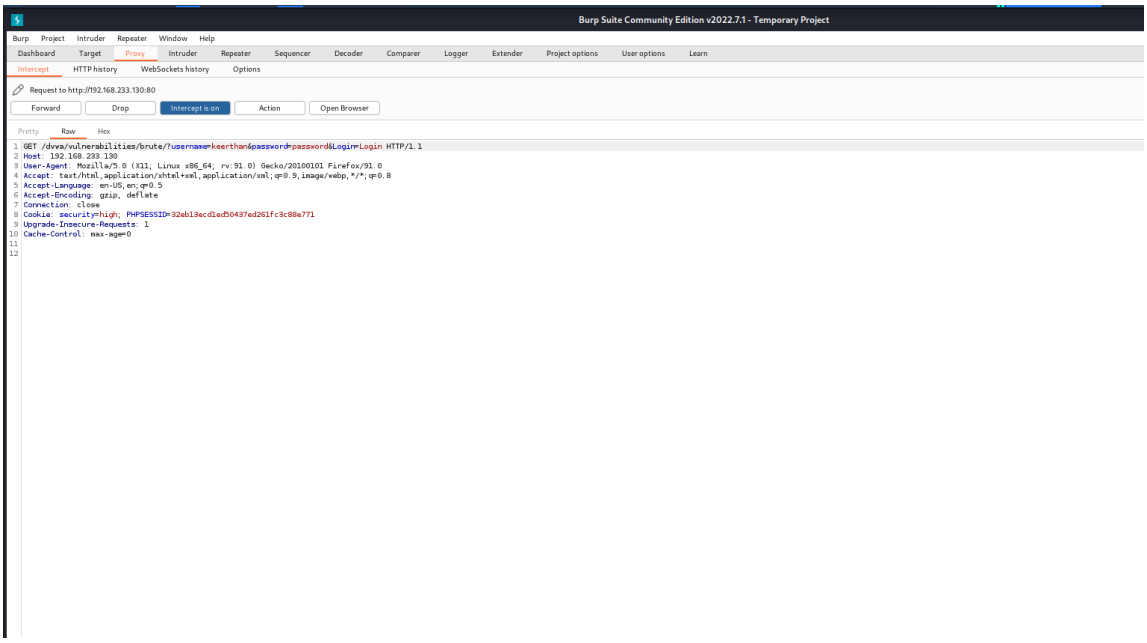


Security level: medium



Security level: high





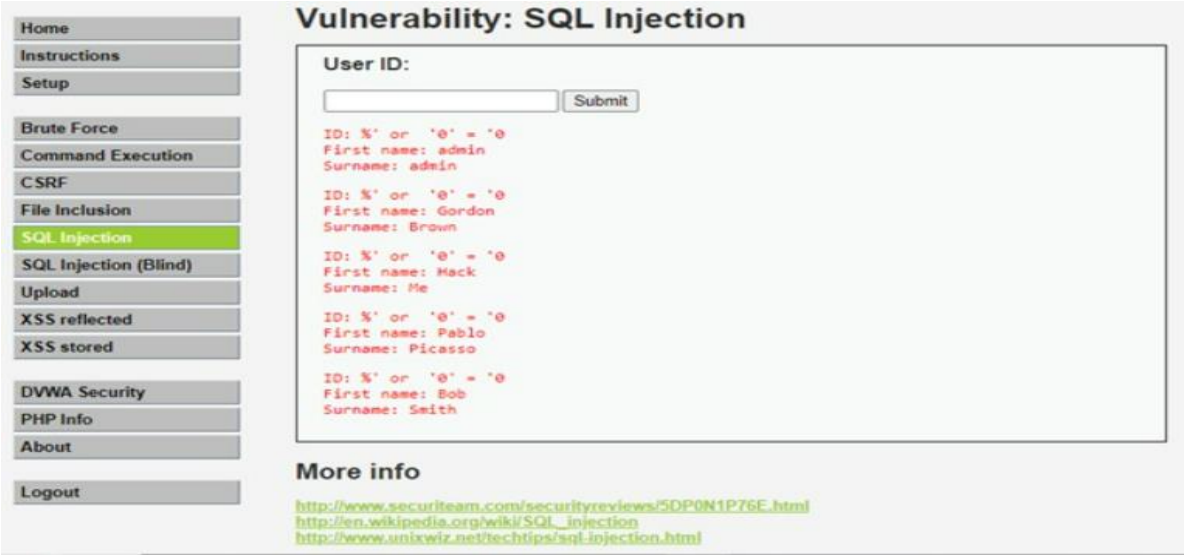
3) Sql Injection vulnerability :

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

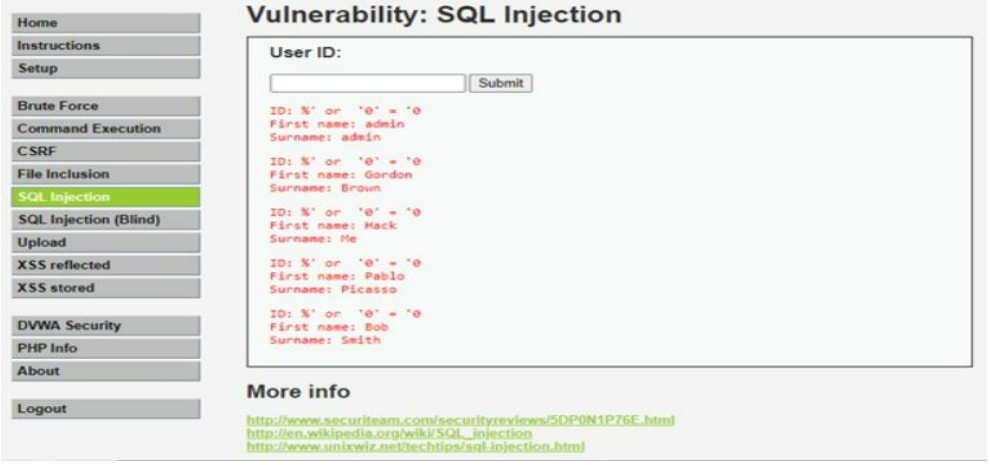
that the application itself is able to access. In many cases, an attacker can modify or delete this data, causing persistent changes to the application's content or behavior.

Security level: medium

Security level: high



Security level: low



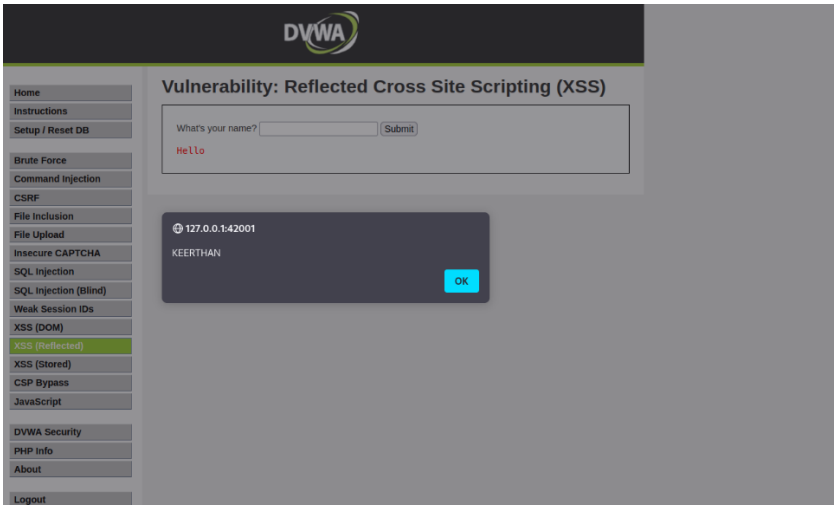
4) Cross site scripting :

Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it.

