Executive Summary

After a data breach associated with the launch of a new online application, the City of Kelowna is conducting a cybersecurity audit using the guidelines of the PCI-DSS v3.2 and the assistance of external auditors. This preliminary report discusses the initial findings of the audit and includes some recommendations for best practice changes. These recommendations include organizational policy changes, network changes to increase segmentation and application server policy changes.

Inventory

Section 2 of the PCI-DSS requires a review of the physical and logical infrastructure associated with providing city services online to citizens and internally for the organization. The goal is to ensure all devices and their business functions are documented, and that the factory-default security settings have been updated in line with the security policies of the City of Kelowna.

PCI-DSS 2.4.a

ID	Name	Function	Type
1	Application server	Hosts City of Kelowna website	Hardware
2	Data server	Hosts backup of financial transactions for data warehouse	Hardware
3	Workstation PC	Data processing	Hardware
4	Point-of-sale terminal (tablet)	Data processing (financial)	Portable hardware
5	Workstation laptop	Data processing	Portable hardware
6	Android mobile phone	Cellular communication	Portable hardware
7	Apple mobile phone	Cellular communication	Portable hardware
8	Point-of-sale software	Cloud SAAS software for processing in-person transactions	Software
9	City website	Online payment system for fines	Software
10	External web browsers	Local software	Software
11	Modem	Internet communication	Static device
12	Router	Internet communication	Static device
13	Firewall	Internet segmentation	Static device
14	Wireless access point	Internet communication	Static device

15	Cash register	Cash float for in-person transactions	Static device
16	Wireless display screen	Display content during meetings	Static device

Recommendation #1: previous inventory was missing item 16, the wireless display in the meeting room. As a result, this item was not set to the correct network segment and had unnecessary access to the application and web servers (items 1 & 2). Item 16 should be reassigned to the same network segment as the mobile devices and laptops.

