

7783 Information Security

Cloud Security Audit & Penetration Testing

Presented by: Xuanren Wei, Xinyue He, Zeru Cai, Mengfei Liu

>>>>>

Agenda

- 1 **Web-hosted app set up on EC2**
- 2 **Security Review & Vulnerability Scan**
- 3 **Severity Analysis**
- 4 **Remediation Implementation**
- 5 **Summary**

<<<<<

Web App Deployment on EC2

- A basic web application was deployed on an AWS EC2 instance running Ubuntu 20.04.
- Apache HTTP Server was installed to serve web content over port 80.
- SSH (port 22) was enabled for secure remote management.

The screenshot displays the AWS Management Console interface. The top navigation bar shows 'EC2' and 'Instances (1) info'. The main content area lists a single instance named 'DVWA-Test-Se...' with ID 'i-0d215ca4068af0d6c', in a 'Running' state, using 't2.micro' instance type. The 'Status check' shows 'Initializing'. On the right, the 'Console-to-Code' panel is visible, indicating it generates code for CloudFormation templates.

Below the console, a terminal window shows the command prompt 'suenzim@ubuntu@ip-172-31-36-115: ~ -- ssh -i ~/Downloads/dvwa-key.pe...'. The terminal output includes system information for Ubuntu 20.04.2 LTS, system load, and network details. It also shows the installation of git and the cloning of the DVWA repository from GitHub. The user then navigates to the DVWA directory and runs 'sudo nano config.inc.php'.

To the right of the terminal, a web browser window shows the DVWA Security page. The page title is 'DVWA Security' and the URL is '3.144.192.224/DVWA/security.php'. The 'Security Level' is set to 'low'. The page lists various security features and their status, including CSRF, File Upload, Insecure CAPTCHA, SQL Injection, and XSS (DOM, Reflected, Stored).

EC2 Instance Configuration & Exposure

- EC2 instance ID: i-0d215ca4068af0d6c (Region: us-east-2)
- Ports 22 (SSH) and 80 (HTTP) were publicly accessible
- Confirmed by AWS Inspector with Medium and Low severity
- Configuration reviewed for exposure baseline

Scan Summary

- Tool Used: AWS Amazon Inspector
- Instance ID: i-0d215ca4068af0d6c
- Region: us-east-2
- Scan Time: 2025-07-12 20:30 (GMT-7)
- Scan Type: Network Reachability

Findings Overview

Severity	Title	Type	Status
Medium	Port 22 is reachable from an Internet Gateway – TCP	Network Reachability	Active
Low	Port 80 is reachable from an Internet Gateway – TCP	Network Reachability	Active

Detailed Analysis

1. Port 22 (SSH) Open to Internet

- Severity: Medium
- Description: SSH port is publicly accessible via TCP, which may allow brute-force login attempts if not properly secured.
- Remediation:
 - Restrict SSH access to known IP addresses via AWS Security Groups.
 - Consider using a VPN or a bastion host for secure access.
 - Enforce key-based authentication and disable password login.

