invicti

4/17/2025 12:12:21 PM (UTC+02:00)

Detailed Scan Report

http://100.26.242.68:5000/

Scan Time	: 4/17/2025 12:04:23 PM (UTC+02:00)
Scan Duration	: 00:00:06:44
Total Requests	: 4,207
Average Speed	: 10.4r/s

Risk Level:
MEDIUM

10 IDENTIFIED	**2** CONFIRMED	**0** CRITICAL
0 HIGH	1 MEDIUM	4 LOW
	2 BEST PRACTICE	3 INFORMATION

Identified Vulnerabilities

Critical	0
High	0
Medium	1
Low	4
Best Practice	2
Information	3
TOTAL	**10**

Confirmed Vulnerabilities

Critical	0
High	0
Medium	0
Low	1
Best Practice	1
Information	0
TOTAL	**2**

Vulnerability Summary

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER	PARAMETER TYPES
	SSL/TLS Not Implemented	GET	https://100.26.242.68/	No Parameters	No Parameter Types
	Misconfigured Access-Control-Allow-Origin Header	GET	http://100.26.242.68:5000/	No Parameters	No Parameter Types
	Missing X-Content-Type-Options Header	GET	http://100.26.242.68:5000/swagger/swagger-ui.css	No Parameters	No Parameter Types
	Version Disclosure (SwaggerUI)	GET	http://100.26.242.68:5000/swagger/swagger-ui-bundle.js	No Parameters	No Parameter Types
	Internal Server Error	POST	http://100.26.242.68:5000/api/Auth/login	No Parameters	No Parameter Types
	Referrer-Policy Not Implemented	GET	http://100.26.242.68:5000/swagger/oauth2-redirect.html	No Parameters	No Parameter Types
	Content Security Policy (CSP) Not Implemented	GET	http://100.26.242.68:5000/swagger/oauth2-redirect.html	No Parameters	No Parameter Types
	Kestrel Detected	GET	http://100.26.242.68:5000/	No Parameters	No Parameter Types
	Out-of-date Version (Swagger UI)	GET	http://100.26.242.68:5000/swagger/swagger-ui-bundle.js	No Parameters	No Parameter Types
	SwaggerUI Identified	GET	http://100.26.242.68:5000/swagger/swagger-ui-bundle.js	No Parameters	No Parameter Types

1. SSL/TLS Not Implemented

MEDIUM | 1

Invicti Standard detected that SSL/TLS is not implemented after trying to establish a secure connection to the target website.

Impact

An attacker who is able to intercept your - or your users' - network traffic can read and modify any messages that are exchanged with your server.

That means that an attacker can see passwords in clear text, modify the appearance of your website, redirect the user to other web pages or steal session information.

Therefore no message you send to the server remains confidential.

Vulnerabilities

1.1. https://100.26.242.68/

Certainty

Request | Response

Request

```
[SSL Connection]
```

Response

Response Time (ms) : 1
Total Bytes Received : 16
Body Length : 0
Is Compressed : No

```
[SSL Connection]
```

Remedy

We suggest that you implement SSL/TLS properly, for example by using the Certbot tool provided by the Let's Encrypt certificate authority. It can automatically configure most modern web servers, e.g. Apache and Nginx to use SSL/TLS. Both the tool and the certificates are free and are usually installed within minutes.

CLASSIFICATION

PCI DSS v3.2	6.5.4
PCI DSS v4.0	6.2.4
OWASP 2013	A6
OWASP 2017	A3
CWE	311
CAPEC	217
WASC	4
HIPAA	164.306
ASVS 4.0	9.1.1
NIST SP 800-53	SC-8
DISA STIG	V-6136
OWASP API Top Ten 2019	API7
ISO27001	A.14.1.3
ISO27001 2022	A.5.14
ISO27001 2022	A.8.27
OWASP Top Ten 2021	A02
OWASP API Top 10 2023	API8

CVSS 3.0 SCORE

Base	6.8 (Medium)
Temporal	6.1 (Medium)
Environmental	6.1 (Medium)

CVSS Vector String

CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C

CVSS 3.1 SCORE

Base	6.8 (Medium)
Temporal	6.1 (Medium)
Environmental	6.1 (Medium)

CVSS Vector String

CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C

CVSS 4.0 Score

5.1 / Medium	
Exploitability	Medium
Complexity	High
Vulnerable system	Low
Subsequent system	Low

CVSS 4.0 Score

Exploitation	High
Security requirements	Medium

CVSS Vector String

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N

2. Internal Server Error

LOW | 1 | CONFIRMED | 1

Invicti Standard identified an internal server error.