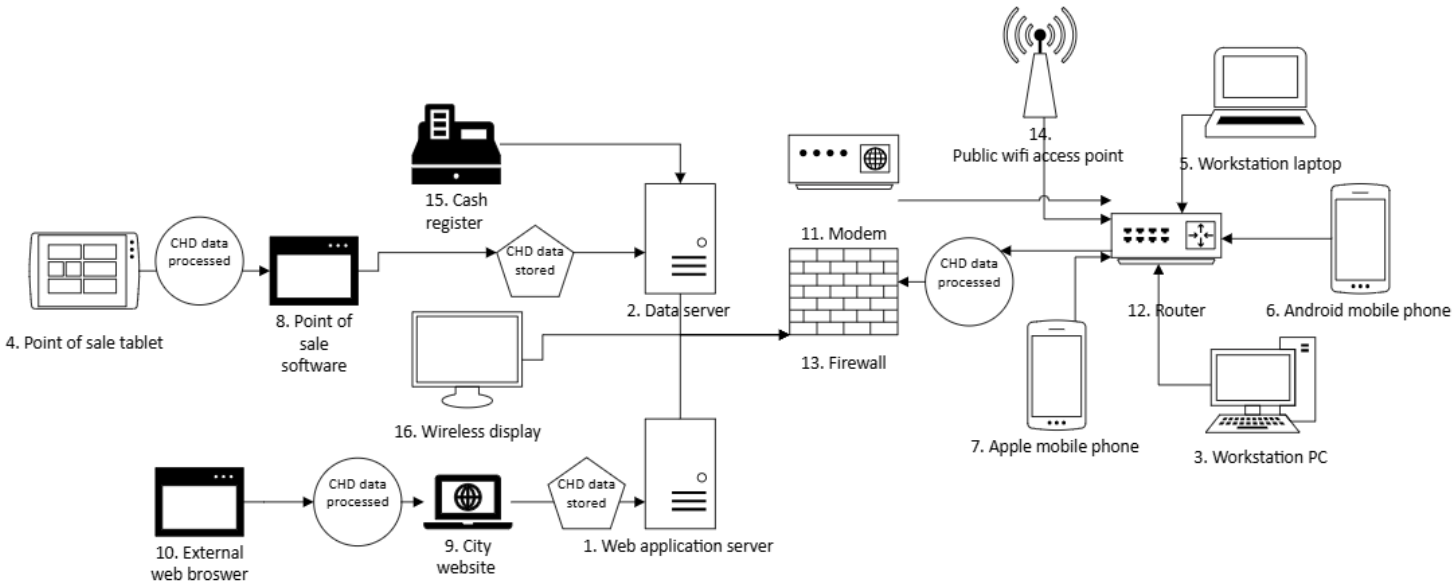
PCI-DSS 2.4.b

“I attest this list is current”. Louise Macdonald, Director Information Services

Recommendation #2: Designation of responsible job title for sign-off on inventory related to PCI-DSS compliance. During the creation of this report, an organizational policy problem was uncovered. No individual had been specified as responsible for maintaining an accurate inventory in the City of Kelowna cybersecurity policies. Previously, Frank Delongo had been responsible but since his retirement, this job task had not been reassigned.

PCI-DSS 1.1.2 and 1.1.3

Current network diagram with data flows



The City of Kelowna processes in-person and online credit card information. Credit card information and authentication information is stored on the web application server, and the City stores anonymized copies of financial transactions on their data server for reporting and audit

purposes. The security of both data flows must be considered separately. The city also uses both Apple and Android mobile devices and must ensure that security review takes the OS differences into account.

Recommendation #3: The current network topography does not achieve compliance with standard 1.1.4 which states: “Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone”. There is a firewall between the web application server and the host browser connections, but another firewall should be present between the public wi-fi access point that the City provides and the internal network. An intruder who physically visits city buildings could gain access to internal networks through this route.

Network scan

Compliance with PCI-DSS 11.2 dictates that organizations are responsible for conducting internal and external network vulnerability scans at least quarterly or after any significant change to a network component. All vulnerabilities discovered should be documented. All “high risk” vulnerabilities must be addressed and rescanned within 7 business days according to the City of Kelowna organizational policy. Once the scan has been completed, then compliance with PCI-DSS 1.1.6 requires the documentation, justification and approval for all open ports.

PCI-DSS-1.1.6 Evidence (External)

Service	Justification	Access Control
Domain	DNS services	Strong password
Http	Web hosting	Strong password Disabled by default
Https	Web hosting	Strong password Disabled by default
UPnp	Plug n play device	Normally disconnected

PCI-DSS-1.1.6 Evidence (External)

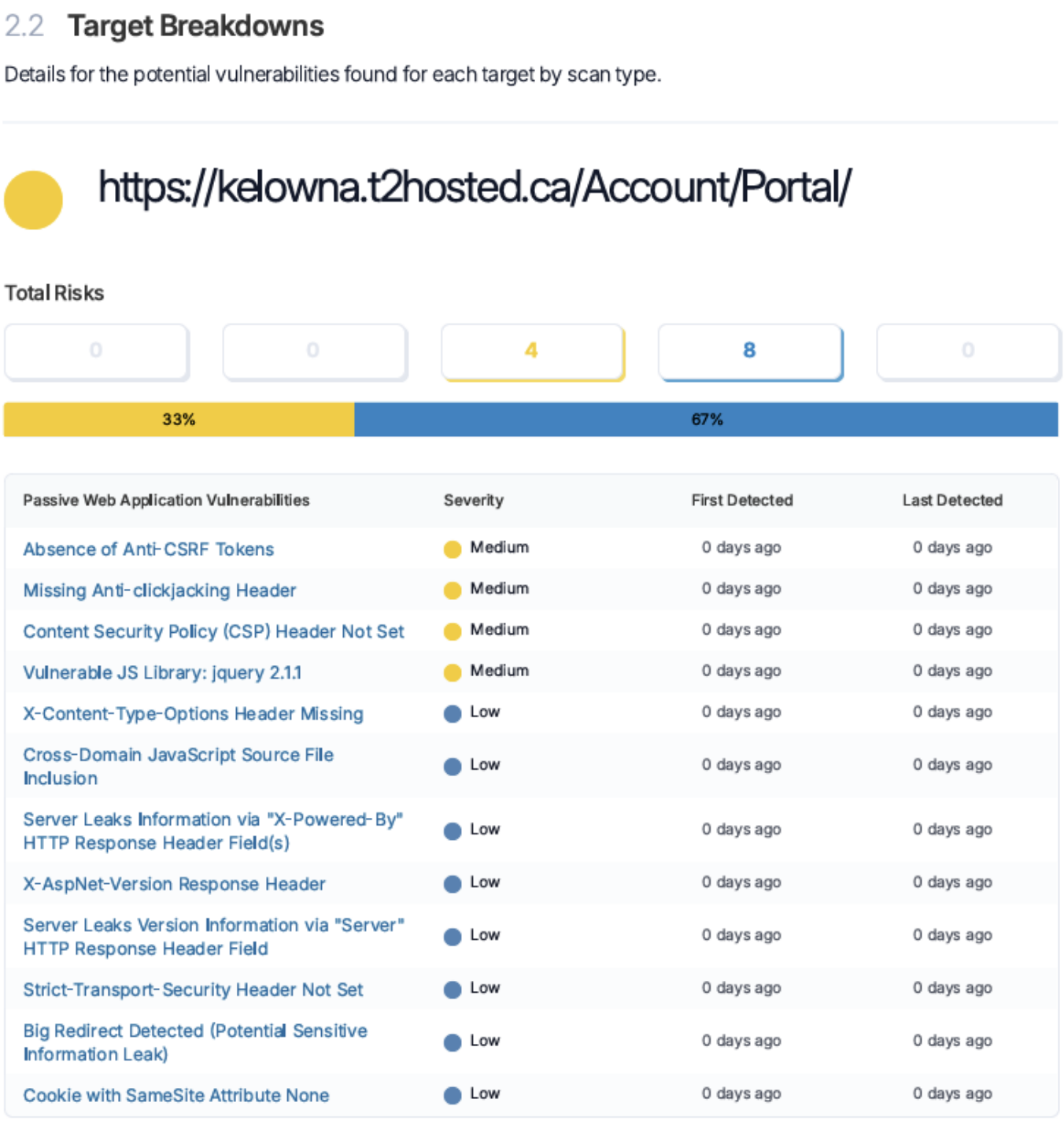
Device	Service	Justification	Access Control
10.0.0.76 – Laptop	5900 VNC Server	UI Remote control	Weak password

Web App Vulnerability Scan

The web application scan was completed using the free product by HostedScan security on March 30, 2025. The full report is available for members of the City’s Information Services team. Four medium priority vulnerabilities were identified, including two server-side vulnerabilities.

Updates to item 1 application server from the inventory will need to be performed to address the vulnerabilities.

PCI-DSS-6.6 Evidence



2.2 Target Breakdowns

Details for the potential vulnerabilities found for each target by scan type.

https://kelowna.t2hosted.ca/Account/Portal/

Total Risks

0	0	4	8	0

33% 67%

Passive Web Application Vulnerabilities	Severity	First Detected	Last Detected
Absence of Anti-CSRF Tokens	Medium	0 days ago	0 days ago
Missing Anti-clickjacking Header	Medium	0 days ago	0 days ago
Content Security Policy (CSP) Header Not Set	Medium	0 days ago	0 days ago
Vulnerable JS Library: jquery 2.1.1	Medium	0 days ago	0 days ago
X-Content-Type-Options Header Missing	Low	0 days ago	0 days ago
Cross-Domain JavaScript Source File Inclusion	Low	0 days ago	0 days ago
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	0 days ago	0 days ago
X-AspNet-Version Response Header	Low	0 days ago	0 days ago
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	0 days ago	0 days ago
Strict-Transport-Security Header Not Set	Low	0 days ago	0 days ago
Big Redirect Detected (Potential Sensitive Information Leak)	Low	0 days ago	0 days ago
Cookie with SameSite Attribute None	Low	0 days ago	0 days ago

PCI-DSS-6.1 Analysis

Vulnerability Name: Vulnerable JS Library: jquery 2.11

Vulnerability Impact Summary:

Out of date Javascript libraries is a common security issue for web applications. This kind of vulnerability leave the web application more open to attacks such as cross-site scripting attacks, man-in-the-middle attacks or data breaches.

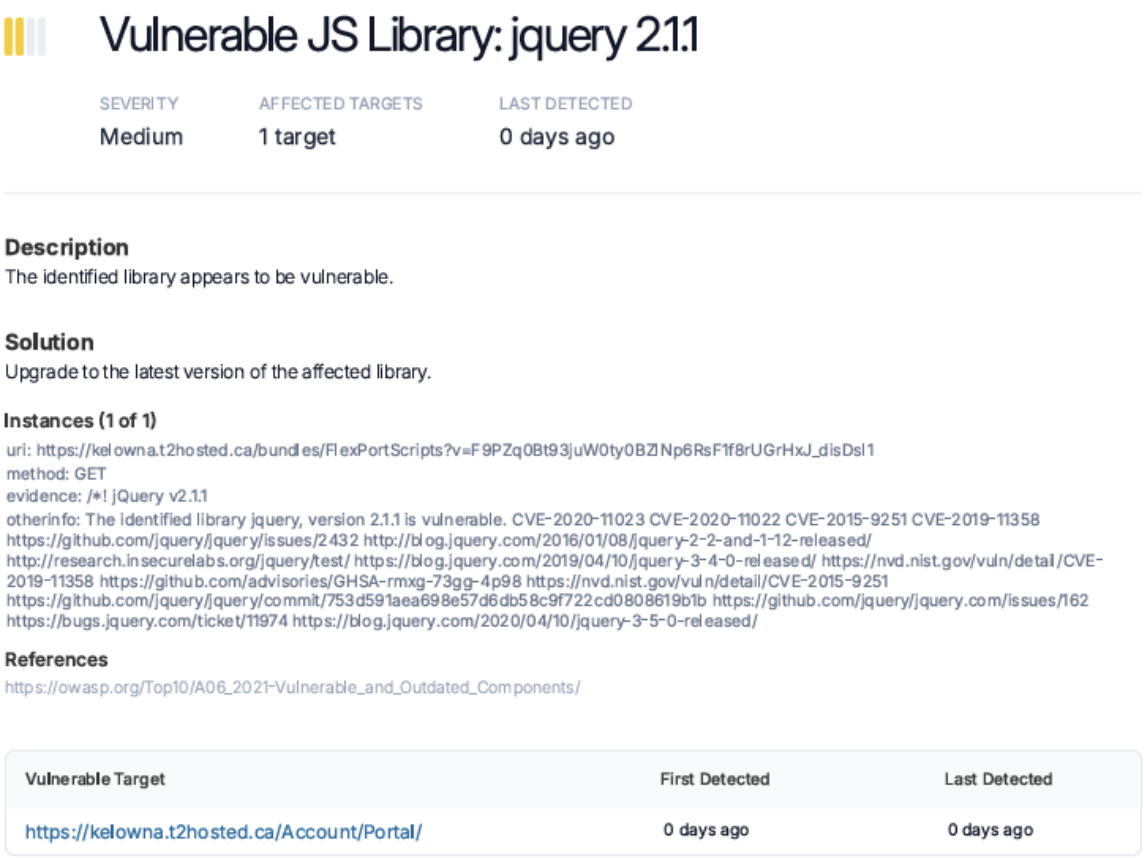
Evidence:

https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/

Controls:

Update to the latest version of the affected library within the web application

Screenshot:



Vulnerability Name: Content Security Policy (CSP) Header not set

Vulnerability Impact Summary:

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources

of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

Evidence:

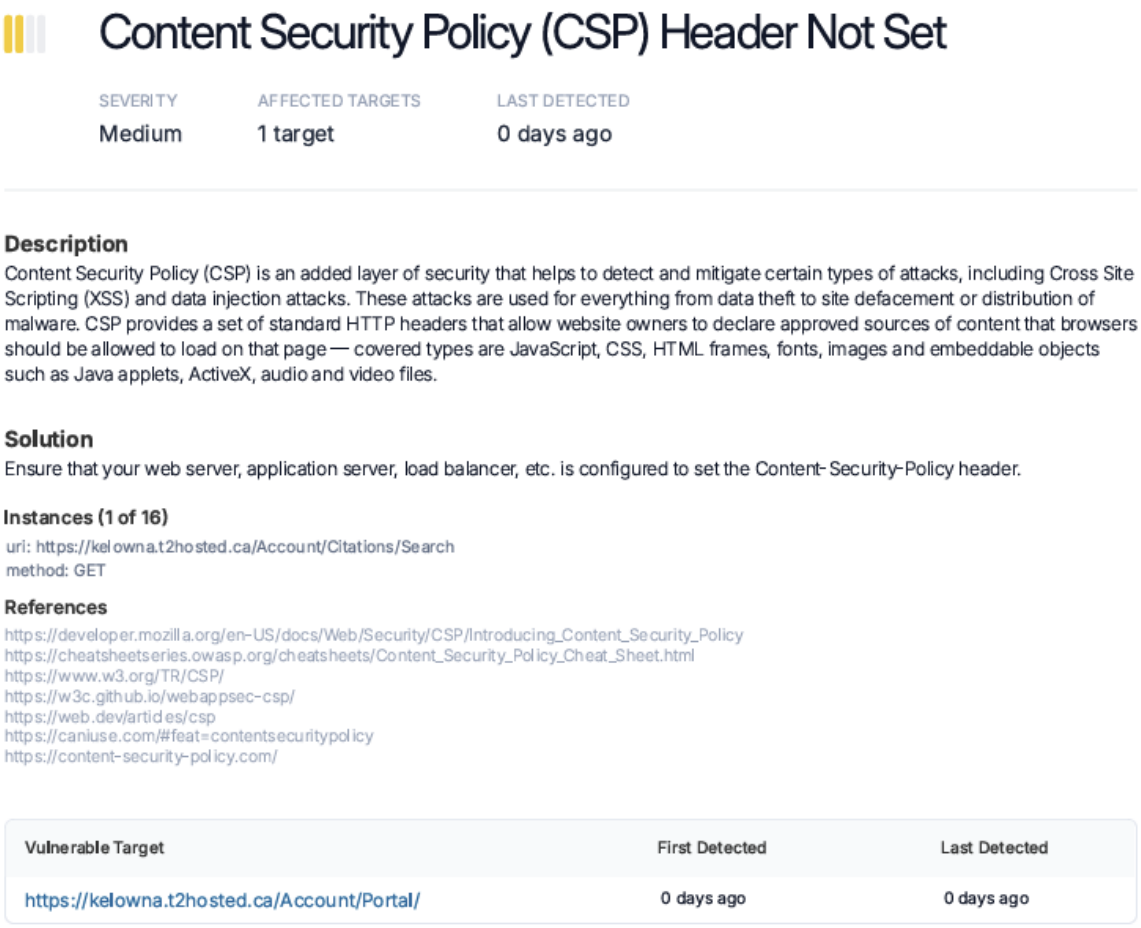
https://w3c.github.io/webappsec-csp/

https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html

Controls:

Ensure that your web server, application server, load balancer and other servers is configured to set the Content-Security-Policy header.

Screenshot:



Client-side vulnerabilities

Client-side vulnerabilities cannot be centrally addressed on the web server as they require updates on the web browsers or host computers of those accessing the city website. However,

the City should ensure their policies for browser updates on corporate hardware take the following information into account.

Vulnerability Name: Missing Anti-clickjacker Header

Vulnerability Impact Summary:

Clickjacking is also known as a “UI redress attack”, where UI components such as buttons or links have been layered with other addresses and redirect a click intended for the top-level page. This can be used to monitor keystrokes or trick a user into entering their password. This could potentially be used to steal credit card information. It can also be used to gain access to a user’s cookies from their web browser, which potentially hold large amounts of data.

Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app.

Evidence:

https://www.okta.com/identity-101/clickjacking/

https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/X-Frame-Options

Controls:

Set this property on all web browsers.

Screenshot:

Missing Anti-clickjacking Header

SEVERITY	AFFECTED TARGETS	LAST DETECTED
Medium	1 target	0 days ago

Description

The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.

Solution

Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app.

If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive.

Instances (1 of 8)

uri: https://kelowna.t2hosted.ca/cmn/auth.aspx
method: GET
param: x-frame-options

References

https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

Vulnerable Target	First Detected	Last Detected
https://kelowna.t2hosted.ca/Account/Portal/	0 days ago	0 days ago

Access Control Research

The free vulnerability scanner https://pentest-tools.com/ offers two free scans every 24 hours. This restriction is imposed through cookies.

Yes, it can be bypassed by running the test in a browser in incognito mode or by deleting cookies for the session.

Summary and Recommendations

While the City of Kelowna has taken important steps towards compliance with PCI DSS, some further changes to infrastructure and policy are required. The audit team has outlined the following list of recommendations and encourages the city to assign personnel and due dates towards the implementation of these changes:

1) Update network topography to ensure all internet of things (IoT) devices such as wireless displays are segmented from financial data flows
2) An organizational policy change to specify a job title of the person in charge of maintaining an accurate inventory of devices
3) Add additional firewall or other protection between public Wi-Fi wireless access point and the City's internal business network
4) Implement CSP header and update JS library on web application server