Highmark

Provider Directory Search DAST 2019

DAST - Standard

Friday, March 29, 2019

This work was performed under contract to:

Highmark

120 5th Avenue Place Pittsburgh PA

For more information contact:

Suraksha M N
Security Consultant

Manoj Pandey
Senior Security Consultant

Larry Cox
Managing Consultant

Proprietary Statement

The information in this documentation is subject to change without notice and should not be construed as a commitment by Synopsys, Inc. Synopsys, Inc. makes no representations or warranties, express or implied, with respect to the documentation and shall not be liable for any damages, including any indirect, incidental, consequential damages (such as loss of profit, loss of use of assets, loss of business opportunity, loss of data or claims for or on behalf of user’s customers), that may be suffered by the user.

Synopsys, Inc.
185 Berry Street, Suite 6500
San Francisco, CA 94107 USA

U.S. Sales: 800.873.8193
International Sales: +1 415.321.5237
Email: sig-info@synopsys.com
www.synopsys.com/software.

version 2019.03

Table of Contents

Document Revision History

Version	Modification	Date	Author
1.0	Security Report	03/29/2019	Suraksha M N
1.1	Security Report Review	03/29/2019	Manoj Pandey

Contacts

Contact	Title	Organization	Phone #	Email Address
Larry Cox	Managing Consultant	Synopsys, Inc.	+1.703.404.9293	lcox@synopsys.com
Manoj Pandey	Senior Security Consultant	Synopsys, Inc.	+91.80.674.26897	manojp@synopsys.com
Suraksha M N	Security Consultant	Synopsys, Inc.	+91.80.674.27053	suraksha@synopsys.com

Executive Summary

Highmark has engaged Synopsys, Inc. to perform a DAST - Standard assessment on Provider Directory Search DAST 2019. Provider Directory Search application provides facility to search physician according to the requirement. The purpose of this assessment was to assess the overall security posture of the application from a black-box perspective. This includes determining the application's ability to resist common attack patterns and identifying vulnerable areas in the internal or external interfaces that may be exploited by a malicious user.

During the assessment, Synopsys identified 4 findings characterized as follows:

- 2 *Low priority* findings
- 2 *Minimal priority* findings

1 Introduction

Highmark engaged Synopsys, Inc. to perform a DAST - Standard assessment on Provider Directory Search DAST 2019 beginning on March 27, 2019 and ending on March 29, 2019. Provider Directory Search application provides facility to search physician according to the requirement. Provider Directory Search application provides facility to search physician according to the requirement.

1.1 Objective

The objective of this assessment was to assess the overall security posture of the application from a black-box perspective. This includes determining the application's ability to resist common attack patterns and identifying vulnerable areas in the internal or external interfaces that may be exploited by a malicious user.

1.2 Scope

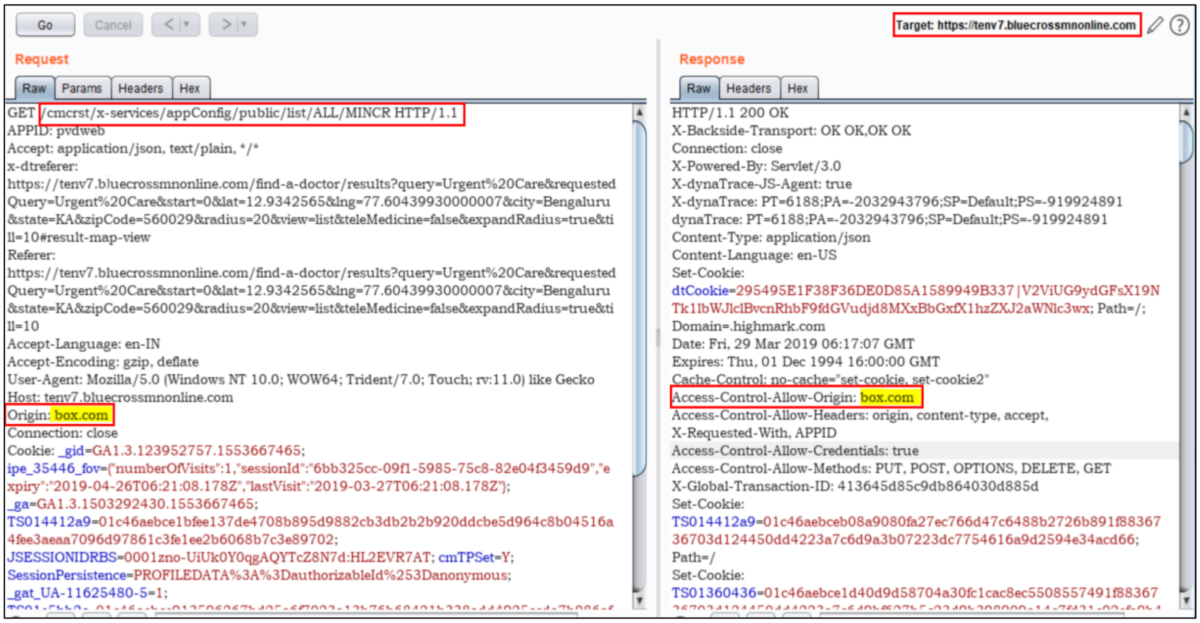
The scope of this assessment was limited to components and interfaces specific to Provider Directory Search DAST 2019. The following URL was considered in-scope:

- https://tenv7.bluecrossmnonline.com/find-a-doctor/landing

1.3 Assessment Notes

- During assessment, Synopsys observed that the application is configured with an overly permissive Cross-Origin Resource Sharing (CORS) policy that exposes application resources to untrusted origins. As below mentioned, URL is not in scope, Synopsys did not reported it as a finding.