An attacker can use XSS to send a malicious script to an unsuspecting user. The end user's browser has no way to know that the script should not be trusted, and will execute the script. Because it thinks the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by the browser and used with that site. These scripts can even rewrite the content of the HTML page.

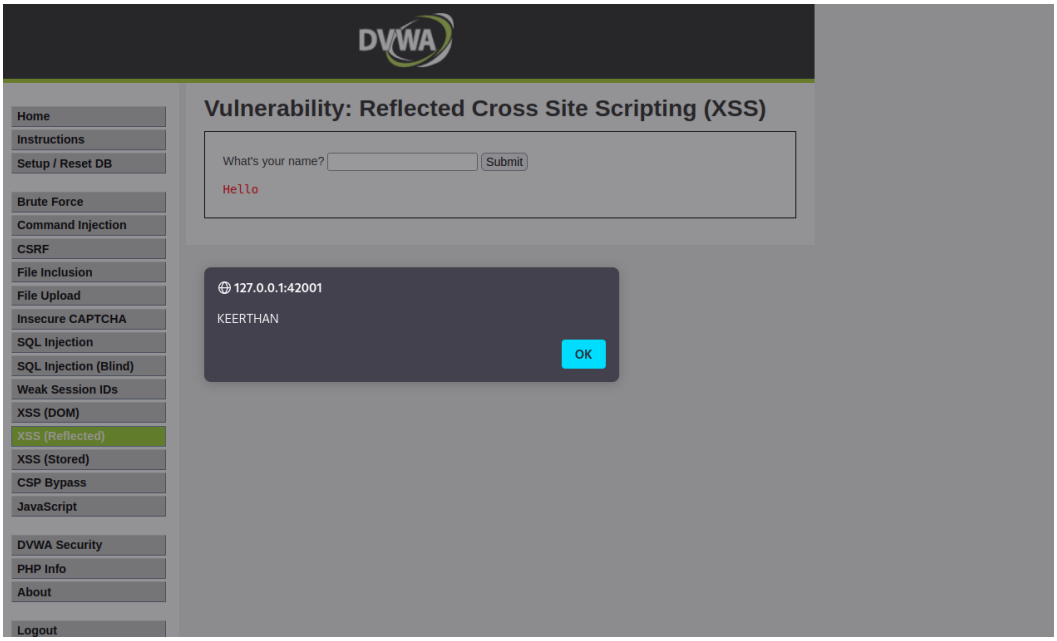
<u>Security level low:</u>

XSS reflected:



Security level: medium

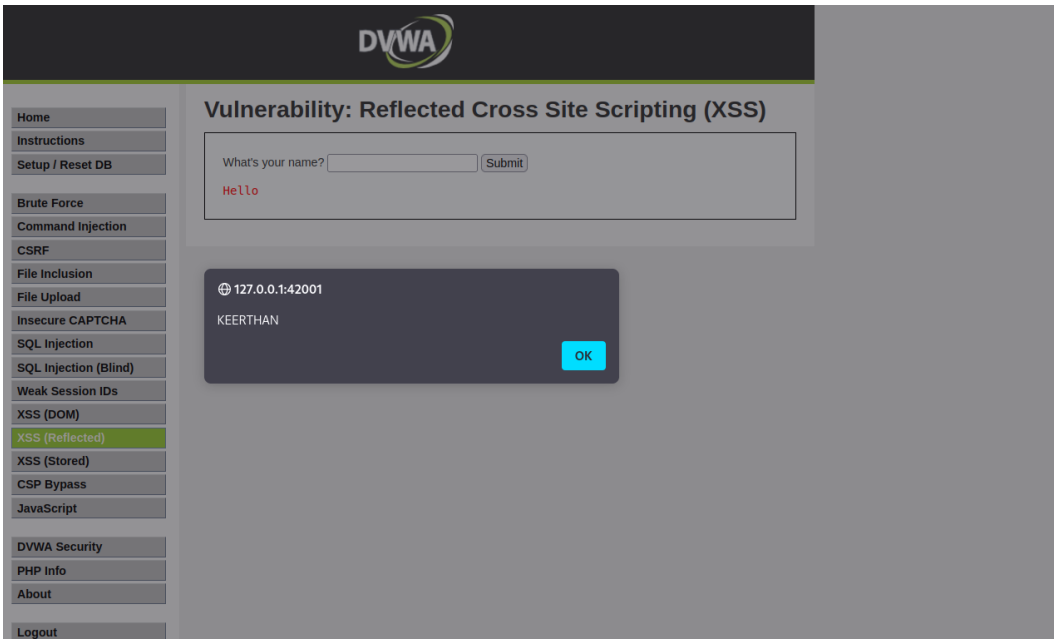
XSS reflected:



XSS stored

Security level: high

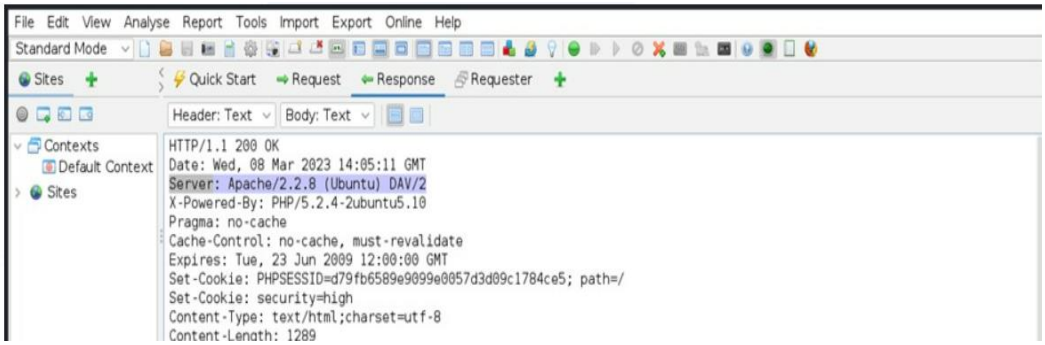
XSS reflected:



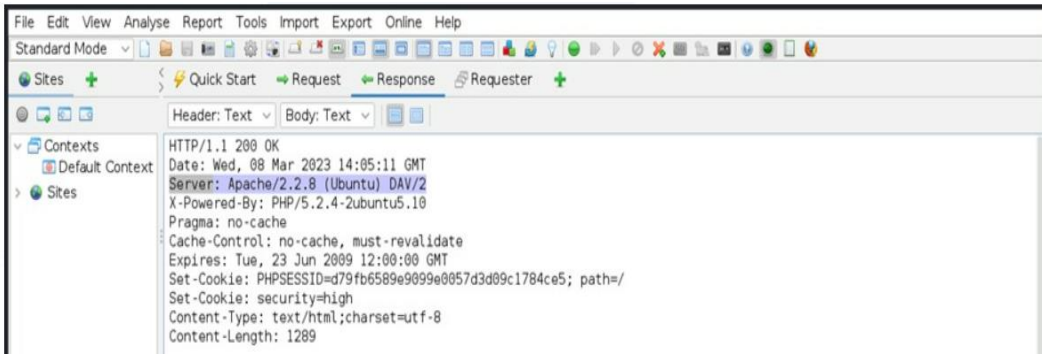
5)Sensitive information disclosure

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, including: Data about other users, such as usernames or financial information.

