

# E-Gov Guardian Security Report

## Executive Summary

Target URL: <https://imatmocktests.vercel.app/> Risk Rating: Critical Compliance Score: 0/100 Total Issues: 11

## Detailed Vulnerability Analysis

Severity	Count
MEDIUM	11

## Detailed Vulnerability Analysis

### 1. Http Methods

Severity	MEDIUM
Location	<a href="https://imatmocktests.vercel.app/">https://imatmocktests.vercel.app/</a>
Description	http_methods vulnerability detected
Technical Details	
Remediation	Fix http_methods vulnerability

### 2. Missing Security Header: X-Frame-Options

Severity	MEDIUM
Location	<a href="https://imatmocktests.vercel.app/">https://imatmocktests.vercel.app/</a>
Description	Missing clickjacking protection
Technical Details	Header: X-Frame-Options
Remediation	Add the missing security header

### 3. Missing Security Header: X-Content-Type-Options

Severity	MEDIUM
Location	https://imatmocktests.vercel.app/
Description	Missing MIME type sniffing protection
Technical Details	Header: X-Content-Type-Options
Remediation	Add the missing security header

#### 4. Missing Security Header: X-XSS-Protection

Severity	MEDIUM
Location	https://imatmocktests.vercel.app/
Description	Missing XSS protection
Technical Details	Header: X-XSS-Protection
Remediation	Add the missing security header

#### 5. Missing Security Header: Content-Security-Policy

Severity	MEDIUM
Location	https://imatmocktests.vercel.app/
Description	Missing CSP protection
Technical Details	Header: Content-Security-Policy
Remediation	Add the missing security header

#### 6. Missing Security Header: Referrer-Policy

Severity	MEDIUM
Location	https://imatmocktests.vercel.app/
Description	Missing referrer policy
Technical Details	Header: Referrer-Policy
Remediation	Add the missing security header

#### 7. Missing Security Header: Permissions-Policy

Severity	MEDIUM
Location	https://imatmocktests.vercel.app/
Description	Missing permissions policy
Technical Details	Header: Permissions-Policy
Remediation	Add the missing security header

## 8. Permissive CORS Policy

Severity	MEDIUM
Location	https://imatmocktests.vercel.app/
Description	CORS allows origin: *
Technical Details	Access-Control-Allow-Origin: *
Remediation	### Security Recommendations for Permissive CORS Policy **Overview:** Cross-Origin Resource Sharing (CORS) is a security feature implemented in web browsers that allows or restricts resources requested from another domain outside the domain from which the first resource was served. A permissive CORS policy, such as `Access-Control-Allow-Origin: *`, can expose your application to various security risks, including Cross-Site Request Forgery (CSRF) and data theft. ...
AI Recommendation	### Security Recommendations for Permissive CORS Policy **Overview:** Cross-Origin Resource Sharing (CORS) is a security feature implemented in web browsers that allows or restricts resources requested from another domain outside the domain from whic...

## 9. Permissive CORS Policy

Severity	MEDIUM
Location	https://imatmocktests.vercel.app/
Description	CORS allows origin: *
Technical Details	Access-Control-Allow-Origin: *
Remediation	### Security Recommendations for Permissive CORS Policy ##### Understanding CORS Cross-Origin Resource Sharing (CORS) is a security feature implemented by web browsers to prevent malicious websites from making requests to a different domain than the one that served the web page. A permissive CORS policy, such as `Access-Control-Allow-Origin: *`, allows any website to access resources from your server, which can lead to various security vulnerabilities, including data theft and unauthorized actions. ...

AI Recommendation	### Security Recommendations for Permissive CORS Policy ##### Understanding CORS Cross-Origin Resource Sharing (CORS) is a security feature implemented by web browsers to prevent malicious websites from making requests to a different domain than the o...
-------------------	--

## 10. Permissive CORS Policy

Severity	MEDIUM
Location	https://imatmocktests.vercel.app/
Description	CORS allows origin: *
Technical Details	Access-Control-Allow-Origin: *
Remediation	### Security Recommendations for Permissive CORS Policy ##### Understanding CORS Cross-Origin Resource Sharing (CORS) is a security feature implemented in web browsers that allows or restricts resources requested from another domain outside the domain from which the first resource was served. A permissive CORS policy, such as `Access-Control-Allow-Origin: *`, can expose your application to various security risks, including Cross-Site Request Forgery (CSRF) and data theft. ...
AI Recommendation	### Security Recommendations for Permissive CORS Policy ##### Understanding CORS Cross-Origin Resource Sharing (CORS) is a security feature implemented in web browsers that allows or restricts resources requested from another domain outside the domain...

## 11. Permissive CORS Policy

Severity	MEDIUM
Location	https://imatmocktests.vercel.app/
Description	CORS allows origin: *
Technical Details	Access-Control-Allow-Origin: *
Remediation	### Security Recommendations for Permissive CORS Policy **Overview:** Cross-Origin Resource Sharing (CORS) is a security feature implemented in web browsers that allows or restricts resources requested from another domain outside the domain from which the first resource was served. A permissive CORS policy, such as `Access-Control-Allow-Origin: *`, can expose your application to various security risks, including Cross-Site Request Forgery (CSRF) and data theft. ...
AI Recommendation	### Security Recommendations for Permissive CORS Policy **Overview:** Cross-Origin Resource Sharing (CORS) is a security feature implemented in web browsers that allows or restricts resources requested from another domain outside the domain from whic...

## **Security Recommendations**

1. Conduct regular security assessments and penetration testing
2. Implement Web Application Firewall (WAF) for additional protection
3. Establish security monitoring and incident response procedures
4. Train development team on secure coding practices