2. Port 80 (HTTP) Open to Internet

OWASP ZAP Scan

– Directory Browsing

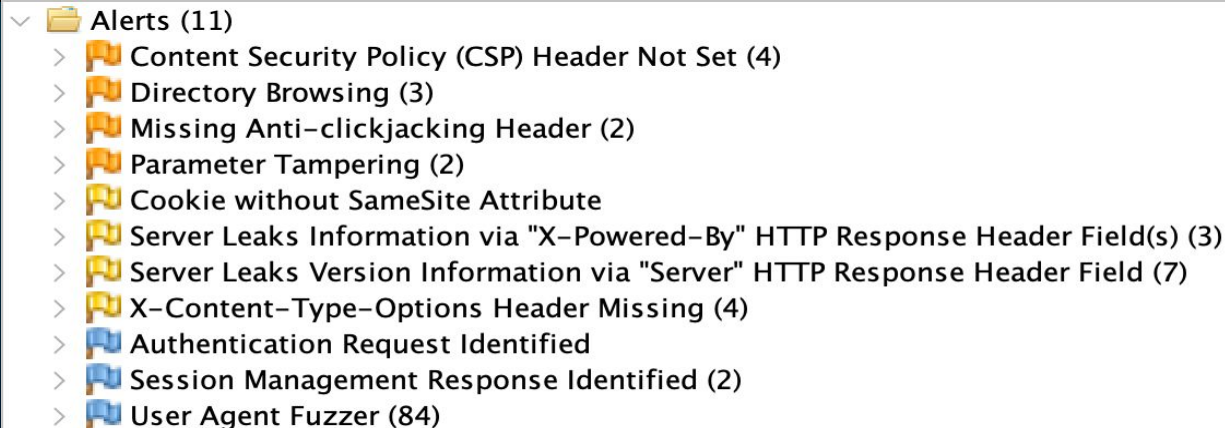
- **Issue:** The server allows directory listing, exposing contents of sensitive folders like /images, /css, etc.

– Parameter Tampering

- **Issue:** Application parameters (e.g., user ID, page ID) can be manipulated to access unauthorized data.

– Clickjacking Vulnerability

- **Issue:** Missing X-Frame-Options header allows framing by other websites, leading to clickjacking attacks.

- 
- A screenshot of the OWASP ZAP Alerts list. The list is titled 'Alerts (11)' and contains 11 items, each with a folder icon and a count in parentheses. The items are: Content Security Policy (CSP) Header Not Set (4), Directory Browsing (3), Missing Anti-clickjacking Header (2), Parameter Tampering (2), Cookie without SameSite Attribute, Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) (3), Server Leaks Version Information via "Server" HTTP Response Header Field (7), X-Content-Type-Options Header Missing (4), Authentication Request Identified, Session Management Response Identified (2), and User Agent Fuzzer (84).
- ✓ Alerts (11)
 - > Content Security Policy (CSP) Header Not Set (4)
 - > Directory Browsing (3)
 - > Missing Anti-clickjacking Header (2)
 - > Parameter Tampering (2)
 - > Cookie without SameSite Attribute
 - > Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) (3)
 - > Server Leaks Version Information via "Server" HTTP Response Header Field (7)
 - > X-Content-Type-Options Header Missing (4)
 - > Authentication Request Identified
 - > Session Management Response Identified (2)
 - > User Agent Fuzzer (84)

Key Vulnerabilities – Medium Severity

Directory Browsing

URL: <http://34.207.86.176/DVWA/dvwa/>
Risk: 🟡 Medium
Confidence: Medium
Parameter:
Attack: <http://34.207.86.176/DVWA/dvwa/>
Evidence: Parent Directory
CWE ID: 548
WASC ID: 48
Source: Active (0 – Directory Browsing)
Input Vector:

Description:

It is possible to view the directory listing. Directory listing may reveal hidden scripts, include files, backup source files, etc. which can be accessed to read sensitive information.

Other Info:

Solution:

Disable directory browsing. If this is required, make sure the listed files does not induce risks.

3. Missing Security Headers (MEDIUM)

X-Frame-Options Missing:

- CVSS Score: 6.1
- Enables clickjacking attacks

X-Content-Type-Options Missing:

- CVSS Score: 5.3
- Enables MIME type confusion attacks

Current Response Headers:

```
HTTP/1.1 302 Found
Date: Sun, 13 Jul 2025 03:37:05 GMT
Server: Apache/2.4.58 (Ubuntu)
Set-Cookie: security=impossible; path=/; HttpOnly
Set-Cookie: PHPSESSID=...; HttpOnly; SameSite=Strict
Location: login.php
```

Missing Headers:

```
- X-Frame-Options
- X-Content-Type-Options
- X-XSS-Protection
- Content-Security-Policy
- Strict-Transport-Security
```


Security Review – Nmap & Nikto

Risk High – “/server-status”
(Exposure of Apache status
page, risk of sensitive
information leakage)

