Web Application Report

This report includes important security information about your web application.

Security Report

This report was created by HCL AppScan Standard 10.3.0
Scan started: 11/21/2025 9:24:57 PM

Table of Contents

Introduction

- General Information
- Login Settings

Summary

- Issue Types
- Vulnerable URLs
- Fix Recommendations
- Security Risks
- Causes
- WASC Threat Classification

Issues Sorted by Issue Type

- Autocomplete HTML Attribute Not Disabled for Password Field 1
- Body Parameters Accepted in Query 1
- Cacheable SSL Page Found 2
- Check for SRI (Subresource Integrity) support 2
- Cookie with Insecure or Improper or Missing SameSite attribute 1
- Hidden Directory Detected 1
- Missing "Content-Security-Policy" header 1
- Missing Secure Attribute in Encrypted Session (SSL) Cookie 1
- Missing or insecure "X-Content-Type-Options" header 1
- Missing or insecure HTTP Strict-Transport-Security Header 1
- SHA-1 cipher suites were detected 1
- Unnecessary Http Response Headers found in the Application 1
- Weak Cipher Suites - ROBOT Attack : Vulnerable cipher suites are supported by the server 1
- Weak Ciphers are detected: Not all cipher suites support Perfect Forward Secrecy 1
- Application Error 1
- Email Address Pattern Found 4
- Missing "Referrer policy" Security Header 1

How to Fix

- Autocomplete HTML Attribute Not Disabled for Password Field
- Body Parameters Accepted in Query
- Cacheable SSL Page Found
- Check for SRI (Subresource Integrity) support
- Cookie with Insecure or Improper or Missing SameSite attribute
- Hidden Directory Detected
- Missing "Content-Security-Policy" header
- Missing Secure Attribute in Encrypted Session (SSL) Cookie
- Missing or insecure "X-Content-Type-Options" header
- Missing or insecure HTTP Strict-Transport-Security Header
- SHA-1 cipher suites were detected
- Unnecessary Http Response Headers found in the Application
- Weak Cipher Suites - ROBOT Attack : Vulnerable cipher suites are supported by the server
- Weak Ciphers are detected: Not all cipher suites support Perfect Forward Secrecy
- Application Error
- Email Address Pattern Found
- Missing "Referrer policy" Security Header

Application Data

- Cookies
- JavaScripts
- Parameters
- Comments
- Visited URLs
- Failed Requests
- Filtered URLs
- Components

Introduction

This report contains the results of a web application security scan performed by HCL AppScan Standard.

Medium severity issues:	16
Informational severity issues:	6
Total security issues included in the report:	22
Total security issues discovered in the scan:	22

General Information

Scan file name:	DRIMS DEV Scan
Scan started:	11/21/2025 9:24:57 PM
Test policy:	Default
CVSS version:	3.1
Test optimization level:	Fast

Host	drims.nginxdev.egovja.com
Port	443
Operating system:	Unknown
Web server:	Unknown
Application server:	Any

Login Settings

Login method:	Recorded login
Concurrent logins:	Enabled
In-session detection:	Enabled
In-session pattern:	
Tracked or session ID cookies:	
Tracked or session ID parameters:	
Login sequence:	

Summary

Issue Types 17

TOC

	Issue Type	Number of Issues
M	Autocomplete HTML Attribute Not Disabled for Password Field	1
M	Body Parameters Accepted in Query	1
M	Cacheable SSL Page Found	2
M	Check for SRI (Subresource Integrity) support	2
M	Cookie with Insecure or Improper or Missing SameSite attribute	1
M	Hidden Directory Detected	1
M	Missing "Content-Security-Policy" header	1
M	Missing Secure Attribute in Encrypted Session (SSL) Cookie	1
M	Missing or insecure "X-Content-Type-Options" header	1
M	Missing or insecure HTTP Strict-Transport-Security Header	1
M	SHA-1 cipher suites were detected	1
M	Unnecessary Http Response Headers found in the Application	1
M	Weak Cipher Suites - ROBOT Attack : Vulnerable cipher suites are supported by the server	1
M	Weak Ciphers are detected: Not all cipher suites support Perfect Forward Secrecy	1
I	Application Error	1
I	Email Address Pattern Found	4
I	Missing "Referrer policy" Security Header	1

Vulnerable URLs 4

TOC

	URL	Number of Issues
M	https://drims.nginxdev.egovja.com/login	6
M	https://drims.nginxdev.egovja.com/account-requests/submit	3
M	https://drims.nginxdev.egovja.com/	12
I	https://drims.nginxdev.egovja.com/account-requests/	1

Fix Recommendations 15

TOC

	Remediation Task	Number of Issues
M	Add the 'Secure' attribute to all sensitive cookies	1
M	Add to each third-party script/link element support to SRI(Subresource Integrity).	2
M	Change server's supported ciphersuites	3
M	Config your server to use the "Content-Security-Policy" header with secure policies	1
M	Config your server to use the "X-Content-Type-Options" header with "nosniff" value	1
M	Correctly set the "autocomplete" attribute to "off"	1
M	Do not accept body parameters that are sent in the query string	1
M	Do not allow sensitive information to leak.	1
M	Implement the HTTP Strict-Transport-Security policy with a long "max-age"	1
M	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely	1
M	Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.	2
M	Review possible solutions for configuring SameSite Cookie attribute to recommended values	1
L	Config your server to use the "Referrer Policy" header with secure policies	1
L	Remove e-mail addresses from the website	4
L	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions	1

Security Risks 9

TOC

	Risk	Number of Issues
M	It may be possible to bypass the web application's authentication mechanism	1
M	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations	12
M	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.	5
M	In case the third-party server is compromised, the content/behavior of the site will change	2
M	Prevent cookie information leakage by restricting cookies to first-party or same-site context, Attacks can extend to Cross-Site-Request-Forgery (CSRF) attacks if there are no additional protections in place (such as Anti-CSRF tokens).	1
M	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site	1
M	It may be possible to steal user and session information (cookies) that was sent during an encrypted session	1
M	It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user	3
I	It is possible to gather sensitive debugging information	1

Causes 9

TOC

	Cause	Number of Issues
M	Insecure web application programming or configuration	11
M	Sensitive information might have been cached by your browser	2
M	There is no support to Subresource Integrity.	2
M	Sensitive Cookie with Improper or Insecure or Missing SameSite Attribute	1
M	The web server or application server are configured in an insecure way	3
M	The web application sends non-secure cookies over SSL	1
M	Cipher Suites that support TLS-RSA key exchange were detected. The web server or application server with TLS implementation flaw may be vulnerable to ROBOT Attack. This issue does not necessarily mean that you are vulnerable. Please follow the advisory guideline.	1
I	Proper bounds checking were not performed on incoming parameter values	1
I	No validation was done in order to make sure that user input matches the data type expected	1

WASC Threat Classification

TOC

Threat	Number of Issues
Information Leakage	16
Remote File Inclusion	2
Server Misconfiguration	4

Issues Sorted by Issue Type

M Autocomplete HTML Attribute Not Disabled for Password Field 1 TOC

Issue 1 of 1 TOC

Autocomplete HTML Attribute Not Disabled for Password Field

Severity:	Medium
CVSS Score:	5.3
URL:	https://drims.nginxdev.egovja.com/login
Entity:	login (Page)
Risk:	It may be possible to bypass the web application's authentication mechanism
Cause:	Insecure web application programming or configuration
Fix:	Correctly set the "autocomplete" attribute to "off"

Difference:

Reasoning: AppScan has found that a password field does not enforce the disabling of the autocomplete feature.

Test Requests and Responses:

```
GET /login?next=%2F HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://drims.nginxdev.egovja.com/
Host: drims.nginxdev.egovja.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: session=eyJfZnJlc2giOmZhbHNlfQ.aSEfKw.SM5yxUK0BBPJmHkTb-ZxH5m7m_g
Content-Length: 0


HTTP/1.1 200 OK
Server: nginx
Date: Sat, 22 Nov 2025 02:33:41 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 4388
Connection: keep-alive
Vary: Cookie


<!doctype html>
<html lang="en">
<head>
  <meta charset="utf-8">
  <title>Login · DMIS</title>
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.3/dist/css/bootstrap.min.css" rel="stylesheet">
  <link rel="stylesheet" href="https://cdn.jsdelivr.net/npm/bootstrap-icons@1.11.3/font/bootstrap-icons.css">
```

```
    <link rel="stylesheet" href="/static/css/modern-ui.css">
  </head>
  <body>
    <div class="login-container">
      <div>
        <!-- Login Card -->
        <div class="login-card">
          <div class="login-header">
            <div class="login-header-logos">
            <img src="/static/images/jamaica-coat-of-arms.png"
            alt="Jamaica Coat of Arms">
            <img src="/static/images/odpem-logo.png"
            alt="ODPEM Logo">
            </div>
            <h1>Disaster Management Information System</h1>
            <p class="login-header-subtitle">DMIS</p>
            <p class="login-header-meta">Government of Jamaica</p>
          </div>

          <div class="login-body">
            <h2>Sign in to your account</h2>
            <p class="subtitle">Use your email and password to access DMIS.</p>

            <!-- Flash messages -->




            <form method="post" action="/login" novalidate>
            <div class="form-group">
            <label for="email" class="form-label">Email Address</label>
            <input
            id="email"
            name="email"
            type="email"
            required
            autocomplete="email"
            class="form-control"
            placeholder="your.email@odpem.gov.jm"
            value=""
            aria-describedby="email-help">
            <div id="email-help" class="form-text">
            Enter the email address associated with your DMIS account
            </div>
            </div>

            <div class="form-group">
            <label for="password" class="form-label">Password</label>
            <input
            id="password"
            name="password"
            type="password"
            required
            autocomplete="current-password"
            class="form-control"
            placeholder="Enter your password">
            </div>

            <div class="mb-4">
            <div class="form-check">
            <input type="checkbox" name="remember" class="form-check-input" id="remember">
            <label class="form-check-label" for="remember">
            Remember me
            </label>
            </div>
            </div>

            <button type="submit" class="btn-login">
            <i class="bi bi-box-arrow-in-right me-2"></i>
            Sign In
            </button>
            </form>
          </div>
        </div>

        <!-- Agency CTA Card -->
        <div class="agency-cta">
          <div class="agency-cta-title">
            <i class="bi bi-building"></i>
            <span>New Agency?</span>
          </div>
          <p class="subtitle">
            Relief agencies can request access to DMIS to submit relief requests and manage disaster response distributions.
          </p>
```

```
          <a href="/account-requests/submit" class="btn-agency-request">
            <i class="bi bi-plus-circle"></i>
            Request Agency Account
          </a>
          <ul class="info-list">
            <li>
            <i class="bi bi-check-circle-fill"></i>
            <span>Approval by ODPEM required</span>
            </li>
            <li>
            <i class="bi bi-check-circle-fill"></i>
            <span>Email updates on request status</span>
            </li>
            <li>
            <i class="bi bi-check-circle-fill"></i>
            <span>Full access after approval</span>
            </li>
          </ul>
        </div>

        <!-- Footer -->
        <div class="login-footer">
          <div class="login-footer-badge">
            <i class="bi bi-shield-check"></i>
            <span>Secure Government System</span>
          </div>
          <p>© 2025 DMIS - Disaster Management Information System</p>
          <p class="login-footer-small">By signing in you agree to the acceptable use and data policies</p>
        </div>
      </div>
    </div>

    <script src="https://cdn.jsdelivr.net/npm/bootstrap@5.3.3/dist/js/bootstrap.bundle.min.js">
...
...
...
```

M Body Parameters Accepted in Query 1

TOC

Issue 1 of 1

TOC

Body Parameters Accepted in Query

Severity:	Medium
CVSS Score:	5.3
URL:	https://drims.nginxdev.egovja.com/login
Entity:	login (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	Insecure web application programming or configuration
Fix:	Do not accept body parameters that are sent in the query string

Difference: **Body Parameter** removed from request: `test@altoromutual.com`
Query Parameter added to request: `test@altoromutual.com`
Body Parameter removed from request: `—`
Query Parameter added to request: `—`

Method manipulated from: `POST` to: `GET`

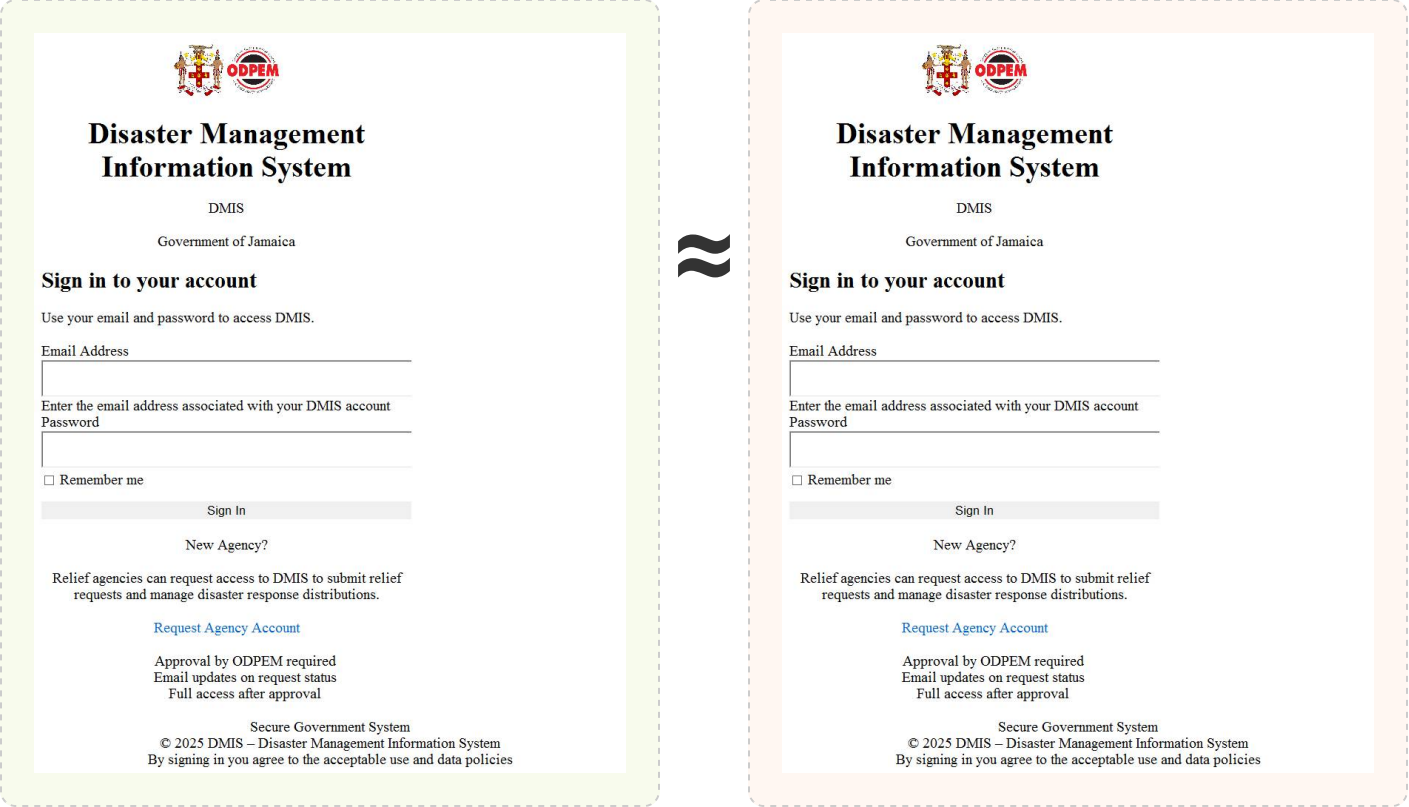
Reasoning: The test result seems to indicate a vulnerability because the Test Response is similar to the Original Response, indicating that the application processed body parameters that were submitted in the query

Test Requests and Responses:

```
GET /login?email=test%40altoromutual.com&password= HTTP/1.1
Host: drims.nginxdev.egovja.com
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: https://drims.nginxdev.egovja.com
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://drims.nginxdev.egovja.com/login?next=%2F
Cookie: session=eyJfZnJlc2giOmZhbHNlfQ.aSEfKw.SM5yxUK0BBPJmHkTb-ZxH5m7m_g
Content-Length: 0


HTTP/1.1 200 OK
Server: nginx
Date: Sat, 22 Nov 2025 02:33:41 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 4388
Connection: keep-alive
Vary: Cookie


<!doctype html>
<html lang="en">
<head>
  <meta charset="utf-8">
  <title>Login · DMIS</title>
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.3/dist/css/bootstrap.min.css" rel="stylesheet">
  <link rel="stylesheet" href="https://cdn.jsdelivr.net/npm/bootstrap-icons@1.11.3/font/bootstrap-icons.css">
  <link rel="stylesheet" href="/static/css/modern-ui.css">
</head>
<body>
  <div class="login-container">
    <div>
      <!-- Login Card -->
      <div class="login-card">
        <div class="login-header">
          <div class="login-header-logos">
          <img src="/static/images/jamaica-coat-of-arms.png"
          alt="Jamaica Coat of Arms">
          <img src="/static/images/odpem-logo.png"
          alt="ODPEM Logo">
          </div>
          <h1>Disaster Management Information System</h1>
          <p class="login-header-subtitle">DMIS</p>
          <p class="login-header-meta">Government of Jamaica</p>
        </div>

        <div class="login-body">
          <h2>Sign in to your account</h2>
          <p class="subtitle">Use your email and password to access DMIS.</p>

          <!-- Flash messages -->



          <form method="post" action="/login" novalidate>
          <div class="form-group">
          <label for="email" class="form-label">Email Address</label>
          <input
          id="email"
          name="email"
          type="email"
          required
          autocomplete="email"
```

```
          class="form-control"
          placeholder="your.email@odpem.gov.jm"
          value=""
          aria-describedby="email-help">
          <div id="email-help" class="form-text">
          Enter the email address associated with your DMIS account
          </div>
          </div>

          <div class="form-group">
          <label for="password" class="form-label">Password</label>
          <input
          id="password"
          name="password"
          type="password"
          required
          autocomplete="current-password"
          class="form-control"
          placeholder="Enter your password">
          </div>

          <div class="mb-4">
          <div class="form-check">
          <input type="checkbox" name="remember" class="form-check-input" id="remember">
          <label class="form-check-label" for="remember">
          Remember me
          </label>
          </div>
          </div>

          <button type="submit" class="btn-login">
          <i class="bi bi-box-arrow-in-right me-2"></i>
          Sign In
          </button>
          </form>
        </div>
      </div>

      <!-- Agency CTA Card -->
      <div class="agency-cta">
        <div class="agency-cta-title">
          <i class="bi bi-building"></i>
          <span>New Agency?</span>
        </div>
        <p class="subtitle">
          Relief agencies can request access to DMIS to submit relief requests and manage disaster response distributions.
        </p>
        <a href="/account-requests/submit" class="btn-agency-request">
          <i class="bi bi-plus-circle"></i>
          Request Agency Account
        </a>
        <ul class="info-list">
          <li>
          <i class="bi bi-check-circle-fill"></i>
          <span>Approval by ODPEM required</span>
          </li>
          <li>
          <i class="bi bi-check-circle-fill"></i>
          <span>Email updates on request status</span>
          </li>
          <li>
          <i class="bi bi-check-circle-fill"></i>
          <span>Full access after approval</span>
          </li>
        </ul>
      </div>

      <!-- Footer -->
      <div class="login-footer">

...
...
...
```

Original Response **Test Response**



M Cacheable SSL Page Found 2

TOC

Issue 1 of 2

TOC

Cacheable SSL Page Found	
Severity:	Medium
CVSS Score:	5.3
URL:	https://drims.nginxdev.egovja.com/login
Entity:	login (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Sensitive information might have been cached by your browser
Fix:	Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Difference:

Reasoning: The application has responded with a response that indicates the page should be cached, but cache controls aren't set (you can set "Cache-Control: no-store" or "Cache-Control: no-cache" or "Pragma: no-cache" to prevent caching).

