



PENETRATION TEST REPORT

EXPLOITING VULNERABILITIES IN DVWA

PRESENTER:

Lingampally Anjali

CSE-Cybersecurity

Institute of Aeronautical Engineering

Lingampally Anjali

CSE-Cybersecurity undergrad student
at the Institute of Aeronautical
Engineering.

anjaliraolingampalli@gmail.com

+91 9490403628

:

Table of Contents:

- Executive Summary
- Severity Scale
- Information Gathering
- Exploitation
- Mitigation
- Tools Utilized
- References
- Conclusion

:

Executive Summary:

The penetration testing initiative was conducted with the primary objective of evaluating the security posture of our organization's systems, networks, and applications. This strategic assessment aimed to identify and address potential vulnerabilities that could be exploited by malicious actors, ultimately enhancing our overall cybersecurity resilience.

DVWA, or Damn Vulnerable Web Application, is a deliberately insecure web application designed for educational and testing purposes. It serves as a practical tool for security professionals, ethical hackers, and developers to gain hands-on experience in identifying, exploiting, and mitigating common web application vulnerabilities.

:

SEVERITY SCALE

CRITICAL Severity Issue: A "Critical Severity Issue" is a severe and potentially damaging vulnerability discovered during the assessment. It signifies a significant security weakness attackers could exploit to compromise the system or network. Addressing critical severity issues promptly is crucial to enhancing the overall security posture and preventing potential security breaches.

HIGH Severity issue: A "High Severity Issue" denotes a serious vulnerability that, while not as critical as a critical severity issue, still poses a substantial risk to the security of the system or network. Addressing high-severity issues is important to enhance overall security and reduce the potential for exploitation by malicious actors. Though not an immediate threat, these issues should be addressed on time to mitigate potential security risks.

MEDIUM Severity Issue: A "Medium Severity Issue" refers to a significant vulnerability that may not pose an immediate or critical threat to the security of the system or network. While not as serious as high or critical severity issues, addressing medium severity issues is important for maintaining a robust security

:

posture. These issues should be resolved to prevent potential exploitation or to limit the cumulative impact when combined with other vulnerabilities.

LOW Severity Issue: A "Low Severity Issue" in penetration testing indicates a relatively minor vulnerability and may not present an immediate or significant threat to the security of the system or network. While these issues are not as critical as higher severity ones, they should still be addressed to maintain a comprehensive security stance.

INFORMATION GATHERING:

TARGET: 10.0.2.4

I used the “nmap -sV -A 10.0.2.4” command to find the open ports.

```
(kali㉿kali)-[~]
└─$ nmap -sV -A 10.0.2.4
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-05 04:30 EST
Nmap scan report for 10.0.2.4
Host is up (0.00062s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-syst:
|   STAT: 220 PROFTPD-2.3.4 Server (vsFTPD 2.3.4 - secure, fast, stable)
|   FTP server status:
|     Connected to 10.0.2.15
|     Logged in as ftp
|     TYPE: ASCII
|     No session bandwidth limit
|     Session timeout in seconds is 300
|     Control connection is plain text
|     Data connections will be plain text
|     vsFTPD 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|   2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY,
  ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_ssl-date: 2024-01-05T09:32:28+00:00; +22s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|_high  SSL2_DES_192_EDE3_CBC_WITH_MD5
53/tcp    open  domain       ISC BIND 9.4.2
| dns-nsid:
|   bind.version: 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp   open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version  port/proto  service
|   100000  2          111/tcp    rpcbind
```

```
|_http-title: Metasploitable2 - Linux utilities/sql/?id=1&Submit=Submit#    90% ⭐
111/tcp open  rpcbind      2 (RPC #100000)
| rpcinfo:
|   program version  port/proto  service
|     100000  2          111/tcp    rpcbind
|     100000  2          111/udp    rpcbind
|     100003  2,3,4     2049/tcp   nfs
|     100003  2,3,4     2049/udp   nfs
|     100005  1,2,3     40908/udp mounted
|     100005  1,2,3     57069/tcp mounted
|     100021  1,3,4     37852/udp nlockmgr
|     100021  1,3,4     44896/tcp nlockmgr
|     100024  1          33408/tcp status
|     100024  1          54501/udp status
139/tcp open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  EDG        Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp open  exec       netkit-rsh rexecd
513/tcp open  login      OpenBSD or Solaris rlogind
514/tcp open  shell?     rlogin
1099/tcp open  java-rmi   GNU Classpath grmiregistry
1524/tcp open  bindshell  Metasploitable root shell
2049/tcp open  nfs        2-4 (RPC #100003)
2121/tcp open  ftp        ProFTPD 1.3.1
3306/tcp open  mysql     MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 15
|   Capabilities flags: 43564
|   Some Capabilities: SupportsTransactions, Support41Auth, LongColumnFlag, SupportsCompression, SwitchToSSLAfterHandshake, Speaks41ProtocolNew, ConnectWithDatabase
|   Status: Autocommit
|   Salt: oI^~}yi"hg06_]63;o@0
5432/tcp open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2024-01-05T09:32:16+00:00; +22s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=0COSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
| Not valid after: 2010-04-16T14:07:45
|_View Source
5900/tcp open  vnc        VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|     VNC Authentication (2)
6000/tcp open  X11        (access denied)
6667/tcp open  irc        UnrealIRCd
8009/tcp open  ajp13     Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http       Apache Tomcat/Coyote JSP engine 1.1
```

