CYBER PROTECTION GROUP

Web Application Penetration Test

For

Implex

By

Cyber Protection Group LLC

Submission Date: February 1, 2021

Index……1

1. Confidentiality Acknowledgement

A. Handling

CPG embodies an understanding of the need for standard quality assurance and control procedures. The protection, confidentiality and security of client documentation and systems is of the utmost importance.

CPG limits access to client documentation used for testing. Only the penetration testing team at CPG has access to materials exchanged between the client and CPG.

Further, when transmitting and receiving sensitive documentation before, during, and after testing CPG prioritizes the confidentiality, integrity and accessibility of such documentation.

B. Exchange and Submission of Reports

After the completion of the assessment, CPG asks for client preference on the submission of reports. This includes inquiring if a secure portal or other form of secure submission means is available.

The reports are submitted at the client's preference in regards to a secure portal or email exchange.

Following the exchange of testing documents and reports, it is now the client's responsibility in regards to storage and distribution of such reports.

2. Executive Summary

A. Purpose

During the period of 8am(EST) on January 10, 2022, to 11:59pm(EST) on February 1, 2022 Cyber Protection Group was contracted to perform a web application penetration test for Implex. The goal of the web application penetration test is to discover and inform the client of any identified vulnerabilities of the eligible systems that have been tested.

Further, this report allows the client to view the exploitable vulnerabilities as well as explanations into the issue and mitigation techniques.

In the designated testing time frame, Cyber Protection Group performed the assessments with both automated and manual tool sets (please see section **3. Methodology** for information on testing protocol and tools)

B. Scope of Work

Cyber Protection Group performed a web application penetration test. CPG executed the web application penetration test on the provided systems and or endpoints listed below. Please note, the systems listed below are also referenced in the rules of engagement and letter of authorization.

1. Tested Systems and Endpoints

https://global.quikcast.tv/

C. Timeline

During the period of 8am(EST) on January 10, 2022, to 11:59pm(EST) on February 1, 2022, Cyber Protection Group was contracted to perform several security assessments for Implex. The table below outlines the timeline for the testing period.

Start Date	**January 10, 2022**
Testing Period	**January 10, 2022 - February 1, 2022**
Reporting	**February 1, 2022**
Submission Date	**February 1, 2022**

CPG offers free retesting 30 days after the completion of the assessment. If the client remediates any vulnerabilities on previously tested systems, CPG will retest the systems and confirm vulnerability status. Please see the **remediation** section for details.

D. CVE Ranking Breakdown

The risk and vulnerability ranking system utilized by CPG for testing and reporting is featured below. The vulnerability scoring system is based on the Current CVSS Score Distribution For All Vulnerabilities.

The Common Vulnerability Scoring System is a free and open industry standard for assessing the severity of computer system security vulnerabilities. CVSS attempts to assign severity scores to vulnerabilities, allowing responders to prioritize responses and resources according to threat.

All CVSS data rankings are taken from CVE vulnerability data published by National Vulnerability Database, NVD along with other industry standard documentation and testing standards. The NVD is a system managed and maintained by the National Institute of Standards and Technology. NIST is an agency of the United States Department of Commerce.

CVSS Score	Ranking
0.0	None
0.1-3.9	Low
4.0-6.9	Medium
7.0-8.9	High
9.0-10.0	Critical

If or when a vulnerability reports a CVSS score of 7.0 - 10.0 during testing, the client is immediately notified of the vulnerability so immediate action or remediation can take place.

E. Testing Restrictions and Limiting Factors

This report is intended to outline the discovered vulnerabilities uncovered on the designated endpoints and systems submitted by the client (for a list of all endpoints, please reference: 2. Executive Summary, B. Scope of Work, 2. Systems to be Tested).

While testing, certain restrictions and limitations are presented due to the nature of this type of testing and format. This includes the following scenarios.

The testing of the designated systems and endpoints was limited and confined to a predetermined schedule and testing window. In that, CPG and Implex agreed upon a timeframe for the assessment in which the endpoints would be tested. During this timeframe of testing, industry standard tools and methodology are used to perform the penetration test (for more information on the tools and methodology see section: 3. Methodology).

During testing, the confidentiality, integrity and availability of the tested endpoints was not compromised. No attempts to delete, destroy, change or take systems offline were carried out. This does not rule out factors that unauthorized users could attempt to attack the endpoints with similar tactics as stated above.

Please see section 4. Penetration Test / Security Assessment Results and the attached technical reports for the penetration test results.

F. Summary of Findings

During the testing period, several technical vulnerabilities were identified. This includes a range of informational to medium rated vulnerabilities.

Throughout the entire assessment, industry standard tools as well as manual efforts were performed. At the time of writing this report, Cyber Protection Group is not finding any vulnerabilities within the scope of the assessment of high or critical nature.

Identified vulnerabilities are common and can be easily mitigated in most environments.

3. Methodology

CPG's methodology for a penetration test and security assessment is as follows.

The goal of a penetration test and security assessment performed by CPG is to give the client insight as to what a cyber threat or hacker could access. Essentially, discover and identify what security vulnerabilities currently exist in or on the designated testing endpoint and system environments.

Testing is performed with the personnel responsible for the systems being informed of and when the testing procedures occur. It should be noted that penetration testing mimics but does not fully resemble the threat or persistence of an actual attack or threat from an unauthorized user. The procedure for testing is executed in the following order.