  https://tenv7.bluecrossmnonline.com/cmcrst/x-services/appConfig/public/list/ALL/MINCR



Target: https://tenv7.bluecrossmnonline.com

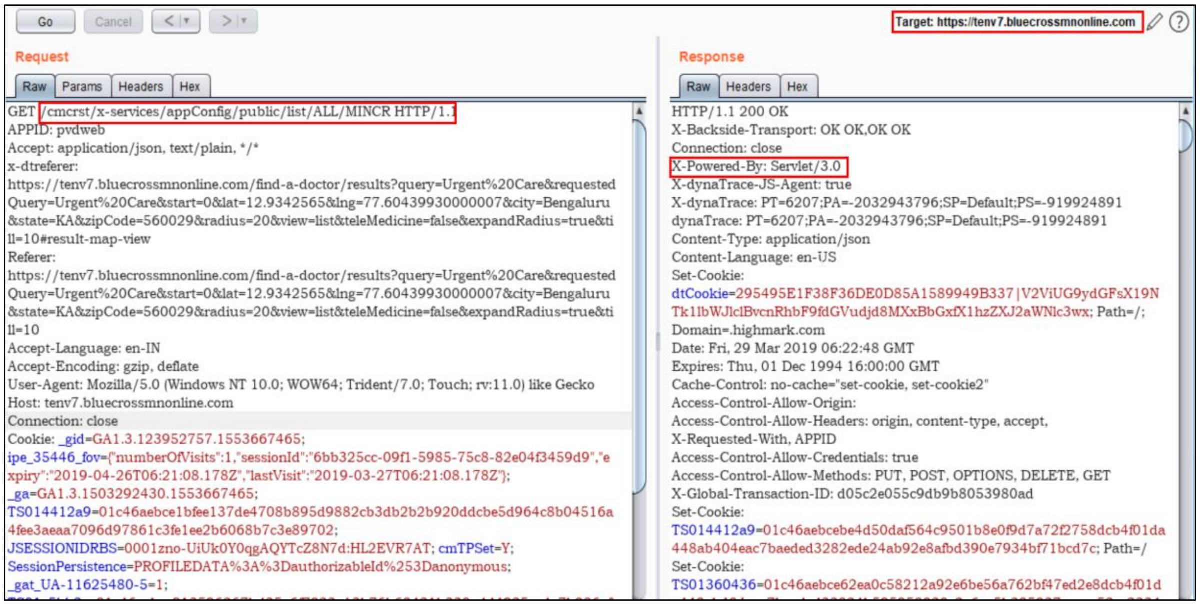
```
GET /cmcrst/x-services/appConfig/public/list/ALL/MINCR HTTP/1.1
APPID: pvdweb
Accept: application/json, text/plain, */*
x-dtreferer:
https://tenv7.bluecrossmnonline.com/find-a-doctor/results?query=Urgent%20Care&requested
Query=Urgent%20Care&start=0&lat=12.9342565&lng=77.60439930000007&city=Bengaluru
&state=KA&zipCode=560029&radius=20&view=list&teleMedicine=false&expandRadius=true&ti
ll=10#result-map-view
Referer:
https://tenv7.bluecrossmnonline.com/find-a-doctor/results?query=Urgent%20Care&requested
Query=Urgent%20Care&start=0&lat=12.9342565&lng=77.60439930000007&city=Bengaluru
&state=KA&zipCode=560029&radius=20&view=list&teleMedicine=false&expandRadius=true&ti
ll=10
Accept-Language: en-IN
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; Touch; rv:11.0) like Gecko
Host: tenv7.bluecrossmnonline.com
Origin: box.com
Connection: close
Cookie: _gid=GA1.3.123952757.1553667465;
ipe_35446_fov={"numberOfVisits":1,"sessionId":"6bb325cc-09f1-5985-75c8-82e04f3459d9","e
xpiry":"2019-04-26T06:21:08.178Z","lastVisit":"2019-03-27T06:21:08.178Z"};
_ga=GA1.3.1503292430.1553667465;
TS014412a9=01c46aebce1bfee137de4708b895d9882cb3db2b2b920ddcbe5d964c8b04516a
4fee3aeaa7096d97861c3fe1ee2b6068b7c3e89702;
JSESSIONIDRBS=0001zno-UiUk0Y0qgAQYTcZ8N7d:HL2EVR7AT; cmTPSet=Y;
SessionPersistence=PROFILEDATA%3A%3DauthorizableId%253Danonymous;
_gat_UA-11625480-5=1;
```

```
HTTP/1.1 200 OK
X-Backside-Transport: OK OK,OK OK
Connection: close
X-Powered-By: Servlet/3.0
X-dynaTrace-JS-Agent: true
X-dynaTrace: PT=6188;PA=-2032943796;SP=Default;PS=-919924891
dynaTrace: PT=6188;PA=-2032943796;SP=Default;PS=-919924891
Content-Type: application/json
Content-Language: en-US
Set-Cookie:
dtCookie=295495E1F38F36DE0D85A1589949B337|V2ViUG9ydGFsX19N
Tk1lbWJlclBvcnRhbF9fdGVudjd8MXxBbGxfX1hzZXJ2aWNlc3wx; Path=/;
Domain=.highmark.com
Date: Fri, 29 Mar 2019 06:17:07 GMT
Expires: Thu, 01 Dec 1994 16:00:00 GMT
Cache-Control: no-cache="set-cookie, set-cookie2"
Access-Control-Allow-Origin: box.com
Access-Control-Allow-Headers: origin, content-type, accept,
X-Requested-With, APPID
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: PUT, POST, OPTIONS, DELETE, GET
X-Global-Transaction-ID: 413645d85c9db864030d885d
Set-Cookie:
TS014412a9=01c46aebceb08a9080fa27ec766d47c6488b2726b891f88367
36703d124450dd4223a7c6d9a3b07223dc7754616a9d2594e34acd66;
Path=/
Set-Cookie:
TS01360436=01c46aebce1d40d9d58704a30fc1cac8ec5508557491f88367
```

Figure 1: Burp Repeater showing that the "Access-Control-Allow-Origin" header is set to “box.com” as shown in the response.