DVWA Vulnerability Scanning

EXPLOITATION:

Vulnerability I: Command Execution

:

VULNERABILITY EXPLOITED SEVERITY: LOW

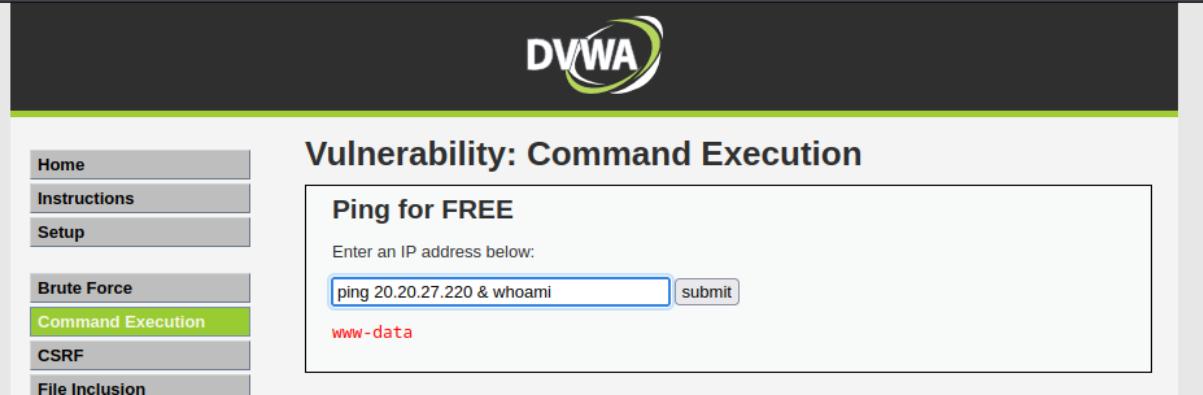
Command execution vulnerabilities occur when an application allows an attacker to execute arbitrary commands on a host OS.

I entered an IP address in the search bar and used the ls command.

The screenshot shows the DVWA Command Execution interface. On the left, there's a sidebar with links: Home, Instructions, Setup, Brute Force, Command Execution (which is highlighted in green), CSRF, File Inclusion, and SQL Injection. The main area has a title 'Vulnerability: Command Execution' and a section titled 'Ping for FREE'. It says 'Enter an IP address below:' and contains a text input field with 'ping 127.0.0.1 & ls' and a 'submit' button. Below the input field, there are three red links: 'help', 'index.php', and 'source'.