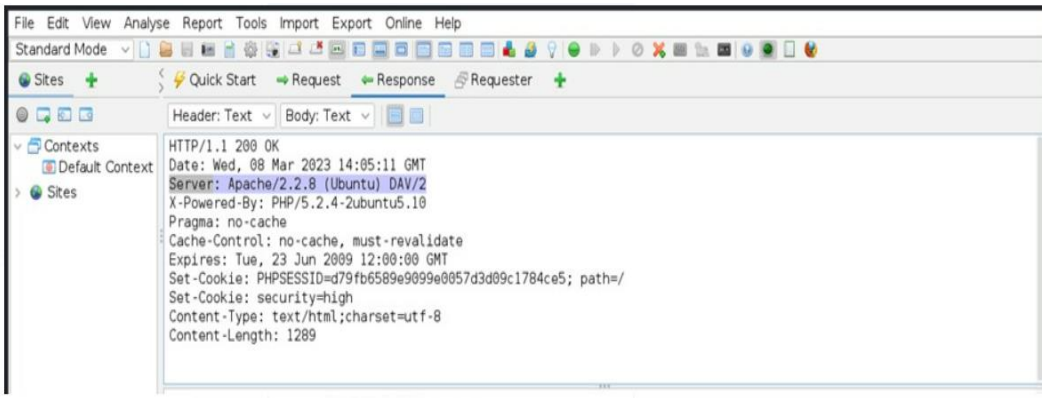
Security level: low



Security level: medium



Security level: high

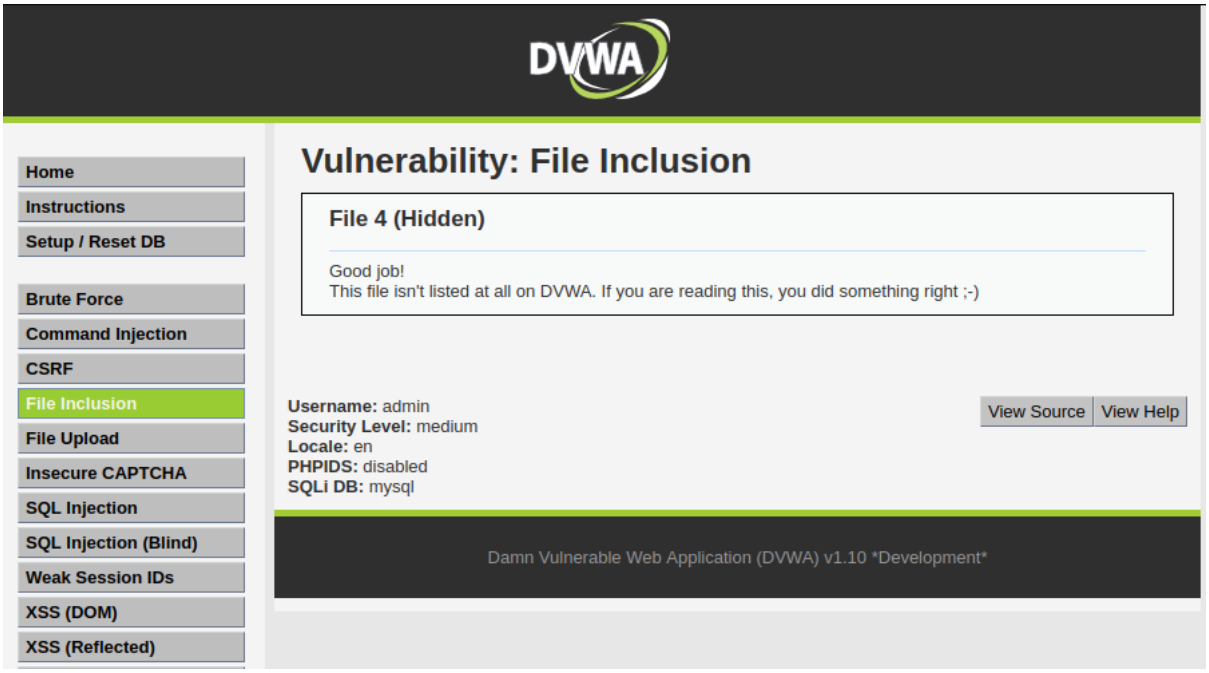


6) Local file inclusion :

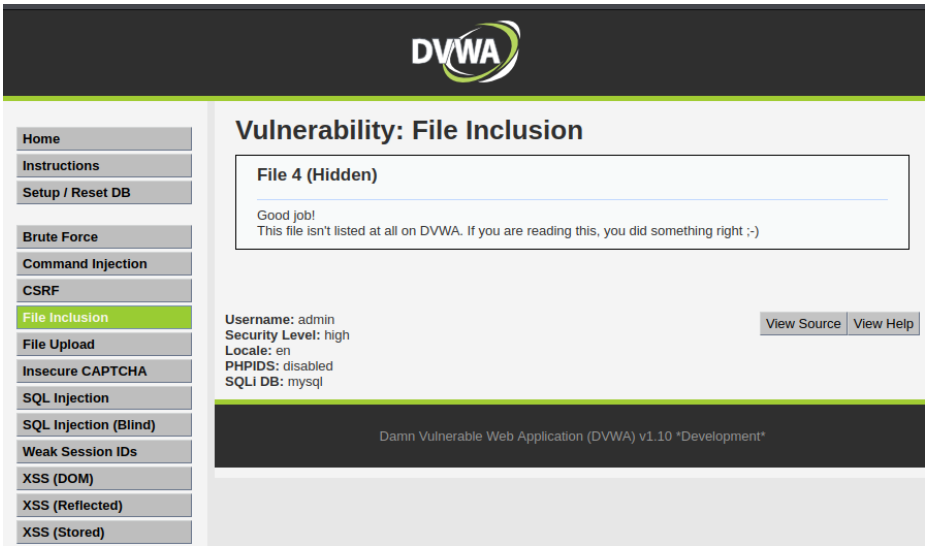
Local file inclusion (also known as LFI) is the process of including files, that are already locally present on the server, through the exploiting of vulnerable inclusion procedures implemented in the application.