The server responded with an HTTP status 500, indicating there is a server-side error. Reasons may vary, and the behavior should be analyzed carefully. If Invicti Standard is able to find a security issue in the same resource, it will report this as a separate vulnerability.

Impact

The impact may vary depending on the condition. Generally this indicates poor coding practices, not enough error checking, sanitization and whitelisting. However, there might be a bigger issue, such as SQL injection. If that's the case, Invicti Standard will check for other possible issues and report them separately.
While the body content of the error page may not expose any information about the technical error, knowing whether certain inputs trigger a server error can aid or inform an attacker on potential vulnerabilities.

Vulnerabilities

2.1. http://100.26.242.68:5000/api/Auth/login

CONFIRMED

Method	Parameter	Parameter Type	Value
POST	username	Json	string
POST	password	Json	string

Request | Response

Request

```
POST /api/Auth/login HTTP/1.1
Host: 100.26.242.68:5000
Accept: */*
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Type: application/json
Referer: http://100.26.242.68:5000/swagger/index.html?urls.primaryName=BrokenWebAPI%20v1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36

{"username":"string","password":"string"}
```

Response

Response Time (ms) : 14945.8728
Total Bytes Received : 5045
Body Length : 4884
Is Compressed : No

```
HTTP/1.1 500 Internal Server Error
Server: Kestrel
Content-Type: text/plain; charset=utf-8
Transfer-Encoding: chunked
DHTTP/1.1 500 Internal Server Error

Server: Kestrel
Content-Type: text/plain; charset=utf-8
Transfer-Encoding: chunked
Date: Thu, 17 Apr 2025 10:08:31 GMT

System.Data.SqlClient.SqlException (0x80131904): A network-related or inst
…
```

Remedy

Analyze this issue and review the application code in order to handle unexpected errors; this should be a generic practice, which does not disclose further information upon an error. All errors should be handled server-side only.

CLASSIFICATION

CWE	550
WASC	13
NIST SP 800-53	SI-11
DISA STIG	V-6166
ISO27001	A.14.1.2
ISO27001 2022	A.8.15
ISO27001 2022	A.8.26
ISO27001 2022	A.8.27

3. Misconfigured Access-Control-Allow-Origin Header

LOW | 1

Invicti Standard detected a possibly misconfigured Access-Control-Allow-Origin header in resource's HTTP response.

Cross-origin resource sharing (CORS) is a mechanism that allows resources on a web page to be requested outside the domain through XMLHttpRequest.

Unless this HTTP header is present, such "cross-domain" requests are forbidden by web browsers, per the same-origin security policy.

Impact

This is generally not appropriate when using the same-origin security policy. The only case where this is appropriate when using the same-origin policy is when a page or API response is considered completely public content and it is intended to be accessible to everyone.

Vulnerabilities

3.1. http://100.26.242.68:5000/

Method	Parameter	Parameter Type	Value
GET	URI-BASED	FullUrl	

Access-Control-Allow-Origin

- *

Certainty

Request | Response

Request

```
GET / HTTP/1.1
Host: 100.26.242.68:5000
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: foo=bar
Origin: http://r87.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
```

Response

Response Time (ms) : 138.4631
Total Bytes Received : 131
Body Length : 0
Is Compressed : No

```
HTTP/1.1 404 Not Found
Server: Kestrel
Content-Length: 0
Access-Control-Allow-Origin: *
Date: Thu, 17 Apr 2025 10:04:51 GMT
```

Remedy

If this page is intended to be accessible to everyone, you don't need to take any action. Otherwise please follow the guidelines for different architectures below in order to set this header and permit outside domain.
Apache

- Add the following line inside either the <directory>, <location>, <files> or <virtualhost> sections of your server config (usually located in `httpd.conf`or `apache.conf`), or within a `.htaccess`file.

  ```
  Header set Access-Control-Allow-Origin "domain"
  ```

IIS6

1. Open Internet Information Service (IIS) Manager
2. Right click the site you want to enable CORS for and go to Properties
3. Change to the HTTP Headers tab
4. In the Custom HTTP headers section, click Add
5. Enter Access-Control-Allow-Origin as the header name
6. Enter `domain`as the header value

IIS7

- Merge the following xml into the web.config file at the root of your application or site:

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
  <system.webserver>
    <httpprotocol>
      <customheaders>
        <add name="Access-Control-Allow-Origin" value="domain" />
      </customheaders>
    </httpprotocol>
  </system.webserver>
</configuration>
```

ASP.NET

- If you don't have access to configure IIS, you can still add the header through ASP.NET by adding the following line to your source pages:

```
Response.AppendHeader("Access-Control-Allow-Origin", "domain");
```

External References

- Cross-Origin Resource Sharing
- HTTP access control (CORS)
- Using CORS

CLASSIFICATION

PCI DSS v3.2	6.5.8
PCI DSS v4.0	6.2.4
OWASP 2013	A5
OWASP 2017	A6
CWE	16
WASC	15
ASVS 4.0	14.5.3 , 14.5.2
NIST SP 800-53	CM-6
DISA STIG	V-6141
OWASP API Top Ten 2019	API7
ISO27001	A.14.1.2
ISO27001 2022	A.5.14
ISO27001 2022	A.5.15
OWASP Top Ten 2021	A05
OWASP API Top 10 2023	API8

4. Missing X-Content-Type-Options Header

LOW | 1

Invicti Standard detected a missing X-Content-Type-Options header which means that this website could be at risk of a MIME-sniffing attacks.

Impact

MIME type sniffing is a standard functionality in browsers to find an appropriate way to render data where the HTTP headers sent by the server are either inconclusive or missing.

This allows web browsers such as Google Chrome to perform MIME-Sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the intended content type.

The problem arises once a website allows users to upload content which is then published on the web server. If an attacker can carry out XSS (Cross-site Scripting) attack by manipulating the content in a way to be accepted by the web application and rendered as HTML by the browser, it is possible to inject code in e.g. an image file and make the victim execute it by viewing the image.

Vulnerabilities

4.1. http://100.26.242.68:5000/swagger/swagger-ui.css

Certainty

Request | Response

Request

```
GET /swagger/swagger-ui.css HTTP/1.1
Host: 100.26.242.68:5000
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: http://100.26.242.68:5000/swagger/index.html
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
```

Response

Response Time (ms) : 587.0623
Total Bytes Received : 143846
Body Length : 143632
Is Compressed : No

```
HTTP/1.1 200 OK
Server: Kestrel
Content-Length: 143632
Last-Modified: Sat, 16 Oct 2021 12:54:30 GMT
Accept-Ranges: bytes
Content-Type: text/css
Date: Thu, 17 Apr 2025 10:04:41 GMT
ETag: "1d7c28cf576f610"

.swagger-ui{color:#3b4151;
/*! normalize.css v7.0.0 | MIT License | github.com/necolas/normalize.css */font-family:sans-
serif}.swagger-ui html{-ms-text-size-adjust:100%;-webkit-text-size-adjust:100%;line-
height:1.15}.swagger-ui body{margin:0}.swagger-ui article,.swagger-ui aside,.swagger-ui
footer,.swagger-ui header,.swagger-ui nav,.swagger-ui section{display:block}.swagger-ui h1{font-
size:2em;margin:.67em 0}.swagger-ui figcaption,.swagger-ui figure,.swagger-ui
main{display:block}.swagger-ui figure{margin:1em 40px}.swagger-ui hr{box-sizing:content-
box;height:0;overflow:visible}.swagger-ui pre{font-family:monospace,monospace;font-size:1em}.swagger-ui
a{-webkit-text-decoration-skip:objects;background-color:transparent}.swagger-ui abbr[title]{border-
bottom:none;text-decoration:underline;-webkit-text-decoration:underline dotted;text-
decoration:underline dotted}.swagger-ui b,.swagger-ui strong{font-weight:inherit;font-
weight:bolder}.swagger-ui code,.swagger-ui kbd,.swagger-ui samp{font-family:monospace,monospace;font-
size:1em}.swagger-ui dfn{font-style:italic}.swagger-ui mark{background-color:#ff0;color:#000}.swagger-
ui small{font-size:80%}.swagger-ui sub,.swagger-ui sup{font-size:75%;line-
height:0;position:relative;vertical-align:baseline}.swagger-ui sub{bottom:-.25em}.swagger-ui
sup{top:-.5em}.swagger-ui audio,.swagger-ui video{display:inline-block}.swagger-ui
audio:not([controls]){display:none;height:0}.swagger-ui img{border-style:none}.swagger-ui
svg:not(:root){overflow:hidden}.swagger-ui button,.swagger-ui input,.swagger-ui optgroup,.swagger-ui
select,.swagger-ui textarea{font-family:sans-serif;font-size:100%;line-height:1.15;margin:0}.swagger-ui
button,.swagger-ui input{overflow:visible}.swagger-ui button,.swagger-ui select{text-
transform:none}.swagger-
…
```

Remedy

Add the X-Content-Type-Options header with a value of "nosniff" to inform the browser to trust what the site has sent is the appropriate content-type, and to not attempt "sniffing" the real content-type.