Test Requests and Responses:

```
GET /login?next=%2F HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://drims.nginxdev.egovja.com/
Host: drims.nginxdev.egovja.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: session=eyJfZnJlc2giOmZhbHNlfQ.aSEfKw.SM5yxUK0BBPJmHkTb-ZxH5m7m_g
Content-Length: 0


HTTP/1.1 200 OK
Server: nginx
Date: Sat, 22 Nov 2025 02:33:41 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 4388
Connection: keep-alive
Vary: Cookie


<!doctype html>
<html lang="en">
<head>
  <meta charset="utf-8">
  <title>Login · DMIS</title>
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.3/dist/css/bootstrap.min.css" rel="stylesheet">
  <link rel="stylesheet" href="https://cdn.jsdelivr.net/npm/bootstrap-icons@1.11.3/font/bootstrap-icons.css">
  <link rel="stylesheet" href="/static/css/modern-ui.css">
</head>
<body>
  <div class="login-container">
    <div>
      <!-- Login Card -->
      <div class="login-card">
        <div class="login-header">
          <div class="login-header-logos">
          <img src="/static/images/jamaica-coat-of-arms.png"
          alt="Jamaica Coat of Arms">
          <img src="/static/images/odpem-logo.png"
          alt="ODPEM Logo">
          </div>
          <h1>Disaster Management Information System</h1>
          <p class="login-header-subtitle">DMIS</p>
          <p class="login-header-meta">Government of Jamaica</p>
        </div>

        <div class="login-body">
          <h2>Sign in to your account</h2>
          <p class="subtitle">Use your email and password to access DMIS.</p>

          <!-- Flash messages -->




          <form method="post" action="/login" novalidate>
          <div class="form-group">
          <label for="email" class="form-label">Email Address</label>
          <input
          id="email"
          name="email"
          type="email"
          required
          autocomplete="email"
          class="form-control"
          placeholder="your.email@odpem.gov.jm"
          value=""
          aria-describedby="email-help">
          <div id="email-help" class="form-text">
          Enter the email address associated with your DMIS account
          </div>
          </div>

          <div class="form-group">
          <label for="password" class="form-label">Password</label>
          <input
          id="password"
          name="password"
          type="password"
          required
          autocomplete="current-password"
          class="form-control"
          placeholder="Enter your password">
          </div>
```

```
          <div class="mb-4">
          <div class="form-check">
          <input type="checkbox" name="remember" class="form-check-input" id="remember">
          <label class="form-check-label" for="remember">
          Remember me
          </label>
          </div>
          </div>

          <button type="submit" class="btn-login">
          <i class="bi bi-box-arrow-in-right me-2"></i>
          Sign In
          </button>
          </form>
        </div>
      </div>

      <!-- Agency CTA Card -->
      <div class="agency-cta">
        <div class="agency-cta-title">
          <i class="bi bi-building"></i>
          <span>New Agency?</span>
        </div>
        <p class="subtitle">
          Relief agencies can request access to DMIS to submit relief requests and manage disaster response distributions.
        </p>
        <a href="/account-requests/submit" class="btn-agency-request">
          <i class="bi bi-plus-circle"></i>
          Request Agency Account
        </a>
        <ul class="info-list">
          <li>
          <i class="bi bi-check-circle-fill"></i>
          <span>Approval by ODPEM required</span>
          </li>
          <li>
          <i class="bi bi-check-circle-fill"></i>
          <span>Email updates on request status</span>
          </li>
          <li>
          <i class="bi bi-check-circle-fill"></i>
          <span>Full access after approval</span>
          </li>
        </ul>
      </div>

      <!-- Footer -->
      <div class="login-footer">
        <div class="login-footer-badge">
          <i class="bi bi-shield-check"></i>
          <span>Secure Government System</span>
        </div>
        <p>© 2025 DMIS - Disaster Management Information System</p>
        <p class="login-footer-small">By signing in you agree to the acceptable use and data policies</p>
      </div>
    </div>
  </div>

  <script src="https://cdn.jsdelivr.net/npm/bootstrap@5.3.3/dist/js/bootstrap.bundle.min.js"></script>
</body>
</html>
```

Issue 2 of 2

TOC

Cacheable SSL Page Found

Severity:	Medium
CVSS Score:	5.3
URL:	https://drims.nginxdev.egovja.com/account-requests/submit
Entity:	submit (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Sensitive information might have been cached by your browser
Fix:	Prevent caching of SSL pages by adding "Cache-Control: no-store" and "Pragma: no-cache" headers to their responses.

Difference:

Reasoning: The application has responded with a response that indicates the page should be cached, but cache controls aren't set (you can set "Cache-Control: no-store" or "Cache-Control: no-cache" or "Pragma: no-cache" to prevent caching).

Test Requests and Responses:

```
GET /account-requests/submit HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://drims.nginxdev.egovja.com/account-requests/
Host: drims.nginxdev.egovja.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: session=eyJfZnJlc2giOmZhbHNlfQ.aSEfKw.SM5yxUK0BBPJmHkTb-ZxH5m7m_g
Content-Length: 0


HTTP/1.1 200 OK
Server: nginx
Date: Sat, 22 Nov 2025 02:32:04 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 26664
Connection: keep-alive
Vary: Cookie

<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Request Agency Account - DMIS - Disaster Management Information System</title>
    <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.3/dist/css/bootstrap.min.css" rel="stylesheet">
    <link rel="stylesheet" href="https://cdn.jsdelivr.net/npm/bootstrap-icons@1.11.3/font/bootstrap-icons.css">
    <!-- DMIS Modern UI Design System -->
    <link rel="stylesheet" href="/static/css/modern-ui.css">
    <link rel="stylesheet" href="/static/css/workflow-sidebar.css">
    <link rel="stylesheet" href="/static/css/notifications-ui.css">
    <style>
        :root {
          --goj-green: #009639;
          --goj-gold: #FDB913;
          --goj-black: #000000;
          --goj-light-green: #E8F5E9;
          --sidebar-width: 260px;
          --sidebar-collapsed-width: 70px;
          --header-height: 60px;
        }

        body {
          font-family: 'Segoe UI', Tahoma, Geneva, Verdana, sans-serif;
          font-size: 0.9rem;
          background-color: #f5f7fa;
          margin: 0;
          padding: 0;
        }

        .top-header {
          position: fixed;
          top: 0;
          left: 0;
          right: 0;
          height: var(--header-height);
```

```
  background: linear-gradient(135deg, var(--goj-green) 0%, #007d42 100%);
  color: white;
  display: flex;
  align-items: center;
  padding: 0 20px;
  z-index: 1030;
  box-shadow: 0 2px 4px rgba(0,0,0,0.1);
}

.hamburger-menu {
  background: none;
  border: none;
  color: white;
  font-size: 1.5rem;
  cursor: pointer;
  padding: 8px 12px;
  margin-right: 15px;
  min-width: 44px;
  min-height: 44px;
  display: flex;
  align-items: center;
  justify-content: center;
  border-radius: 4px;
  transition: background-color 0.2s ease;
  -webkit-tap-highlight-color: transparent;
  position: relative;
  z-index: 1;
}

.hamburger-menu:hover {
  background-color: rgba(255,255,255,0.1);
}

.hamburger-menu:active {
  background-color: rgba(255,255,255,0.2);
}

.hamburger-menu:focus-visible {
  outline: 3px solid var(--goj-gold);
  outline-offset: 2px;
}

.brand-logo {
  display: flex;
  align-items: center;
  color: white;
  text-decoration: none;
  font-size: 1.5rem;
  font-weight: bold;
  gap: 12px;
}

.brand-logo:hover {
  color: var(--goj-gold);
}

.brand-logo img {
  height: 40px;
  width: auto;
  transition: transform 0.2s;
}

.brand-logo:hover img {
  transform: scale(1.05);
}

.brand-text {
  display: flex;
  flex-direction: column;
  line-height: 1.2;
}

.brand-text-main {
  font-size: 1.3rem;
  font-weight: 700;
  letter-spacing: 0.5px;
}

.brand-text-sub {
  font-size: 0.65rem;
  opacity: 0.9;
  font-weight: 400;
}
```

```
          .header-right {
            margin-left: auto;
            display: flex;
            align-items: center;
            gap: 20px;
          }

          .notification-bell {
            position: relative;
            background: none;
            border: none;
            color: white;
            font-size: 1.3rem;
            cursor: pointer;
            padding: 5px 10px;
          }

          .notification-bell:hover {
            background-color: rgba(255,255,255,0.1);
            border-radius: 4px;
          }

          .notification-badge {
            position: absolute;
            top: 0;
            right: 5px;
            background-color: #dc3545;
            color: white;
            border-radius: 50%;
            padding: 2px 6px;

...
...
...
```

M Check for SRI (Subresource Integrity) support 2 TOC

Issue 1 of 2 TOC

Check for SRI (Subresource Integrity) support

Severity:	Medium
CVSS Score:	5.3
URL:	https://drims.nginxdev.egovja.com/login
Entity:	login (Page)
Risk:	In case the third-party server is compromised, the content/behavior of the site will change
Cause:	There is no support to Subresource Integrity.
Fix:	Add to each third-party script/link element support to SRI(Subresource Integrity).

Difference:

Reasoning: The third-party links/scripts don't have integrity attribute for the browser to confirm they didn't compromised

Test Requests and Responses:

```
GET /login?next=%2F HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://drims.nginxdev.egovja.com/
```

```
Host: drims.nginxdev.egovja.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: session=eyJfZnJlc2giOmZhbHNlfQ.aSEfKw.SM5yxUK0BBPJmHkTb-ZxH5m7m_g
Content-Length: 0


HTTP/1.1 200 OK
Server: nginx
Date: Sat, 22 Nov 2025 02:33:41 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 4388
Connection: keep-alive
Vary: Cookie


<!doctype html>
<html lang="en">
<head>
  <meta charset="utf-8">
  <title>Login · DMIS</title>
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.3/dist/css/bootstrap.min.css" rel="stylesheet">
  <link rel="stylesheet" href="https://cdn.jsdelivr.net/npm/bootstrap-icons@1.11.3/font/bootstrap-icons.css">
  <link rel="stylesheet" href="/static/css/modern-ui.css">
</head>
<body>
  <div class="login-container">
    <div>
      <!-- Login Card -->
      <div class="login-card">
        <div class="login-header">
          <div class="login-header-logos">
          <img src="/static/images/jamaica-coat-of-arms.png"
          alt="Jamaica Coat of Arms">
          <img src="/static/images/odpem-logo.png"
          alt="ODPEM Logo">
          </div>
          <h1>Disaster Management Information System</h1>
          <p class="login-header-subtitle">DMIS</p>
          <p class="login-header-meta">Government of Jamaica</p>
        </div>

        <div class="login-body">
          <h2>Sign in to your account</h2>
          <p class="subtitle">Use your email and password to access DMIS.</p>

          <!-- Flash messages -->




          <form method="post" action="/login" novalidate>
          <div class="form-group">
          <label for="email" class="form-label">Email Address</label>
          <input
          id="email"
          name="email"
          type="email"
          required
          autocomplete="email"
          class="form-control"
          placeholder="your.email@odpem.gov.jm"
          value=""
          aria-describedby="email-help">
          <div id="email-help" class="form-text">
          Enter the email address associated with your DMIS account
          </div>
          </div>

          <div class="form-group">
          <label for="password" class="form-label">Password</label>
          <input
          id="password"
          name="password"
          type="password"
          required
          autocomplete="current-password"
          class="form-control"
          placeholder="Enter your password">
          </div>

          <div class="mb-4">
          <div class="form-check">
          <input type="checkbox" name="remember" class="form-check-input" id="remember">
```

```
          <label class="form-check-label" for="remember">
          Remember me
          </label>
          </div>
          </div>

          <button type="submit" class="btn-login">
          <i class="bi bi-box-arrow-in-right me-2"></i>
          Sign In
          </button>
          </form>
        </div>
      </div>

      <!-- Agency CTA Card -->
      <div class="agency-cta">
        <div class="agency-cta-title">
          <i class="bi bi-building"></i>
          <span>New Agency?</span>
        </div>
        <p class="subtitle">
          Relief agencies can request access to DMIS to submit relief requests and manage disaster response distributions.
        </p>
        <a href="/account-requests/submit" class="btn-agency-request">
          <i class="bi bi-plus-circle"></i>
          Request Agency Account
        </a>
        <ul class="info-list">
          <li>
          <i class="bi bi-check-circle-fill"></i>
          <span>Approval by ODPEM required</span>
          </li>
          <li>
          <i class="bi bi-check-circle-fill"></i>
          <span>Email updates on request status</span>
          </li>
          <li>
          <i class="bi bi-check-circle-fill"></i>
          <span>Full access after approval</span>
          </li>
        </ul>
      </div>

      <!-- Footer -->
      <div class="login-footer">
        <div class="login-footer-badge">
          <i class="bi bi-shield-check"></i>
          <span>Secure Government System</span>
        </div>
        <p>© 2025 DMIS - Disaster Management Information System</p>
        <p class="login-fo
...
...
...

  <script src="https://cdn.jsdelivr.net/npm/bootstrap@5.3.3/dist/js/bootstrap.bundle.min.js"></script>
</body>
</html>
```

Issue 2 of 2

TOC

Check for SRI (Subresource Integrity) support

Severity:	Medium
CVSS Score:	5.3
URL:	https://drims.nginxdev.egovja.com/account-requests/submit
Entity:	submit (Page)
Risk:	In case the third-party server is compromised, the content/behavior of the site will change
Cause:	There is no support to Subresource Integrity.
Fix:	Add to each third-party script/link element support to SRI(Subresource Integrity).

Difference:

Reasoning: The third-party links/scripts don't have integrity attribute for the browser to confirm they didn't compromised

Test Requests and Responses:

```
GET /account-requests/submit HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://drims.nginxdev.egovja.com/account-requests/
Host: drims.nginxdev.egovja.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: session=eyJfZnJlc2giOmZhbHNlfQ.aSEfKw.SM5yxUK0BBPJmHkTb-ZxH5m7m_g
Content-Length: 0


HTTP/1.1 200 OK
Server: nginx
Date: Sat, 22 Nov 2025 02:32:04 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 26664
Connection: keep-alive
Vary: Cookie

<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Request Agency Account - DMIS - Disaster Management Information System</title>
    <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.3/dist/css/bootstrap.min.css" rel="stylesheet">
    <link rel="stylesheet" href="https://cdn.jsdelivr.net/npm/bootstrap-icons@1.11.3/font/bootstrap-icons.css">
    <!-- DMIS Modern UI Design System -->
    <link rel="stylesheet" href="/static/css/modern-ui.css">
    <link rel="stylesheet" href="/static/css/workflow-sidebar.css">
    <link rel="stylesheet" href="/static/css/notifications-ui.css">
    <style>
        :root {
          --goj-green: #009639;
          --goj-gold: #FDB913;
          --goj-black: #000000;
          --goj-light-green: #E8F5E9;
          --sidebar-width: 260px;
          --sidebar-collapsed-width: 70px;
          --header-height: 60px;
        }

        body {
          font-family: 'Segoe UI', Tahoma, Geneva, Verdana, sans-serif;
          font-size: 0.9rem;
          background-color: #f5f7fa;
          margin: 0;
          padding: 0;
        }

        .top-header {
          position: fixed;
          top: 0;
          left: 0;
          right: 0;
          height: var(--header-height);
          background: linear-gradient(135deg, var(--goj-green) 0%, #007d42 100%);
          color: white;
          display: flex;
```

```
    align-items: center;
    padding: 0 20px;
    z-index: 1030;
    box-shadow: 0 2px 4px rgba(0,0,0,0.1);
  }

  .hamburger-menu {
    background: none;
    border: none;
    color: white;
    font-size: 1.5rem;
    cursor: pointer;
    padding: 8px 12px;
    margin-right: 15px;
    min-width: 44px;
    min-height: 44px;
    display: flex;
    align-items: center;
    justify-content: center;
    border-radius: 4px;
    transition: background-color 0.2s ease;
    -webkit-tap-highlight-color: transparent;
    position: relative;
    z-index: 1;
  }

  .hamburger-menu:hover {
    background-color: rgba(255,255,255,0.1);
  }

  .hamburger-menu:active {
    background-color: rgba(255,255,255,0.2);
  }

  .hamburger-menu:focus-visible {
    outline: 3px solid var(--goj-gold);
    outline-offset: 2px;
  }

  .brand-logo {
    display: flex;
    align-items: center;
    color: white;
    text-decoration: none;
    font-size: 1.5rem;
    font-weight: bold;
    gap: 12px;
  }

  .brand-logo:hover {
    color: var(--goj-gold);
  }

  .brand-logo img {
    height: 40px;
    width: auto;
    transition: transform 0.2s;
  }

  .brand-logo:hover img {
    transform: scale(1.05);
  }

  .brand-text {
    display: flex;
    flex-direction: column;
    line-height: 1.2;
  }

  .brand-text-main {
    font-size: 1.3rem;
    font-weight: 700;
    letter-spacing: 0.5px;
  }

  .brand-text-sub {
    font-size: 0.65rem;
    opacity: 0.9;
    font-weight: 400;
  }

  .header-right {
    margin-left: auto;
    display: flex;
```

```
            align-items: center;
            gap: 20px;
        }

        .notification-bell {
            position: relative;
            background: none;
            border: none;
            color: white;
            font-size: 1.3rem;

...
...
...

    <script src="https://cdn.jsdelivr.net/npm/bootstrap@5.3.3/dist/js/bootstrap.bundle.min.js"></script>
    <script>
        document.addEventListener('DOMContentLoaded', function() {
            const sidebar = document.getElementById('sidebar');
            const sidebarToggle = document.getElementById('sidebarToggle');
...
...
...
```

M Cookie with Insecure or Improper or Missing SameSite attribute 1 TOC

Issue 1 of 1 TOC

Cookie with Insecure or Improper or Missing SameSite attribute

Severity:	Medium
CVSS Score:	4.7
URL:	https://drims.nginxdev.egovja.com/
Entity:	session (Cookie)
Risk:	Prevent cookie information leakage by restricting cookies to first-party or same-site context, Attacks can extend to Cross-Site-Request-Forgery (CSRF) attacks if there are no additional protections in place (such as Anti-CSRF tokens).
Cause:	Sensitive Cookie with Improper or Insecure or Missing SameSite Attribute
Fix:	Review possible solutions for configuring SameSite Cookie attribute to recommended values

Difference:

Reasoning: The response contains Sensitive Cookie with Insecure or Improper or Missing SameSite attribute, which may lead to Cookie information leakage, which may extend to Cross-Site-Request-Forgery(CSRF) attacks if there are no additional protections in place.

Test Requests and Responses:

```
GET / HTTP/1.1
Host: drims.nginxdev.egovja.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
```

```
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Content-Length: 0


HTTP/1.1 302 FOUND
Server: nginx
Date: Sat, 22 Nov 2025 02:31:22 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 217
Connection: keep-alive
Location: /login?next=%2F
Vary: Cookie
Set-Cookie:
session=eyJfZmxhc2hlcyI6W3siIHQiOlsibWVzc2FnZSIsIlBsZWFzZSBsb2cgaW4gdG8gYWNjZXNzIHRoaXMgcGFnZS4iXX1dfQ.aSEgeQ.Ry1F0JUteRGqn
lzsM7fpfIQSnpk; HttpOnly; Path=/

<!doctype html>
<html lang=en>
<title>Redirecting...</title>
<h1>Redirecting...</h1>
<p>You should be redirected automatically to the target URL: <a href="/login?next=%2F">/login?next=%2F</a>. If not, click
the link.


GET /login?next=%2F HTTP/1.1
Cookie:
session=eyJfZmxhc2hlcyI6W3siIHQiOlsibWVzc2FnZSIsIlBsZWFzZSBsb2cgaW4gdG8gYWNjZXNzIHRoaXMgcGFnZS4iXX1dfQ.aSEgeQ.Ry1F0JUteRGqn
lzsM7fpfIQSnpk
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://drims.nginxdev.egovja.com/
Host: drims.nginxdev.egovja.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Content-Length: 0


HTTP/1.1 200 OK
Server: nginx
Date: Sat, 22 Nov 2025 02:31:22 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 4835
Connection: keep-alive
Vary: Cookie
Set-Cookie: session=eyJfZnJlc2giOmZhbHNlfQ.aSEgeQ.cI-wN_RGAuPYUAgihlA5wn5Zhzk; HttpOnly; Path=/


<!doctype html>
<html lang="en">
<head>
  <meta charset="utf-8">
  <title>Login · DMIS</title>
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.3/dist/css/bootstrap.min.css" rel="stylesheet">
  <link rel="stylesheet" href="https://cdn.jsdelivr.net/npm/bootstrap-icons@1.11.3/font/bootstrap-icons.css">
  <link rel="stylesheet" href="/static/css/modern-ui.css">
</head>
<body>
  <div class="login-container">
    <div>
      <!-- Login Card -->
      <div class="login-card">
        <div class="login-header">
          <div class="login-header-logos">
          <img src="/static/images/jamaica-coat-of-arms.png"
          alt="Jamaica Coat of Arms">
          <img src="/static/images/odpem-logo.png"
          alt="ODPEM Logo">
          </div>
          <h1>Disaster Management Information System</h1>
          <p class="login-header-subtitle">DMIS</p>
          <p class="login-header-meta">Government of Jamaica</p>
        </div>

        <div class="login-body">
          <h2>Sign in to your account</h2>
          <p class="subtitle">Use your email and password to access DMIS.</p>

          <!-- Flash messages -->


          <div class="mb-3">

          <div class="alert alert-success alert-dismissible fade show" role="alert">
```

```
            <i class="bi bi-check-circle me-2"></i>
            Please log in to access this page.
            <button type="button" class="btn-close" data-bs-dismiss="alert" aria-label="Close"></button>
            </div>

            </div>



            <form method="post" action="/login" novalidate>
            <div class="form-group">
            <label for="email" class="form-label">Email Address</label>
            <input
            id="email"
            name="email"
            type="email"
            required
            autocomplete="email"
            class="form-control"
            placeholder="your.email@odpem.gov.jm"
            value=""
            aria-describedby="email-help">
            <div id="email-help" class="form-text">
            Enter the email address associated with your DMIS account
            </div>
            </div>

            <div class="form-group">
            <label for="password" class="form-label">Password</label>
            <input
            id="password"
            name="password"
            type="password"
            required
            autocomplete="current-password"
            class="form-control"
            placeholder="Enter your password">
            </div>

            <div class="mb-4">
            <div class="form-check">
            <input type="checkbox" name="remember" class="form-check-input" id="remember">
            <label class="form-check-label" for="remember">
            Remember me
            </label>
            </di
...
...
...
```

M Hidden Directory Detected 1 TOC

Issue 1 of 1 TOC

Hidden Directory Detected

Severity:	Medium
CVSS Score:	5.3
URL:	https://drims.nginxdev.egovja.com/
Entity:	static/ (Page)
Risk:	It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
Cause:	The web server or application server are configured in an insecure way
Fix:	Issue a "404 - Not Found" response status code for a forbidden resource, or remove it completely

Difference: **Path** manipulated from: `/` to: `/static/`

Reasoning: The test tried to detect hidden directories on the server. The 403 Forbidden response reveals the existence of the directory, even though access is not allowed.