Security level: low

Security level: medium



ecurity level: high



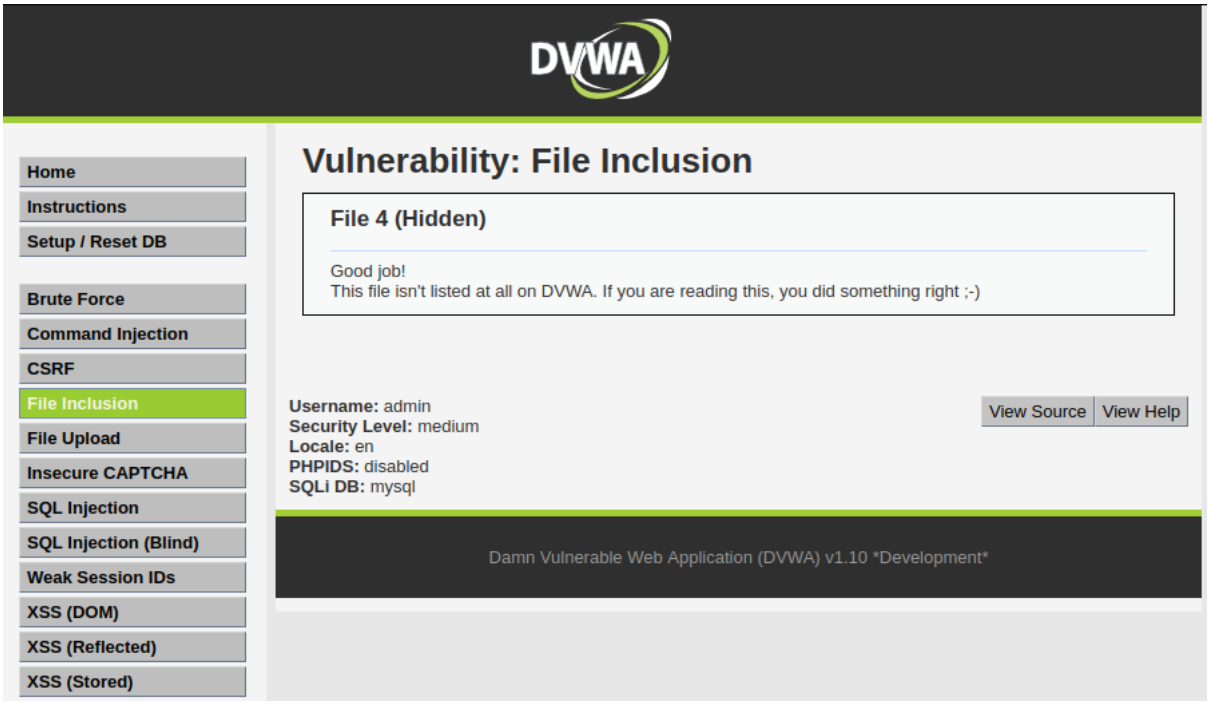
7)Remote file inclusion :

Remote file inclusion (RFI) is an attack targeting vulnerabilities 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) from a remote URL located within a different domain.

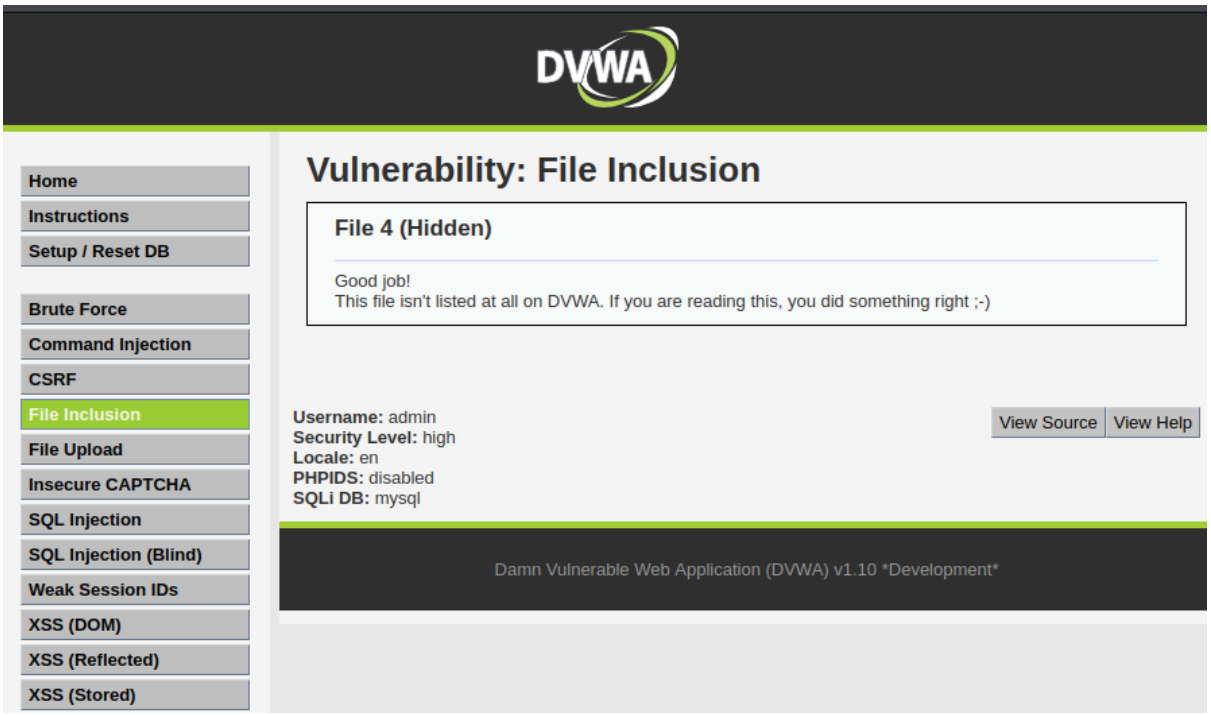
The consequences of a successful RFI attack include information theft, compromised servers and a site takeover that allows for content modification.

