SECURITY ANALYSIS REPORT

Generated By

Backstage Rookie

Provider: Backstage Rookie

contact - swarajdarekar9@gmail.com

Client: Chandrakant Darekar

darekar138@gmail.com

Scan ID: 23cf6916-85c5-4fb6-9003-2313efbe1e63

Date: 2026-02-08 23:10:27

Version: 1.0.0

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The security assessment of the repository revealed one low-severity vulnerability related to information exposure. Specifically, internal IP addresses are configured within the application's `ALLOWED_HOSTS` setting, which, combined with debug mode being active, could aid attackers in reconnaissance efforts. While not immediately exploitable for direct system compromise, such information leaks are considered poor security practice, particularly within the sensitive healthcare sector.

Identified Vulnerabilities

ID	Title	CVSS	Page
L1	Internal IP Addresses Exposed in Configuration	3.1	

METHODOLOGY

Introduction

This report details the results of a security assessment conducted on the specified repository. The analysis involved a multi-layered approach, combining automated static analysis tools with advanced, AI-driven verification and enrichment to identify potential security vulnerabilities.

Objective

The primary objective of this assessment was to identify security weaknesses, assess their potential impact, and provide actionable recommendations for remediation to improve the overall security posture of the application.

Scope

The assessment was performed on the source code of the repository cloned at the time of the scan. The analysis focused on common web application vulnerabilities, insecure coding practices, and dependency risks.

Systems in Scope

No systems explicitly defined.

User Accounts

As this was a static source code analysis, no user accounts were provisioned or tested.

FINDINGS

L1 – Internal IP Addresses Exposed in Configuration

Severity: Low

CVSS Score: 3.1

CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Target: Application configuration file (myHospital/settings.py)

Overview

The application's `settings.py` file explicitly lists internal IP addresses within the `ALLOWED_HOSTS` configuration. This information, while not directly exploitable for code execution, represents an information leak that could be leveraged by an attacker during reconnaissance to map internal network infrastructure. Coupled with `DEBUG = True` in the same file, this significantly increases the risk of inadvertent information disclosure about the internal environment.

Details

The `ALLOWED_HOSTS` setting in Django is designed to protect against HTTP Host header attacks. However, including internal IP addresses ('192.168.0.111', '192.168.43.155') in this list reveals details about the internal network topology. In a healthcare environment, any information that could assist an adversary in understanding the network layout is critical. If this application were to be inadvertently exposed to the internet with these settings, an attacker could deduce internal network segments without requiring active scanning, aiding in targeted attacks. The presence of `DEBUG = True` further exacerbates this by enabling verbose error pages that might leak even more sensitive system information.

Evidence

- **myHospital\settings.py:28:** Line 28 of myHospital/settings.py shows internal IP addresses listed in ALLOWED_HOSTS: ALLOWED_HOSTS = ['192.168.0.111', '127.0.0.1', '192.168.43.155'] This is within the context where DEBUG is also set to True (line 26).

References

- https://docs.djangoproject.com/en/stable/ref/settings/#allowed-hosts
- https://docs.djangoproject.com/en/stable/howto/deployment/checklist/#allowed-hosts

Recommendation

- For production deployments, ensure `ALLOWED_HOSTS` contains only the domain names or external IP addresses that the Django application should serve. - Never include internal IP addresses in `ALLOWED_HOSTS` when deployed to production environments. - Set `DEBUG = False` in all production environments to prevent information disclosure via verbose error messages. - Implement strict network segmentation and firewall rules to prevent direct access to internal IPs from external networks. - Review and adhere to Django's deployment checklist and security best practices.