Risk medium –
“X-Frame-options” (Implies
that easy to be attacked by
Clickjacking)

```
==> nmap
If using 'ndiff' returns an error about not being able to import the ndiff module, try:
  chmod go-w /opt/homebrew/Cellar
suenzim@Alarics-MacBook-Pro ~ % nmap -sV -p- 3.144.192.224

Starting Nmap 7.97 ( https://nmap.org ) at 2025-07-12 19:23 -0700
Stats: 0:00:19 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 0.51% done
Stats: 0:00:20 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 0.55% done
Stats: 0:00:22 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 0.62% done
Stats: 0:00:23 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 0.66% done
Stats: 0:00:24 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 0.67% done
Stats: 0:00:24 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 0.69% done
Stats: 0:00:25 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 0.73% done
Stats: 0:00:25 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 0.74% done
Stats: 0:00:26 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 0.75% done
Stats: 0:01:43 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 3.56% done; ETC: 20:11 (0:46:32 remaining)
Stats: 0:02:41 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 5.67% done; ETC: 20:10 (0:44:40 remaining)
Stats: 0:06:30 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 12.91% done; ETC: 20:13 (0:43:51 remaining)
Stats: 0:07:44 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 14.98% done; ETC: 20:14 (0:43:47 remaining)
Stats: 0:26:45 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 53.22% done; ETC: 20:13 (0:23:31 remaining)
Stats: 0:27:14 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 53.72% done; ETC: 20:13 (0:23:28 remaining)
Nmap scan report for ec2-3-144-192-224.us-east-2.compute.amazonaws.com (3.144.192.224)
Host is up (0.075s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.6p1 Ubuntu 3ubuntu13.12 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache/2.4.58
Service Info: Host: ip-172-31-36-116.us-east-2.compute.internal; OS: Linux; CPE: o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 3056.29 seconds
```

```
ubuntu@ip-172-31-88-226:~$ curl -v http://localhost
* Hostname: localhost
* IP address: 127.0.0.1
* Connected to localhost (127.0.0.1) port 80
* Server: Apache/2.4.52 (Ubuntu)
* Server leaks inodes via ETags, header found with file /, fields: 0x29af 0x63a4ea46921db
* The anti-clickjacking X-Frame-Options header is not present.
* No CGI Directories found (use '-C all' to force check all possible dirs)
* Allowed HTTP Methods: POST, OPTIONS, HEAD, GET
* OSVDB-561: /server-status: This reveals Apache information. Comment out appropriate line in httpd.conf or restrict access to
* 6544 items checked: 0 error(s) and 4 item(s) reported on remote host
* End Time: 2025-07-19 22:49:03 (GMT0) (7 seconds)
* 1 host(s) tested
```

Vulnerability Severity Overview

Scan Results Summary

Tool	Finding	Details & Risk
Nmap	Open Port: 22/tcp	Service: OpenSSH 9.6p1 Risk: Standard for server management (SSH). Ensure it is protected with strong passwords or, preferably, SSH keys.
Nmap	Open Port: 80/tcp	Service: Apache httpd 2.4.58 Risk: Standard for web traffic (HTTP). The specific version is identified, which could help an attacker find known exploits.
Nikto	Server Version Leak	Finding: Server: Apache/2.4.58 Risk: Confirms the Nmap finding. Publicly showing the exact server version makes it easier for attackers to find and use version-specific vulnerabilities.
Nikto	Missing Security Header	Finding: The anti-clickjacking X-Frame-Options header is not present. Risk: Your site is vulnerable to Clickjacking attacks, where an attacker can trick users into clicking on things they can't see.
Nikto	Allowed HTTP Methods	Finding: Allowed HTTP Methods: POST, OPTIONS, HEAD, GET Risk: Informational. This lists the acceptable request types. It's good that potentially dangerous methods like PUT or DELETE are not enabled.
Nikto	Server Status Leak	Finding: OSVDB-561: /server-status Risk: If mod_status is enabled and misconfigured, the /server-status page could leak sensitive information about server performance, traffic, and active connections.