Test Requests and Responses:

```
GET /static/ HTTP/1.1
Host: drims.nginxdev.egovja.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Content-Length: 0


HTTP/1.1 403 Forbidden
Server: nginx
Date: Sat, 22 Nov 2025 02:35:03 GMT
Content-Type: text/html
Content-Length: 555
Connection: keep-alive
```

M Missing "Content-Security-Policy" header 1

TOC

Issue 1 of 1

TOC

Missing "Content-Security-Policy" header

Severity:	Medium
CVSS Score:	5.3
URL:	https://drims.nginxdev.egovja.com/
Entity:	drims.nginxdev.egovja.com (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	Insecure web application programming or configuration
Fix:	Config your server to use the "Content-Security-Policy" header with secure policies

Difference:

Reasoning: AppScan detected that the Content-Security-Policy response header is missing or with an insecure policy, which increases exposure to various cross-site injection attacks

Test Requests and Responses:

```
GET /account-requests/submit HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://drims.nginxdev.egovja.com/account-requests/
Host: drims.nginxdev.egovja.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: session=eyJfZnJlc2giOmZhbHNlfQ.aSEfKw.SM5yxUK0BBPJmHkTb-ZxH5m7m_g
Content-Length: 0


HTTP/1.1 200 OK
Server: nginx
Date: Sat, 22 Nov 2025 02:32:04 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 26664
Connection: keep-alive
Vary: Cookie

<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Request Agency Account - DMIS - Disaster Management Information System</title>
    <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.3/dist/css/bootstrap.min.css" rel="stylesheet">
    <link rel="stylesheet" href="https://cdn.jsdelivr.net/npm/bootstrap-icons@1.11.3/font/bootstrap-icons.css">
    <!-- DMIS Modern UI Design System -->
    <link rel="stylesheet" href="/static/css/modern-ui.css">
    <link rel="stylesheet" href="/static/css/workflow-sidebar.css">
    <link rel="stylesheet" href="/static/css/notifications-ui.css">
    <style>
        :root {
          --goj-green: #009639;
          --goj-gold: #FDB913;
          --goj-black: #000000;
          --goj-light-green: #E8F5E9;
          --sidebar-width: 260px;
          --sidebar-collapsed-width: 70px;
          --header-height: 60px;
        }

        body {
          font-family: 'Segoe UI', Tahoma, Geneva, Verdana, sans-serif;
          font-size: 0.9rem;
          background-color: #f5f7fa;
          margin: 0;
          padding: 0;
        }

        .top-header {
          position: fixed;
          top: 0;
          left: 0;
```

```
  right: 0;
  height: var(--header-height);
  background: linear-gradient(135deg, var(--goj-green) 0%, #007d42 100%);
  color: white;
  display: flex;
  align-items: center;
  padding: 0 20px;
  z-index: 1030;
  box-shadow: 0 2px 4px rgba(0,0,0,0.1);
}

.hamburger-menu {
  background: none;
  border: none;
  color: white;
  font-size: 1.5rem;
  cursor: pointer;
  padding: 8px 12px;
  margin-right: 15px;
  min-width: 44px;
  min-height: 44px;
  display: flex;
  align-items: center;
  justify-content: center;
  border-radius: 4px;
  transition: background-color 0.2s ease;
  -webkit-tap-highlight-color: transparent;
  position: relative;
  z-index: 1;
}

.hamburger-menu:hover {
  background-color: rgba(255,255,255,0.1);
}

.hamburger-menu:active {
  background-color: rgba(255,255,255,0.2);
}

.hamburger-menu:focus-visible {
  outline: 3px solid var(--goj-gold);
  outline-offset: 2px;
}

.brand-logo {
  display: flex;
  align-items: center;
  color: white;
  text-decoration: none;
  font-size: 1.5rem;
  font-weight: bold;
  gap: 12px;
}

.brand-logo:hover {
  color: var(--goj-gold);
}

.brand-logo img {
  height: 40px;
  width: auto;
  transition: transform 0.2s;
}

.brand-logo:hover img {
  transform: scale(1.05);
}

.brand-text {
  display: flex;
  flex-direction: column;
  line-height: 1.2;
}

.brand-text-main {
  font-size: 1.3rem;
  font-weight: 700;
  letter-spacing: 0.5px;
}

.brand-text-sub {
  font-size: 0.65rem;
  opacity: 0.9;
  font-weight: 400;
```

```
        }

        .header-right {
          margin-left: auto;
          display: flex;
          align-items: center;
          gap: 20px;
        }

        .notification-bell {
          position: relative;
          background: none;
          border: none;
          color: white;
          font-size: 1.3rem;
          cursor: pointer;
          padding: 5px 10px;
        }

        .notification-bell:hover {
          background-color: rgba(255,255,255,0.1);
          border-radius: 4px;
        }

        .notification-badge {
          position: absolute;
          top: 0;
          right: 5px;
          background-color: #dc3545;
          color: white;
          border-radius: 50%
...
...
...
```

M Missing Secure Attribute in Encrypted Session (SSL) Cookie 1 TOC

Issue 1 of 1 TOC

Missing Secure Attribute in Encrypted Session (SSL) Cookie

Severity:	Medium
CVSS Score:	6.5
URL:	https://drims.nginxdev.egovja.com/
Entity:	session (Cookie)
Risk:	It may be possible to steal user and session information (cookies) that was sent during an encrypted session
Cause:	The web application sends non-secure cookies over SSL
Fix:	Add the 'Secure' attribute to all sensitive cookies

Difference:

Reasoning: AppScan found that an encrypted session (SSL) is using a cookie without the "secure" attribute.

Test Requests and Responses:

```
GET / HTTP/1.1
Host: drims.nginxdev.egovja.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```

```
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Content-Length: 0


HTTP/1.1 302 FOUND
Server: nginx
Date: Sat, 22 Nov 2025 02:31:22 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 217
Connection: keep-alive
Location: /login?next=%2F
Vary: Cookie
Set-Cookie:
session=eyJfZmxhc2hlcyI6W3siIHQiOlsibWVzc2FnZSIsIlBsZWFzZSBsb2cgaW4gdG8gYWNjZXNzIHRoaXMgcGFnZS4iXX1dfQ.aSEgeQ.Ry1F0JUteRGqn
lzsM7fpfIQSnpk; HttpOnly; Path=/

<!doctype html>
<html lang=en>
<title>Redirecting...</title>
<h1>Redirecting...</h1>
<p>You should be redirected automatically to the target URL: <a href="/login?next=%2F">/login?next=%2F</a>. If not, click
the link.


GET /login?next=%2F HTTP/1.1
Cookie:
session=eyJfZmxhc2hlcyI6W3siIHQiOlsibWVzc2FnZSIsIlBsZWFzZSBsb2cgaW4gdG8gYWNjZXNzIHRoaXMgcGFnZS4iXX1dfQ.aSEgeQ.Ry1F0JUteRGqn
lzsM7fpfIQSnpk
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://drims.nginxdev.egovja.com/
Host: drims.nginxdev.egovja.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Content-Length: 0


HTTP/1.1 200 OK
Server: nginx
Date: Sat, 22 Nov 2025 02:31:22 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 4835
Connection: keep-alive
Vary: Cookie
Set-Cookie: session=eyJfZnJlc2giOmZhbHNlfQ.aSEgeQ.cI-wN_RGAuPYUAgihlA5wn5Zhzk; HttpOnly; Path=/


<!doctype html>
<html lang="en">
<head>
  <meta charset="utf-8">
  <title>Login · DMIS</title>
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.3/dist/css/bootstrap.min.css" rel="stylesheet">
  <link rel="stylesheet" href="https://cdn.jsdelivr.net/npm/bootstrap-icons@1.11.3/font/bootstrap-icons.css">
  <link rel="stylesheet" href="/static/css/modern-ui.css">
</head>
<body>
  <div class="login-container">
    <div>
      <!-- Login Card -->
      <div class="login-card">
        <div class="login-header">
          <div class="login-header-logos">
          <img src="/static/images/jamaica-coat-of-arms.png"
          alt="Jamaica Coat of Arms">
          <img src="/static/images/odpem-logo.png"
          alt="ODPEM Logo">
          </div>
          <h1>Disaster Management Information System</h1>
          <p class="login-header-subtitle">DMIS</p>
          <p class="login-header-meta">Government of Jamaica</p>
        </div>

        <div class="login-body">
          <h2>Sign in to your account</h2>
          <p class="subtitle">Use your email and password to access DMIS.</p>
```

```
          <!-- Flash messages -->


          <div class="mb-3">

          <div class="alert alert-success alert-dismissible fade show" role="alert">
          <i class="bi bi-check-circle me-2"></i>
          Please log in to access this page.
          <button type="button" class="btn-close" data-bs-dismiss="alert" aria-label="Close"></button>
          </div>

          </div>



          <form method="post" action="/login" novalidate>
          <div class="form-group">
          <label for="email" class="form-label">Email Address</label>
          <input
          id="email"
          name="email"
          type="email"
          required
          autocomplete="email"
          class="form-control"
          placeholder="your.email@odpem.gov.jm"
          value=""
          aria-describedby="email-help">
          <div id="email-help" class="form-text">
          Enter the email address associated with your DMIS account
          </div>
          </div>

          <div class="form-group">
          <label for="password" class="form-label">Password</label>
          <input
          id="password"
          name="password"
          type="password"
          required
          autocomplete="current-password"
          class="form-control"
          placeholder="Enter your password">
          </div>

          <div class="mb-4">
          <div class="form-check">
          <input type="checkbox" name="remember" class="form-check-input" id="remember">
          <label class="form-check-label" for="remember">
          Remember me
          </label>
          </di
...
...
...
```

M Missing or insecure "X-Content-Type-Options" header 1 TOC

Issue 1 of 1 TOC

Missing or insecure "X-Content-Type-Options" header

Severity:	Medium
CVSS Score:	5.3
URL:	https://drims.nginxdev.egovja.com/
Entity:	drims.nginxdev.egovja.com (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	Insecure web application programming or configuration
Fix:	Config your server to use the "X-Content-Type-Options" header with "nosniff" value

Difference:

Reasoning: AppScan detected that the "X-Content-Type-Options" response header is missing or has an insecure value, which increases exposure to drive-by download attacks

Test Requests and Responses:

```
GET /login?next=%2F HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://drims.nginxdev.egovja.com/
Host: drims.nginxdev.egovja.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: session=eyJfZnJlc2giOmZhbHNlfQ.aSEfKw.SM5yxUK0BBPJmHkTb-ZxH5m7m_g
Content-Length: 0


HTTP/1.1 200 OK
Server: nginx
Date: Sat, 22 Nov 2025 02:33:41 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 4388
Connection: keep-alive
Vary: Cookie


<!doctype html>
<html lang="en">
<head>
  <meta charset="utf-8">
  <title>Login · DMIS</title>
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.3/dist/css/bootstrap.min.css" rel="stylesheet">
  <link rel="stylesheet" href="https://cdn.jsdelivr.net/npm/bootstrap-icons@1.11.3/font/bootstrap-icons.css">
  <link rel="stylesheet" href="/static/css/modern-ui.css">
</head>
<body>
  <div class="login-container">
    <div>
      <!-- Login Card -->
      <div class="login-card">
        <div class="login-header">
          <div class="login-header-logos">
          <img src="/static/images/jamaica-coat-of-arms.png"
          alt="Jamaica Coat of Arms">
          <img src="/static/images/odpem-logo.png"
          alt="ODPEM Logo">
          </div>
          <h1>Disaster Management Information System</h1>
          <p class="login-header-subtitle">DMIS</p>
          <p class="login-header-meta">Government of Jamaica</p>
        </div>

        <div class="login-body">
          <h2>Sign in to your account</h2>
          <p class="subtitle">Use your email and password to access DMIS.</p>

          <!-- Flash messages -->
```

```
          <form method="post" action="/login" novalidate>
          <div class="form-group">
          <label for="email" class="form-label">Email Address</label>
          <input
          id="email"
          name="email"
          type="email"
          required
          autocomplete="email"
          class="form-control"
          placeholder="your.email@odpem.gov.jm"
          value=""
          aria-describedby="email-help">
          <div id="email-help" class="form-text">
          Enter the email address associated with your DMIS account
          </div>
          </div>

          <div class="form-group">
          <label for="password" class="form-label">Password</label>
          <input
          id="password"
          name="password"
          type="password"
          required
          autocomplete="current-password"
          class="form-control"
          placeholder="Enter your password">
          </div>

          <div class="mb-4">
          <div class="form-check">
          <input type="checkbox" name="remember" class="form-check-input" id="remember">
          <label class="form-check-label" for="remember">
          Remember me
          </label>
          </div>
          </div>

          <button type="submit" class="btn-login">
          <i class="bi bi-box-arrow-in-right me-2"></i>
          Sign In
          </button>
          </form>
        </div>
      </div>

      <!-- Agency CTA Card -->
      <div class="agency-cta">
        <div class="agency-cta-title">
          <i class="bi bi-building"></i>
          <span>New Agency?</span>
        </div>
        <p class="subtitle">
          Relief agencies can request access to DMIS to submit relief requests and manage disaster response distributions.
        </p>
        <a href="/account-requests/submit" class="btn-agency-request">
          <i class="bi bi-plus-circle"></i>
          Request Agency Account
        </a>
        <ul class="info-list">
          <li>
          <i class="bi bi-check-circle-fill"></i>
          <span>Approval by ODPEM required</span>
          </li>
          <li>
          <i class="bi bi-check-circle-fill"></i>
          <span>Email updates on request status</span>
          </li>
          <li>
          <i class="bi bi-check-circle-fill"></i>
          <span>Full access after approval</span>
          </li>
        </ul>
      </div>

      <!-- Footer -->
      <div class="login-footer">
        <div class="login-footer-badge">
          <i class="bi bi-shield-check"></i>
          <span>Secure Government System</span>
        </div>
```

```
        <p>© 2025 DMIS - Disaster Management Information System</p>
        <p class="login-footer-small">By signing in you agree to the acceptable use and data policies</p>
      </div>
    </div>
  </div>

  <script src="https://cdn.jsdelivr.net/npm/bootstrap@5.3.3/dist/js/bootstrap.bundle.min.js">
...
...
...
```

M Missing or insecure HTTP Strict-Transport-Security Header 1

TOC

Issue 1 of 1

TOC

Missing or insecure HTTP Strict-Transport-Security Header

Severity:	Medium
CVSS Score:	5.3
URL:	https://drims.nginxdev.egovja.com/
Entity:	drims.nginxdev.egovja.com (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	Insecure web application programming or configuration
Fix:	Implement the HTTP Strict-Transport-Security policy with a long "max-age"

Difference:

Reasoning: AppScan detected that the HTTP Strict-Transport-Security response header is missing or with insufficient "max-age"

Test Requests and Responses:

```
GET /login?next=%2F HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://drims.nginxdev.egovja.com/
Host: drims.nginxdev.egovja.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: session=eyJfZnJlc2giOmZhbHNlfQ.aSEfKw.SM5yxUK0BBPJmHkTb-ZxH5m7m_g
Content-Length: 0


HTTP/1.1 200 OK
Server: nginx
Date: Sat, 22 Nov 2025 02:33:41 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 4388
Connection: keep-alive
Vary: Cookie


<!doctype html>
<html lang="en">
<head>
  <meta charset="utf-8">
  <title>Login · DMIS</title>
```

```
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.3/dist/css/bootstrap.min.css" rel="stylesheet">
  <link rel="stylesheet" href="https://cdn.jsdelivr.net/npm/bootstrap-icons@1.11.3/font/bootstrap-icons.css">
  <link rel="stylesheet" href="/static/css/modern-ui.css">
</head>
<body>
  <div class="login-container">
    <div>
      <!-- Login Card -->
      <div class="login-card">
        <div class="login-header">
          <div class="login-header-logos">
          <img src="/static/images/jamaica-coat-of-arms.png"
          alt="Jamaica Coat of Arms">
          <img src="/static/images/odpem-logo.png"
          alt="ODPEM Logo">
          </div>
          <h1>Disaster Management Information System</h1>
          <p class="login-header-subtitle">DMIS</p>
          <p class="login-header-meta">Government of Jamaica</p>
        </div>

        <div class="login-body">
          <h2>Sign in to your account</h2>
          <p class="subtitle">Use your email and password to access DMIS.</p>

          <!-- Flash messages -->




          <form method="post" action="/login" novalidate>
          <div class="form-group">
          <label for="email" class="form-label">Email Address</label>
          <input
          id="email"
          name="email"
          type="email"
          required
          autocomplete="email"
          class="form-control"
          placeholder="your.email@odpem.gov.jm"
          value=""
          aria-describedby="email-help">
          <div id="email-help" class="form-text">
          Enter the email address associated with your DMIS account
          </div>
          </div>

          <div class="form-group">
          <label for="password" class="form-label">Password</label>
          <input
          id="password"
          name="password"
          type="password"
          required
          autocomplete="current-password"
          class="form-control"
          placeholder="Enter your password">
          </div>

          <div class="mb-4">
          <div class="form-check">
          <input type="checkbox" name="remember" class="form-check-input" id="remember">
          <label class="form-check-label" for="remember">
          Remember me
          </label>
          </div>
          </div>

          <button type="submit" class="btn-login">
          <i class="bi bi-box-arrow-in-right me-2"></i>
          Sign In
          </button>
          </form>
        </div>
      </div>

      <!-- Agency CTA Card -->
      <div class="agency-cta">
        <div class="agency-cta-title">
          <i class="bi bi-building"></i>
          <span>New Agency?</span>
        </div>
```

```
        <p class="subtitle">
          Relief agencies can request access to DMIS to submit relief requests and manage disaster response distributions.
        </p>
        <a href="/account-requests/submit" class="btn-agency-request">
          <i class="bi bi-plus-circle"></i>
          Request Agency Account
        </a>
        <ul class="info-list">
          <li>
          <i class="bi bi-check-circle-fill"></i>
          <span>Approval by ODPEM required</span>
          </li>
          <li>
          <i class="bi bi-check-circle-fill"></i>
          <span>Email updates on request status</span>
          </li>
          <li>
          <i class="bi bi-check-circle-fill"></i>
          <span>Full access after approval</span>
          </li>
        </ul>
      </div>

      <!-- Footer -->
      <div class="login-footer">
        <div class="login-footer-badge">
          <i class="bi bi-shield-check"></i>
          <span>Secure Government System</span>
        </div>
        <p>© 2025 DMIS - Disaster Management Information System</p>
        <p class="login-footer-small">By signing in you agree to the acceptable use and data policies</p>
      </div>
    </div>
  </div>

  <script src="https://cdn.jsdelivr.net/npm/bootstrap@5.3.3/dist/js/bootstrap.bundle.min.js"></script>
</body>
</html>
```

M SHA-1 cipher suites were detected 1 TOC

Issue 1 of 1 TOC

SHA-1 cipher suites were detected

Severity:	Medium
CVSS Score:	5.3
URL:	https://drims.nginxdev.egovja.com/
Entity:	drims.nginxdev.egovja.com (Page)
Risk:	It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user
Cause:	The web server or application server are configured in an insecure way
Fix:	Change server's supported ciphersuites

Difference:

Reasoning: AppScan determined that the site uses weak cipher suites by successfully creating SSL connections using each of the weak cipher suites listed here.

Test Requests and Responses:

```
GET / HTTP/1.1
Host: drims.nginxdev.egovja.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Content-Length: 0


HTTP/1.1 302 FOUND
Server: nginx
Date: Sat, 22 Nov 2025 02:25:05 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 217
Connection: keep-alive
Location: /login?next=%2F
Vary: Cookie
Set-Cookie:
session=eyJfZmxhc2hlcyI6W3siIHQiOlsibWVzc2FnZSIsIlBsZWFzZSBsb2cgaW4gdG8gYWNjZXNzIHRoaXMgcGFnZS4iXX1dfQ.aSEfAA.6tq9Ijf1oKY9K
R9Nak5Dr4Gpdgc; HttpOnly; Path=/

<!doctype html>
<html lang=en>
<title>Redirecting...</title>
<h1>Redirecting...</h1>
<p>You should be redirected automatically to the target URL: <a href="/login?next=%2F">/login?next=%2F</a>. If not, click
the link.