- During assessment, Synopsys observed that the application uses "X-Powered-By" header which contains sensitive server information in the response. As below mentioned URL is not in scope, Synopsys did not reported it as a finding.

  https://tenv7.bluecrossmnonline.com/cmcrst/x-services/appConfig/public/list/ALL/MINCR



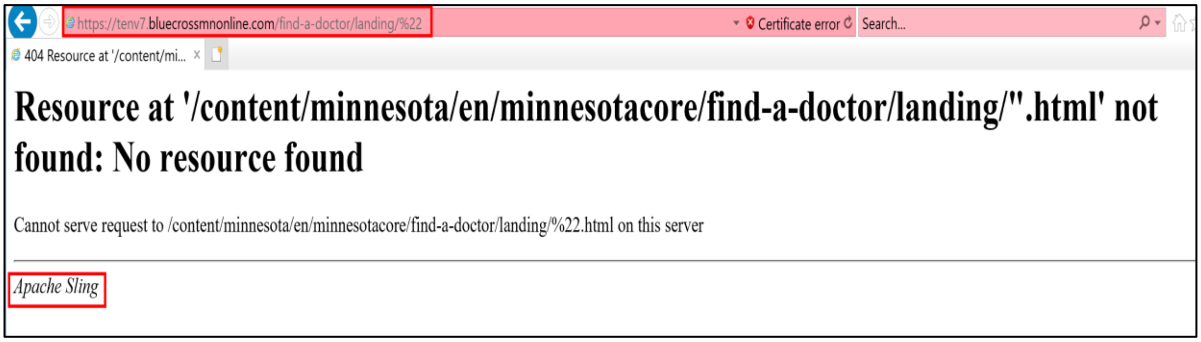
Target: https://tenv7.bluecrossmnonline.com

```
GET /cmcrst/x-services/appConfig/public/list/ALL/MINCR HTTP/1.1
APPID: pvdweb
Accept: application/json, text/plain, */*
x-dtreferer:
https://tenv7.bluecrossmnonline.com/find-a-doctor/results?query=Urgent%20Care&requested
Query=Urgent%20Care&start=0&lat=12.9342565&lng=77.60439930000007&city=Bengaluru
&state=KA&zipCode=560029&radius=20&view=list&teleMedicine=false&expandRadius=true&ti
ll=10#result-map-view
Referer:
https://tenv7.bluecrossmnonline.com/find-a-doctor/results?query=Urgent%20Care&requested
Query=Urgent%20Care&start=0&lat=12.9342565&lng=77.60439930000007&city=Bengaluru
&state=KA&zipCode=560029&radius=20&view=list&teleMedicine=false&expandRadius=true&ti
ll=10
Accept-Language: en-IN
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; Touch; rv:11.0) like Gecko
Host: tenv7.bluecrossmnonline.com
Connection: close
Cookie: _gid=GA1.3.123952757.1553667465;
ipe_35446_fov={"numberOfVisits":1,"sessionId":"6bb325cc-09f1-5985-75c8-82e04f3459d9","e
xpiry":"2019-04-26T06:21:08.178Z","lastVisit":"2019-03-27T06:21:08.178Z"};
_ga=GA1.3.1503292430.1553667465;
TS014412a9=01c46aebce1bfee137de4708b895d9882cb3db2b2b920ddcbe5d964c8b04516a
4fee3aeaa7096d97861c3fe1ee2b6068b7c3e89702;
JSESSIONIDRBS=0001zno-UiUk0Y0qgAQYTcZ8N7d:HL2EVR7AT; cmTPSet=Y;
SessionPersistence=PROFILEDATA%3A%3DauthorizableId%253Danonymous;
_gat_UA-11625480-5=1;
```

```
HTTP/1.1 200 OK
X-Backside-Transport: OK OK,OK OK
Connection: close
X-Powered-By: Servlet/3.0
X-dynaTrace-JS-Agent: true
X-dynaTrace: PT=6207;PA=-2032943796;SP=Default;PS=-919924891
dynaTrace: PT=6207;PA=-2032943796;SP=Default;PS=-919924891
Content-Type: application/json
Content-Language: en-US
Set-Cookie:
dtCookie=295495E1F38F36DE0D85A1589949B337|V2ViUG9ydGFsX19N
Tk1lbWJlclBvcnRhbF9fdGVudjd8MXxBbGxfX1hzZXJ2aWNlc3wx; Path=/;
Domain=.highmark.com
Date: Fri, 29 Mar 2019 06:22:48 GMT
Expires: Thu, 01 Dec 1994 16:00:00 GMT
Cache-Control: no-cache="set-cookie, set-cookie2"
Access-Control-Allow-Origin:
Access-Control-Allow-Headers: origin, content-type, accept,
X-Requested-With, APPID
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: PUT, POST, OPTIONS, DELETE, GET
X-Global-Transaction-ID: d05c2e055c9db9b8053980ad
Set-Cookie:
TS014412a9=01c46aebcebe4d50daf564c9501b8e0f9d7a72f2758dcb4f01da
448ab404eac7baeded3282ede24ab92e8afbd390e7934bf71bcd7c; Path=/
Set-Cookie:
TS01360436=01c46aebce62ea0c58212a92e6be56a762bf47ed2e8dcb4f01d
```

Figure 2: The application response in Burp History showing that the “X-Powered-By” headers discloses information about the technology used.