Vulnerability Summary – AWS Inspector

- AWS Inspector flagged ports 22 (SSH) and 80 (HTTP) as publicly accessible
- Severity levels: Medium (SSH) and Low (HTTP)
- Exposure type: Network Reachability

inspector-findings.md Preview inspector-findings.md nmap-scan.md Remediation.md severity-analysis.md vulnerability-log.md

Step 5: Analyze Inspector Findings and Document Results

Scan Summary

- Tool Used: AWS Amazon Inspector
- Instance ID: i-0d215ca4068af0d6c
- Region: us-east-2
- Scan Time: 2025-07-12 20:30 (GMT-7)
- Scan Type: Network Reachability

Findings Overview

Severity	Title	Type	Status
Medium	Port 22 is reachable from an Internet Gateway – TCP	Network Reachability	Active
Low	Port 80 is reachable from an Internet Gateway – TCP	Network Reachability	Active

Remediation Priority Plan

Phase 1: Harden Server and Header Configurations

- Implement Critical Security Headers
- Conceal Server Information
- Disable Directory Browse

Phase 2: Secure Application Logic and Session Management

- Fix Parameter Tampering
- Cookies

Phase 3: Review, Verify, and Document

- Re-Scan the Application
- Manual Verification
- Document and Report

Next Steps

Run additional vulnerability scans (OWASP ZAP, Nmap, Nikto)