Reconnaissance - Gathering of information and attack planning
Enumeration- Identifying attack vectors
Exploitation - Verify security issues and vulnerabilities

While testing, CPG uses an array of industry standard penetration testing and security assessment tools. This list includes Nmap, Openvas, Nessus, Burp, and Kali.

A. Reconnaissance

At the beginning of the testing period, reconnaissance is the necessary step in starting up testing. The gathering and researching of publicly available information on the intended target is performed. Technical and non technical information aids CPG is forming the testing plan for the intended targets. Publically available resources like centralops.net are used to gain insight into the designated endpoint, target and or client company. The information is what is available to the public and not gathered by exploitation.

B. Enumeration

After the collection of information through reconnaissance is performed, the next phase of testing is enumeration. This phase entails the search for possible entry points or exploitable ports. This phase imitates what an outside threat may do in order to find an access point to internal networks and systems. CPG utilizes port scanning tools and manual efforts to identify possible entry points. The information is collected and systems identified.

C. Exploitation

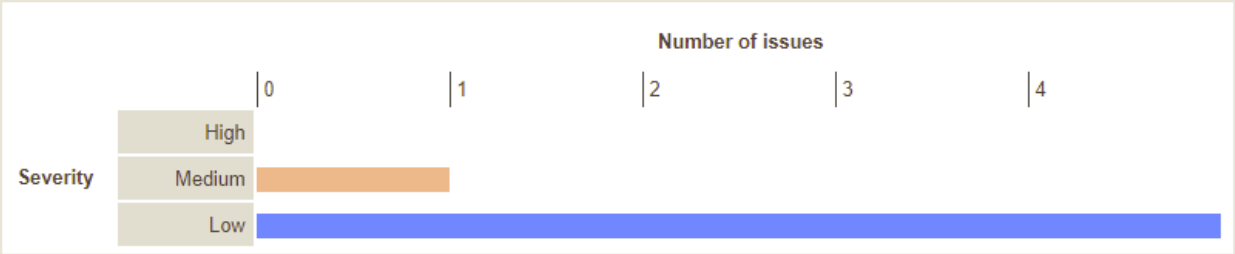
During the final phase of exploitation, the information and identified system information gathered in the previous steps is exploited for weaknesses and vulnerabilities. CPG utilizes the tools (mentioned previously) as well as manual efforts to attempt exploitation of the identified vulnerabilities. It is noted that CPG does not attempt to bring down systems, flood servers or deny access to the client and or company. This step once again is to imitate how an outside threat may attack such systems. After the tested exploitation of the endpoints, the client will then be able to review the penetration test results in section 4 as well as any attached technical reports.

4. Penetration Test / Security Assessment Results

The following information is the results of the external penetration test. The findings below depict the identified vulnerabilities uncovered by CPG during testing.

The findings will begin on the following page. The rest of this page is left intentionally blank.

Severity	Confidence			
	Certain	Firm	Tentative	Total
High	0	0	0	0
Medium	0	1	0	1
Low	5	0	0	5
Information	6	0	0	6



Contents

1. Session Token In URL

Summary
Severity: Medium
Confidence: Firm
Host: https://global.qwikcast.tv
Path: /public/QwikCast/EndSession

Issue Detail
The URL in the request appears to contain a session token within the query string:

- https://global.qwikcast.tv/public/QwikCast/EndSession?userEventVideoSessionId=689384

Description
Sensitive information within URLs may be logged in various locations, including the user's browser, the web server, and any forward or reverse proxy servers between the two endpoints. URLs may also be displayed on-screen, bookmarked or emailed around by users. They may be disclosed to third parties via the Referer header when any off-site links are followed. Placing session tokens into the URL increases the risk that they will be captured by an attacker.

Remediation
Applications should use an alternative mechanism for transmitting session tokens, such as HTTP cookies or hidden fields in forms that are submitted using the POST method.

Vulnerability Classifications

- CWE-200: Information Exposure
- CWE-384: Session Fixation
- CWE-598: Information Exposure Through Query Strings in GET Request
- CAPEC-593: Session Hijacking