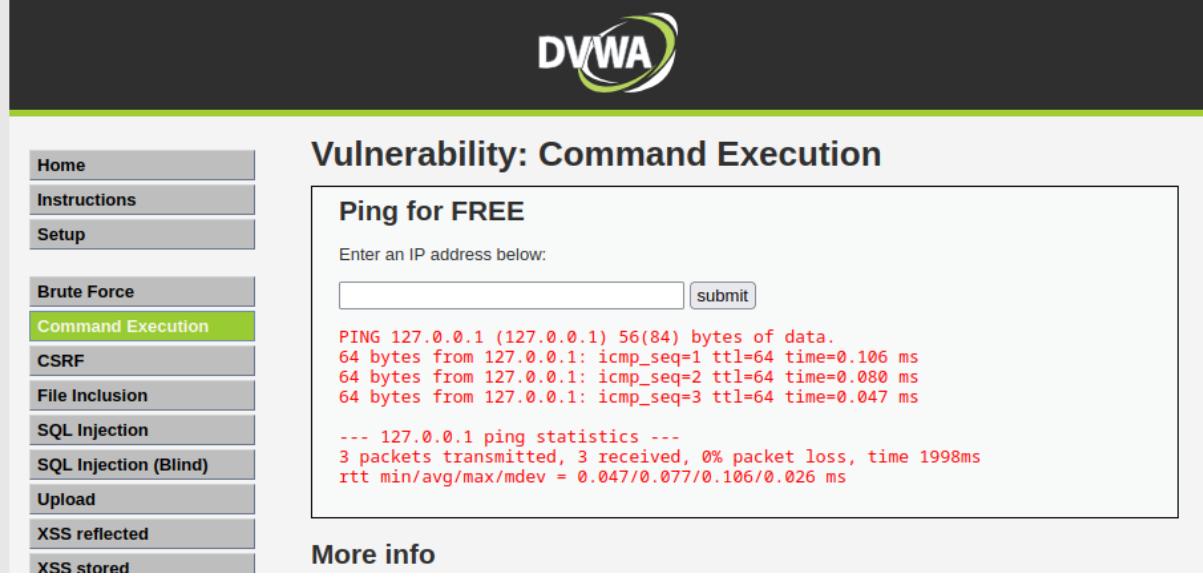
- ls command is used to list the files and directories in a directory.
- As you can see from the picture above, the command execution was successful, server returned the files.
- The next one I used was Whoami.
- It returns the username associated with the current user who is running the command.

:



The screenshot shows the DVWA Command Execution page. The left sidebar has links for Home, Instructions, Setup, Brute Force, Command Execution (which is highlighted in green), CSRF, and File Inclusion. The main content area title is "Vulnerability: Command Execution". A section titled "Ping for FREE" contains a form with a text input field containing "ping 20.20.27.220 & whoami" and a "submit" button. Below the form, the output "www-data" is displayed.

- It gave the username associated with the IP address.



This screenshot is identical to the one above, showing the DVWA Command Execution page. The "Command Execution" link in the sidebar is highlighted. The main content area shows the "Ping for FREE" section with the same input and output. The output now includes the results of the ping command: "PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data. 64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.106 ms 64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.080 ms 64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.047 ms --- 127.0.0.1 ping statistics --- 3 packets transmitted, 3 received, 0% packet loss, time 1998ms rtt min/avg/max/mdev = 0.047/0.077/0.106/0.026 ms".

Vulnerability II: Cross-Site Request Forgery(CSRF)

VULNERABILITY EXPLOITED SEVERITY: LOW

CSRF is a type of security vulnerability that occurs when an attacker tricks a user's browser into making an

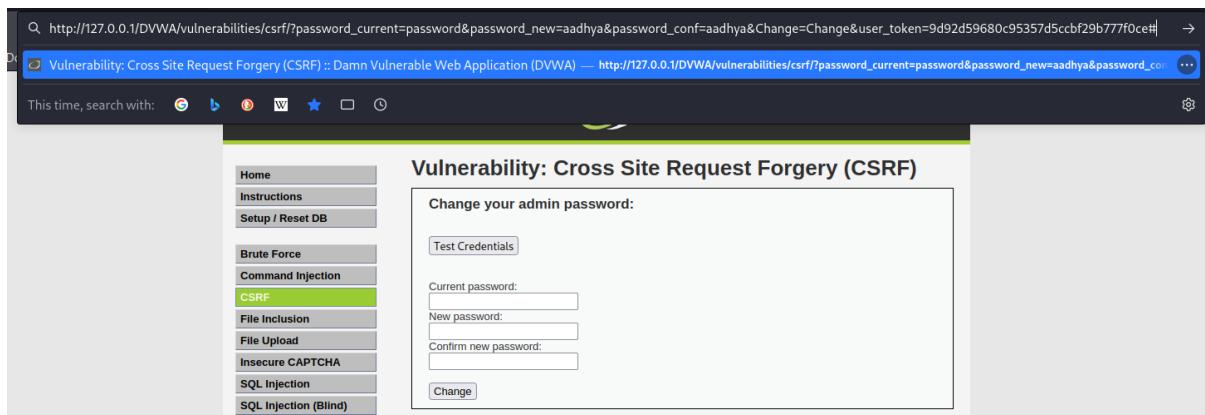
:

unauthorized request on behalf of the user. This can lead to actions being performed on a website without the user's knowledge.

The screenshot shows the DVWA application interface. On the left, a sidebar lists various vulnerabilities: 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, Authorisation Bypass, Open HTTP Redirect, DVWA Security, PHP Info, About, and Logout. The 'CSRF' option is highlighted. The main content area displays the 'Vulnerability: Cross Site Request Forgery (CSRF)' page. It contains a form titled 'Change your admin password:' with fields for 'Current password:', 'New password:', and 'Confirm new password:', and a 'Change' button. Below this is a note about SameSite cookies and browser defaults. A 'Test Credentials' window is overlaid on the main page, showing a 'Test Credentials' form with 'Username' and 'Password' fields and a 'Login' button. The note in the main page states: 'As an alternative to the normal attack of hosting the malicious URL on your own server, you can use other vulnerabilities in this app to store them, the Stored XSS vulnerability is a good example.' At the bottom, there's a link to 'More Information' with three links: <https://owasp.org/www-community/attacks/csrf>, <http://www.cgisecurity.com/csrf-faq.html>, and https://en.wikipedia.org/w/index.php?title=Cross-site_request_forgery&oldid=95357d5ccbf29b777f0ce#. A message at the bottom says 'CSRF token is incorrect'.

✓ I changed the password and copied the URL.

http://127.0.0.1/DVWA/vulnerabilities/csrf/?password_current=password&password_new=aadhya&password_conf=aadhya&Change=Change&user_token=9d92d59680c95357d5ccbf29b777f0ce#



- ✓ I sent this URL to someone and if they click this URL without their knowledge their password changes.

Vulnerability III: SQL Injection:

VULNERABILITY EXPLOITED SEVERITY: LOW

- ✓ SQL injection vulnerabilities occur when a web application allows untrusted user input directly incorporated into SQL queries without proper validation or sanitization.
- ✓ This oversight can lead to attackers manipulating the SQL queries in unexpected ways, potentially compromising the security of the application and its associated database.

EG: An attacker might input something like ' OR '1'='1'; -- into a login form, manipulating the SQL query to always return true, allowing unauthorized access.

:

Vulnerability: SQL Injection

User ID:


```
ID: 1' union select user,password from users#
First name: admin
Surname: admin

ID: 1' union select user,password from users#
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 1' union select user,password from users#
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: 1' union select user,password from users#
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 1' union select user,password from users#
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1' union select user,password from users#
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

Vulnerability IV: XXS(Reflected)

VULNERABILITY EXPLOITED SEVERITY: LOW

- ✓ XSS is a security vulnerability that allows attackers to inject malicious scripts into web pages viewed by other users. In the case of reflected XSS, the injected script is part of the request (e.g., in the URL), and it gets reflected in the response.
- ✓ An attacker can craft a URL containing a script payload. If the application fails to properly sanitize or validate user inputs, the script may be executed when the URL is visited.

:

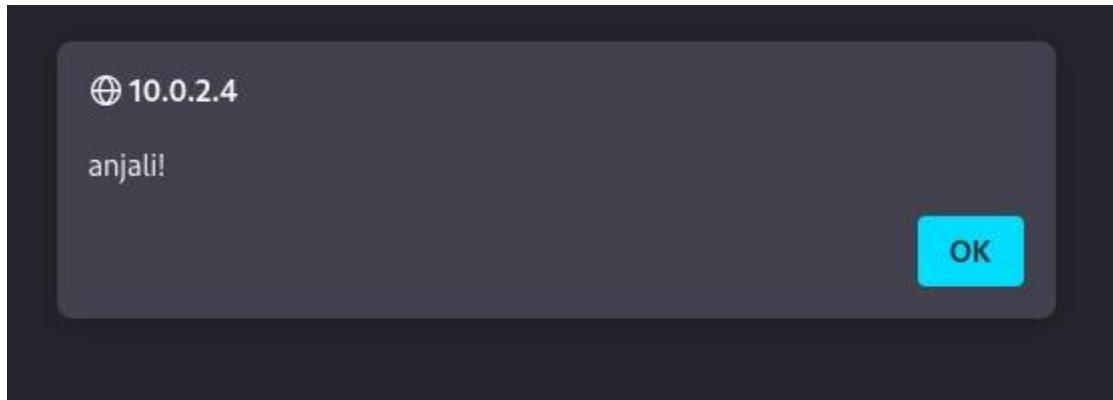
- Example payload:

```
http://example.com/page?name=<script>alert('anjali')</script>
```

Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

Hello



Vulnerability V: XXS(Stored)

**VULNERABILITY EXPLOITED SEVERITY:
LOW**

- ✓ Attackers inject malicious scripts into persistent storage (like a database). When other users retrieve the data, the script is executed.
- Example payload in a comment form:
`<script>alert('wow') </script>`

The screenshot shows the DVWA (Damn Vulnerable Web Application) interface. On the left, a sidebar lists various security modules: Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflector, and XSS stored. The 'XSS stored' module is currently selected and highlighted in green. The main content area is titled 'Vulnerability: Stored Cross Site Scripting (XSS)'. It contains a form with fields for 'Name' (containing 'hi') and 'Message' (containing '<script>alert("wow")</script>'). Below the form, two messages are displayed: one from 'test' with message 'This is a test comment.' and another from 'hi' with message 'hello'. A modal dialog box is overlaid on the page, containing the text '10.0.2.4' with a globe icon, 'WOW', and an 'OK' button. At the bottom of the page, there is user information ('Username: admin', 'Security Level: low', 'PHPIDS: disabled'), and links for 'View Source' and 'View Help'. The footer of the page reads 'Damn Vulnerable Web Application (DVWA) v1.0.7'.

MITIGATION

Mitigating vulnerabilities is a crucial aspect of maintaining a secure and resilient IT environment.

- ✓ Vulnerability Scanning
- ✓ Least Privilege Principle
- ✓ Web Application Security
- ✓ Security Awareness Training
- ✓ Encryption
- ✓ Multi-Factor Authentication (MFA)

:

TOOLS UTILIZED:

Nmap:

- ✓ Nmap, short for "Network Mapper," is a powerful open-source tool used for network discovery and security auditing.
- ✓ It is designed to explore networks, identify hosts, services, and open ports, and create a map of the network topology.
- ✓ Nmap is widely used by network administrators, security professionals, and penetration testers to assess the security of computer networks.

<https://nmap.org/download#windows>

Kali Linux:

- ✓ Kali Linux is a specialized Linux distribution designed for penetration testing, ethical hacking, and security auditing.
- ✓ It provides a wide array of tools and utilities that make it a go-to platform for cybersecurity professionals, penetration testers, and ethical hackers.

<https://www.kali.org/>

:

REFERENCES:

Nmap:

<https://www.geeksforgeeks.org/nmap-command-in-linux-with-examples/>

DVWA:

<https://securingninja.com/dvwa-hacking-tutorial/>

CONCLUSION:

In conclusion, penetration testing is a vital and proactive approach to identifying and addressing security vulnerabilities within an organization's systems, networks, and applications. This process involves simulating real-world cyberattacks to assess the effectiveness of existing security measures and discover potential weaknesses.

Key points to consider regarding penetration testing:

:

- Identification of Vulnerabilities
- Risk Assessment
- Business Impact Evaluation
- Continuous Improvement
- Security Awareness and Training
- Legal and Ethical Considerations