```
X-Content-Type-Options: nosniff
```

External References

- X-Content-Type-Options HTTP Header

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
CWE	16
WASC	15
ASVS 4.0	14.4.1
NIST SP 800-53	CM-6
DISA STIG	V-16786
OWASP API Top Ten 2019	API7
ISO27001	A.14.1.2
ISO27001 2022	A.8.27
OWASP Top Ten 2021	A05
OWASP API Top 10 2023	API8

5. Version Disclosure (SwaggerUI)

LOW | 1

Invicti Standard identified a version disclosure (SwaggerUI) in the target web server's HTTP response.

This information can help an attacker gain a greater understanding of the systems in use and potentially develop further attacks targeted at the specific version of SwaggerUI.

Impact

An attacker might use the disclosed information to harvest specific security vulnerabilities for the version identified.

Vulnerabilities

5.1. http://100.26.242.68:5000/swagger/swagger-ui-bundle.js

Identified Version

- 3.52.1

Certainty

Request | Response

Request

```
GET /swagger/swagger-ui-bundle.js HTTP/1.1
Host: 100.26.242.68:5000
Accept: */*
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: http://100.26.242.68:5000/swagger/index.html
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
```

Response

Response Time (ms) : 817.2019
Total Bytes Received : 1093118
Body Length : 1092889
Is Compressed : No

```
HTTP/1.1 200 OK
Server: Kestrel
Content-Length: 1092889
Last-Modified: Sat, 16 Oct 2021 12:54:30 GMT
Accept-Ranges: bytes
Content-Type: application/javascript
Date: Thu, 17 Apr 2025 10:04:47 GMT
ETag: "1
…
t,ne.default,ee.default,te.default,oe.default,e,t,se.default,n,ue.default,le.default,fe.default,he.defa
ult,de.default,ae.default]},jr=n(322);function Tr(){return[kr,jr.default]}var Ir=n(343);var
Pr=!0,Nr="gfdef4ea",Mr="3.52.1",Rr="Fri, 10 Sep 2021 12:03:52 GMT";function Dr(e){var
t;H.a.versions=H.a.versions||{},H.a.versions.swaggerUi=
{version:Mr,gitRevision:Nr,gitDirty:Pr,buildTimestamp:Rr};var n={dom_id:null,domNode:null
…
```

Remedy

Configure your web server to prevent information leakage.

CLASSIFICATION

OWASP 2013	A5
OWASP 2017	A6
CWE	205
CAPEC	170
WASC	13
HIPAA	164.306(a) , 164.308(a)
ASVS 4.0	14.3.3
NIST SP 800-53	AC-22
DISA STIG	V-16814
OWASP API Top Ten 2019	API7
ISO27001	A.18.1.3
ISO27001 2022	A.8.27
OWASP Top Ten 2021	A05
OWASP API Top 10 2023	API8

6. Content Security Policy (CSP) Not Implemented

BEST PRACTICE | 1 | CONFIRMED | 1

CSP is an added layer of security that helps to mitigate mainly Cross-site Scripting attacks.

CSP can be enabled instructing the browser with a Content-Security-Policy directive in a response header;

```
Content-Security-Policy: script-src 'self';
```

or in a meta tag;