- During assessment, Synopsys observed that the application reveals server name in the error message.



https://tenv7.bluecrossmnonline.com/find-a-doctor/landing/%22
Certificate error
Search...
404 Resource at '/content/mi...

Resource at '/content/minnesota/en/minnesotacore/find-a-doctor/landing/".html' not found: No resource found

Cannot serve request to /content/minnesota/en/minnesotacore/find-a-doctor/landing/%22.html on this server

Apache Sling

Figure 3: Application showing server name in the browser.

2 Methodology

2.1 Assessment Type

Synopsys was engaged to perform a time-boxed manual security assessment against the target application. This assessment involved a deep automated scan using automated scanning tools to discover common vulnerabilities, as well as manual testing. Manual testing includes validation of all issue types covered under the automated scan as well as checks for problems not typically found by automated scanners such as authentication, authorization and business logic flaws.

2.2 Risk Assessment Methodology

The severity assigned to each vulnerability was calculated using the NIST 800-30 Revision 1 standard. This standard determines the risk posed by application based on the likelihood an attacker exploits the vulnerability and the impact that it would have on the business.

Likelihood

The difficulty of exploiting the described security vulnerability includes required skill level and the amount of access necessary to visit the element susceptible to the vulnerability. The difficulty is rated with the following values:

- **Critical:** An attacker is almost certain to initiate the threat event.
- **High**: An untrained user could exploit the vulnerability or the vulnerability is very obvious and easily accessible.
- **Medium**: The vulnerability requires some hacking knowledge or access is restricted in some way.
- **Low**: Exploiting the vulnerability requires application access, significant time, resource or a specialized skillset.
- **Minimal**: Adversaries are highly unlikely to leverage the vulnerability.

Impact

The impact the vulnerability would have on the organization if it were successfully exploited is rated with the following values:

- **Critical:** The issue causes multiple severe or catastrophic effects on organizational operations, organizational assets or other organizations.
- **High**: Exploitation produces severe degradation in mission capability to the point that the organization is not able to perform primary functions or results in damage to organizational assets.
- **Medium**: Threat events trigger degradation in mission capability to an extent the application is able to perform its primary functions, but their effectiveness is reduced and there may be damage to organizational assets.
- **Low**: Successful exploitation has limited degradation in mission capability; the organization is able to perform its primary functions, but their effectiveness is noticeably reduced and may result in minor damage to organizational assets.

- **Minimal**: The threat could have a negligible adverse effect on organizational operations or organizational assets.

Severity

The vulnerability severity is determined using the likelihood and impact weights in the following table:

		Impact				
		Minimal	***Low***	***Medium***	***High***	***Critical***
Likelihood	***Critical***	**Minimal**	**Low**	**Medium**	**High**	**Critical**
	High	**Minimal**	**Low**	**Medium**	**High**	**Critical**
	Medium	**Minimal**	**Low**	**Medium**	**Medium**	**High**
	Low	**Minimal**	**Low**	**Low**	**Low**	**Medium**
	Minimal	**Minimal**	**Minimal**	**Minimal**	**Low**	**Low**

3 Findings

3.1 Summary of Findings

Finding	CWE ID	Likelihood	Impact	Severity	Status
HTTP Strict Transport Security (HSTS) Not Implemented	319	Low	Low	Low	Open
TLSv1.0 Supported	327	Minimal	High	Low	Open
Missing Content-Security-Policy Header	693	Minimal	Minimal	Minimal	Open
Missing X-XSS-Protection Header	933	Minimal	Minimal	Minimal	Open

3.2 Finding Details

3.2.1 Low Priority Findings

3.2.1.1 HTTP Strict Transport Security (HSTS) Not Implemented

Description:

The server does not implement the "HTTP Strict-Transport Security" (HSTS) web security policy mechanism. When HSTS is enabled, the web application sends a special response header, "Strict-Transport-Security" to the client with a duration of time specified. Once a supported browser receives this header, that browser will only make requests to the application over HTTPS for the duration of time specified in the header. Any links to resources over HTTP will be rewritten to HTTPS before the request is made.

Applications that do not utilize the "HTTP Strict-Transport Security" policy are more susceptible to man-in-the-middle attacks via SSL stripping, which occurs when an attacker transparently downgrades a victim's communication with the server from HTTPS to HTTP. Once this is accomplished, the attacker will gain the ability to view and potentially modify the victim's traffic, exposing sensitive information and gaining access to unauthorized functionality.

Instances:

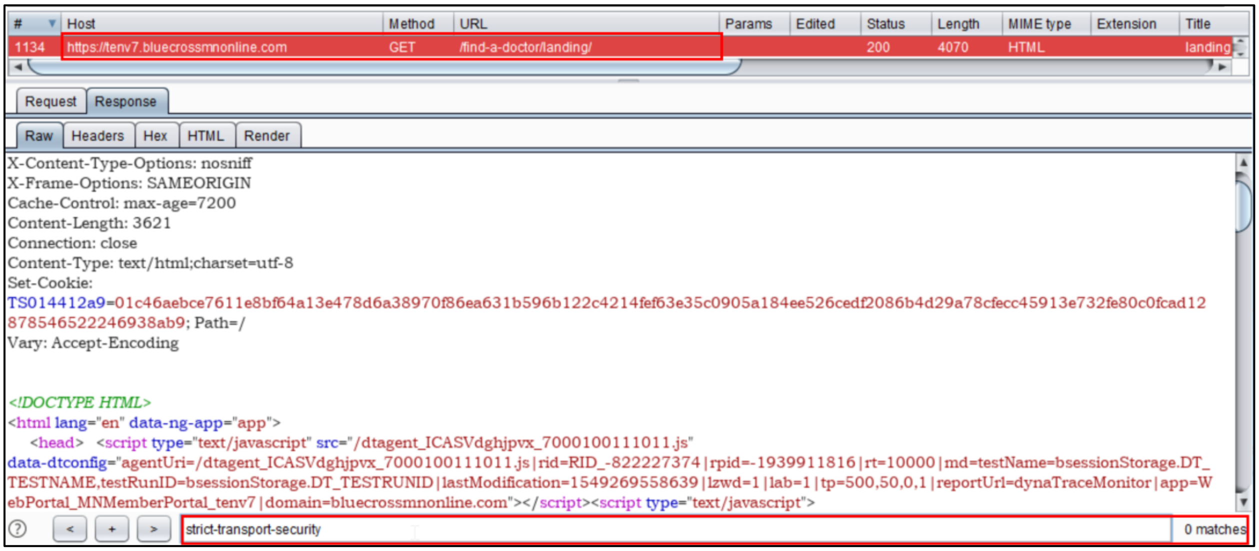
1. https://tenv7.bluecrossmnonline.com/find-a-doctor/landing/
   a. Header: Strict-Transport Security
2. https://tenv7.bluecrossmnonline.com/find-a-doctor/headerProvLinkItem.appTemplate.html/directives/headerProvLinkItem/headerProvLinkItem
   a. Header: Strict-Transport Security
3. https://tenv7.bluecrossmnonline.com/find-a-doctor/landing.appTemplate.html/pages/home/landing/landing
   a. Header: Strict-Transport Security

Note: This finding is systemic throughout the application.

Steps To Reproduce:

1. Configure your browser to use a proxy tool such as Burp Suite.
2. Navigate to any of the URL mentioned in the "Instances" section.
3. Observe the application's response in Burp HTTP History.
4. Note that the Strict-Transport-Security" header is missing from the response indicating HTTP Strict Transport Security is not implemented.

Evidence:



#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title
1134	https://tenv7.bluecrossmnonline.com	GET	/find-a-doctor/landing/			200	4070	HTML		landing

```
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Cache-Control: max-age=7200
Content-Length: 3621
Connection: close
Content-Type: text/html;charset=utf-8
Set-Cookie:
TS014412a9=01c46aebce7611e8bf64a13e478d6a38970f86ea631b596b122c4214fef63e35c0905a184ee526cedf2086b4d29a78cfecc45913e732fe80c0fcad12
878546522246938ab9; Path=/
Vary: Accept-Encoding


<!DOCTYPE HTML>
<html lang="en" data-ng-app="app">
    <head>   <script type="text/javascript" src="/dtagent_ICASVdghjpvx_7000100111011.js"
data-dtconfig="agentUri=/dtagent_ICASVdghjpvx_7000100111011.js|rid=RID_-822227374|rpid=-1939911816|rt=10000|md=testName=bsessionStorage.DT_
TESTNAME,testRunID=bsessionStorage.DT_TESTRUNID|lastModification=1549269558639|lzwd=1|lab=1|tp=500,50,0,1|reportUrl=dynaTraceMonitor|app=W
ebPortal_MNMemberPortal_tenv7|domain=bluecrossmnonline.com"></script><script type="text/javascript">
```

Figure 4: Burp showing the Strict-Transport-Security header is missing in the HTTP response.

Likelihood: Low

Impact: Low

Severity: Low

CWE ID: 319

Remediation:

The application server should send the "Strict-Transport-Security" HTTP header in each response indicating that future requests to the domain use only HTTPS. The following is a basic example of the HSTS HTTP header, setting a max-age of one year:

```
Strict-Transport-Security: max-age=31536000
```

Subdomains should also be configured in this manner, by including the "includeSubDomains" flag:

```
Strict-Transport-Security: max-age=31536000; includeSubDomains;
```

3.2.1.2 TLSv1.0 Supported

Description:

The server-side SSL/TLS endpoint is configured to allow connections using TLS protocol version 1.0 ("TLSv1.0"), which contains known weaknesses. The TLS protocol provides secure transport between endpoints over a network, with the intended effect of offering data integrity and confidentiality. Certain configurations of TLS version 1.0 are vulnerable to known man-in-the-middle ("MitM") attacks, including the BEAST and POODLE attacks. In addition, multiple standards organizations including NIST and PCI have declared that TLSv1.0 no longer provides sufficient data protection.

Weaknesses in TLSv1.0 connections may allow an attacker to decrypt traffic passed between a victim's client and the server. Any sensitive information passed over this connection may be exposed, such as credentials, account data, personally identifiable information (PII), financial records, etc. Exposure of session identifiers may allow an attacker to hijack a victim's session and impersonate the victim in the application. An attacker who decrypts traffic in transit between a victim's client and the server may also modify data in transit, allowing them to modify requests the victim has initiated, and any data being returned to the client.