GET /login?next=%2F HTTP/1.1
Cookie:
session=eyJfZmxhc2hlcyI6W3siIHQiOlsibWVzc2FnZSIsIlBsZWFzZSBsb2cgaW4gdG8gYWNjZXNzIHRoaXMgcGFnZS4iXX1dfQ.aSEfAA.6tq9Ijf1oKY9K
R9Nak5Dr4Gpdgc
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://drims.nginxdev.egovja.com/
Host: drims.nginxdev.egovja.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Content-Length: 0


HTTP/1.1 200 OK
Server: nginx
Date: Sat, 22 Nov 2025 02:25:05 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 4835
Connection: keep-alive
Vary: Cookie
Set-Cookie: session=eyJfZnJlc2giOmZhbHNlfQ.aSEfAA.X5U5FidOpVknp0JhC9bu9RvxJ7o; HttpOnly; Path=/


<!doctype html>
<html lang="en">
<head>
  <meta charset="utf-8">
  <title>Login · DMIS</title>
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.3/dist/css/bootstrap.min.css" rel="stylesheet">
  <link rel="stylesheet" href="https://cdn.jsdelivr.net/npm/bootstrap-icons@1.11.3/font/bootstrap-icons.css">
  <link rel="stylesheet" href="/static/css/modern-ui.css">
</head>
<body>
  <div class="login-container">
    <div>
      <!-- Login Card -->
      <div class="login-card">
        <div class="login-header">
          <div class="login-header-logos">
          <img src="/static/images/jamaica-coat-of-arms.png"
          alt="Jamaica Coat of Arms">
          <img src="/static/images/odpem-logo.png"
          alt="ODPEM Logo">
          </div>
          <h1>Disaster Management Information System</h1>
          <p class="login-header-subtitle">DMIS</p>
```

```
            <p class="login-header-meta">Government of Jamaica</p>
          </div>

          <div class="login-body">
            <h2>Sign in to your account</h2>
            <p class="subtitle">Use your email and password to access DMIS.</p>

            <!-- Flash messages -->


            <div class="mb-3">

            <div class="alert alert-success alert-dismissible fade show" role="alert">
            <i class="bi bi-check-circle me-2"></i>
            Please log in to access this page.
            <button type="button" class="btn-close" data-bs-dismiss="alert" aria-label="Close"></button>
            </div>

            </div>



            <form method="post" action="/login" novalidate>
            <div class="form-group">
            <label for="email" class="form-label">Email Address</label>
            <input
            id="email"
            name="email"
            type="email"
            required
            autocomplete="email"
            class="form-control"
            placeholder="your.email@odpem.gov.jm"
            value=""
            aria-describedby="email-help">
            <div id="email-help" class="form-text">
            Enter the email address associated with your DMIS account
            </div>
            </div>

            <div class="form-group">
            <label for="password" class="form-label">Password</label>
            <input
            id="password"
            name="password"
            type="password"
            required
            autocomplete="current-password"
            class="form-control"
            placeholder="Enter your password">
            </div>

            <div class="mb-4">
            <div class="form-check">
            <input type="checkbox" name="remember" class="form-check-input" id="remember">
            <label class="form-check-label" for="remember">
            Remember me
            </label>
            </div>
            </div>

            <button t
...
...
...
```

Verify that the site uses the cryptographically weak cipher suites listed here.

The following weak cipher suites are supported by the server:

Id	Name	SSL Version
47	TLS_RSA_WITH_AES_128_CBC_SHA	TLS 1.2

Issue 1 of 1

TOC

Unnecessary Http Response Headers found in the Application

Severity:	Medium
CVSS Score:	5.3
URL:	https://drims.nginxdev.egovja.com/
Entity:	drims.nginxdev.egovja.com (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Insecure web application programming or configuration
Fix:	Do not allow sensitive information to leak.

Difference:

Reasoning: The response contains unnecessary headers, which may help attackers in planning further attacks.

Test Requests and Responses:

```
GET / HTTP/1.1
Host: drims.nginxdev.egovja.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Content-Length: 0


HTTP/1.1 302 FOUND
Server: nginx
Date: Sat, 22 Nov 2025 02:27:09 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 217
Connection: keep-alive
Location: /login?next=%2F
Vary: Cookie
Set-Cookie:
session=eyJfZmxhc2hlcyI6W3siIHQiOlsibWVzc2FnZSIsIlBsZWFzZSBsb2cgaW4gdG8gYWNjZXNzIHRoaXMgcGFnZS4iXX1dfQ.aSEffA.HNOnWi46CR1E2
xv7rkWZTpfVCgI; HttpOnly; Path=/

<!doctype html>
<html lang=en>
<title>Redirecting...</title>
<h1>Redirecting...</h1>
<p>You should be redirected automatically to the target URL: <a href="/login?next=%2F">/login?next=%2F</a>. If not, click
the link.


GET /login?next=%2F HTTP/1.1
Cookie:
session=eyJfZmxhc2hlcyI6W3siIHQiOlsibWVzc2FnZSIsIlBsZWFzZSBsb2cgaW4gdG8gYWNjZXNzIHRoaXMgcGFnZS4iXX1dfQ.aSEffA.HNOnWi46CR1E2
xv7rkWZTpfVCgI
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://drims.nginxdev.egovja.com/
Host: drims.nginxdev.egovja.com
```

```
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Content-Length: 0


HTTP/1.1 200 OK
Server: nginx
Date: Sat, 22 Nov 2025 02:27:09 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 4835
Connection: keep-alive
Vary: Cookie
Set-Cookie: session=eyJfZnJlc2giOmZhbHNlfQ.aSEffA.TU0TvaX_XeOEo8_jBITvBS3Ttu4; HttpOnly; Path=/


<!doctype html>
<html lang="en">
<head>
  <meta charset="utf-8">
  <title>Login · DMIS</title>
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.3/dist/css/bootstrap.min.css" rel="stylesheet">
  <link rel="stylesheet" href="https://cdn.jsdelivr.net/npm/bootstrap-icons@1.11.3/font/bootstrap-icons.css">
  <link rel="stylesheet" href="/static/css/modern-ui.css">
</head>
<body>
  <div class="login-container">
    <div>
      <!-- Login Card -->
      <div class="login-card">
        <div class="login-header">
          <div class="login-header-logos">
          <img src="/static/images/jamaica-coat-of-arms.png"
          alt="Jamaica Coat of Arms">
          <img src="/static/images/odpem-logo.png"
          alt="ODPEM Logo">
          </div>
          <h1>Disaster Management Information System</h1>
          <p class="login-header-subtitle">DMIS</p>
          <p class="login-header-meta">Government of Jamaica</p>
        </div>

        <div class="login-body">
          <h2>Sign in to your account</h2>
          <p class="subtitle">Use your email and password to access DMIS.</p>

          <!-- Flash messages -->


          <div class="mb-3">

          <div class="alert alert-success alert-dismissible fade show" role="alert">
          <i class="bi bi-check-circle me-2"></i>
          Please log in to access this page.
          <button type="button" class="btn-close" data-bs-dismiss="alert" aria-label="Close"></button>
          </div>

          </div>



          <form method="post" action="/login" novalidate>
          <div class="form-group">
          <label for="email" class="form-label">Email Address</label>
          <input
          id="email"
          name="email"
          type="email"
          required
          autocomplete="email"
          class="form-control"
          placeholder="your.email@odpem.gov.jm"
          value=""
          aria-describedby="email-help">
          <div id="email-help" class="form-text">
          Enter the email address associated with your DMIS account
          </div>
          </div>

          <div class="form-group">
          <label for="password" class="form-label">Password</label>
          <input
          id="password"
          name="password"
          type="password"
```

```
            required
            autocomplete="current-password"
            class="form-control"
            placeholder="Enter your password">
            </div>

            <div class="mb-4">
            <div class="form-check">
            <input type="checkbox" name="remember" class="form-check-input" id="remember">
            <label class="form-check-label" for="remember">
            Remember me
            </label>
            </di
...
...
...
```

M Weak Cipher Suites - ROBOT Attack : Vulnerable cipher suites are supported by the server 1

TOC

Issue 1 of 1

TOC

Weak Cipher Suites - ROBOT Attack : Vulnerable cipher suites are supported by the server

Severity:	Medium
CVSS Score:	6.5
URL:	https://drims.nginxdev.egovja.com/
Entity:	drims.nginxdev.egovja.com (Page)
Risk:	It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user
Cause:	Cipher Suites that support TLS-RSA key exchange were detected. The web server or application server with TLS implementation flaw may be vulnerable to ROBOT Attack. This issue does not necessarily mean that you are vulnerable. Please follow the advisory guideline.
Fix:	Change server's supported ciphersuites

Difference:

Reasoning: AppScan determined that the site uses weak cipher suites by successfully creating SSL connections using each of the weak cipher suites listed here.

Test Requests and Responses:

```
GET / HTTP/1.1
Host: drims.nginxdev.egovja.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Content-Length: 0
```

```
HTTP/1.1 302 FOUND
Server: nginx
Date: Sat, 22 Nov 2025 02:25:05 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 217
Connection: keep-alive
Location: /login?next=%2F
Vary: Cookie
Set-Cookie:
session=eyJfZmxhc2hlcyI6W3siIHQiOlsibWVzc2FnZSIsIlBsZWFzZSBsb2cgaW4gdG8gYWNjZXNzIHRoaXMgcGFnZS4iXX1dfQ.aSEfAA.6tq9Ijf1oKY9K
R9Nak5Dr4Gpdgc; HttpOnly; Path=/

<!doctype html>
<html lang=en>
<title>Redirecting...</title>
<h1>Redirecting...</h1>
<p>You should be redirected automatically to the target URL: <a href="/login?next=%2F">/login?next=%2F</a>. If not, click
the link.


GET /login?next=%2F HTTP/1.1
Cookie:
session=eyJfZmxhc2hlcyI6W3siIHQiOlsibWVzc2FnZSIsIlBsZWFzZSBsb2cgaW4gdG8gYWNjZXNzIHRoaXMgcGFnZS4iXX1dfQ.aSEfAA.6tq9Ijf1oKY9K
R9Nak5Dr4Gpdgc
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://drims.nginxdev.egovja.com/
Host: drims.nginxdev.egovja.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Content-Length: 0


HTTP/1.1 200 OK
Server: nginx
Date: Sat, 22 Nov 2025 02:25:05 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 4835
Connection: keep-alive
Vary: Cookie
Set-Cookie: session=eyJfZnJlc2giOmZhbHNlfQ.aSEfAA.X5U5FidOpVknp0JhC9bu9RvxJ7o; HttpOnly; Path=/


<!doctype html>
<html lang="en">
<head>
  <meta charset="utf-8">
  <title>Login · DMIS</title>
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.3/dist/css/bootstrap.min.css" rel="stylesheet">
  <link rel="stylesheet" href="https://cdn.jsdelivr.net/npm/bootstrap-icons@1.11.3/font/bootstrap-icons.css">
  <link rel="stylesheet" href="/static/css/modern-ui.css">
</head>
<body>
  <div class="login-container">
    <div>
      <!-- Login Card -->
      <div class="login-card">
        <div class="login-header">
          <div class="login-header-logos">
          <img src="/static/images/jamaica-coat-of-arms.png"
          alt="Jamaica Coat of Arms">
          <img src="/static/images/odpem-logo.png"
          alt="ODPEM Logo">
          </div>
          <h1>Disaster Management Information System</h1>
          <p class="login-header-subtitle">DMIS</p>
          <p class="login-header-meta">Government of Jamaica</p>
        </div>

        <div class="login-body">
          <h2>Sign in to your account</h2>
          <p class="subtitle">Use your email and password to access DMIS.</p>

          <!-- Flash messages -->


          <div class="mb-3">

          <div class="alert alert-success alert-dismissible fade show" role="alert">
          <i class="bi bi-check-circle me-2"></i>
          Please log in to access this page.
          <button type="button" class="btn-close" data-bs-dismiss="alert" aria-label="Close"></button>
          </div>
```

```
            </div>



            <form method="post" action="/login" novalidate>
            <div class="form-group">
            <label for="email" class="form-label">Email Address</label>
            <input
            id="email"
            name="email"
            type="email"
            required
            autocomplete="email"
            class="form-control"
            placeholder="your.email@odpem.gov.jm"
            value=""
            aria-describedby="email-help">
            <div id="email-help" class="form-text">
            Enter the email address associated with your DMIS account
            </div>
            </div>

            <div class="form-group">
            <label for="password" class="form-label">Password</label>
            <input
            id="password"
            name="password"
            type="password"
            required
            autocomplete="current-password"
            class="form-control"
            placeholder="Enter your password">
            </div>

            <div class="mb-4">
            <div class="form-check">
            <input type="checkbox" name="remember" class="form-check-input" id="remember">
            <label class="form-check-label" for="remember">
            Remember me
            </label>
            </div>
            </div>

            <button t
...
...
...
```

Verify that the site uses the cryptographically weak cipher suites listed here.

The following weak cipher suites are supported by the server:

Id	Name	SSL Version
47	TLS_RSA_WITH_AES_128_CBC_SHA	TLS 1.2

M Weak Ciphers are detected: Not all cipher suites support Perfect Forward Secrecy 1 TOC

Issue 1 of 1 TOC

Weak Ciphers are detected: Not all cipher suites support Perfect Forward Secrecy

Severity:	Medium
CVSS Score:	6.5
URL:	https://drims.nginxdev.egovja.com/
Entity:	drims.nginxdev.egovja.com (Page)
Risk:	It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user
Cause:	The web server or application server are configured in an insecure way
Fix:	Change server's supported ciphersuites

Difference:

Reasoning: AppScan determined that the site uses weak cipher suites by successfully creating SSL connections using each of the weak cipher suites listed here.

Test Requests and Responses:

```
GET / HTTP/1.1
Host: drims.nginxdev.egovja.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Content-Length: 0


HTTP/1.1 302 FOUND
Server: nginx
Date: Sat, 22 Nov 2025 02:25:05 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 217
Connection: keep-alive
Location: /login?next=%2F
Vary: Cookie
Set-Cookie:
session=eyJfZmxhc2hlcyI6W3siIHQiOlsibWVzc2FnZSIsIlBsZWFzZSBsb2cgaW4gdG8gYWNjZXNzIHRoaXMgcGFnZS4iXX1dfQ.aSEfAA.6tq9Ijf1oKY9K
R9Nak5Dr4Gpdgc; HttpOnly; Path=/

<!doctype html>
<html lang=en>
<title>Redirecting...</title>
<h1>Redirecting...</h1>
<p>You should be redirected automatically to the target URL: <a href="/login?next=%2F">/login?next=%2F</a>. If not, click
the link.


GET /login?next=%2F HTTP/1.1
Cookie:
session=eyJfZmxhc2hlcyI6W3siIHQiOlsibWVzc2FnZSIsIlBsZWFzZSBsb2cgaW4gdG8gYWNjZXNzIHRoaXMgcGFnZS4iXX1dfQ.aSEfAA.6tq9Ijf1oKY9K
R9Nak5Dr4Gpdgc
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://drims.nginxdev.egovja.com/
Host: drims.nginxdev.egovja.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Content-Length: 0


HTTP/1.1 200 OK
Server: nginx
Date: Sat, 22 Nov 2025 02:25:05 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 4835
Connection: keep-alive
Vary: Cookie
```

```
Set-Cookie: session=eyJfZnJlc2giOmZhbHNlfQ.aSEfAA.X5U5FidOpVknp0JhC9bu9RvxJ7o; HttpOnly; Path=/


<!doctype html>
<html lang="en">
<head>
  <meta charset="utf-8">
  <title>Login · DMIS</title>
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.3/dist/css/bootstrap.min.css" rel="stylesheet">
  <link rel="stylesheet" href="https://cdn.jsdelivr.net/npm/bootstrap-icons@1.11.3/font/bootstrap-icons.css">
  <link rel="stylesheet" href="/static/css/modern-ui.css">
</head>
<body>
  <div class="login-container">
    <div>
      <!-- Login Card -->
      <div class="login-card">
        <div class="login-header">
          <div class="login-header-logos">
          <img src="/static/images/jamaica-coat-of-arms.png"
          alt="Jamaica Coat of Arms">
          <img src="/static/images/odpem-logo.png"
          alt="ODPEM Logo">
          </div>
          <h1>Disaster Management Information System</h1>
          <p class="login-header-subtitle">DMIS</p>
          <p class="login-header-meta">Government of Jamaica</p>
        </div>

        <div class="login-body">
          <h2>Sign in to your account</h2>
          <p class="subtitle">Use your email and password to access DMIS.</p>

          <!-- Flash messages -->


          <div class="mb-3">

          <div class="alert alert-success alert-dismissible fade show" role="alert">
          <i class="bi bi-check-circle me-2"></i>
          Please log in to access this page.
          <button type="button" class="btn-close" data-bs-dismiss="alert" aria-label="Close"></button>
          </div>

          </div>



          <form method="post" action="/login" novalidate>
          <div class="form-group">
          <label for="email" class="form-label">Email Address</label>
          <input
          id="email"
          name="email"
          type="email"
          required
          autocomplete="email"
          class="form-control"
          placeholder="your.email@odpem.gov.jm"
          value=""
          aria-describedby="email-help">
          <div id="email-help" class="form-text">
          Enter the email address associated with your DMIS account
          </div>
          </div>

          <div class="form-group">
          <label for="password" class="form-label">Password</label>
          <input
          id="password"
          name="password"
          type="password"
          required
          autocomplete="current-password"
          class="form-control"
          placeholder="Enter your password">
          </div>

          <div class="mb-4">
          <div class="form-check">
          <input type="checkbox" name="remember" class="form-check-input" id="remember">
          <label class="form-check-label" for="remember">
          Remember me
```

```
            </label>
            </div>
            </div>

            <button t
...
...
...
```

Verify that the site uses the cryptographically weak cipher suites listed here.

The following weak cipher suites are supported by the server:

Id	Name	SSL Version
47	TLS_RSA_WITH_AES_128_CBC_SHA	TLS 1.2
53	TLS_RSA_WITH_AES_256_CBC_SHA	TLS 1.2
49308	TLS_RSA_WITH_AES_128_CCM	TLS 1.2
49309	TLS_RSA_WITH_AES_256_CCM	TLS 1.2

I Application Error 1 TOC

Issue 1 of 1 TOC

Application Error

Severity:	Informational
CVSS Score:	0.0
URL:	https://drims.nginxdev.egovja.com/login
Entity:	email (Parameter)
Risk:	It is possible to gather sensitive debugging information
Cause:	Proper bounds checking were not performed on incoming parameter values No validation was done in order to make sure that user input matches the data type expected
Fix:	Verify that parameter values are in their expected ranges and types. Do not output debugging error messages and exceptions

Difference: **Parameter** `email` manipulated from: `test@altoromutual.com` to: `%00`

Reasoning: The application has responded with an error message, indicating an undefined state that may expose sensitive information.

Test Requests and Responses:

```
POST /login HTTP/1.1
Host: drims.nginxdev.egovja.com
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: https://drims.nginxdev.egovja.com
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://drims.nginxdev.egovja.com/login?next=%2F
Cookie: session=eyJfZnJlc2giOmZhbHNlfQ.aSEfKw.SM5yxUK0BBPJmHkTb-ZxH5m7m_g
Content-Length: 19

email=%00&password=

HTTP/1.1 500 INTERNAL SERVER ERROR
Server: nginx
Date: Sat, 22 Nov 2025 02:33:48 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 265
Connection: keep-alive
Vary: Cookie

<!doctype html>
<html lang=en>
<title>500 Internal Server Error</title>
<h1>Internal Server Error</h1>
<p>The server encountered an internal error and was unable to complete your request. Either the server is overloaded or
```

```
there is an error in the application.</p>
```

I Email Address Pattern Found 4 TOC

Issue 1 of 4 TOC

Email Address Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	https://drims.nginxdev.egovja.com/login
Entity:	login (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Insecure web application programming or configuration
Fix:	Remove e-mail addresses from the website

Difference:

Reasoning: The response contains an e-mail address that may be private.

Test Requests and Responses:

```
GET /login?next=%2F HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://drims.nginxdev.egovja.com/
Host: drims.nginxdev.egovja.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: session=eyJfZnJlc2giOmZhbHNlfQ.aSEfKw.SM5yxUK0BBPJmHkTb-ZxH5m7m_g
Content-Length: 0


HTTP/1.1 200 OK
Server: nginx
Date: Sat, 22 Nov 2025 02:33:41 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 4388
Connection: keep-alive
Vary: Cookie


<!doctype html>
<html lang="en">
<head>
  <meta charset="utf-8">
  <title>Login · DMIS</title>
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.3/dist/css/bootstrap.min.css" rel="stylesheet">
  <link rel="stylesheet" href="https://cdn.jsdelivr.net/npm/bootstrap-icons@1.11.3/font/bootstrap-icons.css">
  <link rel="stylesheet" href="/static/css/modern-ui.css">
</head>
<body>
  <div class="login-container">
    <div>
      <!-- Login Card -->
      <div class="login-card">
        <div class="login-header">
          <div class="login-header-logos">
```

```
            <img src="/static/images/jamaica-coat-of-arms.png"
            alt="Jamaica Coat of Arms">
            <img src="/static/images/odpem-logo.png"
            alt="ODPEM Logo">
            </div>
            <h1>Disaster Management Information System</h1>
            <p class="login-header-subtitle">DMIS</p>
            <p class="login-header-meta">Government of Jamaica</p>
          </div>

          <div class="login-body">
            <h2>Sign in to your account</h2>
            <p class="subtitle">Use your email and password to access DMIS.</p>

            <!-- Flash messages -->




            <form method="post" action="/login" novalidate>
            <div class="form-group">
            <label for="email" class="form-label">Email Address</label>
            <input
            id="email"
            name="email"
            type="email"
            required
            autocomplete="email"
            class="form-control"
            placeholder="your.email@odpem.gov.jm"
            value=""
            aria-describedby="email-help">
            <div id="email-help" class="form-text">
            Enter the email address associated with your DMIS account
            </div>
            </div>

            <div class="form-group">
            <label for="password" class="form-label">Password</label>
            <input
            id="password"
            name="password"
            type="password"
            required
            autocomplete="current-password"
            class="form-control"
            placeholder="Enter your password">
            </div>

            <div class="mb-4">
            <div class="form-check">
            <input type="checkbox" name="remember" class="form-check-input" id="remember">
            <label class="form-check-label" for="remember">
            Remember me
            </label>
            </div>
            </div>

            <button type="submit" class="btn-login">
            <i class="bi bi-box-arrow-in-right me-2"></i>
            Sign In
            </button>
            </form>
          </div>
        </div>

        <!-- Agency CTA Card -->
        <div class="agency-cta">
          <div class="agency-cta-title">
            <i class="bi bi-building"></i>
            <span>New Agency?</span>
          </div>
          <p class="subtitle">
            Relief agencies can request access to DMIS to submit relief requests and manage disaster response distributions.
          </p>
          <a href="/account-requests/submit" class="btn-agency-request">
            <i class="bi bi-plus-circle"></i>
            Request Agency Account
          </a>
          <ul class="info-list">
            <li>
            <i class="bi bi-check-circle-fill"></i>
            <span>Approval by ODPEM required</span>
            </li>
```

```
          <li>
          <i class="bi bi-check-circle-fill"></i>
          <span>Email updates on request status</span>
          </li>
          <li>
          <i class="bi bi-check-circle-fill"></i>
          <span>Full access after approval</span>
          </li>
        </ul>
      </div>

      <!-- Footer -->
      <div class="login-footer">
        <div class="login-footer-badge">
          <i class="bi bi-shield-check"></i>
          <span>Secure Government System</span>
        </div>
        <p>© 2025 DMIS - Disaster Management Information System</p>
        <p class="login-footer-small">By signing in you agree to the acceptable use and data policies</p>
      </div>
    </div>
  </div>

  <script src="https://cdn.jsdelivr.net/npm/bootstrap@5.3.3/dist/js/bootstrap.bundle.min.js">
...
...
...
```

Issue 2 of 4

TOC

Email Address Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	https://drims.nginxdev.egovja.com/
Entity:	(Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Insecure web application programming or configuration
Fix:	Remove e-mail addresses from the website

Difference:

Reasoning: The response contains an e-mail address that may be private.

Test Requests and Responses:

```
GET / HTTP/1.1
Host: drims.nginxdev.egovja.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Content-Length: 0


HTTP/1.1 302 FOUND
Server: nginx
Date: Sat, 22 Nov 2025 02:31:23 GMT
```

```
Content-Type: text/html; charset=utf-8
Content-Length: 217
Connection: keep-alive
Location: /login?next=%2F
Vary: Cookie
Set-Cookie:
session=eyJfZmxhc2hlcyI6W3siIHQiOlsibWVzc2FnZSIsIlBsZWFzZSBsb2cgaW4gdG8gYWNjZXNzIHRoaXMgcGFnZS4iXX1dfQ.aSEgeg.BXMvl6YxRSn2E
4nNOo7Be5OPtp8; HttpOnly; Path=/

<!doctype html>
<html lang=en>
<title>Redirecting...</title>
<h1>Redirecting...</h1>
<p>You should be redirected automatically to the target URL: <a href="/login?next=%2F">/login?next=%2F</a>. If not, click
the link.


GET /login?next=%2F HTTP/1.1
Cookie:
session=eyJfZmxhc2hlcyI6W3siIHQiOlsibWVzc2FnZSIsIlBsZWFzZSBsb2cgaW4gdG8gYWNjZXNzIHRoaXMgcGFnZS4iXX1dfQ.aSEgeg.BXMvl6YxRSn2E
4nNOo7Be5OPtp8
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://drims.nginxdev.egovja.com/
Host: drims.nginxdev.egovja.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Content-Length: 0


HTTP/1.1 200 OK
Server: nginx
Date: Sat, 22 Nov 2025 02:31:23 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 4835
Connection: keep-alive
Vary: Cookie
Set-Cookie: session=eyJfZnJlc2giOmZhbHNlfQ.aSEgeg.LK61Zz4xbsmylkcu8QMKHrnIYkI; HttpOnly; Path=/


<!doctype html>
<html lang="en">
<head>
  <meta charset="utf-8">
  <title>Login · DMIS</title>
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.3/dist/css/bootstrap.min.css" rel="stylesheet">
  <link rel="stylesheet" href="https://cdn.jsdelivr.net/npm/bootstrap-icons@1.11.3/font/bootstrap-icons.css">
  <link rel="stylesheet" href="/static/css/modern-ui.css">
</head>
<body>
  <div class="login-container">
    <div>
      <!-- Login Card -->
      <div class="login-card">
        <div class="login-header">
          <div class="login-header-logos">
          <img src="/static/images/jamaica-coat-of-arms.png"
          alt="Jamaica Coat of Arms">
          <img src="/static/images/odpem-logo.png"
          alt="ODPEM Logo">
          </div>
          <h1>Disaster Management Information System</h1>
          <p class="login-header-subtitle">DMIS</p>
          <p class="login-header-meta">Government of Jamaica</p>
        </div>

        <div class="login-body">
          <h2>Sign in to your account</h2>
          <p class="subtitle">Use your email and password to access DMIS.</p>

          <!-- Flash messages -->


          <div class="mb-3">

          <div class="alert alert-success alert-dismissible fade show" role="alert">
          <i class="bi bi-check-circle me-2"></i>
          Please log in to access this page.
          <button type="button" class="btn-close" data-bs-dismiss="alert" aria-label="Close"></button>
          </div>

          </div>
```

```
          <form method="post" action="/login" novalidate>
          <div class="form-group">
          <label for="email" class="form-label">Email Address</label>
          <input
          id="email"
          name="email"
          type="email"
          required
          autocomplete="email"
          class="form-control"
          placeholder="your.email@odpem.gov.jm"
          value=""
          aria-describedby="email-help">
          <div id="email-help" class="form-text">
          Enter the email address associated with your DMIS account
          </div>
          </div>

          <div class="form-group">
          <label for="password" class="form-label">Password</label>
          <input
          id="password"
          name="password"
          type="password"
          required
          autocomplete="current-password"
          class="form-control"
          placeholder="Enter your password">
          </div>

          <div class="mb-4">
          <div class="form-check">
          <input type="checkbox" name="remember" class="form-check-input" id="remember">
          <label class="form-check-label" for="remember">
          Remember me
          </label>
          </di
...
...
...
```

Issue 3 of 4

TOC

Email Address Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	https://drims.nginxdev.egovja.com/account-requests/submit
Entity:	submit (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Insecure web application programming or configuration
Fix:	Remove e-mail addresses from the website

Difference:

Reasoning: The response contains an e-mail address that may be private.

Test Requests and Responses:

```
GET /account-requests/submit HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://drims.nginxdev.egovja.com/account-requests/
Host: drims.nginxdev.egovja.com
```

```
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: session=eyJfZnJlc2giOmZhbHNlfQ.aSEfKw.SM5yxUK0BBPJmHkTb-ZxH5m7m_g
Content-Length: 0


HTTP/1.1 200 OK
Server: nginx
Date: Sat, 22 Nov 2025 02:32:04 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 26664
Connection: keep-alive
Vary: Cookie

<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Request Agency Account - DMIS - Disaster Management Information System</title>
    <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.3/dist/css/bootstrap.min.css" rel="stylesheet">
    <link rel="stylesheet" href="https://cdn.jsdelivr.net/npm/bootstrap-icons@1.11.3/font/bootstrap-icons.css">
    <!-- DMIS Modern UI Design System -->
    <link rel="stylesheet" href="/static/css/modern-ui.css">
    <link rel="stylesheet" href="/static/css/workflow-sidebar.css">
    <link rel="stylesheet" href="/static/css/notifications-ui.css">
    <style>
        :root {
          --goj-green: #009639;
          --goj-gold: #FDB913;
          --goj-black: #000000;
          --goj-light-green: #E8F5E9;
          --sidebar-width: 260px;
          --sidebar-collapsed-width: 70px;
          --header-height: 60px;
        }

        body {
          font-family: 'Segoe UI', Tahoma, Geneva, Verdana, sans-serif;
          font-size: 0.9rem;
          background-color: #f5f7fa;
          margin: 0;
          padding: 0;
        }

        .top-header {
          position: fixed;
          top: 0;
          left: 0;
          right: 0;
          height: var(--header-height);
          background: linear-gradient(135deg, var(--goj-green) 0%, #007d42 100%);
          color: white;
          display: flex;
          align-items: center;
          padding: 0 20px;
          z-index: 1030;
          box-shadow: 0 2px 4px rgba(0,0,0,0.1);
        }

        .hamburger-menu {
          background: none;
          border: none;
          color: white;
          font-size: 1.5rem;
          cursor: pointer;
          padding: 8px 12px;
          margin-right: 15px;
          min-width: 44px;
          min-height: 44px;
          display: flex;
          align-items: center;
          justify-content: center;
          border-radius: 4px;
          transition: background-color 0.2s ease;
          -webkit-tap-highlight-color: transparent;
          position: relative;
          z-index: 1;
        }

        .hamburger-menu:hover {
          background-color: rgba(255,255,255,0.1);
        }

        .hamburger-menu:active {
```

```
          background-color: rgba(255,255,255,0.2);
        }

        .hamburger-menu:focus-visible {
          outline: 3px solid var(--goj-gold);
          outline-offset: 2px;
        }

        .brand-logo {
          display: flex;
          align-items: center;
          color: white;
          text-decoration: none;
          font-size: 1.5rem;
          font-weight: bold;
          gap: 12px;
        }

        .brand-logo:hover {
          color: var(--goj-gold);
        }

        .brand-logo img {
          height: 40px;
          width: auto;
          transition: transform 0.2s;
        }

        .brand-logo:hover img {
          transform: scale(1.05);
        }

        .brand-text {
          display: flex;
          flex-direction: column;
          line-height: 1.2;
        }

        .brand-text-main {
          font-size: 1.3rem;
          font-weight: 700;
          letter-spacing: 0.5px;
        }

        .brand-text-sub {
          font-size: 0.65rem;
          opacity: 0.9;
          font-weight: 400;
        }

        .header-right {
          margin-left: auto;
          display: flex;
          align-items: center;
          gap:
...
...
...

          <label for="contact_email" class="form-label">
          <i class="bi bi-envelope text-primary"></i> Contact Email <span class="text-danger">*</span>
          </label>
          <input type="email" class="form-control" id="contact_email" name="contact_email"
          placeholder="contact@agency.gov.jm" required
          maxlength="200">
          <div class="form-text">Email address where login credentials will be sent</div>
          </div>
...
...
...
```

Email Address Pattern Found

Severity:	Informational
CVSS Score:	0.0
URL:	https://drims.nginxdev.egovja.com/account-requests/
Entity:	(Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Insecure web application programming or configuration
Fix:	Remove e-mail addresses from the website

Difference:

Reasoning: The response contains an e-mail address that may be private.

Test Requests and Responses:

```
POST /account-requests/ HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://drims.nginxdev.egovja.com/account-requests/submit
Host: drims.nginxdev.egovja.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Cookie: session=eyJfZnJlc2giOmZhbHNlfQ.aSEfKw.SM5yxUK0BBPJmHkTb-ZxH5m7m_g
Content-Length: 108

agency_name=&contact_name=&contact_phone=555-555-5555&contact_email=test%40altoromutual.com&reason_text=1234

HTTP/1.1 302 FOUND
Server: nginx
Date: Sat, 22 Nov 2025 02:31:23 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 235
Connection: keep-alive
Location: /account-requests/submit
Vary: Cookie
Set-Cookie:
session=eyJfZmxhc2hlcyI6W3siIHQiOlsiZGFuZ2VyIiwiQWxsIGZpZWxkcyBhcmUgcmVxdWlyZWQuIl19XSwiX2ZyZXNoIjpmYWxzZX0.aSEgeg.KMAMwybs
E9-ECDhAYFYyX27tcqc; HttpOnly; Path=/

<!doctype html>
<html lang=en>
<title>Redirecting...</title>
<h1>Redirecting...</h1>
<p>You should be redirected automatically to the target URL: <a href="/account-requests/submit">/account-
requests/submit</a>. If not, click the link.


GET /account-requests/submit HTTP/1.1
Cookie:
session=eyJfZmxhc2hlcyI6W3siIHQiOlsiZGFuZ2VyIiwiQWxsIGZpZWxkcyBhcmUgcmVxdWlyZWQuIl19XSwiX2ZyZXNoIjpmYWxzZX0.aSEgeg.KMAMwybs
E9-ECDhAYFYyX27tcqc
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://drims.nginxdev.egovja.com/account-requests/
Host: drims.nginxdev.egovja.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Content-Length: 0


HTTP/1.1 200 OK
Server: nginx
Date: Sat, 22 Nov 2025 02:31:23 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 26979
Connection: keep-alive
Vary: Cookie
Set-Cookie: session=eyJfZnJlc2giOmZhbHNlfQ.aSEgeg.LK61Zz4xbsmylkcu8QMKHrnIYkI; HttpOnly; Path=/

<!DOCTYPE html>
<html lang="en">
<head>
```

```
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Request Agency Account - DMIS - Disaster Management Information System</title>
    <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.3/dist/css/bootstrap.min.css" rel="stylesheet">
    <link rel="stylesheet" href="https://cdn.jsdelivr.net/npm/bootstrap-icons@1.11.3/font/bootstrap-icons.css">
    <!-- DMIS Modern UI Design System -->
    <link rel="stylesheet" href="/static/css/modern-ui.css">
    <link rel="stylesheet" href="/static/css/workflow-sidebar.css">
    <link rel="stylesheet" href="/static/css/notifications-ui.css">
    <style>
        :root {
          --goj-green: #009639;
          --goj-gold: #FDB913;
          --goj-black: #000000;
          --goj-light-green: #E8F5E9;
          --sidebar-width: 260px;
          --sidebar-collapsed-width: 70px;
          --header-height: 60px;
        }

        body {
          font-family: 'Segoe UI', Tahoma, Geneva, Verdana, sans-serif;
          font-size: 0.9rem;
          background-color: #f5f7fa;
          margin: 0;
          padding: 0;
        }

        .top-header {
          position: fixed;
          top: 0;
          left: 0;
          right: 0;
          height: var(--header-height);
          background: linear-gradient(135deg, var(--goj-green) 0%, #007d42 100%);
          color: white;
          display: flex;
          align-items: center;
          padding: 0 20px;
          z-index: 1030;
          box-shadow: 0 2px 4px rgba(0,0,0,0.1);
        }

        .hamburger-menu {
          background: none;
          border: none;
          color: white;
          font-size: 1.5rem;
          cursor: pointer;
          padding: 8px 12px;
          margin-right: 15px;
          min-width: 44px;
          min-height: 44px;
          display: flex;
          align-items: center;
          justify-content: center;
          border-radius: 4px;
          transition: background-color 0.2s ease;
          -webkit-tap-highlight-color: transparent;
          position: relative;
          z-index: 1;
        }

        .hamburger-menu:hover {

...
...
...

          <label for="contact_email" class="form-label">
          <i class="bi bi-envelope text-primary"></i> Contact Email <span class="text-danger">*</span>
          </label>
          <input type="email" class="form-control" id="contact_email" name="contact_email"
          placeholder="contact@agency.gov.jm" required
          maxlength="200">
          <div class="form-text">Email address where login credentials will be sent</div>
          </div>
...
...
...
```

Issue 1 of 1

TOC

Missing "Referrer policy" Security Header

Severity:	Informational
CVSS Score:	0.0
URL:	https://drims.nginxdev.egovja.com/
Entity:	drims.nginxdev.egovja.com (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	Insecure web application programming or configuration
Fix:	Config your server to use the "Referrer Policy" header with secure policies

Difference:

Reasoning: AppScan detected that the Referrer Policy Response header is missing or with an insecure policy, which increases exposure to various cross-site injection attacks

Test Requests and Responses:

```
HEAD /static/css/modern-ui.css HTTP/1.1
Cookie: session=eyJfZnJlc2giOmZhbHNlfQ.aSEfKw.SM5yxUK0BBPJmHkTb-ZxH5m7m_g
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: https://drims.nginxdev.egovja.com/login?next=%2F
Host: drims.nginxdev.egovja.com
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
Content-Length: 0