Request

```
POST /public/QwikCast/EndSession?userEventVideoSessionId=689384 HTTP/1.1
Host: global.qwikcast.tv
Cookie: _gat=1; ARRAffinity=327e34219519df25bedba7e0d77e23fac1d7c3ad5d9549029cf01e7a4117edac;
ARRAffinitySameSite=327e34219519df25bedba7e0d77e23fac1d7c3ad5d9549029cf01e7a4117edac;
_pk_id.2.c6cf=46a81f16e9d1ec80.1643390694.1.1643391211.1643390694.; _pk_ses.2.c6cf=*;
_ga=GA1.2.946418973.1643390694; _gid=GA1.2.1703015334.1643390694;
__RequestVerificationToken=0FXyJKkXw8lPXG2EAgvX9bYoWOe7d4zEVsjhn85fMc7Vpwcb7KRDbZreDg4e
dQDtg9qynBHqnxixt5sP58NtQbRZvSk1; ai_user=cZCk8|2022-01-28T17:32:53.028Z;
ai_session=ZN4MI|1643391173256|1643391182653;
.ASPXAUTH=2BDAE0C141972993891B4BD1F62EC778A4444D9F6C4D4616AA692A1346E0F1B7D79F0
DC91D1C22D4F81BA47813D04FB2F589887997291A4C376FC339F731CC4BAB1157A8754EA49BA7681
2DDDDF7182C43E8185E2A0A09A6CAF022A0339C1074E313231F911F750AA84AC23C44D531E54697D
0B54D883F2D865646D2938D269581117B95DFBEA0AD3152950750466E86AEF1959CA1EC735D060065
C6DBD5663B1ED09FE5A826573D254EEEFD3C1B263D7B620AE09186F4B3251EF83EC1F9EB7DA4085
11F2B3980640EFE4A856031C6CC758D929F34FED968B37A22C3F1CD7E6B1E877E88
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:96.0) Gecko/20100101 Firefox/96.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Origin: https://global.qwikcast.tv
Referer:
https://global.qwikcast.tv/public/QwikCast/QwikCastEventById?eventKey=06f9ea1c-dd53-442c-ab8b-3f2e56
e9d8c9&eventPageId=2834
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Content-Length: 0
Te: trailers
Connection: close
```

Response

```
HTTP/1.1 200 OK
Cache-Control: public, no-store, max-age=0
Content-Type: text/html
Expires: Fri, 28 Jan 2022 17:35:27 GMT
Last-Modified: Fri, 28 Jan 2022 17:35:27 GMT
Vary: *
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: *
Access-Control-Allow-Methods: *
Date: Fri, 28 Jan 2022 17:35:26 GMT
Connection: close
Content-Length: 0
```

2. Password Field With Autocomplete Enabled

Summary
Severity: Low
Confidence: Certain
Host: https://global.qwikcast.tv
Path: /QwikCast/QwikCastEvent

Issue Detail
The page contains a form with the following action URL:
https://global.qwikcast.tv/Account/LoginEventPasswordOnly?Length=7

The form contains the following password field with autocomplete enabled: EventPassword

Description
Most browsers have a facility to remember user credentials that are entered into HTML forms. This function can be configured by the user and also by applications that employ user credentials. If the function is enabled, then credentials entered by the user are stored on their local computer and retrieved by the browser on future visits to the same application.

The stored credentials can be captured by an attacker who gains control over the user's computer. Further, an attacker who finds a separate application vulnerability such as cross-site scripting may be able to exploit this to retrieve a user's browser-stored credentials.

Remediation
To prevent browsers from storing credentials entered into HTML forms, include the attribute **autocomplete="off"** within the FORM tag (to protect all form fields) or within the relevant INPUT tags (to protect specific individual fields).

Please note that modern web browsers may ignore this directive. In spite of this there is a chance that not disabling autocomplete may cause problems obtaining PCI compliance.

Vulnerability Classifications

- CWE-200: Information Exposure

Request

```
GET /QwikCast/QwikCastEvent?eventKey=06f9ea1c-dd53-442c-ab8b-3f2e56e9d8c9 HTTP/1.1
Host: global.qwikcast.tv
Sec-Ch-Ua: "Chromium";v="97", " Not;A Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/97.0.4692.71 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applicatio
n/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Response

```
HTTP/1.1 200 OK
Cache-Control: public, no-store, max-age=0
Content-Length: 10159
Content-Type: text/html; charset=utf-8
Expires: Fri, 28 Jan 2022 17:35:58 GMT
Last-Modified: Fri, 28 Jan 2022 17:35:58 GMT
Vary: *
Server: Microsoft-IIS/10.0
customheader: value
X-Frame-Options: SAMEORIGIN
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: *
Access-Control-Allow-Methods: *
Set-Cookie:
ARRAffinity=327e34219519df25bedba7e0d77e23fac1d7c3ad5d9549029cf01e7a4117edac;Path=/;HttpOnly;
Secure;Domain=global.qwikcast.tv
Set-Cookie:
ARRAffinitySameSite=327e34219519df25bedba7e0d77e23fac1d7c3ad5d9549029cf01e7a4117edac;Path=/;
HttpOnly;SameSite=None;Secure;Domain=global.qwikcast.tv
Date: Fri, 28 Jan 2022 17:35:58 GMT
Connection: close
```

3. Strict Transport Security Not Enforced

Instances: 4

1. https://global.qwikcast.tv/
2. https://global.qwikcast.tv/QwikCastEvent
3. https://global.qwikcast.tv/public/QwikCast/EndSession
4. https://global.qwikcast.tv/public/QwikCast/UpdateEventSession

Description

The application fails to prevent users from connecting to it over unencrypted connections. An attacker able to modify a legitimate user's network traffic could bypass the application's use of SSL/TLS encryption, and use the application as a platform for attacks against its users. This attack is performed by rewriting HTTPS links as HTTP, so that if a targeted user follows a link to the site from an HTTP page, their browser never attempts to use an encrypted connection. The sslstrip tool automates this process.

To exploit this vulnerability, an attacker must be suitably positioned to intercept and modify the victim's network traffic.This scenario typically occurs when a client communicates with the server over an insecure connection such as public Wi-Fi, or a corporate or home network that is shared with a compromised computer. Common defenses such as switched networks are not sufficient to prevent this. An attacker situated in the user's ISP or the application's hosting infrastructure could also perform this attack. Note that an advanced adversary could potentially target any connection made over the Internet's core infrastructure

Remediation

The application should instruct web browsers to only access the application using HTTPS. To do this, enable HTTP Strict Transport Security (HSTS) by adding a response header with the name 'Strict-Transport-Security' and the value 'max-age=expireTime', where expireTime is the time in seconds that browsers should remember that the site should only be accessed using HTTPS. Consider adding the 'includeSubDomains' flag if appropriate.

Note that because HSTS is a "trust on first use" (TOFU) protocol, a user who has never accessed the application will never have seen the HSTS header, and will therefore still be vulnerable to SSL stripping attacks. To mitigate this risk, you can optionally add the 'preload' flag to the HSTS header, and submit the domain for review by browser vendors.

References

- HTTP Strict Transport Security
- sslstrip
- HSTS Preload Form

Vulnerability Classifications

- CWE-523: Unprotected Transport of Credentials
- CAPEC-94: Man in the Middle Attack
- CAPEC-157: Sniffing Attacks

3.1. https://global.qwikcast.tv/

Summary
Severity: Low
Confidence: Certain
Host: https://global.qwikcast.tv
Path: /

Issue Detail
This issue was found in multiple locations under the reported path.

Request

```
GET /public/bundles/jqueryval?v=vYbr-3ljCYjg2jHwbJx9Mf2pxLtJnYWhypxESEKxYw41 HTTP/1.1
Host: global.qwikcast.tv
Cookie: ARRAffinity=327e34219519df25bedba7e0d77e23fac1d7c3ad5d9549029cf01e7a4117edac;
ARRAffinitySameSite=327e34219519df25bedba7e0d77e23fac1d7c3ad5d9549029cf01e7a4117edac
Sec-Ch-Ua: "Chromium";v="97", " Not;A Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/97.0.4692.71 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Accept: */*
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer:
https://global.qwikcast.tv/QwikCast/QwikCastEvent?eventKey=06f9ea1c-dd53-442c-ab8b-3f2e56e9d8c9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Response

```
HTTP/1.1 200 OK
Cache-Control: public
Content-Length: 28149
Content-Type: text/javascript; charset=utf-8
Expires: Sat, 28 Jan 2023 17:35:58 GMT
Last-Modified: Fri, 28 Jan 2022 17:35:58 GMT
Vary: User-Agent,Accept-Encoding
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: *
Access-Control-Allow-Methods: *
Date: Fri, 28 Jan 2022 17:35:58 GMT
Connection: close

(function(n){function i(n,t){for(var i=window,r=(n||"").split(".");i&&r.length;)i=i[r.shift()];return typeof
i=="function"?i:(t.push(n),Function.constructor.apply(null,t))}function r(n){return n==="GE
...[SNIP]...
```

3.2. https://global.qwikcast.tv/QwikCast/QwikCastEvent

Summary
Severity: Low
Confidence: Certain
Host: https://global.qwikcast.tv
Path: /QwikCast/QwikCastEvent

Request

```
GET /QwikCast/QwikCastEvent?eventKey=06f9ea1c-dd53-442c-ab8b-3f2e56e9d8c9 HTTP/1.1
Host: global.qwikcast.tv
Sec-Ch-Ua: "Chromium";v="97", " Not;A Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/97.0.4692.71 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applicatio
n/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Response

```
HTTP/1.1 200 OK
Cache-Control: public, no-store, max-age=0
Content-Length: 10159
Content-Type: text/html; charset=utf-8
Expires: Fri, 28 Jan 2022 17:35:58 GMT
Last-Modified: Fri, 28 Jan 2022 17:35:58 GMT
Vary: *
Server: Microsoft-IIS/10.0
customheader: value
X-Frame-Options: SAMEORIGIN
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: *
Access-Control-Allow-Methods: *
Set-Cookie:
ARRAffinity=327e34219519df25bedba7e0d77e23fac1d7c3ad5d9549029cf01e7a4117edac;Path=/;HttpOnly;
Secure;Domain=global.qwikcast.tv
Set-Cookie:
ARRAffinitySameSite=327e34219519df25bedba7e0d77e23fac1d7c3ad5d9549029cf01e7a4117edac;Path=/;
HttpOnly;SameSite=None;Secure;Domain=global.qwikcast.tv
Date: Fri, 28 Jan 2022 17:35:58 GMT
Connection: close
```

3.2. https://global.qwikcast.tv/public/QwikCast/EndSession

Summary

Severity: Low
Confidence: Certain
Host: https://global.qwikcast.tv
Path: /public/QwikCast/EndSession

Request

```
POST /public/QwikCast/EndSession?userEventVideoSessionId=689384 HTTP/1.1
Host: global.qwikcast.tv
Cookie: _gat=1; ARRAffinity=327e34219519df25bedba7e0d77e23fac1d7c3ad5d9549029cf01e7a4117edac;
ARRAffinitySameSite=327e34219519df25bedba7e0d77e23fac1d7c3ad5d9549029cf01e7a4117edac;
_pk_id.2.c6cf=46a81f16e9d1ec80.1643390694.1.1643391211.1643390694.; _pk_ses.2.c6cf=*;
_ga=GA1.2.946418973.1643390694; _gid=GA1.2.1703015334.1643390694;
__RequestVerificationToken=0FXyJKkXw8lPXG2EAgvX9bYoWOe7d4zEVsjhn85fMc7Vpwcb7KRDbZreDg4e
dQDtg9qynBHqnxixt5sP58NtQbRZvSk1; ai_user=cZCk8|2022-01-28T17:32:53.028Z;
ai_session=ZN4MI|1643391173256|1643391182653;
.ASPXAUTH=2BDAE0C141972993891B4BD1F62EC778A4444D9F6C4D4616AA692A1346E0F1B7D79F0
DC91D1C22D4F81BA47813D04FB2F589887997291A4C376FC339F731CC4BAB1157A8754EA49BA7681
2DDDDF7182C43E8185E2A0A09A6CAF022A0339C1074E313231F911F750AA84AC23C44D531E54697D
0B54D883F2D865646D2938D269581117B95DFBEA0AD3152950750466E86AEF1959CA1EC735D060065
C6DBD5663B1ED09FE5A826573D254EEEFD3C1B263D7B620AE09186F4B3251EF83EC1F9EB7DA4085
11F2B3980640EFE4A856031C6CC758D929F34FED968B37A22C3F1CD7E6B1E877E88
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:96.0) Gecko/20100101 Firefox/96.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Origin: https://global.qwikcast.tv
Referer:
https://global.qwikcast.tv/public/QwikCast/QwikCastEventById?eventKey=06f9ea1c-dd53-442c-ab8b-3f2e56
e9d8c9&eventPageId=2834
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Content-Length: 0
Te: trailers
Connection: close
```

Response

```
HTTP/1.1 200 OK
Cache-Control: public, no-store, max-age=0
Content-Type: text/html
Expires: Fri, 28 Jan 2022 17:35:27 GMT
Last-Modified: Fri, 28 Jan 2022 17:35:27 GMT
Vary: *
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: *
Access-Control-Allow-Methods: *
Date: Fri, 28 Jan 2022 17:35:26 GMT
Connection: close
Content-Length: 0
```

3.2. https://global.qwikcast.tv/public/public/QwikCast/UpdateEventSession

Summary

Severity: Low
Confidence: Certain
Host: https://global.qwikcast.tv
Path: /public/QwikCast/UpdateEventSession

Request

```
POST /public/QwikCast/UpdateEventSession HTTP/1.1
Host: global.qwikcast.tv
Cookie: _gat=1; ARRAffinity=327e34219519df25bedba7e0d77e23fac1d7c3ad5d9549029cf01e7a4117edac;
ARRAffinitySameSite=327e34219519df25bedba7e0d77e23fac1d7c3ad5d9549029cf01e7a4117edac;
_pk_id.2.c6cf=46a81f16e9d1ec80.1643390694.1.1643391211.1643390694.; _pk_ses.2.c6cf=*;
_ga=GA1.2.946418973.1643390694; _gid=GA1.2.1703015334.1643390694;
__RequestVerificationToken=0FXyJKkXw8lPXG2EAgvX9bYoWOe7d4zEVsjhn85fMc7Vpwcb7KRDbZreDg4e
dQDtg9qynBHqnxixt5sP58NtQbRZvSk1; ai_user=cZCk8|2022-01-28T17:32:53.028Z;
ai_session=ZN4MI|1643391173256|1643391182653;
.ASPXAUTH=2BDAE0C141972993891B4BD1F62EC778A4444D9F6C4D4616AA692A1346E0F1B7D79F0
DC91D1C22D4F81BA47813D04FB2F589887997291A4C376FC339F731CC4BAB1157A8754EA49BA7681
2DDDDF7182C43E8185E2A0A09A6CAF022A0339C1074E313231F911F750AA84AC23C44D531E54697D
0B54D883F2D865646D2938D269581117B95DFBEA0AD3152950750466E86AEF1959CA1EC735D060065
C6DBD5663B1ED09FE5A826573D254EEEFD3C1B263D7B620AE09186F4B3251EF83EC1F9EB7DA4085
11F2B3980640EFE4A856031C6CC758D929F34FED968B37A22C3F1CD7E6B1E877E88
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:96.0) Gecko/20100101 Firefox/96.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 26
Origin: https://global.qwikcast.tv
Referer:
https://global.qwikcast.tv/public/QwikCast/QwikCastEventById?eventKey=06f9ea1c-dd53-442c-ab8b-3f2e56
e9d8c9&eventPageId=2834
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Te: trailers
Connection: close
userEventSessionId=1030249
```

Response

```
HTTP/1.1 200 OK
Cache-Control: public, no-store, max-age=0
Content-Type: text/html
Expires: Fri, 28 Jan 2022 17:35:27 GMT
Last-Modified: Fri, 28 Jan 2022 17:35:27 GMT
Vary: *
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: *
Access-Control-Allow-Methods: *
Date: Fri, 28 Jan 2022 17:35:26 GMT
Connection: close
Content-Length: 0
```

4. TLS Cookie Without Secure Flag Set

Summary
Severity: Information
Confidence: Certain
Host: https://global.qwikcast.tv
Path: /Account/LoginEventPasswordOnly

Issue Detail
The following cookie was issued by the application and does not have the secure flag set:
.ASPXAUTH
The cookie does not appear to contain a session token, which may reduce the risk associated with this issue. You should review the contents of the cookie to determine its function.

Description
If the secure flag is set on a cookie, then browsers will not submit the cookie in any requests that use an unencrypted HTTP connection, thereby preventing the cookie from being trivially intercepted by an attacker monitoring network traffic. If the secure flag is not set, then the cookie will be transmitted in clear-text if the user visits any HTTP URLs within the cookie's scope. An attacker may be able to induce this event by feeding a user suitable links, either directly or via another web site. Even if the domain that issued the cookie does not host any content that is accessed over HTTP, an attacker may be able to use links of the form http://example.com:443/ to perform the same attack.

To exploit this vulnerability, an attacker must be suitably positioned to eavesdrop on the victim's network traffic. This scenario typically occurs when a client communicates with the server over an insecure connection such as public Wi-Fi, or a corporate or home network that is shared with a compromised computer. Common defenses such as switched networks are not sufficient to prevent this. An attacker situated in the user's ISP or the application's hosting infrastructure could also perform this attack. Note that an advanced adversary could potentially target any connection made over the Internet's core infrastructure.

Remediation
The secure flag should be set on all cookies that are used for transmitting sensitive data when accessing content over HTTPS. If cookies are used to transmit session tokens, then areas of the application that are accessed over HTTPS should employ their own session handling mechanism, and the session tokens used should never be transmitted over unencrypted communications.

Vulnerability Classifications

- CWE-614: Sensitive Cookie in HTTPS Session Without 'Secure' Attribute

Request

```
POST /Account/LoginEventPasswordOnly?Length=7 HTTP/1.1
Host: global.qwikcast.tv
Cookie: ARRAffinity=327e34219519df25bedba7e0d77e23fac1d7c3ad5d9549029cf01e7a4117edac;
ARRAffinitySameSite=327e34219519df25bedba7e0d77e23fac1d7c3ad5d9549029cf01e7a4117edac;
_ga=GA1.2.1788573453.1643391360; _gid=GA1.2.19972241.1643391360; _gat=1;
_pk_id.2.c6cf=4014f73af248e609.1643391360.1.1643391360.1643391360.; _pk_ses.2.c6cf=*
Content-Length: 238
Sec-Ch-Ua: "Chromium";v="97", " Not;A Brand";v="99"
Accept: */*
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/97.0.4692.71 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Origin: https://global.qwikcast.tv
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://global.qwikcast.tv/QwikCast/QwikCastEvent?eventKey=06f9ea1c-dd53-442c-ab8b-3f2e56e9d8c9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

EventKey=06f9ea1c-dd53-442c-ab8b-3f2e56e9d8c9&ReturnUrl=%2FQwikCast%2FQwikCastEventById%3F
eventKey%3D06f9ea1c-dd53-442c-ab8b-3f2e56e9d8c9%26eventPageId%3D2833&IsMiniPlayer=False&Ev
entPassword=zqVcX9ig
...[SNIP]...
```

Response

```
HTTP/1.1 200 OK
Content-Length: 172
Connection: close
Content-Type: application/json; charset=utf-8
Date: Fri, 28 Jan 2022 17:36:14 GMT
Server: Microsoft-IIS/10.0
Access-Control-Allow-Headers: *
Access-Control-Allow-Methods: *
Access-Control-Allow-Origin: *
Cache-Control: private
Set-Cookie:
.ASPXAUTH=175F2D521E5EABB48929639CA631AD5E02D2CC2050AA3D083074592FD3D864A4F09246
D5B1ECAF98E50D2D13B98AEA6678DCA50C66F3CB7D4A21F72748393DD41C170F398A2A91DB9DB09
A79BF209F54E6F0EBE779F5100C3B23AFB21A521AC5E70D920C3E367ED4B6EF542EDDFD366B0975
42E57A1DF6D674ECDB4650AD7FD6D1D40BFFBF2E198AEB2677692C82D5075C1448DB596F406765D
FD5F40A0F9A2F3A19BFDFF524CFB0E8AD4D0F116156A7358751845181E4461360EC6FD30DC3E2A0F
3EF5FB8C90FEC7DC8B3F9BE97F3467363ADC0C4F247F9E40985AB842CA2BE057201DA; path=/;
HttpOnly
Set-Cookie:
ARRAffinity=327e34219519df25bedba7e0d77e23fac1d7c3ad5d9549029cf01e7a4117edac;Path=/;HttpOnly;
Secure;Domain=global.qwikcast.tv
Set-Cookie:
ARRAffinitySameSite=327e34219519df25bedba7e0d77e23fac1d7c3ad5d9549029cf01e7a4117edac;Path=/;
HttpOnly;SameSite=None;Secure;Domain=global.qwikcast.tv
Vary: Accept-Encoding

{"IsAuthenticated":true,"AuthenticationType":5,"ReturnUrl":"/QwikCast/QwikCastEventById?eventKey=06f9e
a1c-dd53-442c-ab8b-3f2e56e9d8c9\u0026eventPageId=2833","Payload":null}
```

5. Cross-Domain Referer Leakage

Summary
Severity: Information
Confidence: Certain
Host: https://global.qwikcast.tv
Path: /public/QwikCast/QwikCastEventByID

Issue Detail
The page was loaded from a URL containing a query string:
https://global.qwikcast.tv/public/QwikCast/QwikCastEventById

The response contains the following link to another domain:
https://globalchat.qwikcast.tv/ClientChat/ClientChat?chatId=06de95b6-ecf2-4f5d-8298-cb4315262261&userId=347677

Description
When a web browser makes a request for a resource, it typically adds an HTTP header, called the "Referer" header, indicating the URL of the resource from which the request originated. This occurs in numerous situations, for example when a web page loads an image or script, or when a user clicks on a link or submits a form. If the resource being requested resides on a different domain, then the Referer header is still generally included in the cross-domain request. If the originating URL contains any sensitive information within its query string, such as a session token, then this information will be transmitted to the other domain. If the other domain is not fully trusted by the application, then this may lead to a security compromise. You should review the contents of the information being transmitted to other domains, and also determine whether those domains are fully trusted by the originating application. Today's browsers may withhold the Referer header in some situations (for example, when loading a non-HTTPS resource from a page that was loaded over HTTPS, or when a Refresh directive is issued), but this behavior should not be relied upon to protect the originating URL from disclosure. Note also that if users can author content within the application then an attacker may be able to inject links referring to a domain they control in order to capture data from URLs used within the application.

Remediation
Applications should never transmit any sensitive information within the URL query string. In addition to being leaked in the Referer header, such information may be logged in various locations and may be visible on-screen to untrusted parties. If placing sensitive information in the URL is unavoidable, consider using the Referer-Policy HTTP header to reduce the chance of it being disclosed to third parties.

References

- Referer Policy
- Web Security Academy: Information disclosure

Vulnerability Classifications

- CWE-200: Information Exposure

Request

```
GET
/public/QwikCast/QwikCastEventById?eventKey=06f9ea1c-dd53-442c-ab8b-3f2e56e9d8c9&eventPageId=2
834 HTTP/1.1
Host: global.qwikcast.tv
Cookie: ARRAffinity=327e34219519df25bedba7e0d77e23fac1d7c3ad5d9549029cf01e7a4117edac;
ARRAffinitySameSite=327e34219519df25bedba7e0d77e23fac1d7c3ad5d9549029cf01e7a4117edac;
_ga=GA1.2.1788573453.1643391360; _gid=GA1.2.19972241.1643391360; _gat=1; _pk_ses.2.c6cf=*;
.ASPXAUTH=175F2D521E5EABB48929639CA631AD5E02D2CC2050AA3D083074592FD3D864A4F09246
D5B1ECAF98E50D2D13B98AEA6678DCA50C66F3CB7D4A21F72748393DD41C170F398A2A91DB9DB09
A79BF209F54E6F0EBE779F5100C3B23AFB21A521AC5E70D920C3E367ED4B6EF542EDDFD366B0975
42E57A1DF6D674ECDB4650AD7FD6D1D40BFFBF2E198AEB2677692C82D5075C1448DB596F406765D
FD5F40A0F9A2F3A19BFDFF524CFB0E8AD4D0F116156A7358751845181E4461360EC6FD30DC3E2A0F
3EF5FB8C90FEC7DC8B3F9BE97F3467363ADC0C4F247F9E40985AB842CA2BE057201DA;
_pk_id.2.c6cf=4014f73af248e609.1643391360.1.1643391376.1643391360.
Sec-Ch-Ua: "Chromium";v="97", " Not;A Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/97.0.4692.71 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applicatio
n/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer:
https://global.qwikcast.tv/QwikCast/QwikCastEventById?eventKey=06f9ea1c-dd53-442c-ab8b-3f2e56e9d8c
9&eventPageId=2833
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Response

```
HTTP/1.1 200 OK
Cache-Control: public, no-store, max-age=0
Content-Length: 12258
Content-Type: text/html; charset=utf-8
Expires: Fri, 28 Jan 2022 17:36:22 GMT
Last-Modified: Fri, 28 Jan 2022 17:36:22 GMT
Vary: *
Server: Microsoft-IIS/10.0
customheader: value
X-Frame-Options: SAMEORIGIN
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: *
Access-Control-Allow-Methods: *
Date: Fri, 28 Jan 2022 17:36:22 GMT
Connection: close


<!DOCTYPE html>

<html lang="en" class="no-js" manifest="https://global.qwikcast.tv:443/QC4.manifest?eventPageId=2834"
style="background-color: #FFFFFF;">
<head>
<meta charset="utf-8" />
...[SNIP]...
<div class='row'>
<iframe
src="https://globalchat.qwikcast.tv/ClientChat/ClientChat?chatId=06de95b6-ecf2-4f5d-8298-cb4315262261&
userId=347677" style="height: 450px;width: 650px;"></iframe>
...[SNIP]...
```

6. Cacheable HTTPS Response

Summary
Severity: Information
Confidence: Certain
Host: https://global.qwikcast.tv
Path: /Account/LoginEventPasswordOnly

Description
Unless directed otherwise, browsers may store a local cached copy of content received from web servers. Some browsers, including Internet Explorer, cache content accessed via HTTPS. If sensitive information in application responses is stored in the local cache, then this may be retrieved by other users who have access to the same computer at a future time.

