Web Application Report

This report includes important security information about your web application.

Security report

This report was created by HCL AppScan Standard 10.7.0
Scan started: 3/5/2025 3:30:34 PM

Table of Contents

Introduction

Summary

Issues Grouped by Issue Type

Introduction

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

Low severity issues:	3
Informational severity issues:	5
Total security issues included in the report:	8
Total security issues discovered in the scan:	8

General Information

Scan file name:	Untitled
Scan started:	3/5/2025 3:30:34 PM
Test policy:	Default
CVSS version:	3.1
Test optimization level:	Fast

Host	localhost
Port	5222
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 7

TOC

	Issue Type	Number of Issues
L	Missing "Content-Security-Policy" header	1
L	Missing or insecure "X-Content-Type-Options" header	1
L	Unnecessary Http Response Headers found in the Application	1
I	Client-Side (JavaScript) Cookie References	1
I	Email Address Pattern Found	2
I	Missing "Referrer policy" Security Header	1
I	Possible Server Path Disclosure Pattern Found	1

Vulnerable URLs 3

TOC

	URL	Number of Issues
L	http://localhost:5222/	4
I	http://localhost:5222/swagger/swagger-ui-bundle.js	3
I	http://localhost:5222/swagger/swagger-ui-standalone-preset.js	1

Fix Recommendations 7

TOC

	Remediation Task	Number of Issues
L	Config your server to use the "Content-Security-Policy" header with secure policies	1
L	Config your server to use the "Referrer Policy" header with secure policies	1
L	Config your server to use the "X-Content-Type-Options" header with "nosniff" value	1
L	Do not allow sensitive information to leak.	1
L	Download the relevant security patch for your web server or web application.	1
L	Remove business and security logic from the client side	1
L	Remove e-mail addresses from the website	2

Security Risks 4

TOC

	Risk	Number of Issues
L	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations	6
L	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.	3
I	The worst case scenario for this attack depends on the context and role of the cookies that are created at the client side	1
I	It is possible to retrieve the absolute path of the web server installation, which might help an attacker to develop further attacks and to gain information about the file system structure of the web application	1

Causes 3

TOC

	Cause	Number of Issues
L	Insecure web application programming or configuration	6
I	Cookies are created at the client side	1
I	Latest patches or hotfixes for 3rd. party products were not installed	1

WASC Threat Classification

TOC

Threat	Number of Issues
Information Leakage	8

Issues Grouped by Issue Type

L Missing "Content-Security-Policy" header 1 TOC

Issue 1 of 1 TOC

Missing "Content-Security-Policy" header

Severity:	Low
CVSS Score:	3.7
CVSS Vector:	AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N/E:X/RL:X/RC:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MPR:X/MUI:X/MS:X/MC:X/MI:X/MA:X
URL:	http://localhost:5222/
Entity:	localhost (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

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

Raw Test Response:

```
...
GET /swagger/index.html HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Host: localhost:5222
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
Content-Type: text/html;charset=utf-8
Date: Wed, 05 Mar 2025 08:32:41 GMT
Server: Kestrel
Transfer-Encoding: chunked

<!-- HTML for static distribution bundle build -->
<!DOCTYPE html>
<html lang="en">
<head>
...
```

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

Issue 1 of 1 TOC

Missing or insecure "X-Content-Type-Options" header	
Severity:	Low
CVSS Score:	3.7
CVSS Vector:	AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N/E:X/RL:X/RC:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MPR:X/MUI:X/MS:X/MC:X/MI:X/MA:X
URL:	http://localhost:5222/
Entity:	localhost (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

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

Raw Test Response:

```
...
GET /swagger/oauth2-redirect.html HTTP/1.1
Accept-Language: en-US
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://localhost:5222/swagger/index.html
Host: localhost:5222
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
Content-Type: text/html
Date: Wed, 05 Mar 2025 08:32:15 GMT
Server: Kestrel
Accept-Ranges: bytes
ETag: "1d89b8343538482"
Last-Modified: Tue, 19 Jul 2022 15:21:48 GMT
Transfer-Encoding: chunked

<!doctype html>
...
```