Low:

Medium:



High



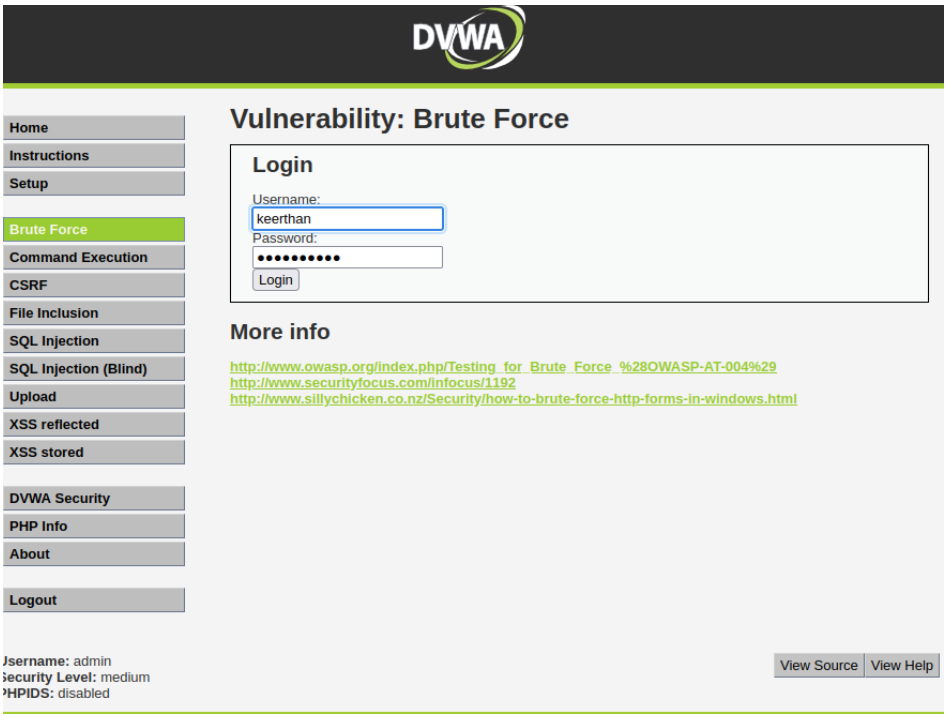
8)Bruteforce attack:

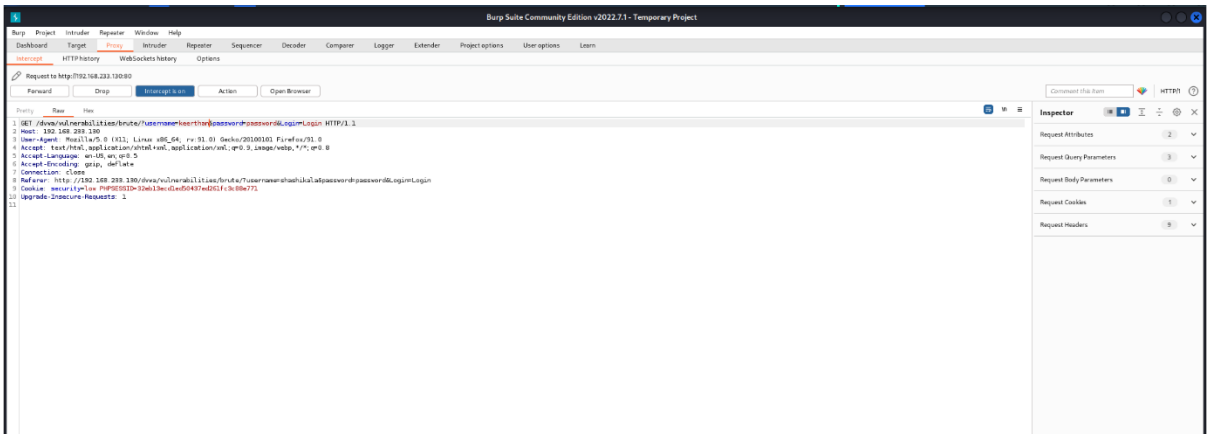
A brute force attack uses trial-and-error to guess login info, encryption keys, or find a hidden web page. Hackers work through all possible combinations hoping to guess correctly.

These attacks are done by ‘brute force’ meaning they use excessive forceful attempts to try and ‘force’ their way into your private account(s).

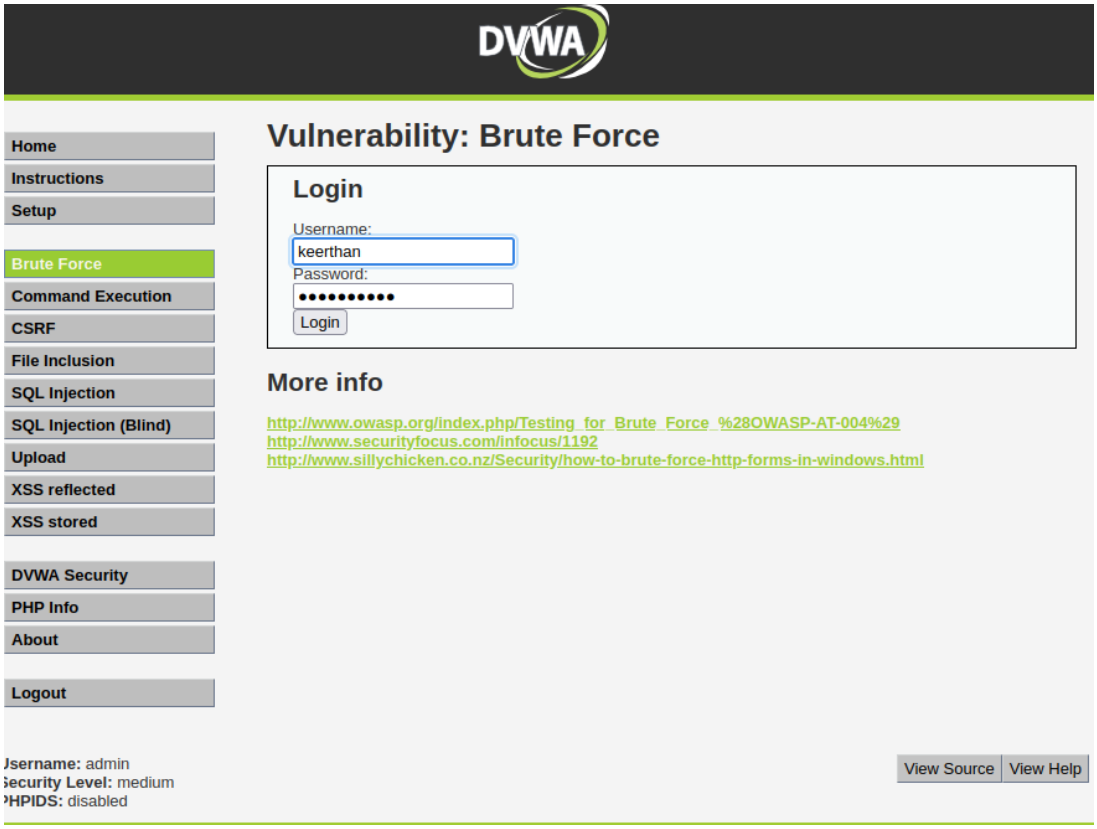
This is an old attack method, but it's still effective and popular with hackers. Because depending on the length and complexity of the password, cracking it can take anywhere from a few seconds to many years.