```
<meta http-equiv="Content-Security-Policy" content="script-src 'self';">
```

In the above example, you can restrict script loading only to the same domain. It will also restrict inline script executions both in the element attributes and the event handlers. There are various directives which you can use by declaring CSP:

- **script-src:**Restricts the script loading resources to the ones you declared. By default, it disables inline script executions unless you permit to the evaluation functions and inline scripts by the unsafe-eval and unsafe-inline keywords.
- **base-uri:**The base element is used to resolve a relative URL to an absolute one. By using this CSP directive, you can define all possible URLs which could be assigned to the base-href attribute of the document.
- **frame-ancestors**: It is very similar to X-Frame-Options HTTP header. It defines the URLs by which the page can be loaded in an iframe.
- **frame-src / child-src**: frame-src is the deprecated version of child-src. Both define the sources that can be loaded by iframe on the page. (Please note that frame-src was brought back in CSP 3)
- **object-src**: Defines the resources that can be loaded by embedding such as Flash files, Java Applets.
- **img-src**: As its name implies, it defines the resources where the images can be loaded from.
- **connect-src**: Defines the whitelisted targets for XMLHttpRequest and WebSocket objects.
- **default-src**: It is a fallback for the directives that mostly end with -src suffix. When the directives below are not defined, the value set to default-src will be used instead:
    - child-src
    - connect-src
    - font-src
    - img-src
    - manifest-src
    - media-src
    - object-src
    - script-src
    - style-src

When setting the CSP directives, you can also use some CSP keywords:

- **none**: Denies loading resources from anywhere.
- **self** : Points to the document's URL (domain + port).
- **unsafe-inline**: Permits running inline scripts.
- **unsafe-eval**: Permits execution of evaluation functions such as eval().

In addition to CSP keywords, you can also use wildcard or only a scheme when defining whitelist URLs for the points. Wildcard can be used for subdomain and port portions of the URLs:

```
Content-Security-Policy: script-src https://*.example.com;
Content-Security-Policy: script-src https://example.com:*;
Content-Security-Policy: script-src https:;
```

It is also possible to set a CSP in Report-Only mode instead of forcing it immediately in the migration period. Thus you can see the violations of the CSP policy in the current state of your web site while migrating to CSP:

```
Content-Security-Policy-Report-Only: script-src 'self'; report-uri: https://example.com;
```

Impact

There is no direct impact of not implementing CSP on your website. However, if your website is vulnerable to a Cross-site Scripting attack CSP can prevent successful exploitation of that vulnerability. By not implementing CSP you'll be missing out on this extra layer of security.

Vulnerabilities

6.1. http://100.26.242.68:5000/swagger/oauth2-redirect.html

CONFIRMED

Request | Response

Request

```
GET /swagger/oauth2-redirect.html HTTP/1.1
Host: 100.26.242.68:5000
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: http://100.26.242.68:5000/swagger/index.html
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
```

Response

Response Time (ms) : 142.518
Total Bytes Received : 2808
Body Length : 2595
Is Compressed : No

```
HTTP/1.1 200 OK
Server: Kestrel
Content-Length: 2595
Last-Modified: Sat, 16 Oct 2021 12:54:30 GMT
Accept-Ranges: bytes
Content-Type: text/html
Date: Thu, 17 Apr 2025 10:04:41 GMT
ETag: "1d7c28cf574cd23"

<!doctype html>
<html lang="en-US">
<head>
<title>Swagger UI: OAuth2 Redirect</title>
</head>
<body>
<script>
'use strict';
function run () {
var oauth2 = window.opener.swaggerUIRedirectOauth2;
var sentState = oauth2.state;
var redirectUrl = oauth2.redirectUrl;
var isValid, qp, arr;

if (/code|token|error/.test(window.location.hash)) {
qp = window.location.hash.substring(1);
} else {
qp = location.search.substring(1);
}

arr = qp.split("&");
arr.forEach(function (v,i,_arr) { _arr[i] = '"' + v.replace('=', '":"') + '"';});
qp = qp ? JSON.parse('{' + arr.join() + '}',
function (key, value) {
return key === "" ? value : decodeURIComponent(value);
}
) : {};

isValid = qp.state === sentState;

if ((
oauth2.auth.schema.get("flow") === "accessCode" ||
oauth2.auth.schema.get("flow") === "authorizationCode" ||
oauth2.auth.schema.get("flow") === "authorization_code"
) && !oauth2.auth.code) {
```

```
if (!isValid) {
oauth2.errCb({
authId: oauth2.auth.name,
source: "auth",
level: "warning",
message: "Authorization may be unsafe, passed state was changed in server Passed state wasn't returned
from auth server"
});
}