L Unnecessary Http Response Headers found in the Application 1 TOC

Unnecessary Http Response Headers found in the Application

Severity:	Low
CVSS Score:	3.7
CVSS Vector:	AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N/E:X/RL:X/RC:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MPR:X/MUI:X/MS:X/MC:X/MI:X/MA:X
URL:	http://localhost:5222/
Entity:	localhost (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.

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

Raw Test Response:

```
HTTP/1.1 404 Not Found
Content-Length: 0
Date: Wed, 05 Mar 2025 08:32:15 GMT
Server: Kestrel
Content-Security-Policy: default-src 'self';
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
Referrer-Policy: no-referrer...
```

I Client-Side (JavaScript) Cookie References 1 TOC

Issue 1 of 1 TOC

Client-Side (JavaScript) Cookie References

Severity:	Informational
CVSS Score:	0.0
CVSS Vector:	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N/E:X/RL:X/RC:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MPR:X/MUI:X/MS:X/MC:X/MI:X/MA:X
URL:	http://localhost:5222/swagger/swagger-ui-bundle.js
Entity:	/*! For license information please see swagger-ui-bundle.js.LICENSE.txt */ (Page)
Risk:	The worst case scenario for this attack depends on the context and role of the cookies that are created at the client side
Cause:	Cookies are created at the client side
Fix:	Remove business and security logic from the client side

Reasoning: AppScan found a reference to cookies in the JavaScript.

Original Response

```
HTTP/1.1 200 OK
Content-Length: 1096145
Content-Type: text/javascript
Date: Wed, 05 Mar 2025 08:32:15 GMT
Server: Kestrel
Accept-Ranges: bytes
ETag: "1d89b83434337d1"
Last-Modified: Tue, 19 Jul 2022 15:21:48 GMT

/*! For license information please see swagger-ui-bundle.js.LICENSE.txt */
!function(e,t){"object"==typeof exports&&"object"==typeof module?module.exports=t():"function"==typeof define&&define.amd?
define([],t):"object"==typeof exports?exports.SwaggerUIBundle=t():e.SwaggerUIBundle=t()}(this,(function(){return(()=>{var
e={66419:(e,t,n)=>{e.exports=n(24848)},41511:(e,t,n)=>{e.exports=n(83363)},11128:(e,t,n)=>{e.exports=n(57784)},54103:
(e,t,n)=>{e.exports=n(28196)},77766:(e,t,n)=>{e.exports=n(8065)},72119:(e,t,n)=>{e.exports=n(57448)},10062:(e,t,n)=>
{e.exports=n(29455)},44494:(e,t,n)=>{e.exports=n(69743)},20116:(e,t,n)=>{e.exports=n(11955)},62462:(e,t,n)=>
{e.exports=n(96064)},94473:(e,t,n)=>{e.exports=n(61577)....
```

I Email Address Pattern Found 2 TOC

Issue 1 of 2 TOC

Email Address Pattern Found

Severity:	Informational
CVSS Score:	0.0
CVSS Vector:	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N/E:X/RL:X/RC:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MPR:X/MUI:X/MS:X/MC:X/MI:X/MA:X
URL:	http://localhost:5222/swagger/swagger-ui-standalone-preset.js
Entity:	swagger-ui-standalone-preset.js (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

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

Raw Test Response:

```
...
...rn new(et())(t).gen()}catch(t){return"string"}}(t.pattern):"string"},string_email:function()
{return"user@example.com"},"string_date-time":function(){return(new Date).toISOString()},string_date:function(){return(new
D...

...
```