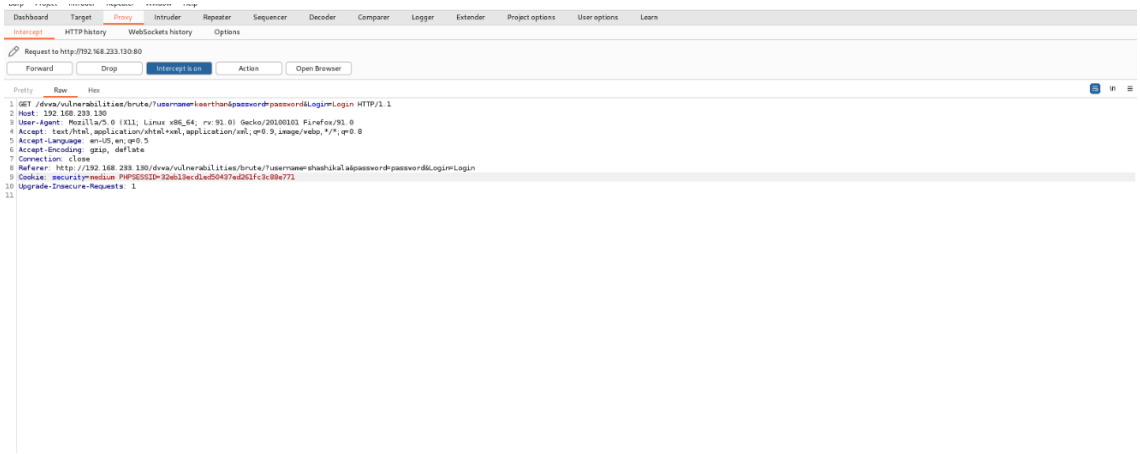
Security level : low



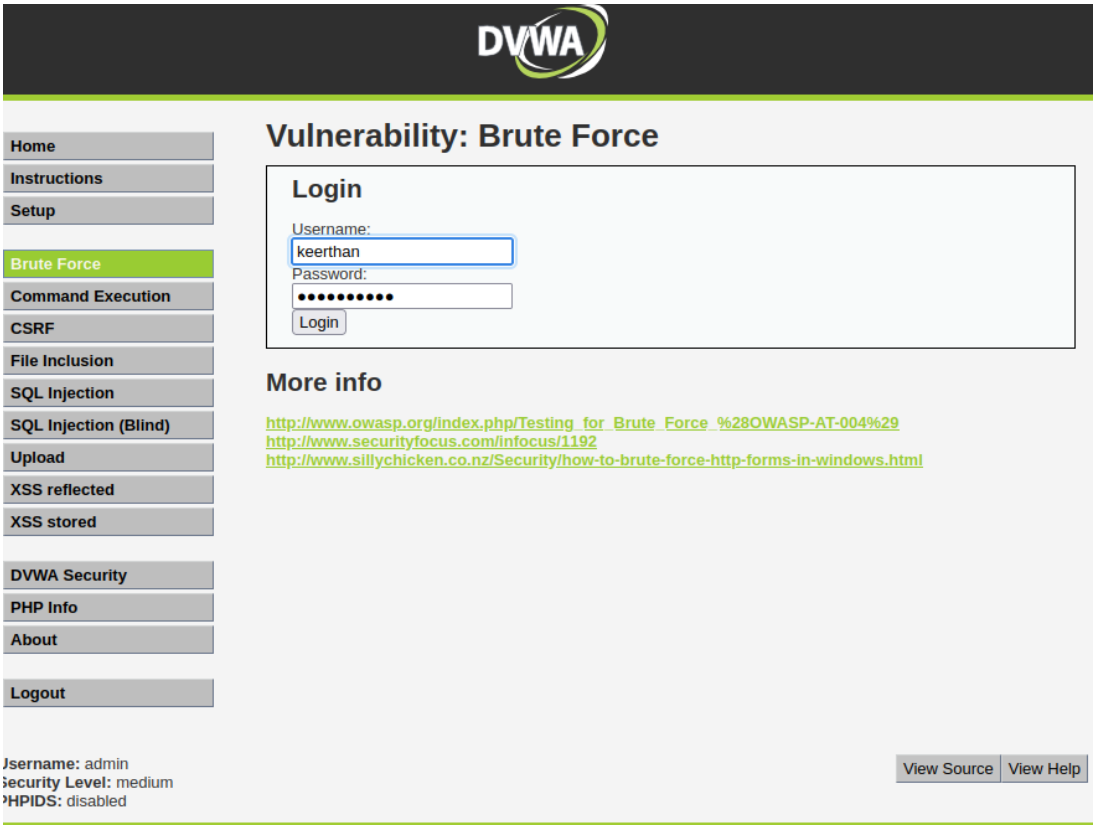


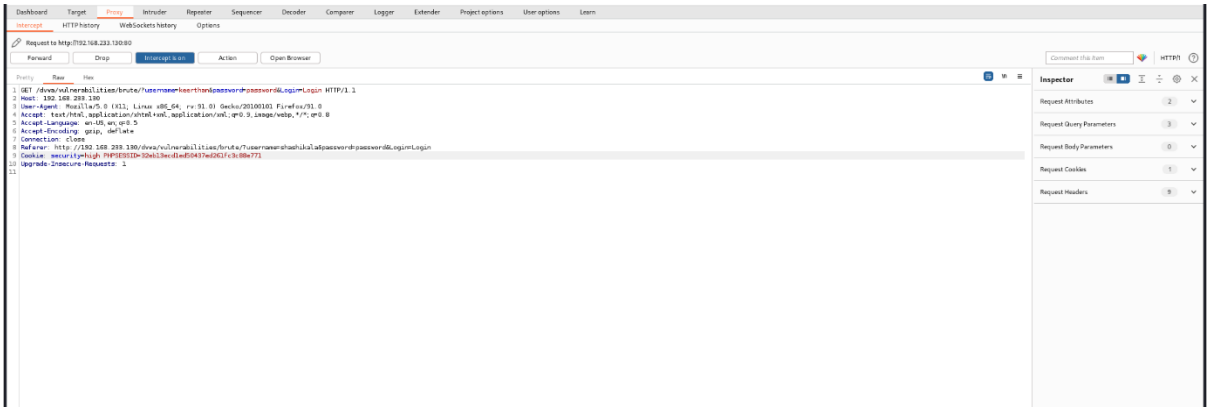
Security level : medium





Security level : high





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. Misconfiguration vulnerabilities may exist in subsystems or software components.