if (qp.code) {
delete oauth2.state;
oauth2.auth.code = qp.code;
oauth2.callback({auth: oauth2.auth, redirectUrl: redirectUrl});
} else {
let oauthErrorMsg;
if (qp.error) {
oauthErrorM
…
```

Actions to Take

- Enable CSP on your website by sending the `Content-Security-Policy`in HTTP response headers that instruct the browser to apply the policies you specified.
- Apply the whitelist and policies as strict as possible.
- Rescan your application to see if Invicti Standard identifies any weaknesses in your policies.

Remedy

Enable CSP on your website by sending the `Content-Security-Policy`in HTTP response headers that instruct the browser to apply the policies you specified.

External References

- An Introduction to Content Security Policy
- Content Security Policy (CSP) HTTP Header
- Content Security Policy (CSP)

CLASSIFICATION

CWE	16
WASC	15
ASVS 4.0	14.4.3
NIST SP 800-53	CM-6
DISA STIG	V-16786
ISO27001	A.14.2.5
ISO27001 2022	A.8.27

7. Referrer-Policy Not Implemented

BEST PRACTICE | 1

Invicti Standard detected that no Referrer-Policy header implemented.

Referrer-Policy is a security header designed to prevent cross-domain Referer leakage.

Impact

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.

The lack of Referrer-Policy header might affect privacy of the users and site's itself

Vulnerabilities

7.1. http://100.26.242.68:5000/swagger/oauth2-redirect.html

Certainty

Request | Response

Request

```
GET /swagger/oauth2-redirect.html HTTP/1.1
Host: 100.26.242.68:5000
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: http://100.26.242.68:5000/swagger/index.html
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
```

Response

Response Time (ms) : 142.518
Total Bytes Received : 2808
Body Length : 2595
Is Compressed : No

```
HTTP/1.1 200 OK
Server: Kestrel
Content-Length: 2595
Last-Modified: Sat, 16 Oct 2021 12:54:30 GMT
Accept-Ranges: bytes
Content-Type: text/html
Date: Thu, 17 Apr 2025 10:04:41 GMT
ETag: "1d7c28cf574cd23"

<!doctype html>
<html lang="en-US">
<head>
<title>Swagger UI: OAuth2 Redirect</title>
</head>
<body>
<script>
'use strict';
function run () {
var oauth2 = window.opener.swaggerUIRedirectOauth2;
var sentState = oauth2.state;
var redirectUrl = oauth2.redirectUrl;
var isValid, qp, arr;

if (/code|token|error/.test(window.location.hash)) {
qp = window.location.hash.substring(1);
} else {
qp = location.search.substring(1);
}

arr = qp.split("&");
arr.forEach(function (v,i,_arr) { _arr[i] = '"' + v.replace('=', '":"') + '"';});
qp = qp ? JSON.parse('{' + arr.join() + '}',
function (key, value) {
return key === "" ? value : decodeURIComponent(value);
}
) : {};

isValid = qp.state === sentState;

if ((
oauth2.auth.schema.get("flow") === "accessCode" ||
oauth2.auth.schema.get("flow") === "authorizationCode" ||
oauth2.auth.schema.get("flow") === "authorization_code"
) && !oauth2.auth.code) {
```

```
if (!isValid) {
oauth2.errCb({
authId: oauth2.auth.name,
source: "auth",
level: "warning",
message: "Authorization may be unsafe, passed state was changed in server Passed state wasn't returned
from auth server"
});
}

if (qp.code) {
delete oauth2.state;
oauth2.auth.code = qp.code;
oauth2.callback({auth: oauth2.auth, redirectUrl: redirectUrl});
} else {
let oauthErrorMsg;
if (qp.error) {
oauthErrorM
…
```

Actions to Take

In a response header:

```
Referrer-Policy: no-referrer | same-origin | origin | strict-origin | no-origin-when-downgrading
```

In a META tag

```
<meta name="Referrer-Policy" value="no-referrer | same-origin"/>
```

In an element attribute

```
<a href="http://crosssite.example.com" rel="noreferrer"></a>
```

or

```
<a href="http://crosssite.example.com" referrerpolicy="no-referrer | same-origin | origin | strict-
origin | no-origin-when-downgrading"></a>
```

Remedy

Please implement a Referrer-Policy by using the Referrer-Policy response header or by declaring it in the meta tags. It's also possible to control referrer information over an HTML-element by using the rel attribute.

External References

- Referrer Policy
- Referrer Policy - MDN
- Referrer Policy HTTP Header
- A New Security Header: Referrer Policy
- Can I Use Referrer-Policy

CLASSIFICATION

OWASP 2013	A6
OWASP 2017	A3
CWE	200
ASVS 4.0	14.4.6
NIST SP 800-53	AC-22
DISA STIG	V-16814
ISO27001	A.14.2.5
ISO27001 2022	A.8.27

8. Kestrel Detected

INFORMATION | 1

Invicti Standard identified that the target web site is using Kestrel. Kestrel is a cross-platform web server for ASP.NET Core.

Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

Vulnerabilities

8.1. http://100.26.242.68:5000/

Certainty

Request | Response

Request