Issue 2 of 2

TOC

Email Address Pattern Found

Severity:	Informational
CVSS Score:	0.0
CVSS Vector:	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N/E:X/RL:X/RC:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MPR:X/MUI:X/MS:X/MC:X/MI:X/MA:X
URL:	http://localhost:5222/swagger/swagger-ui-bundle.js
Entity:	swagger-ui-bundle.js (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

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

Raw Test Response:

```
...
...urn new(O())(e).gen()}catch(e){return"string"}}(e.pattern):"string"},string_email:function()
{return"user@example.com"},"string_date-time":function(){return(new Date).toISOString()},string_date:function(){return(new
D...

...
```

I Missing "Referrer policy" Security Header 1 TOC

Issue 1 of 1 TOC

Missing "Referrer policy" Security Header

Severity:	Informational
CVSS Score:	0.0
CVSS Vector:	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N/E:X/RL:O/RC:C/CR:X/IR:X/AR:X/MAV:X/MAC:X/MPR:X/MUI:X/MS:X/MC:X/MI:X/MA:X
URL:	http://localhost:5222/
Entity:	localhost (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

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

Raw Test Response:

```
HTTP/1.1 200 OK
Content-Length: 13784
Content-Type: application/javascript; charset=utf-8
Date: Wed, 05 Mar 2025 08:31:22 GMT
Server: Kestrel
Cache-Control: no-store

setTimeout(async function () {
  const hotReloadActiveKey = '_dotnet_watch_hot_reload_active';
  // Ensure we only try to connect once, even if the script is both injected and manually inserted
  const scriptInjectedSentinel = '_dotnet_watch_ws_injected';
  if (window.hasOwnProperty(scriptInjectedSentinel)) {
    return;
  }
  window[scriptInjectedSentinel] = true;

  // dotnet-watch browser reload script
  const webSocketUrls = 'wss://localhost:44310/ShopDoGiaDungAPI/,ws://localhost:50406/ShopDoGiaDungAPI/'.split(',');
  const sharedSecret = await
getSecret('MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA9JOcczJSYDTBWd8O37MHIpiGdTEt3VlAiJQDlHDi4SCdMCGhm8H5eU45Axj7ogTRHUBb
s1vRo7F60O6vgqlClGPALF1eZLEfS+xm+G3T5pFFn4Qm3qUc1PeKVO0IeuvoucGWSrrRAcjoVLMTXS6g4rimhlLaUWX2IyT/VzRA6ttNHVIr+XdCAPdT7iuX4pS
WqS1ViH2BTwq7mNuE0KhowXgyXvDFQWaoOGS+O13zBUzNA6eDf1+O1oDGBXiOOWgwyz9VYr+uFcHw4fxRufChEYHX7LEoxOaUhi+ys7FrO8kzWt6Maxp8BeYvyP
7zk8...
```

I Possible Server Path Disclosure Pattern Found 1 TOC

Possible Server Path Disclosure Pattern Found

Severity:	Informational
CVSS Score:	0.0
CVSS Vector:	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N/E:X/RL:X/RC:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MPR:X/MUI:X/MS:X/MC:X/MI:X/MA:X
URL:	http://localhost:5222/swagger/swagger-ui-bundle.js
Entity:	swagger-ui-bundle.js (Page)
Risk:	It is possible to retrieve the absolute path of the web server installation, which might help an attacker to develop further attacks and to gain information about the file system structure of the web application
Cause:	Latest patches or hotfixes for 3rd. party products were not installed
Fix:	Download the relevant security patch for your web server or web application.

Reasoning: The response contains the absolute paths and/or filenames of files on the server.

Raw Test Response:

```
...
...n/g,"^\n"))?e.replace(/-d /g,"-d ^\n"):/^[_\/-]/g.test(e)?e:'"'+e+'"'},I=function(e){return"-d "===e?
e:/\n/.test(e)?'@"\n'+e.replace(/"/g,'\\"').replace(/`/g,"``").replace(/\$/,"`$")+'\n"@':/^[_\/-]/g.tes...

...
```