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 takeover.

```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ nmap -sV -p 80 192.168.233.130
Starting Nmap 7.92 ( https://nmap.org ) at 2023-03-15 06:20 EDT
Nmap scan report for 192.168.233.130
Host is up (0.011s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.06 seconds

┌──(kali㉿kali)-[~]
└─$
```

cvedetails.com/vulnerability-list/vendor_id-45/product_id-66/version_id-416233/Apache-Http-Server-2.2.8.html

CVE Details
The ultimate security vulnerability datasource

Apache » Http Server » 2.2.8 * * * : Security Vulnerabilities

Cpe Name:cpe:2.3:a:apache:http_server:2.2.8:*:*:*:*:*:*:*

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2016-4975	93		Http R.Spl.	2018-08-14	2021-06-06	4.3	None	Remote	Medium	Not required	None	Partial	None
Possible CRLF injection allowing HTTP response splitting attacks for sites which use mod_userdir. This issue was mitigated by changes made in 2.4.25 and 2.2.32 which prohibit CR or LF injection into the "Location" or other outbound header key or value. Fixed in Apache HTTP Server 2.4.25 (Affected 2.4.1-2.4.23). Fixed in Apache HTTP Server 2.2.32 (Affected 2.2.0-2.2.31).														
2	CVE-2014-0231	399		DoS	2014-07-20	2021-06-06	5.0	None	Remote	Low	Not required	None	None	Partial
The mod_cgid module in the Apache HTTP Server before 2.4.10 does not have a timeout mechanism, which allows remote attackers to cause a denial of service (process hang) via a request to a CGI script that does not read from its stdin file descriptor.														
3	CVE-2013-5704			Bypass	2014-04-15	2022-04-14	5.0	None	Remote	Low	Not required	None	Partial	None
The mod_headers module in the Apache HTTP Server 2.2.22 allows remote attackers to bypass "RequestHeader unset" directives by placing a header in the trailer portion of data sent with chunked transfer coding. NOTE: the vendor states "this is not a security issue in httpd as such."														
4	CVE-2012-4558	79		XSS	2013-02-26	2021-06-06	4.3	None	Remote	Medium	Not required	None	Partial	None
Multiple cross-site scripting (XSS) vulnerabilities in the balancer_handler function in the manager interface in mod_proxy_balancer.c in the mod_proxy_balancer module in the Apache HTTP Server 2.2.x before 2.2.24-dev and 2.4.x before 2.4.4 allow remote attackers to inject arbitrary web script or HTML via a crafted string.														
5	CVE-2012-3499	79		XSS	2013-02-26	2021-06-06	4.3	None	Remote	Medium	Not required	None	Partial	None
Multiple cross-site scripting (XSS) vulnerabilities in the Apache HTTP Server 2.2.x before 2.2.24-dev and 2.4.x before 2.4.4 allow remote attackers to inject arbitrary web script or HTML via vectors involving hostnames and URIs in the (1) mod_imagemap, (2) mod_info, (3) mod_ldap, (4) mod_proxy_ftp, and (5) mod_status modules.														
6	CVE-2012-2687	79		XSS	2012-08-22	2021-06-06	2.6	None	Remote	High	Not required	None	Partial	None
Multiple cross-site scripting (XSS) vulnerabilities in the make_variant_list function in mod_negotiation.c in the mod_negotiation module in the Apache HTTP Server 2.4.x before 2.4.3, when the MultiViews option is enabled, allow remote attackers to inject arbitrary web script or HTML via a crafted filename that is not properly handled during construction of a variant list.														
7	CVE-2011-4415	20		DoS	2011-11-08	2012-07-03	1.2	None	Local	High	Not required	None	None	Partial
The ap_pregsub function in server/util.c in the Apache HTTP Server 2.0.x through 2.0.64 and 2.2.x through 2.2.21, when the mod_setenvif module is enabled, does not restrict the size of values of environment variables, which allows local users to cause a denial of service (memory consumption or NULL pointer dereference) via a .htaccess file with a crafted SetEnvIf directive, in conjunction with a crafted HTTP request														

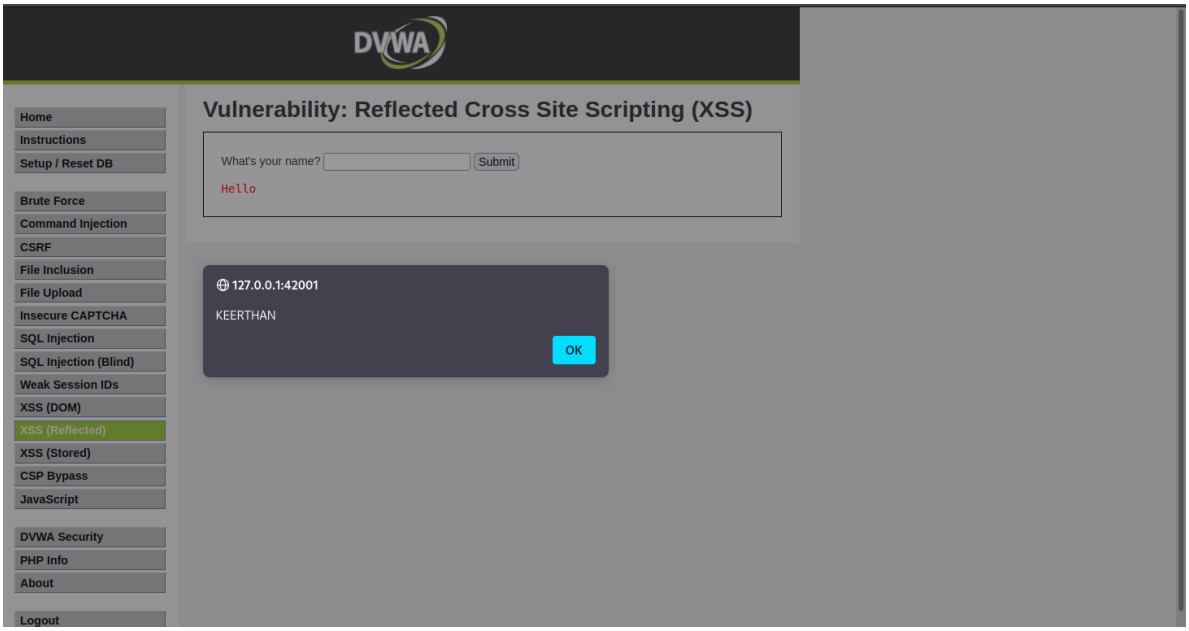
11)Html injection:

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.

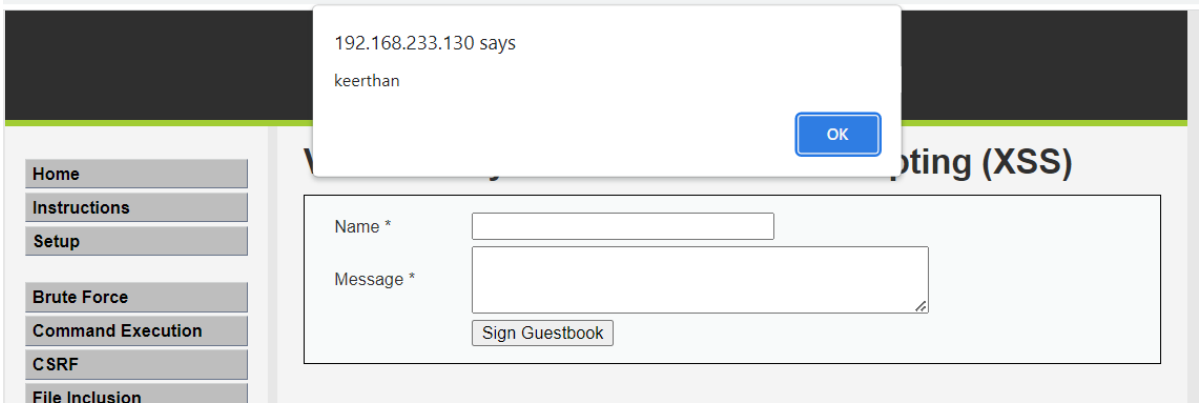
Attackers often inject malicious JavaScript, VBScript, ActiveX, and/or HTML into vulnerable applications to deceive the user in order to gather data from them. Cross-site scripting (XSS) vulnerabilities can be used by attackers to bypass authentication controls there by gaining access to sensitive data on your system. Well crafted malicious code can even help the attacker gain access to the entire system.