Prompt to Solve the Vulnerability:

In `myHospital/settings.py` at line 28, the `ALLOWED_HOSTS` variable includes internal IP addresses like '192.168.0.111' and '192.168.43.155'. To resolve this information disclosure vulnerability, especially for production, these internal IP addresses should be removed. Instead, `ALLOWED_HOSTS` should only list the fully qualified domain names (e.g., `['www.example.com', 'api.example.com']`) or external IP addresses that the application is expected to serve. Additionally, ensure `DEBUG` is set to `False` for production deployments to prevent verbose error pages from revealing sensitive information. A corrected `ALLOWED_HOSTS` in a production-ready `settings.py` might look like `ALLOWED_HOSTS = ['.yourdomain.com', 'your.external.ip']` or similar, depending on deployment specifics. For development, a more permissive `ALLOWED_HOSTS` is acceptable but should not be migrated to production.

ENDPOINT SECURITY ANALYSIS

Endpoint Path /admin/

Endpoint Path	/admin/
HTTP Methods	GET, POST, PUT, DELETE, PATCH
Source Location	..\urls.py - 22
Authentication Required	Yes (recommended)
Risk Severity	Critical
CVSS Score	10.0

Authentication Analysis

This endpoint enforces authentication using a recommended-based mechanism. Authentication checks were detected at the following code locations: .

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes: 200, 403

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
HIPAA	No	low	Admin panel, access controlled by authentication and authorization.
HITECH	No	low	Admin panel, access controlled by authentication and authorization.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /

Endpoint Path	/
HTTP Methods	GET
Source Location	..\urls.py - 6
Authentication Required	No
Risk Severity	Critical
CVSS Score	10.0

Authentication Analysis

This endpoint does not enforce authentication, which may expose it to unauthorized access depending on its functionality and the sensitivity of data processed.

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes: 200

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
HIPAA	No	low	Homepage, typically public access.
HITECH	No	low	Homepage, typically public access.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /home/

Endpoint Path	/home/
HTTP Methods	GET
Source Location	..\urls.py - 6
Authentication Required	No

Risk Severity	Critical
CVSS Score	10.0

Authentication Analysis

This endpoint does not enforce authentication, which may expose it to unauthorized access depending on its functionality and the sensitivity of data processed.

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes: 200

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
HIPAA	No	low	Homepage, typically public access.
HITECH	No	low	Homepage, typically public access.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /profile/

Endpoint Path	/profile/
HTTP Methods	GET
Source Location	..\urls.py - 7
Authentication Required	No
Risk Severity	Critical
CVSS Score	10.0

Authentication Analysis

This endpoint does not enforce authentication, which may expose it to unauthorized access depending on its functionality and the sensitivity of data processed.

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes: 200

Contains Sensitive Data: Yes

Identified Security Risks

- **AUTH_MISSING** (high): Authentication is missing for an endpoint that might expose sensitive user profile data.

  Potential Attack Scenario:

  An attacker could access sensitive user profile information without authentication.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
HIPAA	Yes	high	Endpoint exposes user profile data, which may contain Protected Health Information (PHI) and is not protected by authentication.
HITECH	Yes	high	Endpoint exposes user profile data, which may contain Protected Health Information (PHI) and is not protected by authentication, violating HITECH security rules.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /profile/register/

Endpoint Path	/profile/register/
HTTP Methods	GET, POST
Source Location	..\urls.py - 8
Authentication Required	No
Risk Severity	Critical
CVSS Score	10.0

Authentication Analysis

This endpoint does not enforce authentication, which may expose it to unauthorized access depending on its functionality and the sensitivity of data processed.

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes: 200

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
HIPAA	No	low	Registration endpoint, typically used for new user account creation.
HITECH	No	low	Registration endpoint, typically used for new user account creation.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /profile/do_register/

Endpoint Path	/profile/do_register/
HTTP Methods	POST
Source Location	..\urls.py - 9
Authentication Required	No
Risk Severity	Critical
CVSS Score	10.0

Authentication Analysis

This endpoint does not enforce authentication, which may expose it to unauthorized access depending on its functionality and the sensitivity of data processed.

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes: 200, 302

Contains Sensitive Data: No

Identified Security Risks

- **AUTH_MISSING** (high): Authentication is missing for a write operation endpoint.