Instances:

1. https://tenv7.bluecrossmnonline.com/find-a-doctor/landing

Steps To Reproduce:

1. Download the SSL scanning tool SSLyze from the following URL:

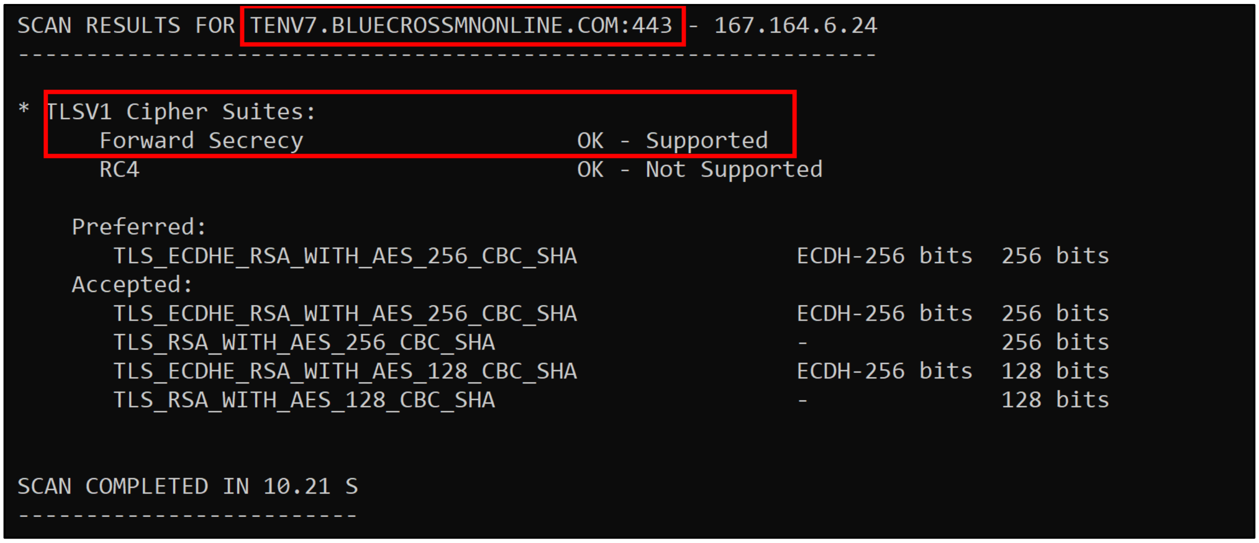
   https://github.com/nabla-c0d3/sslyze

2. Using SSLyze run the following command:

   ```
   sslyze.exe --tlsv1 --hide_rejected_ciphers tenv7.bluecrossmnonline.com
   ```

3. Observe the output in SSLyze.

Evidence:



```
SCAN RESULTS FOR TENV7.BLUECROSSMNONLINE.COM:443 - 167.164.6.24
---------------------------------------------------------------

* TLSV1 Cipher Suites:
      Forward Secrecy                   OK - Supported
      RC4                               OK - Not Supported

    Preferred:
       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA                ECDH-256 bits  256 bits
    Accepted:
       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA                ECDH-256 bits  256 bits
       TLS_RSA_WITH_AES_256_CBC_SHA                      -              256 bits
       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA                ECDH-256 bits  128 bits
       TLS_RSA_WITH_AES_128_CBC_SHA                      -              128 bits


SCAN COMPLETED IN 10.21 S
-------------------------
```

Figure 5: SSLyze output showing that the application domain supports TLSv1.0.

Likelihood: Minimal

Impact: High

Severity: Low

CWE ID: 327

Remediation:

The server-side TLS endpoint's configuration should be updated to allow only TLSv1.2 connections with cipher suites that use:

- Ephemeral Diffie-Hellman for key exchange (optionally, allow RSA for key exchange if necessary, for supporting some clients)
- Block ciphers with key lengths of at least 128 bits (AES-128 and AES-256)
- Block ciphers in GCM mode (optionally, allow block ciphers in CBC mode if necessary, for supporting some clients)
- The SHA2 family of hash functions (SHA256, SHA384, SHA512) for block ciphers in CBC mode if necessary; optionally, allow SHA1 if necessary, for supporting some clients

Note that all modern browsers support TLSv1.2.

For further information on NIST policies surrounding TLS deprecation, please refer to the following link:
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf

3.2.2 Minimal Priority Findings

3.2.2.1 Missing Content-Security-Policy Header

Description:

The application server does not set the Content-Security-Policy (CSP) header in HTTP responses, and, therefore, the application is at a greater risk of having cross-site scripting or other modern application vulnerabilities. The CSP header sets a policy that instructs the browser to only fetch resources, such as scripts, images, or objects, from the specified locations. A compliant browser will deny loading any resources from locations not listed in the policy.

CSP allows browsers to differentiate between trusted and untrusted content requested by the page. By default, it also prohibits inline script execution, as well as dynamic script evaluation. When implemented correctly, the CSP reduces an attacker's ability to inject malicious content and helps protect a web page from attacks like cross-site scripting (XSS), dynamic code execution, clickjacking, remote file inclusion (RFI), and others. The CSP adds an additional line of defense and reduces the overall security risk.

Instances:

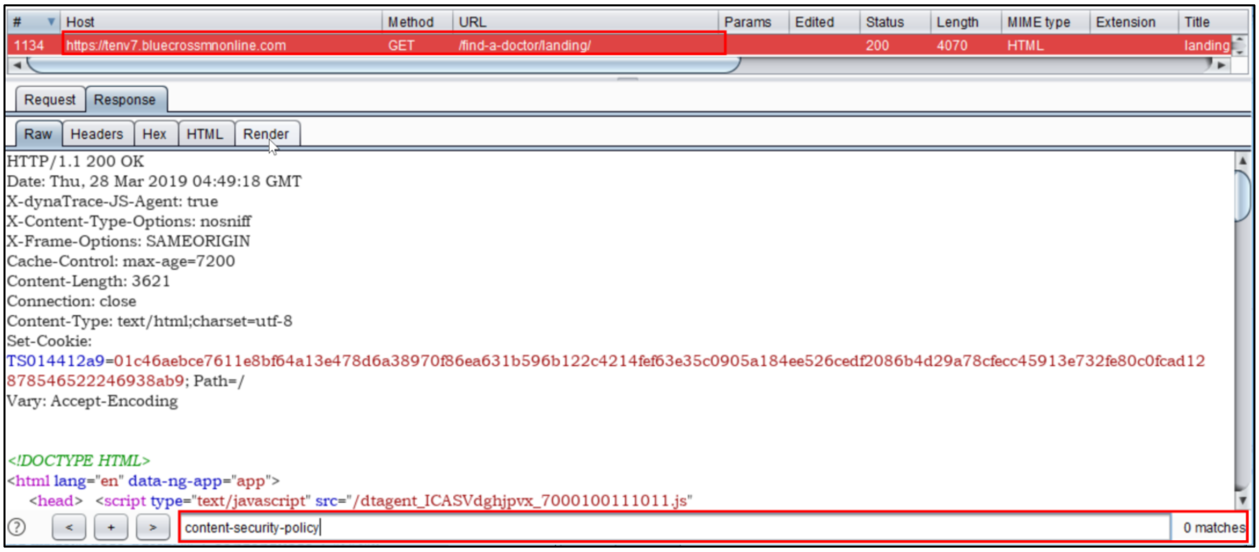
1. https://tenv7.bluecrossmnonline.com/find-a-doctor/landing/
   a. Header: Content-Security-Policy
2. https://tenv7.bluecrossmnonline.com/find-a-doctor/headerProvLinkItem.appTemplate.html/directives/headerProvLinkItem/headerProvLinkItem
   a. Header: Content-Security-Policy
3. https://tenv7.bluecrossmnonline.com/find-a-doctor/landing.appTemplate.html/pages/home/landing/landing
   a. Header: Content-Security-Policy

Note: This finding is systemic throughout the application.

Steps To Reproduce:

1. Configure your browser to use a proxy tool such as Burp Suite.
2. Navigate to any of the URL mentioned in the "Instances" section.
3. Observe the application's response in Burp HTTP History.
4. Note that the "Content-Security-policy" header is missing in the response.

Evidence:



#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title
1134	https://tenv7.bluecrossmnonline.com	GET	/find-a-doctor/landing/			200	4070	HTML		landing

```
HTTP/1.1 200 OK
Date: Thu, 28 Mar 2019 04:49:18 GMT
X-dynaTrace-JS-Agent: true
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Cache-Control: max-age=7200
Content-Length: 3621
Connection: close
Content-Type: text/html;charset=utf-8
Set-Cookie:
TS014412a9=01c46aebce7611e8bf64a13e478d6a38970f86ea631b596b122c4214fef63e35c0905a184ee526cedf2086b4d29a78cfecc45913e732fe80c0fcad12
878546522246938ab9; Path=/
Vary: Accept-Encoding


<!DOCTYPE HTML>
<html lang="en" data-ng-app="app">
   <head>   <script type="text/javascript" src="/dtagent_ICASVdghjpvx_7000100111011.js"
```

content-security-policy

0 matches

Figure 6: The application response in the Burp History showing that the “Content-Security-policy” header is missing in the response.

Likelihood: Minimal

Impact: Minimal

Severity: Minimal

CWE ID: 693

Remediation:

The application server must set the Content-Security-Policy (CSP) header in each HTTP response with the appropriate directives defined to provide the browser with granular control over the resources loaded by the application. Implementing a CSP should be considered a security best practice as part of a larger defense in depth strategy to reduce the risk of various attacks. CSP alone should not be relied on to prevent attacks such as cross-site scripting, dynamic code execution, clickjacking, remote file inclusion, or other injection attacks.

To implement a secure CSP, the application would need to use no inline <script> tags. This often means a rewrite of the whole client side application using one of the CSP-compliant JavaScript frameworks. Otherwise, CSP will block normal execution of the application. Note that setting the script-src directive to 'unsafe-inline' allows execution of any JavaScript injected by an attacker, as well as the execution of legitimate JavaScript.
Here is an example of a secure CSP.

```
Content-Security-Policy: default-src 'none'; img-src *.images.example.com; media-src
media-server.com;script-src apis.example.com; style-src 'self'; object-src 'none';
frame-ancestors 'self'; upgrade-insecure-requests;report-uri https://example.com/csp-
reports/
```

CSP has a lot of different directives and settings. Here are some best practices to create a strong security policy:

- Specify a default policy. It is recommended to set it to 'none'.
- Specify a whitelist of sources for script-src and object-src directives.
- Avoid setting default-src and script-src to 'unsafe-inline' or data:. The 'data:' URIs can be used to inject and execute JavaScript.
- Avoid setting default-src and script-src to 'unsafe-eval'. The 'unsafe-eval' policy allows the use of eval() and similar methods which can be abused for code injection.
- Avoid setting script-src or default-src to 'self' for hosts containing Angular applications, JSONP endpoints, or files uploaded from users, as attackers can manipulate such applications to execute attacker's code uploaded to the application's host.
- Avoid setting the object-src directive to *, as it allows loading of arbitrary plugins that can execute JavaScript.
- Only use third-party URIs that start with https:, as content loaded over HTTP can be modified by an attacker.
- Set the frame-ancestors directive to specify sources from where the current page can be framed or set it to 'none' to avoid clickjacking.