```
GET / HTTP/1.1
Host: 100.26.242.68:5000
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
```

Response

Response Time (ms) : 373.7107
Total Bytes Received : 99
Body Length : 0
Is Compressed : No

```
HTTP/1.1 404 Not Found
Server: Kestrel

Content-Length: 0
Date: Thu, 17 Apr 2025 10:04:25 GMT
```

External References

- Kestrel web server implementation in ASP.NET Core

CLASSIFICATION

OWASP 2017	A6
CWE	205
WASC	13
ASVS 4.0	14.3.3
NIST SP 800-53	AC-22
DISA STIG	V-16814
OWASP API Top Ten 2019	API7
OWASP Proactive Controls	C7
ISO27001	A.14.2.5
OWASP Top Ten 2021	A05

9. Out-of-date Version (Swagger UI)

INFORMATION | 1

Invicti Standard identified that the target web site is using Swagger UI and detected that it is out of date.

Impact

Since this is an old version of the software, it may be vulnerable to attacks.

Vulnerabilities

9.1. http://100.26.242.68:5000/swagger/swagger-ui-bundle.js

Identified Version

- 3.52.1

Latest Version

- 5.21.0

Vulnerability Database

- Result is based on 04/15/2025 17:00:00 vulnerability database content.

Certainty

Request | Response

Request

```
GET /swagger/swagger-ui-bundle.js HTTP/1.1
Host: 100.26.242.68:5000
Accept: */*
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: http://100.26.242.68:5000/swagger/index.html
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
```

Response

Response Time (ms) : 817.2019
Total Bytes Received : 1093118
Body Length : 1092889
Is Compressed : No

```
HTTP/1.1 200 OK
Server: Kestrel
Content-Length: 1092889
Last-Modified: Sat, 16 Oct 2021 12:54:30 GMT
Accept-Ranges: bytes
Content-Type: application/javascript
Date: Thu, 17 Apr 2025 10:04:47 GMT
ETag: "1
…
t,ne.default,ee.default,te.default,oe.default,e,t,se.default,n,ue.default,le.default,fe.default,he.defa
ult,de.default,ae.default]},jr=n(322);function Tr(){return[kr,jr.default]}var Ir=n(343);var
Pr=!0,Nr="gfdef4ea",Mr="3.52.1",Rr="Fri, 10 Sep 2021 12:03:52 GMT";function Dr(e){var
t;H.a.versions=H.a.versions||{},H.a.versions.swaggerUi=
{version:Mr,gitRevision:Nr,gitDirty:Pr,buildTimestamp:Rr};var n={dom_id:null,domNode:null
…
```

Remedy

Please upgrade your installation of Swagger UI to the latest stable version.

Remedy References

- Downloading Swagger UI

CLASSIFICATION

PCI DSS v3.2	6.2
PCI DSS v4.0	6.3.3
OWASP 2013	A9
OWASP 2017	A9
CWE	1035 , 937
CAPEC	310
HIPAA	164.308(a)(1)(i)
ASVS 4.0	1.14.3
NIST SP 800-53	CM-6
DISA STIG	V-16836
OWASP Proactive Controls	C1
ISO27001	A.14.1.2
OWASP Top Ten 2021	A06
OWASP API Top 10 2023	API8

10. SwaggerUI Identified

INFORMATION | 1

Invicti Standard identified the usage of SwaggerUI in the target web server's HTTP response.

This issue is reported as extra information only.

Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

Vulnerabilities

10.1. http://100.26.242.68:5000/swagger/swagger-ui-bundle.js

Certainty

Request | Response

Request

```
GET /swagger/swagger-ui-bundle.js HTTP/1.1
Host: 100.26.242.68:5000
Accept: */*
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: http://100.26.242.68:5000/swagger/index.html
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/131.0.6778.86 Safari/537.36
```

Response

Response Time (ms) : 817.2019
Total Bytes Received : 1093118
Body Length : 1092889
Is Compressed : No