<u>Security level low:</u>

XSS reflected:

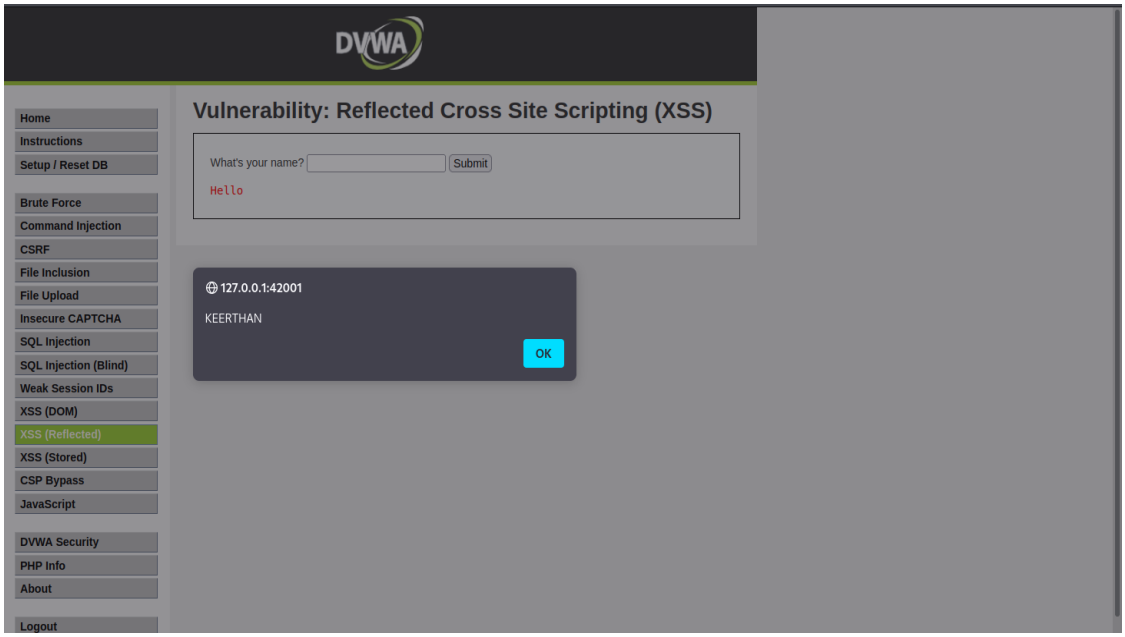


XSS STORED:

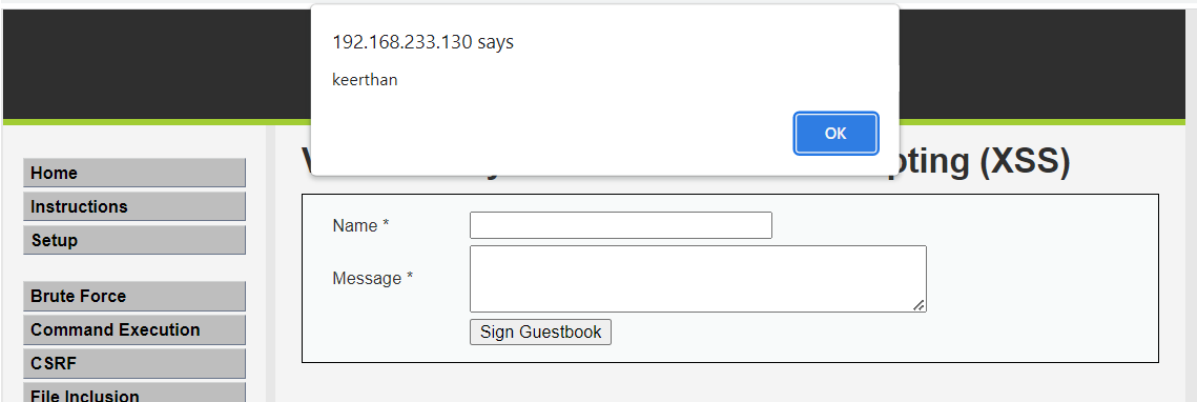


Security level: medium

XSS reflected:

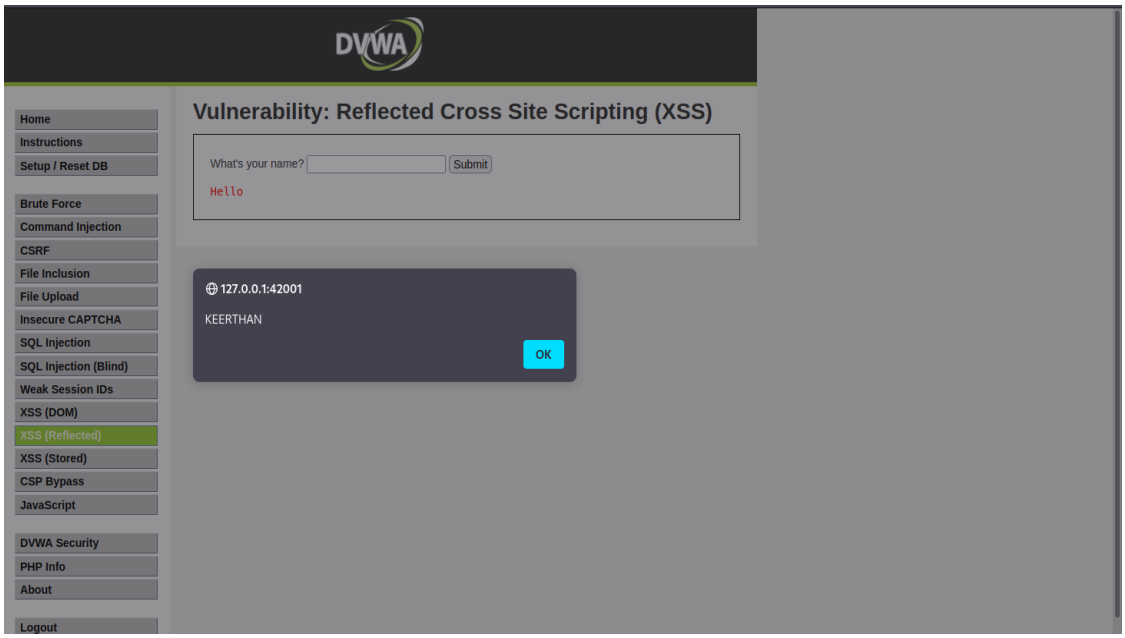


XSS STORED:



Security level: high

XSS reflected:



XSS STORED: