Penetration Testing on Web Server

Presented by

Ritika Sharma 2023a7r002

Manya Malhotra 2023a1r182

Model Institute of Engineering & Technology (Autonomous)

(Permanently Affiliated to the University of Jammu, Accredited by NAAC with “A” Grade)

Jammu, India 2024

Project Overview

Footprinting and Reconnaissance

Gathering information about the target system and network to understand its security posture.

Vulnerablity Scanning and Assessment

Using automated tools and manual techniques to identify potential weaknesses.

Pentesting Execution

Exploiting identified vulnerabilities to assess the real-world impact and potential for compromise.

Remediation Strategies

Developing and recommending actionable steps to address the identified vulnerabilities.

Penetration Testing (Pentesting)

Penetration Testing (Pentesting) is a simulated cyberattack against a computer system, network, or web application to identify security vulnerabilities that could be exploited by malicious hackers.

1. Identify security weaknesses before attackers do.
2. Test security controls (firewalls, IDS/IPS, WAFs).
3. Validate compliance with security standards (PCI-DSS, ISO 27001).
4. Improve incident response preparedness.

Footprinting & Reconnaissance

This phase is like digital detective work—we gather every possible detail about the target before testing its security.

01

Infrastructure Insights

IP address, server location, OS, web server tech, ISP range, and open ports.

02

Employee Profiling

Email IDs, social networking profiles, and LinkedIn searches for company employees.

03

Company Details

Physical address and key personnel like Director/CEO.

04

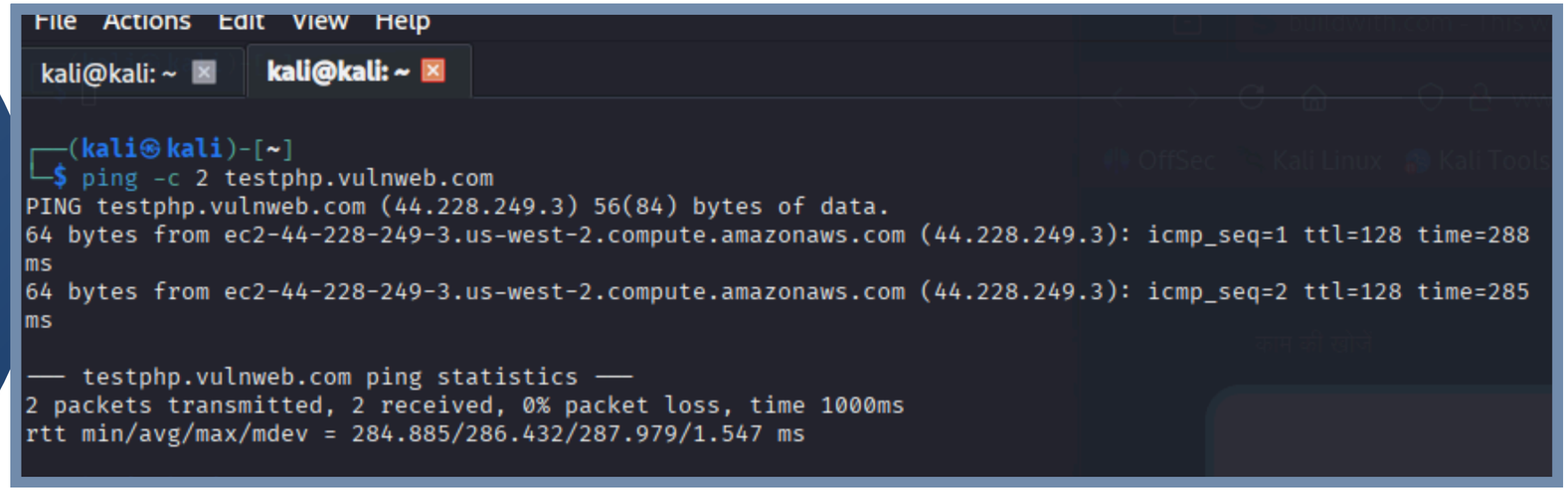
Defensive Measures

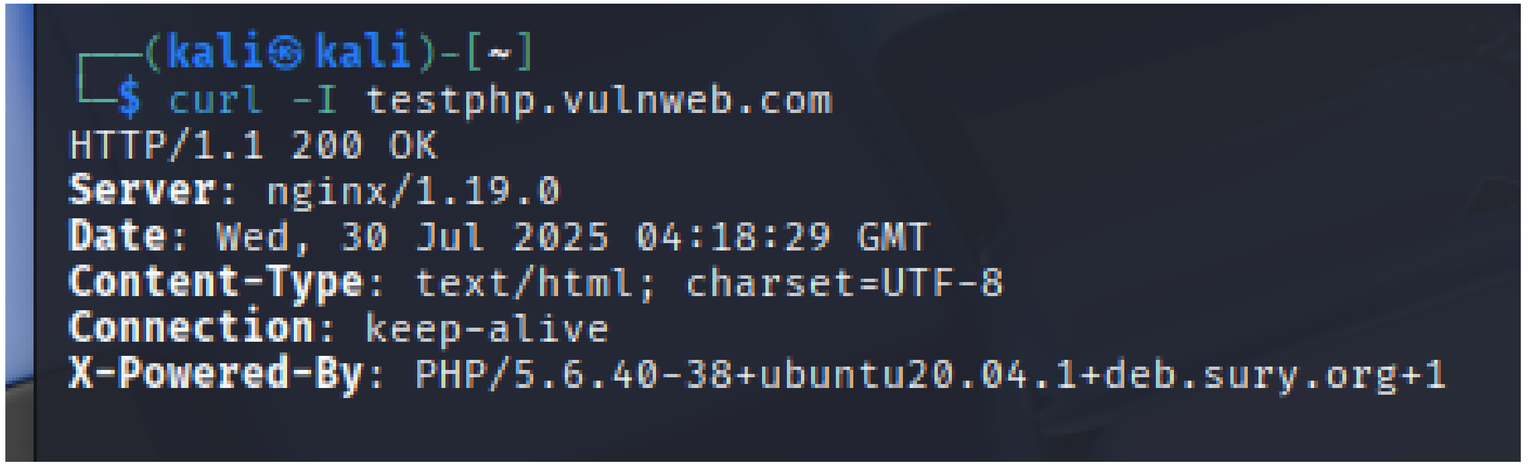
Presence of firewalls, load balancers, and checks for directory listings.

Implementation

Point 1

About company & IP address of Website

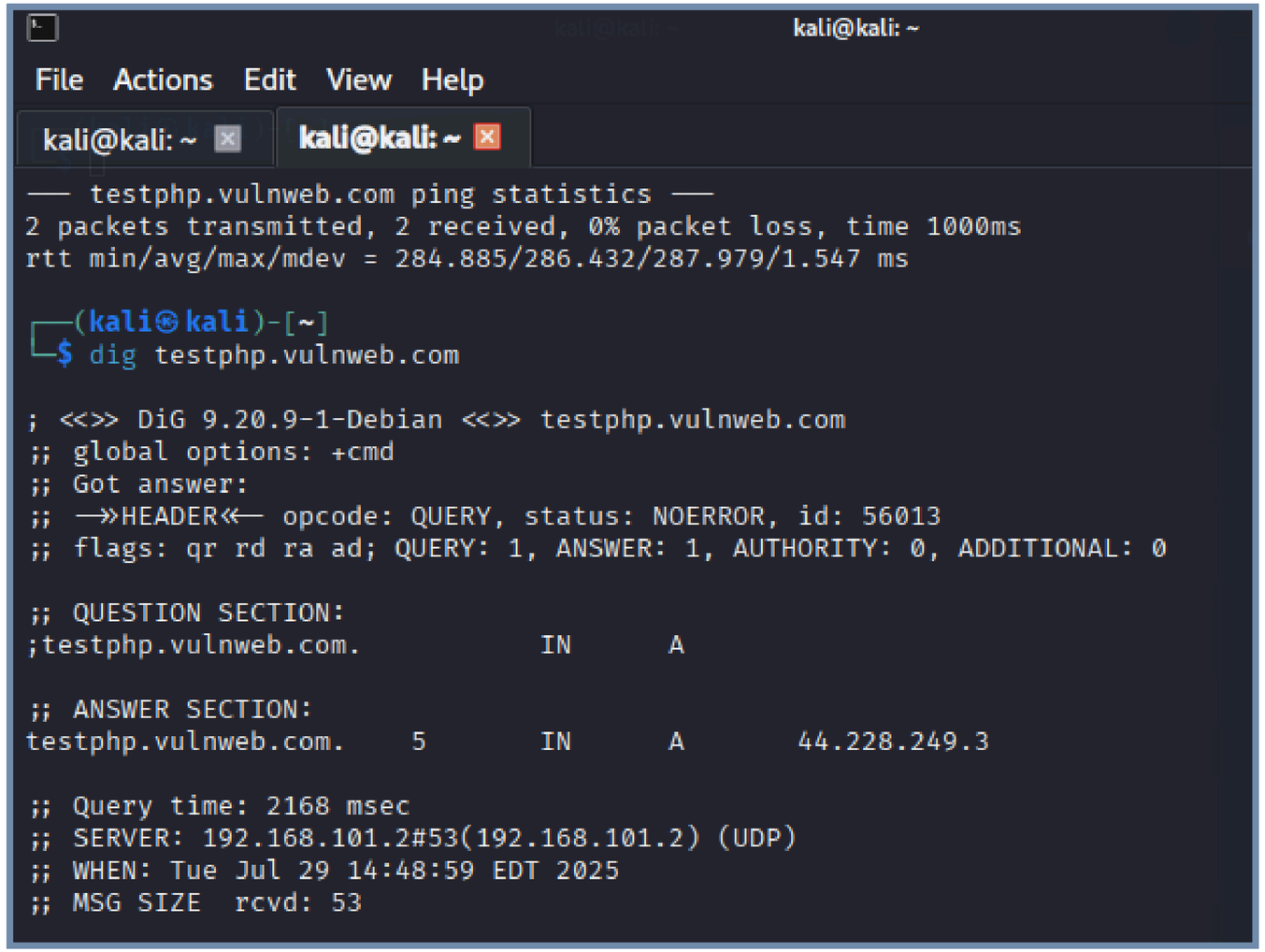




Implementation

Point 2

IP Address of Website



Implementation

Point 3

Geolocation of the server and network info and web server technology

```
┌──(kali㉿kali)-[~]
└─$ curl ipinfo.io/$(dig +short testphp.vulnweb.com)
{
  "ip": "44.228.249.3",
  "hostname": "ec2-44-228-249-3.us-west-2.compute.amazonaws.com",
  "city": "Boardman",
  "region": "Oregon",
  "country": "US",
  "loc": "45.8399,-119.7006",
  "org": "AS16509 Amazon.com, Inc.",
  "postal": "97818",
  "timezone": "America/Los_Angeles",
  "readme": "https://ipinfo.io/missingauth"
}
```

Implementation

Point 4

Os Fingerprinting

```
┌──(kali㉿kali)-[~]
└─$ nmap -O testphp.vulnweb.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 00:45 EDT
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.025s latency).
Other addresses for testphp.vulnweb.com (not scanned): 64:ff9b::2ce4:f903
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
21/tcp   open  ftp
80/tcp   open  http
554/tcp  open  rtsp
1723/tcp open  pptp
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.24 seconds
```

Implementation

Point 5

Vulnerability Scanning

```
┌──(kali㉿kali)-[~]
└─$ nikto -h testphp.vulnweb.com
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 44.228.249.3, 64:ff9b::2ce4:f903
+ Target IP:          44.228.249.3
+ Target Hostname:    testphp.vulnweb.com
+ Target Port:        80
+ Start Time:         2025-07-30 00:55:27 (GMT-4)
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -sS -sV -A testphp.vulnweb.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-30 01:01 EDT
Stats: 0:01:43 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 25.00% done; ETC: 01:05 (0:02:36 remaining)
```

Implementation

Point 6

Web servere Technology
and version

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV -p 80 testphp.vulnweb.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-31 01:09 EDT
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.0018s latency).
Other addresses for testphp.vulnweb.com (not scanned): 64:ff9b::2ce4:f903
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com

PORT   STATE    SERVICE VERSION
80/tcp filtered http

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.17 seconds
```

Implementation

Point 7

Built in Technology
to check http headers

```
┌──(root㉿kali)-[/home/kali]
└─# curl -I http://testphp.vulnweb.com
HTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Thu, 31 Jul 2025 05:11:17 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
```

Implementation

Point 8

ISP IP range server
infomation gathering

```
┌──(root㉿kali)-[/home/kali]
└─# whois 44.228.249.3

#
# 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 1997-2025, American Registry for Internet Numbers, Ltd.
#



# start

NetRange:       44.192.0.0 - 44.255.255.255
CIDR:           44.192.0.0/10
NetName:        AMAZON-4
NetHandle:      NET-44-192-0-0-1
Parent:         NET44 (NET-44-0-0-0-0)
NetType:        Direct Allocation
OriginAS:
Organization:   Amazon.com, Inc. (AMAZON-4)
RegDate:        2019-07-18
Updated:        2019-07-18
Ref:            https://rdap.arin.net/registry/ip/44.192.0.0


OrgName:        Amazon.com, Inc.
OrgId:          AMAZON-4
Address:        Amazon Web Services, Inc.
Address:        P.O. Box 81226
City:           Seattle
StateProv:      WA
PostalCode:     98108-1226
Country:        US
RegDate:        2005-09-29
Updated:        2022-09-30
Comment:        For details of this service please see
Comment:        http://ec2.amazonaws.com
Ref:            https://rdap.arin.net/registry/entity/AMAZON-4


OrgNOCHandle: AANO1-ARIN
OrgNOCName:   Amazon AWS Network Operations
OrgNOCPhone:  +1-206-555-0000
OrgNOCEmail:  amzn-noc-contact@amazon.com
OrgNOCRef:    https://rdap.arin.net/registry/entity/AANO1-ARIN

OrgTechHandle: ANO24-ARIN
```

Implementation

Point 9

Registrar information of domain

```
┌──(root㉿kali)-[/home/kali]
└─# whois testphp.vulnweb.com
No match for "TESTPHP.VULNWEB.COM".
>>> Last update of whois database: 2025-07-31T05:18:33Z <<<

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar.  Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a Whois query, you agree to abide
by the following terms of use: You agree that you may use this Data only
for lawful purposes and that under no circumstances will you use this Data
to: (1) allow, enable, or otherwise support the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail, telephone,
or facsimile; or (2) enable high volume, automated, electronic processes
that apply to VeriSign (or its computer systems). The compilation,
repackaging, dissemination or other use of this Data is expressly
prohibited without the prior written consent of VeriSign. You agree not to
use electronic processes that are automated and high-volume to access or
query the Whois database except as reasonably necessary to register
domain names or modify existing registrations. VeriSign reserves the right
to restrict your access to the Whois database in its sole discretion to ensure
operational stability.  VeriSign may restrict or terminate your access to the
Whois database for failure to abide by these terms of use. VeriSign
reserves the right to modify these terms at any time.