3.2.2.2 Missing X-XSS-Protection Header

Description:

The application server does not set the "X-XSS-Protection" header in HTTP responses. The X-XSS-Protection response header is a mechanism supported by some modern web browsers to provide an additional layer of defense against reflected cross-site scripting attacks. A missing X-XSS-Protection header increases the likelihood of a successful reflected cross-site scripting attack which can give the attacker full control over the HTML and JavaScript running in the victim's browser. Without the X-XSS-Protection header defined, an application has fewer defense layers to prevent reflected cross-site scripting attacks.

Instances:

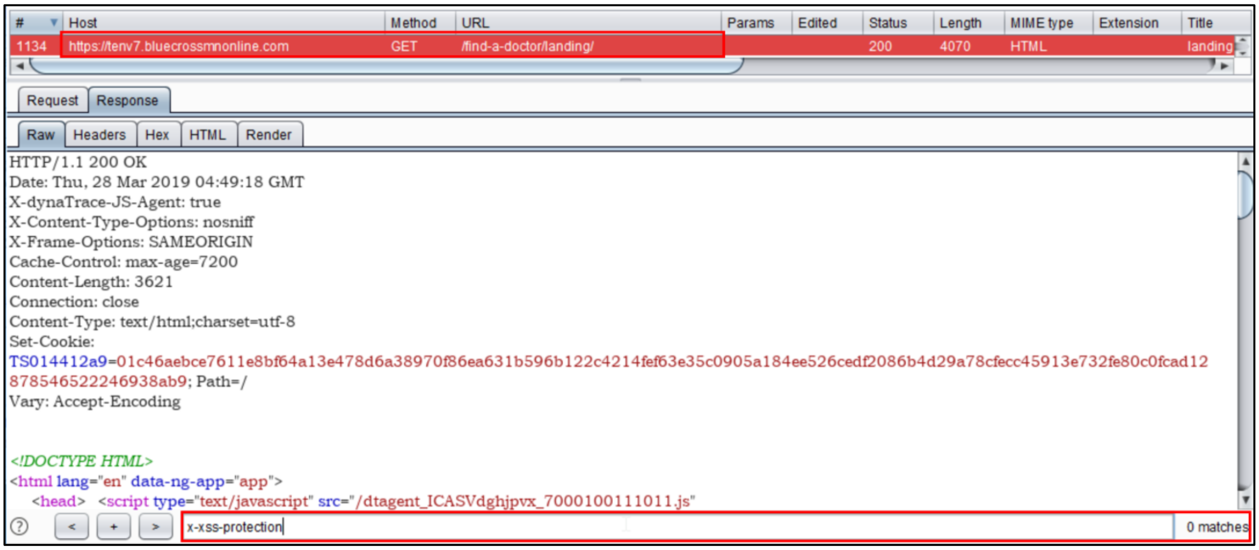
1. https://tenv7.bluecrossmnonline.com/find-a-doctor/landing/
    a. Header: X-XSS-Protection
2. https://tenv7.bluecrossmnonline.com/find-a-doctor/headerProvLinkItem.appTemplate.html/directives/headerProvLinkItem/headerProvLinkItem
    a. Header: X-XSS-Protection
3. https://tenv7.bluecrossmnonline.com/find-a-doctor/landing.appTemplate.html/pages/home/landing/landing
    a. Header: X-XSS-Protection

Note: This finding is systemic throughout the application.

Steps To Reproduce:

1. Configure your browser to use a proxy tool such as Burp Suite.
2. Navigate to any of the URL mentioned in the "Instances" section.
3. Observe the application's response in Burp HTTP History.
4. Note that the "X-XSS-Protection" header is missing in the response body.

Evidence:



#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title
1134	https://tenv7.bluecrossmnonline.com	GET	/find-a-doctor/landing/			200	4070	HTML		landing

```
HTTP/1.1 200 OK
Date: Thu, 28 Mar 2019 04:49:18 GMT
X-dynaTrace-JS-Agent: true
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Cache-Control: max-age=7200
Content-Length: 3621
Connection: close
Content-Type: text/html;charset=utf-8
Set-Cookie:
TS014412a9=01c46aebce7611e8bf64a13e478d6a38970f86ea631b596b122c4214fef63e35c0905a184ee526cedf2086b4d29a78cfecc45913e732fe80c0fcad12
878546522246938ab9; Path=/
Vary: Accept-Encoding


<!DOCTYPE HTML>
<html lang="en" data-ng-app="app">
   <head>  <script type="text/javascript" src="/dtagent_ICASVdghjpvx_7000100111011.js"
```

x-xss-protection
0 matches

Figure 7: The application response in the Burp History showing that the “X-XSS-Protection” header is missing in the response.

Likelihood: Minimal

Impact: Minimal

Severity: Minimal

CWE ID: 933

Remediation:

The application or the web server should set the X-XSS-Protection header to reduce the likelihood of successful reflected cross-site scripting attacks. The X-XSS-Protection should be set to the following:

```
X-XSS-Protection: 1; mode=block
```

Setting the X-XSS-Protection header to "1" enables the browser's built-in cross-site scripting auditor to analyze the response content for malicious scripts. If the browser detects unsafe or malicious content, the browser will sanitize the response before rendering. However, if the value "1" is followed by "mode=block", the browser will prevent the page from rendering in case a cross-site scripting attack is detected. Instead, the browser will display an error message to the user.

Note: Using the X-XSS-Protection header should be considered a security best practice as part of a defense-in-depth strategy to harden the application. The X-XSS-Protection header alone does not guarantee protection against reflected cross-site scripting attacks. The header is not supported by all modern browsers and can also be bypassed using targeted attacks against specific browser versions. To prevent reflected cross-site scripting attacks, output encoding should be implemented in the application whenever data is inserted into a web page.