Perform manual penetration testing

Use AWS Inspector for cloud-specific vulnerabilities

Implement remediation measures

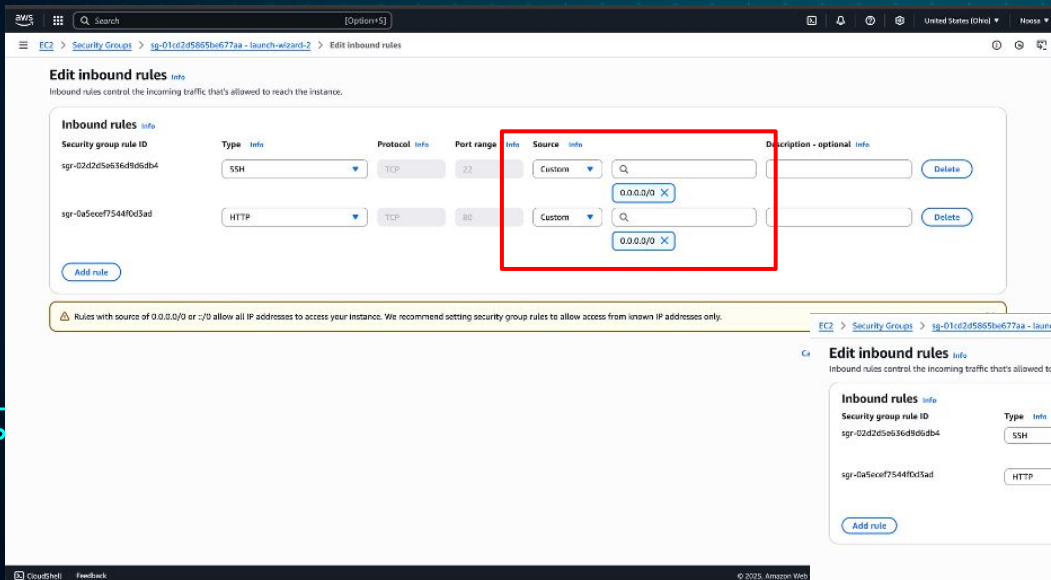
Re-scan to verify fixes

Remediation Implementation

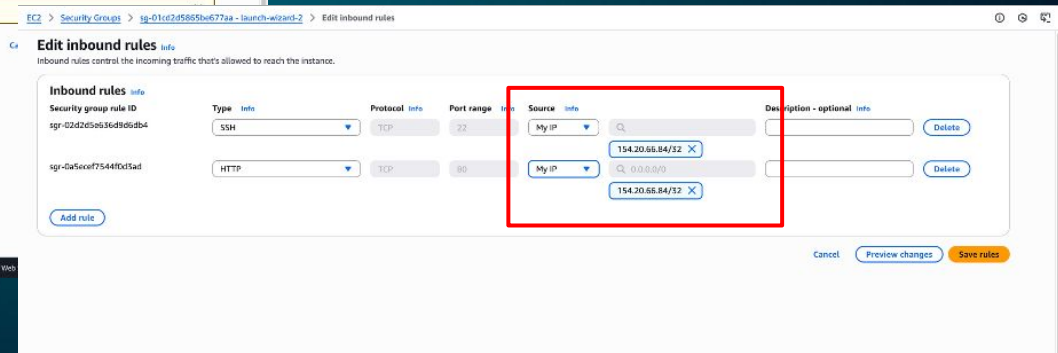
1. Medium – Content Security Policy (CSP) Header Not Set
2. Medium – Directory Browsing
3. Medium – Parameter Tampering
4. Medium – Missing Anti-Clickjacking Header – In Apache doc add (Header always set X-Frame-Options "DENY")

Remediation & Implementation

Vulnerability: Public SSH Access (Severity: High)



With this new rule, all SSH connection attempts from unknown sources will be blocked at the network level, and the corresponding "Network Reachability" finding in AWS Inspector would be resolved.



Fix verification scan report

Inspector

Dashboard

Findings

- By vulnerability
- By instance
- By container image
- By container repository
- By Lambda function

All findings

Code security

Export SBOMs

Suppression rules

On-demand scans

- CIS scans

Vulnerability database search

Account management

Resources coverage

General settings

- EC2 scanning settings
- ECR scanning settings

Usage

Video tutorials

What's New

Switch to Inspector Classic

Finding summary

0 Critical 0 High 53 Medium

Findings (54)

Choose a row to view the finding details. All findings are related to this instance.

Finding statusFilter criteria

ActiveAdd filter

Resource ID EQUALS i-0d215ca4068af0d5cClear filters

Severity	Title	Type	Age	Status
Medium	CVE-2025-37894 - linux-image-aws	Package Vulnerability	2 days	Active
Medium	CVE-2025-37934 - linux-image-aws	Package Vulnerability	2 days	Active
Medium	CVE-2025-37890 - linux-image-aws	Package Vulnerability	2 days	Active
Medium	CVE-2025-37919 - linux-image-aws	Package Vulnerability	2 days	Active
Medium	CVE-2025-37896 - linux-image-aws	Package Vulnerability	2 days	Active
Medium	CVE-2025-37991 - linux-image-aws	Package Vulnerability	2 days	Active
Medium	CVE-2025-37916 - linux-image-aws	Package Vulnerability	2 days	Active
Medium	CVE-2025-37911 - linux-image-aws	Package Vulnerability	2 days	Active
Medium	CVE-2025-37918 - linux-image-aws	Package Vulnerability	2 days	Active
Medium	CVE-2025-37907 - linux-image-aws	Package Vulnerability	2 days	Active
Medium	CVE-2025-37931 - linux-image-aws	Package Vulnerability	2 days	Active
Medium	CVE-2025-37910 - linux-image-aws	Package Vulnerability	2 days	Active
Medium	CVE-2025-37974 - linux-image-aws	Package Vulnerability	2 days	Active
Medium	CVE-2025-37924 - linux-image-aws	Package Vulnerability	2 days	Active
Medium	CVE-2025-37932 - linux-image-aws	Package Vulnerability	2 days	Active
Medium	CVE-2025-37897 - linux-image-aws	Package Vulnerability	2 days	Active

Key Takeaways

- ✓ **Security is a continuous process - Regular scanning is essential**
- ✓ **Common vulnerabilities are still prevalent**
- ✓ **Defense in depth - Multiple layers of security needed**
- ✓ **Automation helps - Tools like Nikto can quickly identify issues**

>>>>>

Thank You