The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
```

Implementation

Point 9

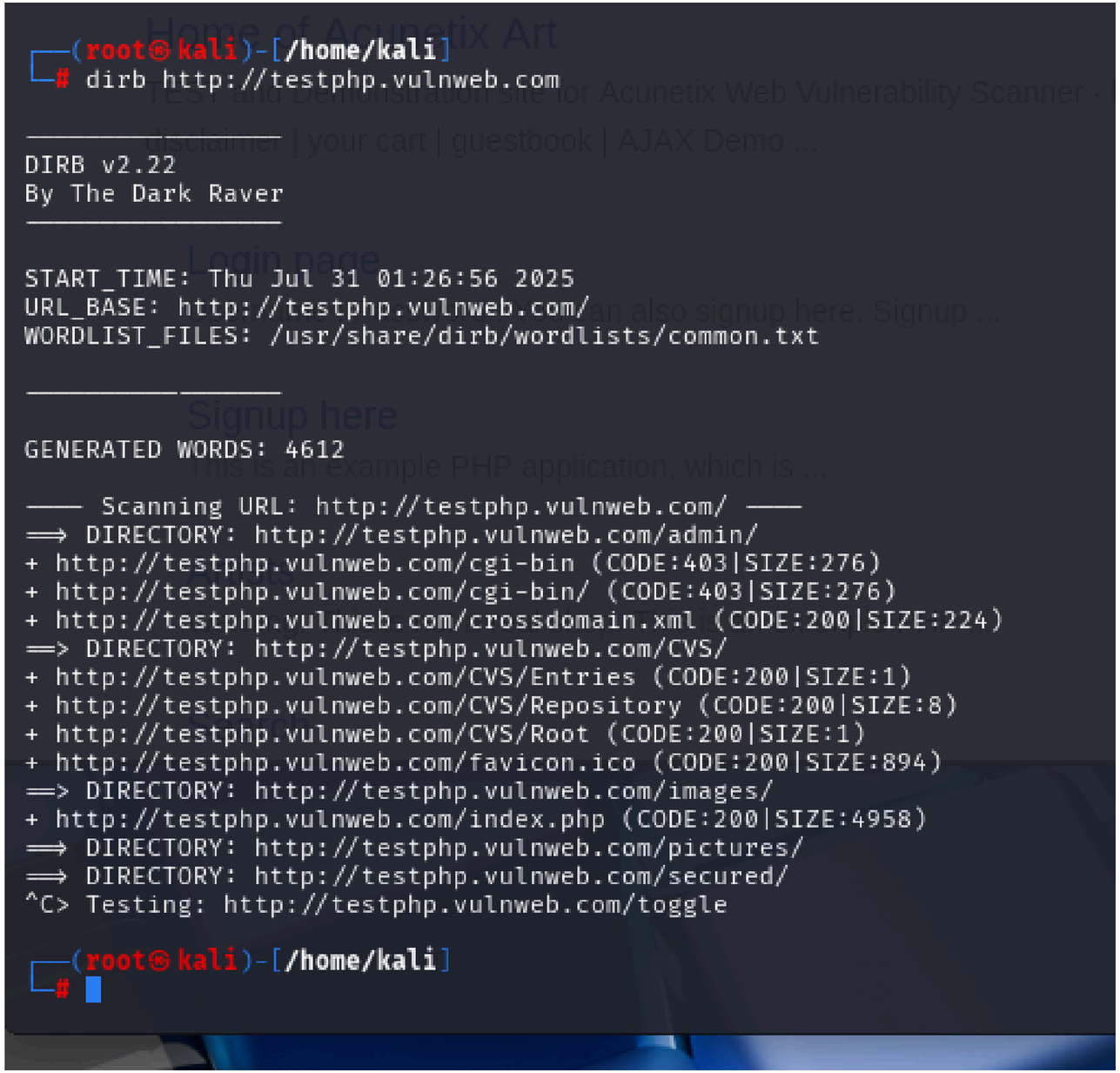
Employee information

```
┌──(root㉿kali)-[/home/kali]
└─# theHarvester -d vulnweb.com -b google,linkedin
Created default proxies.yaml at /root/.theHarvester/proxies.yaml
*******************************************************************
*  _   _                                            _             *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __| '_ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* theHarvester 4.6.0                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************
```

Implementation

Point 9

Check directory listing



Remediation Strategies

Input Validation

Sanitize all user input with whitelist validation approaches

Implement all prepared statements for all database query operations consistently

Authentication Security

Implement multi-factor authentication protocols

Deploy session management security controls

Ongoing Security

Deploy continuous security monitoring solutions

Conduct regular penetration testing assessments

Conclusion & Recommendations

The project culminates in a detailed report outlining all findings, explaining the methodologies, and providing actionable recommendations for strengthening security.

- Vulnerability Assessment

  A summary of all discovered vulnerabilities, categorized by severity and potential impact.
- Remediation Strategies

  Specific, prioritized steps to patch vulnerabilities and enhance defenses.
- Overall Security Posture

  An assessment of the server's current security level and areas for continuous improvement.