HTTP/1.1 200 OK
Server: nginx
Date: Sat, 22 Nov 2025 02:31:47 GMT
Content-Type: text/css
Content-Length: 33972
Connection: keep-alive
Last-Modified: Sat, 22 Nov 2025 02:07:11 GMT
ETag: "69211acf-84b4"
Expires: Mon, 22 Dec 2025 02:31:46 GMT
Cache-Control: max-age=2592000
Accept-Ranges: bytes
```

How to Fix

Autocomplete HTML Attribute Not Disabled for Password Field

TOC

Cause:

Insecure web application programming or configuration

Risk:

It may be possible to bypass the web application's authentication mechanism
The "autocomplete" attribute has been standardized in the HTML5 standard. W3C's site states that the attribute has two states, "on" and "off", and that omitting it altogether is equivalent to setting it to "on".
This page is vulnerable since it does not set the "autocomplete" attribute to "off" for the "password" field in the "input" element.
This may enable an unauthorized user (with local access to an authorized client) to autofill the username and password fields, and thus log in to the site.

Affected Products:

N/A

Fix Recommendation:

General

If the "autocomplete" attribute is missing in the "password" field of the "input" element, add it and set it to "off".
If the "autocomplete" attribute is set to "on", change it to "off".
For example:
Vulnerable site:
<form action="AppScan.html" method="get"> Username: <input type="text" name="firstname" />
 Password: <input type="password" name="lastname" /> <input type="submit" value="Submit" /> <form>
Non-vulnerable site:
<form action="AppScan.html" method="get"> Username: <input type="text" name="firstname" />
 Password: <input type="password" name="lastname" autocomplete="off"/> <input type="submit" value="Submit" /> <form>

CWE:

522

Body Parameters Accepted in Query

TOC

Cause:

Insecure web application programming or configuration

Risk:

It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
GET requests are designed to query the server, while POST requests are for submitting data.
However, aside from the technical purpose, attacking query parameters is easier than body parameters, because sending a link to the original site, or posting it in a blog or comment, is easier and has better results than the alternative - in order to attack a request with body parameters, an attacker would need to create a page containing a form that will be submitted when visited by the victim.
It is a lot harder to convince the victim to visit a page that he doesn't know, than letting him visit the original site. It it therefore not recommended to support body parameters that arrive in the query string.

Affected Products:

This issue may affect different types of products.

Fix Recommendation:

General

Re-program the application to disallow handling of POST parameters that were listed in the Query

CWE:

200

External References:

GET
POST

Cacheable SSL Page Found

TOC

Cause:

Sensitive information might have been cached by your browser

Risk:

It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Most web browsers are configured by default to cache the user's pages during use. This means that SSL pages are cached as well.
It is not recommended to enable the web browser to save any SSL information, since this information might be compromised when a vulnerability exists.

Affected Products:

This issue may affect different types of products.

Fix Recommendation:

General

Disable caching on all SSL pages or all pages that contain sensitive data.
This can be achieved by using "Cache-Control: no-store" and either "Pragma: no-cache" or "Cache-Control: no-cache" response directives in your SSL page headers.
Cache-Control: private - This directive instructs proxies that the page contains private information, and therefore should not be cached by a shared cache. However, it does not instruct browsers to refrain from caching the pages.
Cache-Control: no-cache - This directive also instructs proxies that the page contains private information, and therefore should not be cached. It also instructs the browser to revalidate with the server to check if a new version is available. This means that the browser may store sensitive pages or information to be used in the revalidation. Certain browsers do not necessarily follow the RFC and may treat no-cache as no-store.
Cache-Control: no-store - This is the most secure directive. It instructs both the proxy and the browser not to cache the page or store it in its cache folders.
Pragma: no-cache - This directive is required for older browsers, that do not support the Cache-Control header.

CWE:

525

Check for SRI (Subresource Integrity) support

TOC

Cause:

There is no support to Subresource Integrity.

Risk:

The user-agent can't verify scripts from third-party services. In case of compromise of the third-party service, the user is not protected.
script and link tags with src from another domain are not supporting integrity check.
This can be exploited if the service that have the script is compromise.
Sample Script Element Not Supporting SRI:
<script src="https://example.com/example-framework.js" crossorigin="anonymous"></script>
Sample Script Element Supporting SRI:
<script src="https://example.com/example-framework.js" integrity="sha384-Li9vy3DqF8tnTXuiaAJuML3ky+er10rcgNR/VqsVpcw+ThHmYcwiB1pbOxEbzJr7" crossorigin="anonymous"></script>

Affected Products:

This issue may affect different types of products.

Fix Recommendation:

General

Add Subresource Integrity to every script/link with source not in your domain
W3C Subresource Integrity:
https://www.w3.org/TR/SRI/
SRI Hash Generator:
https://srihash.org
Sample Script Element Not Supporting SRI:
<script src="https://example.com/example-framework.js" crossorigin="anonymous"></script>
Sample Script Element Supporting SRI:
<script src="https://example.com/example-framework.js" integrity="sha384-oqVuAfXRKap7fdgcCY5uykM6+R9GqQ8K/uxy9rx7HNQlGYl1kPzQho1wx4JwY8wC" crossorigin="anonymous"></script>

CWE:

829

External References:

Vendor site
Explanation

Cookie with Insecure or Improper or Missing SameSite attribute

TOC

Cause:

Sensitive Cookie with Improper or Insecure or Missing SameSite Attribute

Risk:

Prevent Cookie information leakage by restricting cookies to first-party or same-site context
Attacks can extend to Cross-Site-Request-Forgery (CSRF) attacks if there are no additional protections in place (such as Anti-CSRF tokens).
The SameSite attribute controls how cookies are sent for cross-domain requests.
The attribute may have three values: 'Lax', 'Strict', or 'None'. If 'None' is used, a website may create a cross-domain POST HTTP request to another website, and the browser automatically adds cookies to this request.
This may lead to Cross-Site-Request-Forgery (CSRF) attacks if there are no additional protections in place (such as Anti-CSRF tokens).
Modes and their uses:
'Lax' mode: the cookie will only be sent with a top-level get request.
'Strict' mode; the cookie will not be sent with any cross-site usage even if the user follows a link to another website.
'None' mode: the cookie will be sent with the cross-site requests.
The attribute having: 'Lax' or 'None' must have 'Secure' Flag set and must be transferred over https.
Example - Set-Cookie: key=value; SameSite=Lax;Secure
Setting attribute to 'Strict' is the recommended option.
Example - Set-Cookie: key=value; SameSite=Strict

Affected Products:

This issue may affect different types of products.

Fix Recommendation:

General

[1] Review possible solutions for configuring SameSite Cookie attribute to recommended values.
[2] Restrict Cookies to a first-party or same-site context.
[3] Verify and set the SameSite attribute of your cookie to Strict, to ensure that the cookie will only be sent in a first-party context.
[4] Or, if you want to relax the restrictions of first-party context, then verify and set the SameSite attribute of the cookie to Lax with Secure Flag enabled and transferred over HTTPS.

CWE:

1275

External References:

WASC Threat Classification: Information Leakage
SameSite Cookies

Hidden Directory Detected

TOC

Cause:

The web server or application server are configured in an insecure way

Risk:

It is possible to retrieve information about the site's file system structure, which may help the attacker to map the web site
The web application has exposed the presence of a directory in the site. Although the directory does not list its content, the information may help an attacker to develop further attacks against the site. For example, by knowing the directory name, an attacker can guess its content type and possibly file names that reside in it, or sub directories under it, and try to access them.
The more sensitive the content is, the more severe this issue may be.

Affected Products:

This issue may affect different types of products.

Fix Recommendation:

General

If the forbidden resource is not required, remove it from the site.
If possible, issue a "404 - Not Found" response status code instead of "403 - Forbidden". This change will obfuscate the presence of the directory in the site, and will prevent the site structure from being exposed.

CWE:

200

Missing "Content-Security-Policy" header

TOC

Cause:

Insecure web application programming or configuration

Risk:

It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
The absence or improper values of CSP can cause the web application being vulnerable to XSS, clickjacking, etc.
The "Content-Security-Policy" header is designed to modify the way browsers render pages, and thus to protect from various cross-site injections, including Cross-Site Scripting. It is important to set the header value correctly, in a way that will not prevent proper operation of the web site. For example, if the header is set to prevent execution of inline JavaScript, the web site must not use inline JavaScript in its pages.
To protect against Cross-Site Scripting, Cross-Frame Scripting and clickjacking, it is important to set the following policies with proper values:
Both of 'default-src' and 'frame-ancestors' policies, *OR* all of 'script-src', 'object-src' and 'frame-ancestors' policies.
For 'default-src', 'script-src' and 'object-src', insecure values such as '*', 'data:', 'unsafe-inline' or 'unsafe-eval' should be avoided.
For 'frame-ancestors', insecure values such as '*' or 'data:' should be avoided.
Additionally for 'script-src', and 'default-src' (fallback directive for 'script-src') 'self' is considered insecure and should be avoided.
Please refer the following links for more information.
Please note that “Content-Security-Policy” includes four different tests. A general test that verifies if the "Content-Security-Policy" header is being used and three additional tests that check if "Frame-Ancestors", "Object-Src" and "Script-Src" were configured correctly.

Affected Products:

This issue may affect different types of products

Fix Recommendation:

General

Configure your server to send the "Content-Security-Policy" header.
It is recommended to configure Content-Security-Policy header with secure values for its directives as below:
For 'default-src', and 'script-src' secure values such as 'none', or https://any.example.com.
For 'frame-ancestors', and 'object-src' secure values such as 'self', 'none' or https://any.example.com are expected.
"unsafe-inline" and "unsafe-eval" must not be used in any circumstance. Using nonce / hash would be only considered for short-term workaround.
For Apache, see:
http://httpd.apache.org/docs/2.2/mod/mod_headers.html
For IIS, see:
https://technet.microsoft.com/pl-pl/library/cc753133%28v=ws.10%29.aspx
For nginx, see:
http://nginx.org/en/docs/http/ngx_http_headers_module.html

CWE:

1032

External References:

List of some secure Headers
An Introduction to Content Security Policy
MDN web docs - Content-Security-Policy

Missing Secure Attribute in Encrypted Session (SSL) Cookie

TOC

Cause:

The web application sends non-secure cookies over SSL

Risk:

It may be possible to steal user and session information (cookies) that was sent during an encrypted session
During the application test, it was detected that the tested web application set a cookie without the "secure" attribute, during an encrypted session. Since this cookie does not contain the "secure" attribute, it might also be sent to the site during an unencrypted session. Any information such as cookies, session tokens or user credentials that are sent to the server as clear text, may be stolen and used later for identity theft or user impersonation.
In addition, several privacy regulations state that sensitive information such as user credentials will always be sent encrypted to the web site

Affected Products:

This issue may affect different types of products

Fix Recommendation:

General

Basically the only required attribute for the cookie is the "name" field. Common optional attributes are: "comment", "domain", "path", etc.
The "secure" attribute must be set accordingly in order to prevent to cookie from being sent unencrypted.
For more information on how to set the secure flag, see OWASP "Secure Attribute" cheatsheet at
https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#secure-attribute
RFC 2965 states:
"The Secure attribute (with no value) directs the user agent to use only (unspecified) secure means to contact the origin server whenever it sends back this cookie, to protect the confidentially and authenticity of the information in the cookie."
For further reference please see the HTTP State Management Mechanism RFC 2965 at:
http://www.ietf.org/rfc/rfc2965.txt
and for "Best current practice" for use of HTTP State Management please see
http://tools.ietf.org/html/rfc2964

CWE:

614

External References:

Financial Privacy: The Gramm-Leach Bliley Act
Health Insurance Portability and Accountability Act (HIPAA)
Sarbanes-Oxley Act
California SB1386

Missing or insecure "X-Content-Type-Options" header

TOC

Cause:

Insecure web application programming or configuration

Risk:

It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
The "X-Content-Type-Options" header (with "nosniff" value) prevents IE and Chrome from ignoring the content-type of a response.
This action may prevent untrusted content (e.g. user uploaded content) from being executed on the user browser (after a malicious naming, for example).

Affected Products:

This issue may affect different types of products

Fix Recommendation:

General

Configure your server to send the "X-Content-Type-Options" header with value "nosniff" on all outgoing requests.
For Apache, see:
http://httpd.apache.org/docs/2.2/mod/mod_headers.html
For IIS, see:
https://technet.microsoft.com/pl-pl/library/cc753133%28v=ws.10%29.aspx
For nginx, see:
http://nginx.org/en/docs/http/ngx_http_headers_module.html

CWE:

200

External References:

List of useful HTTP headers
Reducing MIME type security risks

Missing or insecure HTTP Strict-Transport-Security Header

TOC

Cause:

Insecure web application programming or configuration

Risk:

It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
HTTP Strict Transport Security (HSTS) is a mechanism which protects secure (HTTPS) websites from being downgraded to non-secure HTTP. This mechanism enables web servers to instruct their clients (web browsers or other user agents) to use secure HTTPS connections when interacting with the server, and never use the insecure HTTP protocol.
It is important to set the 'max-age' to a high enough value to prevent falling back to an insecure connection prematurely.
The HTTP Strict Transport Security policy is communicated by the server to its clients using a response header named "Strict-Transport-Security". The value of this header is a period of time during which the client should access the server in HTTPS only. Other header attributes include "includeSubDomains" and "preload".

Affected Products:

This issue may affect different types of products.

Fix Recommendation:

General

Implement the The HTTP Strict Transport Security policy by adding the "Strict-Transport-Security" response header to the web application responses.
For more information please see
https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html

CWE:

200

External References:

OWASP "HTTP Strict Transport Security"
HSTS Spec

SHA-1 cipher suites were detected

TOC

Cause:

The web server or application server are configured in an insecure way

Risk:

It may be possible to steal or manipulate customer session and cookies, which might be used to impersonate a legitimate user, allowing the hacker to view or alter user records, and to perform transactions as that user
The server supports SHA-1 ciphersuites.
SHA-1 was officially deprecated by NIST in 2011, but many applications still rely on it.
Up until now (2021), only theoretical attacks have been known agsinst SHA-1, which is why many applications still rely on it.
Recently, a practical attack was introduced by CWI Amsterdam and Google Research teams ([1] and [2]).

Affected Products:

This issue may affect different types of products.

Fix Recommendation:

General

Secure Cipher-Suites best practices:
[1]
Use strong cryptographic hashing algorithms
[2]
Server cipher TLS requirements

CWE:

327

External References:

[1] SHATTERED
[2] The first collision for full SHA-1

Unnecessary Http Response Headers found in the Application

TOC

Cause:

Insecure web application programming or configuration

Risk:

It is possible to gather sensitive information about the web server type, version, OS and more.
AppScan detected a Http response header that is unnecessary.
For reasons of security and privacy, The Http response headers like "Server", "X-Powered-By", "X-AspNetMvc-Version" and "X-AspNet-Version" should not appear in web pages.
The "Server" header is a header that is added usually by default whenever a response is sent to the client by the server.
The "X-Powered-By" header is a header that might be added by default whenever a response is sent to the client by the server.
These added header(s) may reveal sensitive information about the internal server software version and type, thus enabling attackers to fingerprint it and attack it with targeted exploits. Moreover, when a new exploit becomes known to the public, the server will most likely get attacked with it.

Affected Products:

This issue may affect different types of products.

Fix Recommendation:

General

Configure your server to remove the default "Server" header from being sent to all outgoing requests.
For IIS, see:
https://techcommunity.microsoft.com/t5/iis-support-blog/remove-unwanted-http-response-headers/ba-p/369710
For nginx, see:
https://www.getpagespeed.com/server-setup/nginx/how-to-remove-the-server-header-in-nginx
For Weblogic, see:
https://docs.oracle.com/cd/E13222_01/wls/docs81/adminguide/web_server.html
For Apache, see:
https://techglimpse.com/set-modify-response-headers-http-tip/

CWE:

200

External References:

Fingerprinting
Preventing Information Leakage

Weak Cipher Suites - ROBOT Attack : Vulnerable cipher suites are supported by the server

TOC

Cause:

Cipher Suites that support TLS-RSA key exchange were detected. The web server or application server with TLS implementation flaw may be vulnerable to ROBOT Attack. This issue does not necessarily mean that you are vulnerable. Please follow the advisory guideline.

Risk:

An attacker can obtain the decrypted RSA ciphertext or sign an arbitrary message with server's private key. This attack allows an attacker to decrypt the recorded traffic of a vulnerable host.
"ROBOT - Return Of Bleichenbacher's Oracle Threat" attack applies to the TLS-RSA key exchange, which is used by all cipher suites names starting with TLS_RSA. An attack may exploit a vulnerable server that responds with different messages based on the ciphertext validity. The attack relies on the flexibility of RSA that allows anybody with an RSA public key to multiply encrypted plaintexts and on PKCS #1 v1.5 padding format that enables an attacker to create valid messages with a high probability.
A host with a flaw in TLS implementation that supports TLS cipher modes that use RSA encryption (TLS_RSA ciphers) is vulnerable to ROBOT Attack.

Affected Products:

For the list of affected products, refer https://robotattack.org/#patches

Fix Recommendation:

General

In case you are using a vulnerable product, please check for patches and updates
The patches and affected products list may change from time to time. For more information on patches and affected products, refer https://robotattack.org/#patches
It is also recommended to fully deprecate RSA encryption-based key exchanges in TLS because it does not provide Forward Secrecy.

CWE:

203

External References:

F5 : BIG-IP SSL vulnerability
Citrix : TLS Padding Oracle Vulnerability in Citrix NetScaler Application Delivery Controller (ADC) and NetScaler Gateway
Radware : CVE-2017-17427
Cisco ACE and Cisco ASA : Bleichenbacher Attack on TLS Affecting Cisco Products
Bouncy Castle : 1.59 beta 9
Bouncy Castle : Patch / Commit
Erlang : OTP 18.3.4.7
Erlang : OTP 19.3.6.4
Erlang : OTP 20.1.7
WolfSSL : Github PR / patch
Palo Alto Networks : PAN-OS exposure to ROBOT attack
IBM GSKit : IBM i is affected by GSKIT vulnerability
IBM GSKit : Information disclosure in IBM HTTP Server
IBM GSKit : WebSphere MQ is vulnerable to disclosing side channel information via discrepencies between valid and invalid PKCS#1 padding
Unisys ClearPath MCP : MCP TLS susceptible to ROBOT attack
Symantec IntelligenceCenter and Symantec SSL Visibility (SSLV) : SA160 Return of the Bleichenbacher Oracle Threat (ROBOT)
Cavium Nitro/Octeon : CVE-2017-17428
FortiGuard SSL Deep Inspection and FortiGuard VIP SSL : PSIRT Advisory FG-IR-17-302
Haskell-TLS : Inconsistencies in answers to RSA errors (possiby Bleichenbacher/ROBOT attack)
MatrixSSL : CVE-2016-6883
Java / JSSE : Oracle Critical Patch Update Advisory - October 2012
More information about ROBOT Attack

Weak Ciphers are detected: Not all cipher suites support Perfect Forward Secrecy

TOC

Cause:

The web server or application server are configured in an insecure way

Risk:

An attacker can decrypt a secure communication by generating a secret key once host's private key is compromised
AppScan detected weak cipher suites that do not support PFS - Perfect Forward Secrecy
When PFS is not supported by the host, in most cases when a Client establishes a connection to the Server, Client is using Server's Public Key
to encrypt the pre-master secret which then sent to the Server. Then the server uses it's Private Key to decrypt the pre-master secret so the Client and the Server can generate the Session Key using the pre-master secret.
If the host's private key is compromised, an attacker can decrypt the pre-master secret and later generate the Secret Key
that is used for secure communication. This is possible because no unique session key is generated for every single communication session between
Client and the Server. Such communication can be achieved for example when DHE - Diffie-Hellman Ephemeral or ECDHE -
Elliptic Curve Diffie-Hellman Ephemeral key exchanges are used.
With PFS every new session between the Client and the Server new random keys are generated to create a pre-master secret. So even if one of the Keys is compromised
an attacker can compromise only one session between the Client and the Server and not all of the previous communication sessions.

Affected Products:

Cipher Suites that do not support DHE and ECDHE key exchanges

Fix Recommendation:

General

Suport PFS by using cipher suites with ECDHE - Elliptic Curve Diffie-Hellman Ephemeral and DHE - Diffie-Hellman Ephemeral key exchanges.

CWE:

327

External References:

Wikipedia : Perfect Forward Secrecy
RFC : Perfect Forward Secrecy

Application Error

TOC

Cause:

- Proper bounds checking were not performed on incoming parameter values
- No validation was done in order to make sure that user input matches the data type expected

Risk:

It is possible to gather sensitive debugging information
If an attacker probes the application by forging a request that contains parameters or parameter values other than the ones expected by the application (examples are listed below), the application may enter an undefined state that makes it vulnerable to attack. The attacker can gain useful information from the application's response to this request, which information may be exploited to locate application weaknesses.
For example, if the parameter field should be an apostrophe-quoted string (e.g. in an ASP script or SQL query), the injected apostrophe symbol will prematurely terminate the string stream, thus changing the normal flow/syntax of the script.
Another cause of vital information being revealed in error messages, is when the scripting engine, web server, or database are misconfigured.
Here are some different variants:
[1] Remove parameter
[2] Remove parameter value
[3] Set parameter value to null
[4] Set parameter value to a numeric overflow (+/- 99999999)
[5] Set parameter value to hazardous characters, such as ' " \' \") ;
[6] Append some string to a numeric parameter value
[7] Append "." (dot) or "[]" (angle brackets) to the parameter name

Affected Products:

This issue may affect different types of products.

Fix Recommendation:

General

[1] Check incoming requests for the presence of all expected parameters and values. When a parameter is missing, issue a proper error message or use default values.
[2] The application should verify that its input consists of valid characters (after decoding). For example, an input value containing the null byte (encoded as %00), apostrophe, quotes, etc. should be rejected.
[3] Enforce values in their expected ranges and types. If your application expects a certain parameter to have a value from a certain set, then the application should ensure that the value it receives indeed belongs to the set. For example, if your application expects a value in the range 10..99, then it should make sure that the value is indeed numeric, and that its value is in 10..99.
[4] Verify that the data belongs to the set offered to the client.
[5] Do not output debugging error messages and exceptions in a production environment.
In order to disable debugging in ASP.NET, edit your web.config file to contain the following:
<compilation
debug="false"
/>
For more information, see "HOW TO: Disable Debugging for ASP.NET Applications" in:
http://support.microsoft.com/default.aspx?scid=kb;en-us;815157
You can add input validation to Web Forms pages by using validation controls. Validation controls provide an easy-to-use mechanism for all common types of standard validation (for example, testing for valid dates or values within a range), plus ways to provide custom-written validation. In addition, validation controls allow you to completely customize how error information is displayed to the user. Validation controls can be used with any controls that are processed in a Web Forms page's class file, including both HTML and Web server controls.
To make sure that all the required parameters exist in a request, use the "RequiredFieldValidator" validation control. This control ensures that the user does not skip an entry in the web form.
To make sure user input contains only valid values, you can use one of the following validation controls:
[1] "RangeValidator": checks that a user's entry (value) is between specified lower and upper boundaries. You can check ranges within pairs of numbers, alphabetic characters, and dates.
[2] "RegularExpressionValidator": checks that the entry matches a pattern defined by a regular expression. This type of validation allows you to check for predictable sequences of characters, such as those in social security numbers, e-mail addresses, telephone numbers, postal codes, and so on.
Important note: validation controls do not block user input or change the flow of page processing; they only set an error state, and produce error messages. It is the programmer's responsibility to test the state of the controls in the code before performing further application-specific actions. There are two ways to check for user input validity:
1. Test for a general error state:
In your code, test the page's IsValid property. This property rolls up the values of the IsValid properties of all the validation controls on the page (using a logical AND). If one of the validation controls is set to invalid, the page's property will return false.
2. Test for the error state of individual controls:
Loop through the page's Validators collection, which contains references to all the validation controls. You can then examine the IsValid property of each validation control.
** Input Data Validation:
While data validations may be provided as a user convenience on the client-tier, data validation must be performed on the server-tier using Servlets. Client-side validations are inherently insecure because they can be easily bypassed, e.g. by disabling Javascript.
A good design usually requires the web application framework to provide server-side utility routines to validate the following:
[1] Required field
[2] Field data type (all HTTP request parameters are Strings by default)
[3] Field length
[4] Field range
[5] Field options
[6] Field pattern
[7] Cookie values
[8] HTTP Response
A good practice is to implement the above routine as static methods in a "Validator" utility class. The following sections describe an example validator class.
[1] Required field
Always check that the field is not null and its length is greater than zero, excluding leading and trailing white spaces.
Example of how to validate required fields:
// Java example to validate required fields public Class Validator { ... public static boolean validateRequired(String value) { boolean isFieldValid = false; if (value != null && value.trim().length() > 0) { isFieldValid = true; } return isFieldValid; } ... } ... String fieldValue = request.getParameter("fieldName"); if (Validator.validateRequired(fieldValue)) { // fieldValue is valid, continue processing request ... }
[2] Field data type
In web applications, input parameters are poorly typed. For example, all HTTP request parameters or cookie values are of type String. The developer is responsible for verifying the input is of the correct data type. Use the Java primitive wrapper classes to check if the field value can be safely converted to the desired primitive data type.
Example of how to validate a numeric field (type int):

// Java example to validate that a field is an int number public Class Validator { ... public static boolean validateInt(String value) { boolean isFieldValid = false; try { Integer.parseInt(value); isFieldValid = true; } catch (Exception e) { isFieldValid = false; } return isFieldValid; } ... } ... // check if the HTTP request parameter is of type int String fieldValue = request.getParameter("fieldName"); if (Validator.validateInt(fieldValue)) { // fieldValue is valid, continue processing request ... }

A good practice is to convert all HTTP request parameters to their respective data types. For example, store the "integerValue" of a request parameter in a request attribute and use it as shown in the following example:

// Example to convert the HTTP request parameter to a primitive wrapper data type // and store this value in a request attribute for further processing String fieldValue = request.getParameter("fieldName"); if (Validator.validateInt(fieldValue)) { // convert fieldValue to an Integer Integer integerValue = Integer.getInteger(fieldValue); // store integerValue in a request attribute request.setAttribute("fieldName", integerValue); } ... // Use the request attribute for further processing Integer integerValue = (Integer)request.getAttribute("fieldName"); ...

The primary Java data types that the application should handle:

- Byte
- Short
- Integer
- Long
- Float
- Double
- Date

[3] Field length

Always ensure that the input parameter (whether HTTP request parameter or cookie value) is bounded by a minimum length and/or a maximum length.

Example to validate that the length of the userName field is between 8 and 20 characters:

// Example to validate the field length public Class Validator { ... public static boolean validateLength(String value, int minLength, int maxLength) { String validatedValue = value; if (!validateRequired(value)) { validatedValue = ""; } return (validatedValue.length() >= minLength && validatedValue.length() <= maxLength); } ... } ... String userName = request.getParameter("userName"); if (Validator.validateRequired(userName)) { if (Validator.validateLength(userName, 8, 20)) { // userName is valid, continue further processing ... } }

[4] Field range

Always ensure that the input parameter is within a range as defined by the functional requirements.

Example to validate that the input numberOfChoices is between 10 and 20:

// Example to validate the field range public Class Validator { ... public static boolean validateRange(int value, int min, int max) { return (value >= min && value <= max); } ... } ... String fieldValue = request.getParameter("numberOfChoices"); if (Validator.validateRequired(fieldValue)) { if (Validator.validateInt(fieldValue)) { int numberOfChoices = Integer.parseInt(fieldValue); if (Validator.validateRange(numberOfChoices, 10, 20)) { // numberOfChoices is valid, continue processing request ... } } }

[5] Field options

Often, the web application presents the user with a set of options to choose from, e.g. using the SELECT HTML tag, but fails to perform server-side validation to ensure that the selected value is one of the allowed options. Remember that a malicious user can easily modify any option value. Always validate the selected user value against the allowed options as defined by the functional requirements.

Example to validate the user selection against a list of allowed options:

// Example to validate user selection against a list of options public Class Validator { ... public static boolean validateOption(Object[] options, Object value) { boolean isValidValue = false; try { List list = Arrays.asList(options); if (list != null) { isValidValue = list.contains(value); } } catch (Exception e) { } return isValidValue; } ... } ... // Allowed options String[] options = {"option1", "option2", "option3"); // Verify that the user selection is one of the allowed options String userSelection = request.getParameter("userSelection"); if (Validator.validateOption(options, userSelection)) { // valid user selection, continue processing request ... }

[6] Field pattern

Always check that the user input matches a pattern as defined by the functionality requirements. For example, if the userName field should only allow alpha-numeric characters, case insensitive, then use the following regular expression:

^[a-zA-Z0-9]*$

Java 1.3 or earlier versions do not include any regular expression packages. Apache Regular Expression Package (see Resources below) is recommended for use with Java 1.3 to resolve this lack of support.

Example to perform regular expression validation:

// Example to validate that a given value matches a specified pattern // using the Apache regular expression package import org.apache.regexp.RE; import org.apache.regexp.RESyntaxException; public Class Validator { ... public static boolean matchPattern(String value, String expression) { boolean match = false; if (validateRequired(expression)) { RE r = new RE(expression); match = r.match(value); } return match; } ... } ... // Verify that the userName request parameter is alpha-numeric String userName = request.getParameter("userName"); if (Validator.matchPattern(userName, "^[a-zA-Z0-9]*$")) { // userName is valid, continue processing request ... }

Java 1.4 introduced a new regular expression package (java.util.regex). Here is a modified version of Validator.matchPattern using the new Java 1.4 regular expression package:

// Example to validate that a given value matches a specified pattern // using the Java 1.4 regular expression package import java.util.regex.Pattern; import java.util.regexe.Matcher; public Class Validator { ... public static boolean matchPattern(String value, String expression) { boolean match = false; if (validateRequired(expression)) { match = Pattern.matches(expression, value); } return match; } ... }

[7] Cookie value

Use the javax.servlet.http.Cookie object to validate the cookie value. The same validation rules (described above) apply to cookie values depending on the application requirements, e.g. validate a required value, validate length, etc.

Example to validate a required cookie value:

// Example to validate a required cookie value // First retrieve all available cookies submitted in the HTTP request Cookie[] cookies = request.getCookies(); if (cookies != null) { // find the "user" cookie for (int i=0; i<cookies.length; ++i) { if (cookies[i].getName().equals("user")) { //

validate the cookie value if (Validator.validateRequired(cookies[i].getValue()) { // valid cookie value, continue processing request ... } } } }
[8] HTTP Response
[8-1] Filter user input
To guard the application against cross-site scripting, sanitize HTML by converting sensitive characters to their corresponding character entities. These are the HTML sensitive characters:
< > " ' % ;) (& +
Example to filter a specified string by converting sensitive characters to their corresponding character entities:
// Example to filter sensitive data to prevent cross-site scripting public Class Validator { ... public static String filter(String value) { if (value == null) { return null; } StringBuffer result = new StringBuffer(value.length()); for (int i=0; i<value.length(); ++i) { switch (value.charAt(i)) { case '<': result.append("<"); break; case '>': result.append(">"); break; case '"': result.append("""); break; case '\'': result.append("'"); break; case '%': result.append("%"); break; case ';': result.append(";"); break; case '(': result.append("("); break; case ')': result.append(")"); break; case '&': result.append("&"); break; case '+': result.append("+"); break; default: result.append(value.charAt(i)); break; } return result; } ... } ... // Filter the HTTP response using Validator.filter PrintWriter out = response.getWriter(); // set output response out.write(Validator.filter(response)); out.close();
The Java Servlet API 2.3 introduced Filters, which supports the interception and transformation of HTTP requests or responses.
Example of using a Servlet Filter to sanitize the response using Validator.filter:
// Example to filter all sensitive characters in the HTTP response using a Java Filter. // This example is for illustration purposes since it will filter all content in the response, including HTML tags! public class SensitiveCharsFilter implements Filter { ... public void doFilter(ServletRequest request, ServletResponse response, FilterChain chain) throws IOException, ServletException { PrintWriter out = response.getWriter(); ResponseWrapper wrapper = new ResponseWrapper((HttpServletResponse)response); chain.doFilter(request, wrapper); CharArrayWriter caw = new CharArrayWriter(); caw.write(Validator.filter(wrapper.toString())); response.setContentType("text/html"); response.setContentLength(caw.toString().length()); out.write(caw.toString()); out.close(); } ... public class CharResponseWrapper extends HttpServletResponseWrapper { private CharArrayWriter output; public String toString() { return output.toString(); } public CharResponseWrapper(HttpServletResponse response){ super(response); output = new CharArrayWriter(); } public PrintWriter getWriter(){ return new PrintWriter(output); } } } }
[8-2] Secure the cookie
When storing sensitive data in a cookie, make sure to set the secure flag of the cookie in the HTTP response, using Cookie.setSecure(boolean flag) to instruct the browser to send the cookie using a secure protocol, such as HTTPS or SSL.
Example to secure the "user" cookie:
// Example to secure a cookie, i.e. instruct the browser to // send the cookie using a secure protocol Cookie cookie = new Cookie("user", "sensitive"); cookie.setSecure(true); response.addCookie(cookie);
RECOMMENDED JAVA TOOLS
The two main Java frameworks for server-side validation are:
[1] Jakarta Commons Validator (integrated with Struts 1.1)
The Jakarta Commons Validator is a powerful framework that implements all the above data validation requirements. These rules are configured in an XML file that defines input validation rules for form fields. Struts supports output filtering of dangerous characters in the [8] HTTP Response by default on all data written using the Struts 'bean:write' tag. This filtering may be disabled by setting the 'filter=false' flag.
Struts defines the following basic input validators, but custom validators may also be defined:
required: succeeds if the field contains any characters other than white space.
mask: succeeds if the value matches the regular expression given by the mask attribute.
range: succeeds if the value is within the values given by the min and max attributes ((value >= min) & (value <= max)).
maxLength: succeeds if the field is length is less than or equal to the max attribute.
minLength: succeeds if the field is length is greater than or equal to the min attribute.
byte, short, integer, long, float, double: succeeds if the value can be converted to the corresponding primitive.
date: succeeds if the value represents a valid date. A date pattern may be provided.
creditCard: succeeds if the value could be a valid credit card number.
e-mail: succeeds if the value could be a valid e-mail address.
Example to validate the userName field of a loginForm using Struts Validator:
<form-validation> <global> ... <validator name="required" classname="org.apache.struts.validator.FieldChecks" method="validateRequired" msg="errors.required"> </validator> <validator name="mask" classname="org.apache.struts.validator.FieldChecks" method="validateMask" msg="errors.invalid"> </validator> ... </global> <formset> <form name="loginForm"> <!-- userName is required and is alpha-numeric case insensitive --> <field property="userName" depends="required,mask"> <!-- message resource key to display if validation fails --> <msg name="mask" key="login.userName.maskmsg"/> <arg0 key="login.userName.displayname"/> <var> <var-name>mask</var-name> <var-value>^[a-zA-Z0-9]*$</var-value> </var> </field> ... </form> ... </formset> </form-validation>
[2] JavaServer Faces Technology
JavaServer Faces Technology is a set of Java APIs (JSR 127) to represent UI components, manage their state, handle events and input validation.
The JavaServer Faces API implements the following basic validators, but custom validators may be defined:
validate_doublerange: registers a DoubleRangeValidator on a component
validate_length: registers a LengthValidator on a component
validate_longrange: registers a LongRangeValidator on a component
validate_required: registers a RequiredValidator on a component
validate_stringrange: registers a StringRangeValidator on a component
validator: registers a custom Validator on a component
The JavaServer Faces API defines the following UIInput and UIOutput Renderers (Tags):
input_date: accepts a java.util.Date formatted with a java.text.Date instance

output_date: displays a java.util.Date formatted with a java.text.Date instance
input_datetime: accepts a java.util.Date formatted with a java.text.DateTime instance
output_datetime: displays a java.util.Date formatted with a java.text.DateTime instance
input_number: displays a numeric data type (java.lang.Number or primitive), formatted with a java.text.NumberFormat
output_number: displays a numeric data type (java.lang.Number or primitive), formatted with a java.text.NumberFormat
input_text: accepts a text string of one line.
output_text: displays a text string of one line.
input_time: accepts a java.util.Date, formatted with a java.text.DateFormat time instance
output_time: displays a java.util.Date, formatted with a java.text.DateFormat time instance
input_hidden: allows a page author to include a hidden variable in a page
input_secret: accepts one line of text with no spaces and displays it as a set of asterisks as it is typed
input_textarea: accepts multiple lines of text
output_errors: displays error messages for an entire page or error messages associated with a specified client identifier
output_label: displays a nested component as a label for a specified input field
output_message: displays a localized message
Example to validate the userName field of a loginForm using JavaServer Faces:
<%@ taglib uri="https://docs.oracle.com/javaee/6/tutorial/doc/glxce.html" prefix="h" %> <%@ taglib uri="http://mrbool.com/how-to-create-a-login-validation-with-jsf-java-server-faces/27046" prefix="f" %> ... <jsp:useBean id="UserBean" class="myApplication.UserBean" scope="session" /> <f:use_faces> <h:form formName="loginForm" > <h:input_text id="userName" size="20" modelReference="UserBean.userName"> <f:validate_required/> <f:validate_length minimum="8" maximum="20"/> </h:input_text> <!-- display errors if present --> <h:output_errors id="loginErrors" clientId="userName"/> <h:command_button id="submit" label="Submit" commandName="submit" /><p> </h:form> </f:use_faces>
REFERENCES
Java API 1.3 -
https://www.oracle.com/java/technologies/java-archive-13docs-downloads.html
Java API 1.4 -
https://www.oracle.com/java/technologies/java-archive-142docs-downloads.html
Java Servlet API 2.3 -
https://mvnrepository.com/artifact/javax.servlet/javax.servlet-api
Java Regular Expression Package -
http://jakarta.apache.org/regexp/
Jakarta Validator -
http://jakarta.apache.org/commons/validator/
JavaServer Faces Technology -
http://www.javaserverfaces.org/
** Error Handling:
Many J2EE web application architectures follow the Model View Controller (MVC) pattern. In this pattern a Servlet acts as a Controller. A Servlet delegates the application processing to a JavaBean such as an EJB Session Bean (the Model). The Servlet then forwards the request to a JSP (View) to render the processing results. Servlets should check all input, output, return codes, error codes and known exceptions to ensure that the expected processing actually occurred.
While data validation protects applications against malicious data tampering, a sound error handling strategy is necessary to prevent the application from inadvertently disclosing internal error messages such as exception stack traces. A good error handling strategy addresses the following items:
[1] Defining Errors
[2] Reporting Errors
[3] Rendering Errors
[4] Error Mapping
[1] Defining Errors
Hard-coded error messages in the application layer (e.g. Servlets) should be avoided. Instead, the application should use error keys that map to known application failures. A good practice is to define error keys that map to validation rules for HTML form fields or other bean properties. For example, if the "user_name" field is required, is alphanumeric, and must be unique in the database, then the following error keys should be defined:
(a) ERROR_USERNAME_REQUIRED: this error key is used to display a message notifying the user that the "user_name" field is required;
(b) ERROR_USERNAME_ALPHANUMERIC: this error key is used to display a message notifying the user that the "user_name" field should be alphanumeric;
(c) ERROR_USERNAME_DUPLICATE: this error key is used to display a message notifying the user that the "user_name" value is a duplicate in the database;
(d) ERROR_USERNAME_INVALID: this error key is used to display a generic message notifying the user that the "user_name" value is invalid;
A good practice is to define the following framework Java classes which are used to store and report application errors:
- ErrorKeys: defines all error keys
// Example: ErrorKeys defining the following error keys: // - ERROR_USERNAME_REQUIRED // - ERROR_USERNAME_ALPHANUMERIC // - ERROR_USERNAME_DUPLICATE // - ERROR_USERNAME_INVALID // ... public Class ErrorKeys { public static final String ERROR_USERNAME_REQUIRED = "error.username.required"; public static final String ERROR_USERNAME_ALPHANUMERIC = "error.username.alphanumeric"; public static final String ERROR_USERNAME_DUPLICATE = "error.username.duplicate"; public static final String ERROR_USERNAME_INVALID = "error.username.invalid"; ... }
- Error: encapsulates an individual error

// Example: Error encapsulates an error key. // Error is serializable to support code executing in multiple JVMs. public Class Error implements Serializable { // Constructor given a specified error key public Error(String key) { this(key, null); } // Constructor given a specified error key and array of placeholder objects public Error(String key, Object[] values) { this.key = key; this.values = values; } // Returns the error key public String getKey() { return this.key; } // Returns the placeholder values public Object[] getValues() { return this.values; } private String key = null; private Object[] values = null; }
- Errors: encapsulates a Collection of errors
// Example: Errors encapsulates the Error objects being reported to the presentation layer. // Errors are stored in a HashMap where the key is the bean property name and value is an // ArrayList of Error objects. public Class Errors implements Serializable { // Adds an Error object to the Collection of errors for the specified bean property. public void addError(String property, Error error) { ArrayList propertyErrors = (ArrayList)errors.get(property); if (propertyErrors == null) { propertyErrors = new ArrayList(); errors.put(property, propertyErrors); } propertyErrors.put(error); } // Returns true if there are any errors public boolean hasErrors() { return (errors.size > 0); } // Returns the Errors for the specified property public ArrayList getErrors(String property) { return (ArrayList)errors.get(property); } private HashMap errors = new HashMap(); }
Using the above framework classes, here is an example to process validation errors of the "user_name" field:
// Example to process validation errors of the "user_name" field. Errors errors = new Errors(); String userName = request.getParameter("user_name"); // (a) Required validation rule if (!Validator.validateRequired(userName)) { errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_REQUIRED)); } // (b) Alpha-numeric validation rule else if (!Validator.matchPattern(userName, "^[a-zA-Z0-9]*$")) { errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_ALPHANUMERIC)); } else { // (c) Duplicate check validation rule // We assume that there is an existing UserValidationEJB session bean that implements // a checkIfDuplicate() method to verify if the user already exists in the database. try { ... if (UserValidationEJB.checkIfDuplicate(userName)) { errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_DUPLICATE)); } } catch (RemoteException e) { // log the error logger.error("Could not validate user for specified userName: " + userName); errors.addError("user_name", new Error(ErrorKeys.ERROR_USERNAME_DUPLICATE); } } // set the errors object in a request attribute called "errors" request.setAttribute("errors", errors); ...
[2] Reporting Errors
There are two ways to report web-tier application errors:
(a) Servlet Error Mechanism
(b) JSP Error Mechanism
[2-a] Servlet Error Mechanism
A Servlet may report errors by:
- forwarding to the input JSP (having already stored the errors in a request attribute), OR
- calling response.sendError with an HTTP error code argument, OR
- throwing an exception
It is good practice to process all known application errors (as described in section [1]), store them in a request attribute, and forward to the input JSP. The input JSP should display the error messages and prompt the user to re-enter the data. The following example illustrates how to forward to an input JSP (userInput.jsp):
// Example to forward to the userInput.jsp following user validation errors RequestDispatcher rd = getServletContext().getRequestDispatcher("/user/userInput.jsp"); if (rd != null) { rd.forward(request, response); }
If the Servlet cannot forward to a known JSP page, the second option is to report an error using the response.sendError method with HttpServletResponse.SC_INTERNAL_SERVER_ERROR (status code 500) as argument. Refer to the javadoc of javax.servlet.http.HttpServletResponse for more details on the various HTTP status codes.
Example to return a HTTP error:
// Example to return a HTTP error code RequestDispatcher rd = getServletContext().getRequestDispatcher("/user/userInput.jsp"); if (rd == null) { // messages is a resource bundle with all message keys and values response.sendError(HttpServletResponse.SC_INTERNAL_SERVER_ERROR, messages.getMessage(ErrorKeys.ERROR_USERNAME_INVALID)); }
As a last resort, Servlets can throw an exception, which must be a subclass of one of the following classes:
- RuntimeException
- ServletException
- IOException
[2-b] JSP Error Mechanism
JSP pages provide a mechanism to handle runtime exceptions by defining an errorPage directive as shown in the following example:
<%@ page errorPage="/errors/userValidation.jsp" %>
Uncaught JSP exceptions are forwarded to the specified errorPage, and the original exception is set in a request parameter called javax.servlet.jsp.jspException. The error page must include a isErrorPage directive as shown below:
<%@ page isErrorPage="true" %>
The isErrorPage directive causes the "exception" variable to be initialized to the exception object being thrown.
[3] Rendering Errors
The J2SE Internationalization APIs provide utility classes for externalizing application resources and formatting messages including:
(a) Resource Bundles
(b) Message Formatting
[3-a] Resource Bundles
Resource bundles support internationalization by separating localized data from the source code that uses it. Each resource bundle stores a map of key/value pairs for a specific locale.
It is common to use or extend java.util.PropertyResourceBundle, which stores the content in an external properties file as shown in the following example:
ErrorMessages.properties

required user name error message error.username.required=User name field is required # invalid user name format error.username.alphanumeric=User name must be alphanumeric # duplicate user name error message error.username.duplicate=User name {0} already exists, please choose another one ...
Multiple resources can be defined to support different locales (hence the name resource bundle). For example, ErrorMessages_fr.properties can be defined to support the French member of the bundle family. If the resource member of the requested locale does not exist, the default member is used. In the above example, the default resource is ErrorMessages.properties. Depending on the user's locale, the application (JSP or Servlet) retrieves content from the appropriate resource.
[3-b] Message Formatting
The J2SE standard class java.util.MessageFormat provides a generic way to create messages with replacement placeholders. A MessageFormat object contains a pattern string with embedded format specifiers as shown below:
// Example to show how to format a message using placeholder parameters String pattern = "User name {0} already exists, please choose another one"; String userName = request.getParameter("user_name"); Object[] args = new Object[1]; args[0] = userName; String message = MessageFormat.format(pattern, args);
Here is a more comprehensive example to render error messages using ResourceBundle and MessageFormat:
// Example to render an error message from a localized ErrorMessages resource (properties file) // Utility class to retrieve locale-specific error messages public Class ErrorMessageResource { // Returns the error message for the specified error key in the environment locale public String getErrorMessage(String errorKey) { return getErrorMessage(errorKey, defaultLocale); } // Returns the error message for the specified error key in the specified locale public String getErrorMessage(String errorKey, Locale locale) { return getErrorMessage(errorKey, null, locale); } // Returns a formatted error message for the specified error key in the specified locale public String getErrorMessage(String errorKey, Object[] args, Locale locale) { // Get localized ErrorMessageResource ResourceBundle errorMessageResource = ResourceBundle.getBundle("ErrorMessages", locale); // Get localized error message String errorMessage = errorMessageResource.getString(errorKey); if (args != null) { // Format the message using the specified placeholders args return MessageFormat.format(errorMessage, args); } else { return errorMessage; } } // default environment locale private Locale defaultLocale = Locale.getDefaultLocale(); } ... // Get the user's locale Locale userLocale = request.getLocale(); // Check if there were any validation errors Errors errors = (Errors)request.getAttribute("errors"); if (errors != null && errors.hasErrors()) { // iterate through errors and output error messages corresponding to the "user_name" property ArrayList userNameErrors = errors.getErrors("user_name"); ListIterator iterator = userNameErrors.iterator(); while (iterator.hasNext()) { // Get the next error object Error error = (Error)iterator.next(); String errorMessage = ErrorMessageResource.getErrorMessage(error.getKey(), userLocale); output.write(errorMessage + "\r\n"); } }
It is recommended to define a custom JSP tag, e.g. displayErrors, to iterate through and render error messages as shown in the above example.
[4] Error Mapping
Normally, the Servlet Container will return a default error page corresponding to either the response status code or the exception. A mapping between the status code or the exception and a web resource may be specified using custom error pages. It is a good practice to develop static error pages that do not disclose internal error states (by default, most Servlet containers will report internal error messages). This mapping is configured in the Web Deployment Descriptor (web.xml) as specified in the following example:
<!-- Mapping of HTTP error codes and application exceptions to error pages --> <error-page> <exception-type>UserValidationException</exception-type> <location>/errors/validationError.html</error-page> </error-page> <error-page> <error-code>500</exception-type> <location>/errors/internalError.html</error-page> </error-page> <error-page> ... </error-page> ...
RECOMMENDED JAVA TOOLS
The two main Java frameworks for server-side validation are:
[1] Jakarta Commons Validator (integrated with Struts 1.1)
The Jakarta Commons Validator is a Java framework that defines the error handling mechanism as described above. Validation rules are configured in an XML file that defines input validation rules for form fields and the corresponding validation error keys. Struts provides internationalization support to build localized applications using resource bundles and message formatting.
Example to validate the userName field of a loginForm using Struts Validator:
<form-validation> <global> ... <validator name="required" classname="org.apache.struts.validator.FieldChecks" method="validateRequired" msg="errors.required"> </validator> <validator name="mask" classname="org.apache.struts.validator.FieldChecks" method="validateMask" msg="errors.invalid"> </validator> ... </global> <formset> <form name="loginForm"> <!-- userName is required and is alpha-numeric case insensitive --> <field property="userName" depends="required,mask"> <!-- message resource key to display if validation fails --> <msg name="mask" key="login.userName.maskmsg"/> <arg0 key="login.userName.displayname"/> <var> <var-name>mask</var-name> <var-value>^[a-zA-Z0-9]*$</var-value> </var> </field> ... </form> ... </formset> </form-validation>
The Struts JSP tag library defines the "errors" tag that conditionally displays a set of accumulated error messages as shown in the following example:
<%@ page language="java" %> <%@ taglib uri="/WEB-INF/struts-html.tld" prefix="html" %> <%@ taglib uri="/WEB-INF/struts-bean.tld" prefix="bean" %> <html:html> <head> <body> <html:form action="/logon.do"> <table border="0" width="100%"> <tr> <th align="right"> <html:errors property="username"/> <bean:message key="prompt.username"/> </th> <td align="left"> <html:text property="username" size="16"/> </td> </tr> <tr> <td align="right"> <html:submit><bean:message key="button.submit"/></html:submit> </td> <td align="right"> <html:reset><bean:message key="button.reset"/></html:reset> </td> </tr> </table> </html:form> </body> </html:html>
[2] JavaServer Faces Technology
JavaServer Faces Technology is a set of Java APIs (JSR 127) to represent UI components, manage their state, handle events, validate input, and support internationalization.
The JavaServer Faces API defines the "output_errors" UIOutput Renderer, which displays error messages for an entire page or error messages associated with a specified client identifier.
Example to validate the userName field of a loginForm using JavaServer Faces:
<%@ taglib uri="https://docs.oracle.com/javaee/6/tutorial/doc/glxce.html" prefix="h" %> <%@ taglib uri="http://mrbool.com/how-to-create-a-login-validation-with-jsf-java-server-faces/27046" prefix="f" %> ... <jsp:useBean id="UserBean" class="myApplication.UserBean" scope="session" /> <f:use_faces> <h:form formName="loginForm" > <h:input_text id="userName" size="20"

modelReference="UserBean.userName"> <f:validate_required/> <f:validate_length minimum="8" maximum="20"/> </h:input_text> <!-- display errors if present --> <h:output_errors id="loginErrors" clientId="userName"/> <h:command_button id="submit" label="Submit" commandName="submit" /><p> </h:form> </f:use_faces>
REFERENCES
Java API 1.3 -
https://www.oracle.com/java/technologies/java-archive-13docs-downloads.html
Java API 1.4 -
https://www.oracle.com/java/technologies/java-archive-142docs-downloads.html
Java Servlet API 2.3 -
https://mvnrepository.com/artifact/javax.servlet/javax.servlet-api
Java Regular Expression Package -
http://jakarta.apache.org/regexp/
Jakarta Validator -
http://jakarta.apache.org/commons/validator/
JavaServer Faces Technology -
http://www.javaserverfaces.org/
** Input Data Validation:
While data validations may be provided as a user convenience on the client-tier, data validation must always be performed on the server-tier. Client-side validations are inherently insecure because they can be easily bypassed, e.g. by disabling Javascript.
A good design usually requires the web application framework to provide server-side utility routines to validate the following:
[1] Required field
[2] Field data type (all HTTP request parameters are Strings by default)
[3] Field length
[4] Field range
[5] Field options
[6] Field pattern
[7] Cookie values
[8] HTTP Response
A good practice is to implement a function or functions that validates each application parameter. The following sections describe some example checking.
[1] Required field
Always check that the field is not null and its length is greater than zero, excluding leading and trailing white spaces.
Example of how to validate required fields:
// PHP example to validate required fields function validateRequired($input) { ... $pass = false; if (strlen(trim($input))>0){ $pass = true; } return $pass; ... } ... if (validateRequired($fieldName)) { // fieldName is valid, continue processing request ... }
[2] Field data type
In web applications, input parameters are poorly typed. For example, all HTTP request parameters or cookie values are of type String. The developer is responsible for verifying the input is of the correct data type.
[3] Field length
Always ensure that the input parameter (whether HTTP request parameter or cookie value) is bounded by a minimum length and/or a maximum length.
[4] Field range
Always ensure that the input parameter is within a range as defined by the functional requirements.
[5] Field options
Often, the web application presents the user with a set of options to choose from, e.g. using the SELECT HTML tag, but fails to perform server-side validation to ensure that the selected value is one of the allowed options. Remember that a malicious user can easily modify any option value. Always validate the selected user value against the allowed options as defined by the functional requirements.
[6] Field pattern
Always check that user input matches a pattern as defined by the functionality requirements. For example, if the userName field should only allow alpha-numeric characters, case insensitive, then use the following regular expression:
^[a-zA-Z0-9]+$
[7] Cookie value
The same validation rules (described above) apply to cookie values depending on the application requirements, e.g. validate a required value, validate length, etc.
[8] HTTP Response
[8-1] Filter user input
To guard the application against cross-site scripting, the developer should sanitize HTML by converting sensitive characters to their corresponding character entities. These are the HTML sensitive characters:
< > " ' % ;) (& +
PHP includes some automatic sanitization utility functions, such as htmlentities():
$input = htmlentities($input, ENT_QUOTES, 'UTF-8');
In addition, in order to avoid UTF-7 variants of Cross-site Scripting, you should explicitly define the Content-Type header of the response, for example:
<?php header('Content-Type: text/html; charset=UTF-8'); ?>
[8-2] Secure the cookie
When storing sensitive data in a cookie and transporting it over SSL, make sure that you first set the secure flag of the cookie in the HTTP

response. This will instruct the browser to only use that cookie over SSL connections.
You can use the following code example, for securing the cookie:
<$php $value = "some_value"; $time = time()+3600; $path = "/application/"; $domain = ".example.com"; $secure = 1; setcookie("CookieName", $value, $time, $path, $domain, $secure, TRUE); ?>
In addition, we recommend that you use the HttpOnly flag. When the HttpOnly flag is set to TRUE the cookie will be made accessible only through the HTTP protocol. This means that the cookie won't be accessible by scripting languages, such as JavaScript. This setting can effectively help to reduce identity theft through XSS attacks (although it is not supported by all browsers).
The HttpOnly flag was Added in PHP 5.2.0.
REFERENCES
[1] Mitigating Cross-site Scripting With HTTP-only Cookies:
http://msdn2.microsoft.com/en-us/library/ms533046.aspx
[2] PHP Security Consortium:
http://phpsec.org/
[3] PHP & Web Application Security Blog (Chris Shiflett):
http://shiflett.org/

CWE:

550

External References:

An example for using apostrophe to hack a site can be found in "How I hacked PacketStorm (by Rain Forest Puppy), RFP's site"
"Web Application Disassembly with ODBC Error Messages" (By David Litchfield)
CERT Advisory (CA-1997-25): Sanitizing user-supplied data in CGI scripts

Email Address Pattern Found

TOC

Cause:

Insecure web application programming or configuration

Risk:

It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Spambots crawl internet sites, set out to find e-mail addresses in order to build mailing lists for sending unsolicited e-mail (spam).
AppScan detected a response containing one or more e-mail addresses, which may be exploited to send spam mail
Furthermore, the e-mail addresses found may be private and thus should not be accessible to the general public.

Affected Products:

This issue may affect different types of products.

Fix Recommendation:

General

Remove any e-mail addresses from the website so that they won't be exploited by malicious users.

CWE:

359

External References:

Definition of Spambot (Wikipedia)

Missing "Referrer policy" Security Header

TOC

Cause:

Insecure web application programming or configuration

Risk:

It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
The absence or improper values of Referrer Policy can cause URL leak itself, and even sensitive information contained in the URL will be leaked to the cross-site.
This is a part of ruleset to check if Referrer Policy is present and if so to test its configuration. The "Referer Policy" header defines what data is made available in the Referer header, and for navigation and iframes in the destination's (document.referrer). This header is designed to modify the way browsers render pages, and thus to prevent cross-domain Referer leakage. It is important to set the header value correctly, in a way that will not prevent proper operation of the web site.
Referer header is a request header that indicates the site which the traffic originated from. If there is no adequate prevention in place, the URL itself, and even sensitive information contained in the URL will be leaked to the cross-site.
"no-referrer-when-downgrade" and "unsafe-url" are the policies which leaks the Full Url for the ThirdParty Sites. The remaining policies are"no-referrer", "origin", "origin-when-cross-origin","same-origin", "strict-origin", "strict-origin-when-cross-origin.
Please refer the following links for more information.

Affected Products:

This issue may affect different types of products

Fix Recommendation:

General

Configure your server to send the "Referrer Policy" header.
It is recommended to configure Referrer Policy header with secure values for its directives as below:
"strict-origin-when-cross-origin" offers more privacy. With this policy, only the origin is sent in the Referer header of cross-origin requests.
For Google Chrome, see:
https://developers.google.com/web/updates/2020/07/referrer-policy-new-chrome-default
For Firefox , see:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy.

CWE:

200

External References:

MDN web docs - Referrer-Policy

Application Data

Visited URLs 7

TOC

URL
https://drims.nginxdev.egovja.com/
https://drims.nginxdev.egovja.com/login?next=%2F
https://drims.nginxdev.egovja.com/login
https://drims.nginxdev.egovja.com/account-requests/submit
https://drims.nginxdev.egovja.com/login
https://drims.nginxdev.egovja.com/account-requests/
https://drims.nginxdev.egovja.com/login

Parameters 9

TOC

Name	Value	URL	Type
password		https://drims.nginxdev.egovja.com/login	Password
contact_email	test@altoromutual.com	https://drims.nginxdev.egovja.com/account-requests/	Text
reason_text	1234	https://drims.nginxdev.egovja.com/account-requests/	TextArea
next	/	https://drims.nginxdev.egovja.com/login?next=%2F	Simple Link
agency_name		https://drims.nginxdev.egovja.com/account-requests/	Text
email	test@altoromutual.com	https://drims.nginxdev.egovja.com/login	Text
contact_phone	555-555-5555	https://drims.nginxdev.egovja.com/account-requests/	Text
remember	on	https://drims.nginxdev.egovja.com/login	Checkbox
contact_name		https://drims.nginxdev.egovja.com/account-requests/	Text

Failed Requests 1

TOC

URL	Reason
https://drims.nginxdev.egovja.com/static/	Response Status '403' - Forbidden

Filtered URLs 11

TOC

URL	Reason
https://cdn.jsdelivr.net/npm/bootstrap@5.3.3/dist/js/bootstrap.bundle.min.js	Untested Web Server
https://cdn.jsdelivr.net/npm/bootstrap@5.3.3/dist/js/bootstrap.bundle.min.js	Untested Web Server
https://cdn.jsdelivr.net/npm/bootstrap@5.3.3/dist/css/bootstrap.min.css	Untested Web Server
https://cdn.jsdelivr.net/npm/bootstrap-icons@1.11.3/font/bootstrap-icons.css	Untested Web Server
https://drims.nginxdev.egovja.com/static/css/modern-ui.css	File Extension
https://drims.nginxdev.egovja.com/static/images/jamaica-coat-of-arms.png	File Extension
https://drims.nginxdev.egovja.com/static/images/odpem-logo.png	File Extension
https://drims.nginxdev.egovja.com/static/css/workflow-sidebar.css	File Extension
https://drims.nginxdev.egovja.com/static/css/notifications-ui.css	File Extension
https://drims.nginxdev.egovja.com/account-requests/submit	Similar DOM
https://drims.nginxdev.egovja.com/login	Similar Body

Comments 8

TOC

URL	Comment
https://drims.nginxdev.egovja.com/	<!doctype html>
https://drims.nginxdev.egovja.com/login	Login Card
https://drims.nginxdev.egovja.com/login	Flash messages
https://drims.nginxdev.egovja.com/login	Agency CTA Card
https://drims.nginxdev.egovja.com/login	Footer
https://drims.nginxdev.egovja.com/account-requests/submit	<!DOCTYPE html>
https://drims.nginxdev.egovja.com/account-requests/submit	DMIS Modern UI Design System
https://drims.nginxdev.egovja.com/account-requests/submit	Page-specific scripts

JavaScripts 2

TOC

URL / Code

https://drims.nginxdev.egovja.com/account-requests/submit

```
(function() {
    'use strict';

    var forms = document.querySelectorAll('.needs-validation');

    Array.prototype.slice.call(forms).forEach(function(form) {
        form.addEventListener('submit', function(event) {
          if (!form.checkValidity()) {
          event.preventDefault();
          event.stopPropagation();
          }
```

```
          form.classList.add('was-validated');
        }, false);
    });
})();
```

https://drims.nginxdev.egovja.com/account-requests/submit

```
        document.addEventListener('DOMContentLoaded', function() {
          const sidebar = document.getElementById('sidebar');
          const sidebarToggle = document.getElementById('sidebarToggle');

          if (sidebarToggle) {
          sidebarToggle.addEventListener('click', function() {
          sidebar.classList.toggle('collapsed');
          localStorage.setItem('sidebarCollapsed', sidebar.classList.contains('collapsed'));
          });

          const sidebarCollapsed = localStorage.getItem('sidebarCollapsed') === 'true';
          if (sidebarCollapsed) {
          sidebar.classList.add('collapsed');
          }
          }


        });



        // Mobile Navigation Toggle
        const sidebarToggle = document.getElementById('sidebarToggle');
        const sidebar = document.getElementById('sidebar');
        const sidebarOverlay = document.getElementById('sidebarOverlay');
        const sidebarClose = document.getElementById('sidebarClose');

        function openSidebar() {
          sidebar.classList.add('active');
          sidebarOverlay.classList.add('active');
          sidebarToggle.setAttribute('aria-expanded', 'true');
          sidebarOverlay.setAttribute('aria-hidden', 'false');
          document.body.style.overflow = 'hidden'; // Prevent scrolling when sidebar is open
        }

        function closeSidebar() {
          sidebar.classList.remove('active');
          sidebarOverlay.classList.remove('active');
          sidebarToggle.setAttribute('aria-expanded', 'false');
          sidebarOverlay.setAttribute('aria-hidden', 'true');
          document.body.style.overflow = ''; // Restore scrolling
        }

        // Toggle sidebar on button click
        if (sidebarToggle) {
          sidebarToggle.addEventListener('click', function() {
          if (sidebar.classList.contains('active')) {
          closeSidebar();
          } else {
          openSidebar();
          }
          });
        }

        // Close sidebar on close button click
        if (sidebarClose) {
          sidebarClose.addEventListener('click', closeSidebar);
        }

        // Close sidebar on overlay click
        if (sidebarOverlay) {
          sidebarOverlay.addEventListener('click', closeSidebar);
        }

        // Close sidebar on Escape key
        document.addEventListener('keydown', function(e) {
          if (e.key === 'Escape' && sidebar && sidebar.classList.contains('active')) {
          closeSidebar();
          }
        });
```

```
        // Close sidebar when clicking on a navigation link (mobile)
        if (sidebar) {
          sidebar.addEventListener('click', function(e) {
          if (e.target.closest('a') && window.innerWidth < 992) {
          // Small delay to allow navigation to start
          setTimeout(closeSidebar, 150);
          }
          });
        }

        document.querySelectorAll('.table-clickable tbody tr[data-href]').forEach(row => {
          row.addEventListener('click', function(e) {
          if (!e.target.closest('button') && !e.target.closest('a')) {
          window.location.href = this.dataset.href;
          }
          });
        });
```

Cookies 1

TOC

Name	First Set	Domain	Secure	HTTP Only	Same Site	JS Stack Trace
Value	**Requested URL**		**Expires**			
session	https://drims.nginxdev.egovja.com/login?next=%2F	drims.nginxdev.egovja.com	False	True		
eyJfZnJlc2giOmZhbHNlfQ.aSEfJA.Ma241nHGjlx5NC2c53mM1XUUza0	https://drims.nginxdev.egovja.com/login?next=%2F					

Components 0

TOC

Name	Version	URL