  Potential Attack Scenario:

  An unauthorized user could potentially register an account, leading to system abuse or data integrity issues.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
HIPAA	No	medium	User registration endpoint requires authentication to prevent unauthorized account creation.
HITECH	No	medium	User registration endpoint requires authentication to prevent unauthorized account creation, impacting data integrity.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /appointments/

Endpoint Path	/appointments/
HTTP Methods	GET
Source Location	..\urls.py - 7
Authentication Required	No
Risk Severity	Critical
CVSS Score	10.0

Authentication Analysis

This endpoint does not enforce authentication, which may expose it to unauthorized access depending on its functionality and the sensitivity of data processed.

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes: 200

Contains Sensitive Data: Yes

Identified Security Risks

- **AUTH_MISSING** (high): Authentication is missing for an endpoint that might expose sensitive appointment data.

  Potential Attack Scenario:

  An attacker could access sensitive appointment information of other users.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
HIPAA	Yes	high	Endpoint exposes appointment data, which may contain PHI and is not protected by authentication.
HITECH	Yes	high	Endpoint exposes appointment data, which may contain PHI and is not protected by authentication, violating HITECH security rules.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /appointments/book/

Endpoint Path	/appointments/book/
HTTP Methods	GET, POST
Source Location	..\urls.py - 8
Authentication Required	No
Risk Severity	Critical
CVSS Score	10.0

Authentication Analysis

This endpoint does not enforce authentication, which may expose it to unauthorized access depending on its functionality and the sensitivity of data processed.

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes: 200

Contains Sensitive Data: No

Identified Security Risks

- **AUTH_MISSING** (high): Authentication is missing for a POST request on an appointment booking endpoint.

  Potential Attack Scenario:

  An unauthorized user could potentially book appointments, leading to system abuse or data integrity issues.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
HIPAA	No	medium	Appointment booking endpoint requires authentication to ensure authorized access for booking.
HITECH	No	medium	Appointment booking endpoint requires authentication to ensure authorized access for booking, impacting data integrity.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /appointments/do_book/

Endpoint Path	/appointments/do_book/
HTTP Methods	POST
Source Location	..\urls.py - 9
Authentication Required	No
Risk Severity	Critical
CVSS Score	10.0

Authentication Analysis

This endpoint does not enforce authentication, which may expose it to unauthorized access depending on its functionality and the sensitivity of data processed.

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes: 200, 302

Contains Sensitive Data: No

Identified Security Risks

- **AUTH_MISSING** (high): Authentication is missing for a write operation endpoint (do_book).

  Potential Attack Scenario:

  An unauthorized user could potentially book appointments, leading to system abuse or data integrity issues.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
HIPAA	No	medium	Appointment booking processing endpoint requires authentication to prevent unauthorized booking.
HITECH	No	medium	Appointment booking processing endpoint requires authentication to prevent unauthorized booking, impacting data integrity.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /appointments/do_change/

Endpoint Path	/appointments/do_change/
HTTP Methods	POST
Source Location	..\urls.py - 11
Authentication Required	No
Risk Severity	Critical
CVSS Score	10.0

Authentication Analysis

This endpoint does not enforce authentication, which may expose it to unauthorized access depending on its functionality and the sensitivity of data processed.

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes: 200, 302

Contains Sensitive Data: No

Identified Security Risks

- **AUTH_MISSING** (high): Authentication is missing for a write operation endpoint (do_change).

  Potential Attack Scenario:

  An unauthorized user could potentially change existing appointments, leading to system abuse or data integrity issues.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
HIPAA	No	medium	Appointment modification endpoint requires authentication to prevent unauthorized changes.
HITECH	No	medium	Appointment modification endpoint requires authentication to prevent unauthorized changes, impacting data integrity.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /case/

Endpoint Path	/case/
HTTP Methods	GET
Source Location	..\urls.py - 6
Authentication Required	No
Risk Severity	Critical
CVSS Score	10.0

Authentication Analysis

This endpoint does not enforce authentication, which may expose it to unauthorized access depending on its functionality and the sensitivity of data processed.

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes: 200

Contains Sensitive Data: Yes

Identified Security Risks

- **AUTH_MISSING** (high): Authentication is missing for an endpoint that might expose sensitive case data.

  Potential Attack Scenario:

  An attacker could access sensitive case information of other users.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
HIPAA	Yes	high	Endpoint exposes case data, which may contain PHI and is not protected by authentication.
HITECH	Yes	high	Endpoint exposes case data, which may contain PHI and is not protected by authentication, violating HITECH security rules.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /case/generate/

Endpoint Path	/case/generate/
HTTP Methods	GET, POST
Source Location	..\urls.py - 7
Authentication Required	No
Risk Severity	Critical
CVSS Score	10.0

Authentication Analysis

This endpoint does not enforce authentication, which may expose it to unauthorized access depending on its functionality and the sensitivity of data processed.

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes: 200

Contains Sensitive Data: No

Identified Security Risks

- **AUTH_MISSING** (high): Authentication is missing for a POST request on a case generation endpoint.

  Potential Attack Scenario:

An unauthorized user could potentially generate fake cases, leading to system abuse or data integrity issues.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
HIPAA	No	medium	Case generation endpoint requires authentication to ensure authorized access for case creation.
HITECH	No	medium	Case generation endpoint requires authentication to ensure authorized access for case creation, impacting data integrity.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /case/do_generate/

Endpoint Path	/case/do_generate/
HTTP Methods	POST
Source Location	..\urls.py - 8
Authentication Required	No
Risk Severity	Critical
CVSS Score	10.0

Authentication Analysis

This endpoint does not enforce authentication, which may expose it to unauthorized access depending on its functionality and the sensitivity of data processed.

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes: 200, 302

Contains Sensitive Data: No

Identified Security Risks

- **AUTH_MISSING** (high): Authentication is missing for a write operation endpoint (do_generate).

  Potential Attack Scenario:

  An unauthorized user could potentially generate fake cases, leading to system abuse or data integrity issues.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
HIPAA	No	medium	Case generation processing endpoint requires authentication to prevent unauthorized case creation.
HITECH	No	medium	Case generation processing endpoint requires authentication to prevent unauthorized case creation, impacting data integrity.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /reports/

Endpoint Path	/reports/
HTTP Methods	GET
Source Location	..\urls.py - 6
Authentication Required	No
Risk Severity	Critical
CVSS Score	10.0

Authentication Analysis

This endpoint does not enforce authentication, which may expose it to unauthorized access depending on its functionality and the sensitivity of data processed.

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes: 200

Contains Sensitive Data: Yes

Identified Security Risks

- **AUTH_MISSING** (high): Authentication is missing for an endpoint that might expose sensitive report data.

  Potential Attack Scenario:

  An attacker could access sensitive report information of other users or patients.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
HIPAA	Yes	high	Endpoint exposes report data, which may contain PHI and is not protected by authentication.
HITECH	Yes	high	Endpoint exposes report data, which may contain PHI and is not protected by authentication, violating HITECH security rules.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /reports/generate/

Endpoint Path	/reports/generate/
HTTP Methods	GET, POST
Source Location	..\urls.py - 7
Authentication Required	No
Risk Severity	Critical
CVSS Score	10.0

Authentication Analysis

This endpoint does not enforce authentication, which may expose it to unauthorized access depending on its functionality and the sensitivity of data processed.

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes: 200

Contains Sensitive Data: No

Identified Security Risks

- **AUTH_MISSING** (high): Authentication is missing for a POST request on a report generation endpoint.

  Potential Attack Scenario:

  An unauthorized user could potentially generate unauthorized reports, leading to system abuse or data integrity issues.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
HIPAA	No	medium	Report generation endpoint requires authentication to ensure authorized access for report creation.
HITECH	No	medium	Report generation endpoint requires authentication to ensure authorized access for report creation, impacting data integrity.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /reports/do_generate/

Endpoint Path	/reports/do_generate/
HTTP Methods	POST
Source Location	..\urls.py - 8
Authentication Required	No
Risk Severity	Critical
CVSS Score	10.0

Authentication Analysis

This endpoint does not enforce authentication, which may expose it to unauthorized access depending on its functionality and the sensitivity of data processed.

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes: 200, 302

Contains Sensitive Data: No

Identified Security Risks

- **AUTH_MISSING** (high): Authentication is missing for a write operation endpoint (do_generate).

  Potential Attack Scenario:

  An unauthorized user could potentially generate unauthorized reports, leading to system abuse or data integrity issues.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
HIPAA	No	medium	Report generation processing endpoint requires authentication to prevent unauthorized report creation.
HITECH	No	medium	Report generation processing endpoint requires authentication to prevent unauthorized report creation, impacting data integrity.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /reports/do_change/

Endpoint Path	/reports/do_change/
HTTP Methods	POST
Source Location	..\urls.py - 10
Authentication Required	No
Risk Severity	Critical
CVSS Score	10.0

Authentication Analysis

This endpoint does not enforce authentication, which may expose it to unauthorized access depending on its functionality and the sensitivity of data processed.

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes: 200, 302

Contains Sensitive Data: No

Identified Security Risks

- **AUTH_MISSING** (high): Authentication is missing for a write operation endpoint (do_change).

  Potential Attack Scenario:

  An unauthorized user could potentially modify existing reports, leading to data tampering and integrity issues.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
HIPAA	No	medium	Report modification endpoint requires authentication to prevent unauthorized changes.
HITECH	No	medium	Report modification endpoint requires authentication to prevent unauthorized changes, impacting data integrity.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /bill/

Endpoint Path	/bill/
HTTP Methods	GET
Source Location	..\urls.py - 7
Authentication Required	No
Risk Severity	Critical
CVSS Score	10.0

Authentication Analysis

This endpoint does not enforce authentication, which may expose it to unauthorized access depending on its functionality and the sensitivity of data processed.

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes: 200

Contains Sensitive Data: Yes

Identified Security Risks

- **AUTH_MISSING** (high): Authentication is missing for an endpoint that might expose sensitive billing information.

  Potential Attack Scenario:

  An attacker could access sensitive billing and payment information of other users.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
HIPAA	Yes	high	Endpoint exposes billing data, which may contain financial and potentially PHI, and is not protected by authentication.
HITECH	Yes	high	Endpoint exposes billing data, which may contain financial and potentially PHI, and is not protected by authentication, violating HITECH security rules.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /bill/do_generate/

Endpoint Path	/bill/do_generate/
HTTP Methods	POST
Source Location	..\urls.py - 9
Authentication Required	No
Risk Severity	Critical
CVSS Score	10.0

Authentication Analysis

This endpoint does not enforce authentication, which may expose it to unauthorized access depending on its functionality and the sensitivity of data processed.

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes: 200, 302

Contains Sensitive Data: No

Identified Security Risks

- **AUTH_MISSING** (high): Authentication is missing for a write operation endpoint (do_generate).

  Potential Attack Scenario:

  An unauthorized user could potentially generate fraudulent bills, leading to financial loss and data integrity issues.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
HIPAA	No	medium	Billing generation endpoint requires authentication to prevent unauthorized bill creation.
HITECH	No	medium	Billing generation endpoint requires authentication to prevent unauthorized bill creation, impacting data integrity.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /bill/pay/

Endpoint Path	/bill/pay/
HTTP Methods	POST
Source Location	..\urls.py - 11
Authentication Required	No
Risk Severity	Critical
CVSS Score	10.0

Authentication Analysis

This endpoint does not enforce authentication, which may expose it to unauthorized access depending on its functionality and the sensitivity of data processed.

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes: 200, 302

Contains Sensitive Data: No

Identified Security Risks

- **AUTH_MISSING** (high): Authentication is missing for a write operation endpoint (pay).

  Potential Attack Scenario:

  An attacker could potentially make unauthorized payments on behalf of other users, leading to financial fraud.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
HIPAA	No	medium	Payment endpoint requires authentication to ensure authorized transactions and protect financial data.
HITECH	No	medium	Payment endpoint requires authentication to ensure authorized transactions and protect financial data, impacting data integrity.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /bill/medicines/

Endpoint Path	/bill/medicines/
HTTP Methods	GET
Source Location	..\urls.py - 12
Authentication Required	No
Risk Severity	Critical
CVSS Score	10.0

Authentication Analysis

This endpoint does not enforce authentication, which may expose it to unauthorized access depending on its functionality and the sensitivity of data processed.

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes: 200

Contains Sensitive Data: Yes

Identified Security Risks

- **AUTH_MISSING** (high): Authentication is missing for an endpoint that might expose sensitive medicine/billing data.

  Potential Attack Scenario:

  An attacker could access sensitive information about medicines prescribed and associated billing for other users.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
HIPAA	Yes	high	Endpoint exposes medicine and billing data, which may contain PHI and financial information, and is not protected by authentication.
HITECH	Yes	high	Endpoint exposes medicine and billing data, which may contain PHI and financial information, and is not protected by authentication, violating HITECH security rules.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /login/

Endpoint Path	/login/
HTTP Methods	GET, POST
Source Location	..\urls.py - 30
Authentication Required	No
Risk Severity	Critical
CVSS Score	10.0

Authentication Analysis

This endpoint does not enforce authentication, which may expose it to unauthorized access depending on its functionality and the sensitivity of data processed.

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes: 200

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
HIPAA	No	low	Login endpoint, typically public access for user authentication.

Regulation	Applicable	Risk Level	Reason
HITECH	No	low	Login endpoint, typically public access for user authentication.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /logout/

Endpoint Path	/logout/
HTTP Methods	GET, POST
Source Location	..\urls.py - 31
Authentication Required	Yes (session)
Risk Severity	Critical
CVSS Score	10.0

Authentication Analysis

This endpoint enforces authentication using a session-based mechanism. Authentication checks were detected at the following code locations: .

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes: 200, 302

Contains Sensitive Data: No

Identified Security Risks

No direct security risks were identified for this endpoint.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
HIPAA	No	low	Logout endpoint, requires authentication to log out an active session.
HITECH	No	low	Logout endpoint, requires authentication to log out an active session.

Security Assessment Notes

CVSS Vector:

References

Endpoint Path /loginmodule/auth

Endpoint Path	/loginmodule/auth
HTTP Methods	POST
Source Location	..\urls.py - 7
Authentication Required	No
Risk Severity	Critical
CVSS Score	10.0

Authentication Analysis

This endpoint does not enforce authentication, which may expose it to unauthorized access depending on its functionality and the sensitivity of data processed.

Request Analysis

Content Type: unknown

No request fields were identified for this endpoint.

Response Analysis

Content Type: unknown

Status Codes: 200, 302, 401

Contains Sensitive Data: No

Identified Security Risks

- **AUTH_MISSING** (high): Authentication is missing for a POST request on an authentication endpoint.

  Potential Attack Scenario:

  An attacker could potentially attempt brute-force attacks or unauthorized authentication without proper rate limiting or protection.

Compliance Impact

Regulation	Applicable	Risk Level	Reason
HIPAA	No	medium	Authentication processing endpoint requires proper authentication mechanisms to protect access.
HITECH	No	medium	Authentication processing endpoint requires proper authentication mechanisms to protect access, impacting data integrity.

Security Assessment Notes

CVSS Vector:

References

METRICS SUMMARY

Total Findings: 1

Severity	Count
CRITICAL	0
HIGH	0
MEDIUM	0
LOW	1

BUSINESS RISK ADVICE

Based on a comprehensive security analysis, here are the prioritized recommendations to enhance the security posture and mitigate identified risks.

Enforce Authentication for Sensitive Data Exposure Endpoints (Priority: Immediate)

Description: Numerous endpoints (`/profile/`, `/appointments/`, `/case/`, `/reports/`, `/bill/`, `/bill/medicines/`) currently allow unauthenticated access to sensitive user and patient data, including Protected Health Information (PHI) and financial details.

Why it Matters: This directly violates HIPAA and HITECH regulations, leading to severe data breaches, privacy violations, and potential legal penalties. Unauthorized access to PHI is a critical security and compliance failure.

Recommended Actions:

- Implement robust authentication checks for all GET requests to `/profile/`, `/appointments/`, `/case/`, `/reports/`, `/bill/`, and `/bill/medicines/`.
- Ensure authorization mechanisms are in place to restrict users to only view their own records (e.g., patient profiles, appointments, bills, reports).
- Conduct a thorough review of all other read-only endpoints to confirm no sensitive data is accessible without proper authentication and authorization.

Expected Outcome: Prevent unauthorized disclosure of PHI and financial information, achieving fundamental compliance with HIPAA/HITECH security rules and safeguarding patient privacy.

Secure All Write and Update Endpoints with Authentication and Authorization (Priority: Immediate)

Description: Critical write operations across various modules, including user registration (`/profile/do_register/`), appointment booking/changes (`/appointments/book/`, `/appointments/do_book/`, `/appointments/do_change/`), case/report generation/modification (`/case/generate/`, `/case/do_generate/`, `/reports/generate/`, `/reports/do_generate/`, `/reports/do_change/`), and billing operations (`/bill/do_generate/`, `/bill/pay/`), lack mandatory authentication.

Why it Matters: This allows unauthorized users to create, modify, or delete sensitive patient data, book fraudulent appointments, generate fake cases/reports, or even initiate unauthorized financial transactions. This severely compromises data integrity, system reliability, and financial security, violating HIPAA/HITECH requirements for data integrity.

Recommended Actions:

- Implement mandatory authentication for all POST requests to the identified endpoints, requiring users to be logged in before performing these actions.
- Introduce fine-grained authorization checks to ensure only users with appropriate roles (e.g., patient, doctor, admin) can perform specific write operations.
- For registration endpoints like `/profile/do_register/`, implement anti-bot measures (e.g., CAPTCHA) and consider requiring email verification to prevent mass abuse.

Expected Outcome: Ensure only authorized and authenticated users can create, modify, or process sensitive data and transactions, safeguarding data integrity and preventing system abuse and fraud.

Deactivate Debug Mode and Harden ALLOWED_HOSTS in Production (Priority: Short-Term)

Description: The `myHospital/settings.py` file exposes internal IP addresses in `ALLOWED_HOSTS` and has `DEBUG = True` enabled. This configuration is highly insecure for a production environment.

Why it Matters: The combination provides attackers with direct insight into internal network topology during reconnaissance and risks verbose error page exposure of sensitive system information. While a 'low' severity finding on its own, its presence in a sensitive healthcare context and ease of remediation warrants immediate attention.

Recommended Actions:

- Set `DEBUG = False` in all production deployments to prevent detailed error messages from exposing system internals.
- Remove all internal IP addresses (e.g., '192.168.0.111', '192.168.43.155') from `ALLOWED_HOSTS` in production configurations.
- Configure `ALLOWED_HOSTS` to strictly list only the domain names or external IP addresses that are intended to serve the application.

Expected Outcome: Eliminate critical information leakage, prevent direct internal network mapping, and reduce the attack surface by hiding sensitive debugging information from potential adversaries.

Implement Robust Authentication and Session Management Controls (Priority: Mid-Term)

Description: The `/loginmodule/auth` endpoint lacks explicit authentication requirements, indicating a potential for weak authentication flow, and generally the application shows a widespread lack of authentication across many functional areas.