```
HTTP/1.1 200 OK
Server: Kestrel
Content-Length: 1092889
Last-Modified: Sat, 16 Oct 2021 12:54:30 GMT
Accept-Ranges: bytes
Content-Type: application/javascript
Date: Thu, 17 Apr 2025 10:04:47 GMT
ETag: "1
…
t,ne.default,ee.default,te.default,oe.default,e,t,se.default,n,ue.default,le.default,fe.default,he.defa
ult,de.default,ae.default]},jr=n(322);function Tr(){return[kr,jr.default]}var Ir=n(343);var
Pr=!0,Nr="gfdef4ea",Mr="3.52.1",Rr="Fri, 10 Sep 2021 12:03:52 GMT";function Dr(e){var
t;H.a.versions=H.a.versions||{},H.a.versions.swaggerUi=
{version:Mr,gitRevision:Nr,gitDirty:Pr,buildTimestamp:Rr};var n={dom_id:null,domNode:null
…
```

CLASSIFICATION

OWASP 2017	A6
CWE	205
WASC	13
ASVS 4.0	14.3.3
NIST SP 800-53	AC-22
DISA STIG	V-16814
OWASP API Top Ten 2019	API7
OWASP Proactive Controls	C7
ISO27001	A.14.2.5
OWASP Top Ten 2021	A05
OWASP API Top 10 2023	API8

Show Scan Detail

Enabled Security Checks	:	ActiveMQ OpenWire RCE, Apache Struts S2-045 RCE, Apache Struts S2-046 RCE, Arbitrary Files (IAST), Code Evaluation, Code Evaluation (IAST), Code Evaluation (Out of Band),

Command Injection,
Command Injection (Blind),
Command Injection (IAST),
Configuration Analyzer (IAST),
Content Security Policy,
Content-Type Sniffing,
Cookie,
Cross-Origin Resource Sharing (CORS),
Cross-site Scripting,
Cross-site Scripting (Blind),
Custom Script Checks (Active),
Custom Script Checks (Passive),
Custom Script Checks (Per Directory),
Custom Script Checks (Singular),
Drupal Remote Code Execution,
Expression Language Injection,
File Upload,
GraphQL Library Detection,
Header Analyzer,
Heartbleed,
HSTS,
HTML Content,
HTTP Header Injection,
HTTP Header Injection (IAST),
HTTP Methods,
HTTP Status,
HTTP.sys (CVE-2015-1635),
IFrame Security,
Insecure JSONP Endpoint,
Insecure Reflected Content,
JavaScript Libraries,
JSON Web Token,
LDAP Injection (IAST),
Local File Inclusion,
Local File Inclusion (IAST),
Log4j Code Evaluation (Out of Band),
Login Page Identifier,
Mail Header Injection (IAST),
Malware Analyzer,
Mixed Content,
MongoDB Injection (Blind),
MongoDB Injection (Boolean),
MongoDB Injection (Error Based),
MongoDB Injection (IAST),
MongoDB Injection (Operator),
Open Redirection,
Oracle EBS RCE,
Oracle WebLogic Remote Code Execution,
Referrer Policy,
Reflected File Download,
RegreSSHion Attack,
Remote File Inclusion,
Remote File Inclusion (Out of Band),

		Reverse Proxy Detection, **RoR Code Execution,** **Security Assertion Markup Language (SAML),** **Sensitive Data,** **Server-Side Request Forgery (DNS),** **Server-Side Request Forgery (Pattern Based),** **Server-Side Template Injection,** **Server-Side Template Injection (IAST),** **Signatures,** **Software Composition Analysis (SCA),** **Spring4Shell Remote Code Execution,** **SQL Injection (Blind),** **SQL Injection (Boolean),** **SQL Injection (Error Based),** **SQL Injection (IAST),** **SQL Injection (Out of Band),** **SSL,** **Static Resources (All Paths),** **Static Resources (Only Root Path),** **TorchServe Management,** **Unicode Transformation (Best-Fit Mapping),** **VmWare Aria RCE,** **WAF Identifier,** **Web App Fingerprint,** **Web Cache Deception,** **WebDAV,** **Windows Short Filename,** **Wordpress Plugin Detection,** **Wordpress Theme Detection,** **XML External Entity,** **XML External Entity (Out of Band),** **XML External Entity Injection (IAST),** **XPath Injection (IAST)**
URL Rewrite Mode	:	**Heuristic**
Detected URL Rewrite Rule(s)	:	**None**
Excluded URL Patterns	:	**gtm\.js** **WebResource\.axd** **ScriptResource\.axd**
Authentication	:	**None**
Authentication Profile	:	**None**

Scheduled	**:**	**No**
Additional Website(s)	**:**	**None**

This report created with 24.12.0.46123-release_is-25.1.0-6845a2f
https://www.invicti.com