Why it Matters: Weak authentication processes (e.g., susceptibility to brute-force, lack of MFA) or insecure session handling can lead to unauthorized account access, session hijacking, and compromise of patient data, directly impacting HIPAA/HITECH compliance.

Recommended Actions:

- Harden the `/loginmodule/auth` endpoint with rate limiting, account lockout policies, and consideration for multi-factor authentication (MFA).
- Ensure secure session management by using HttpOnly, Secure, and SameSite attributes for session cookies.
- Implement proper session invalidation upon logout, inactivity, and password changes.
- Utilize Django's built-in authentication system and best practices for password storage (e.g., bcrypt, Argon2).

Expected Outcome: Establish a secure and resilient authentication system, protecting user accounts from common attacks and ensuring robust session integrity.

Enforce Comprehensive Input Validation and Output Encoding (Priority: Mid-Term)

Description: Many endpoints accept user input for registration, appointments, cases, reports, and billing. The scan does not explicitly detail input validation or output encoding mechanisms.

Why it Matters: Lack of robust input validation and output encoding is a common source of critical vulnerabilities such as SQL Injection (SQLi), Cross-Site Scripting (XSS), and other injection attacks. These can lead to data breaches, data tampering, and compromise of user sessions, posing severe HIPAA/HITECH risks.

Recommended Actions:

- Implement strict, server-side input validation for all user-supplied data across all endpoints, verifying data type, format, length, and acceptable values.
- Utilize Django's ORM (Object-Relational Mapper) or parameterized queries for all database interactions to prevent SQL Injection.
- Ensure all dynamic content rendered to the user interface is properly escaped and output-encoded to prevent Cross-Site Scripting (XSS) attacks.

Expected Outcome: Mitigate injection vulnerabilities, prevent data corruption, and protect users from client-side attacks, enhancing the overall security and integrity of the application.

Establish a Secure Development Lifecycle (SDLC) Program (Priority: Long-Term)

Description: The recurring nature of security findings, particularly `AUTH_MISSING` across multiple critical functions, indicates a need for a more proactive security approach integrated into the development process.

Why it Matters: A reactive approach to security leads to costly fixes, delayed deployments, and persistent vulnerabilities. A mature SDLC reduces the introduction of security flaws from the outset, crucial for maintaining continuous compliance and trust in a healthcare application.

Recommended Actions:

- Integrate security requirements, threat modeling, and secure design principles into the early phases of the development pipeline.
- Implement automated security testing tools (SAST, DAST) into CI/CD for continuous vulnerability detection.
- Conduct regular, mandatory security training for all developers on secure coding practices, OWASP Top 10, and HIPAA/HITECH requirements.
- Mandate security code reviews by a dedicated security team or peer review process for all sensitive code changes.

Expected Outcome: Embed security as a core component of the development process, reducing the volume and severity of vulnerabilities released, improving code quality, and fostering a stronger security culture.

Enhance Logging, Monitoring, and Alerting Capabilities (Priority: Long-Term)

Description: While not explicitly flagged as a vulnerability, comprehensive logging, monitoring, and alerting are critical for detecting and responding to security incidents effectively.

Why it Matters: Inadequate visibility into security events can delay incident detection, hinder forensic analysis, and impede compliance reporting, particularly for HIPAA breach notification requirements. Proactive monitoring is essential for identifying anomalous activities and potential breaches in a timely manner.

Recommended Actions:

- Implement comprehensive logging for all security-relevant events, including authentication attempts (success/failure), authorization failures, sensitive data access, configuration changes, and system errors.
- Integrate logs with a centralized Security Information and Event Management (SIEM) system for real-time aggregation and correlation.
- Configure automated alerts for suspicious activities, multiple failed login attempts, unauthorized access attempts, and anomalies in data access patterns.
- Establish a regular log review process to proactively identify potential security incidents or indicators of compromise.

Expected Outcome: Improve the ability to detect, investigate, and respond to security incidents promptly, enhancing overall security posture and supporting compliance with regulatory requirements for incident response and breach notification.