Remediation
Applications should return caching directives instructing browsers not to store local copies of any sensitive data. Often, this can be achieved by configuring the web server to prevent caching for relevant paths within the web root. Alternatively, most web development platforms allow you to control the server's caching directives from within individual scripts. Ideally, the web server should return the following HTTP headers in all responses containing sensitive content:

- Cache-control: no-store
- Pragma: no-cache

References

- Web Security Academy: Information disclosure

Vulnerability Classifications

- CWE-524: Information Exposure Through Caching
- CWE-525: Information Exposure Through Browser Caching
- CAPEC-37: Retrieve Embedded Sensitive Data

Request

```
POST /Account/LoginEventPasswordOnly?Length=7 HTTP/1.1
Host: global.qwikcast.tv
Cookie: ARRAffinity=327e34219519df25bedba7e0d77e23fac1d7c3ad5d9549029cf01e7a4117edac;
ARRAffinitySameSite=327e34219519df25bedba7e0d77e23fac1d7c3ad5d9549029cf01e7a4117edac;
_ga=GA1.2.1788573453.1643391360; _gid=GA1.2.19972241.1643391360; _gat=1;
_pk_id.2.c6cf=4014f73af248e609.1643391360.1.1643391360.1643391360.; _pk_ses.2.c6cf=*
Content-Length: 238
Sec-Ch-Ua: "Chromium";v="97", " Not;A Brand";v="99"
Accept: */*
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/97.0.4692.71 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Origin: https://global.qwikcast.tv
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://global.qwikcast.tv/QwikCast/QwikCastEvent?eventKey=06f9ea1c-dd53-442c-ab8b-3f2e56e9d8c9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

EventKey=06f9ea1c-dd53-442c-ab8b-3f2e56e9d8c9&ReturnUrl=%2FQwikCast%2FQwikCastEventById%3F
eventKey%3D06f9ea1c-dd53-442c-ab8b-3f2e56e9d8c9%26eventPageId%3D2833&IsMiniPlayer=False&Ev
entPassword=zqVcX9ig
...[SNIP]...
```

Response

```
HTTP/1.1 200 OK
Content-Length: 172
Connection: close
Content-Type: application/json; charset=utf-8
Date: Fri, 28 Jan 2022 17:36:14 GMT
Server: Microsoft-IIS/10.0
Access-Control-Allow-Headers: *
Access-Control-Allow-Methods: *
Access-Control-Allow-Origin: *
Cache-Control: private
Set-Cookie:
.ASPXAUTH=175F2D521E5EABB48929639CA631AD5E02D2CC2050AA3D083074592FD3D864A4F09246
D5B1ECAF98E50D2D13B98AEA6678DCA50C66F3CB7D4A21F72748393DD41C170F398A2A91DB9DB09
A79BF209F54E6F0EBE779F5100C3B23AFB21A521AC5E70D920C3E367ED4B6EF542EDDFD366B0975
42E57A1DF6D674ECDB4650AD7FD6D1D40BFFBF2E198AEB2677692C82D5075C1448DB596F406765D
FD5F40A0F9A2F3A19BFDFF524CFB0E8AD4D0F116156A7358751845181E4461360EC6FD30DC3E2A0F
3EF5FB8C90FEC7DC8B3F9BE97F3467363ADC0C4F247F9E40985AB842CA2BE057201DA; path=/;
HttpOnly
Set-Cookie:
ARRAffinity=327e34219519df25bedba7e0d77e23fac1d7c3ad5d9549029cf01e7a4117edac;Path=/;HttpOnly;
Secure;Domain=global.qwikcast.tv
Set-Cookie:
ARRAffinitySameSite=327e34219519df25bedba7e0d77e23fac1d7c3ad5d9549029cf01e7a4117edac;Path=/;
HttpOnly;SameSite=None;Secure;Domain=global.qwikcast.tv
Vary: Accept-Encoding

{"IsAuthenticated":true,"AuthenticationType":5,"ReturnUrl":"/QwikCast/QwikCastEventById?eventKey=06f9e
a1c-dd53-442c-ab8b-3f2e56e9d8c9\u0026eventPageId=2833","Payload":null}
```

7. Mixed Content

Instances: 3

1. https://global.qwikcast.tv/QwikCastEvent
2. https://global.qwikcast.tv/QwikCast/QwikCastEventById
3. https://global.qwikcast.tv/public/QwikCast/QwikCastEventById

Description

The application loads pages over HTTPS that load other resources over unencrypted connections. An attacker suitably positioned to view a legitimate user's network traffic could record and monitor their interactions with these resources, which may indirectly disclose information about the user's activity on the application itself. Furthermore, an attacker able to modify traffic could alter these resources and potentially influence the application's appearance and behavior. Due to these concerns, users' web browsers may automatically display warnings and disable affected components of the page. As a result, this vulnerability currently has more of an impact on usability than security.

To exploit this vulnerability, an attacker must be suitably positioned to eavesdrop on the victim's network traffic. This scenario typically occurs when a client communicates with the server over an insecure connection such as public Wi-Fi, or a corporate or home network that is shared with a compromised computer. Common defenses such as switched networks are not sufficient to prevent this. An attacker situated in the user's ISP or the application's hosting infrastructure could also perform this attack. Note that an advanced adversary could potentially target any connection made over the Internet's core infrastructure.

Remediation

Ensure that all external resources the page references are loaded using HTTPS.

References

- Mixed Content

Vulnerability Classifications

- CWE-16: Configuration
- CWE-319: Cleartext Transmission of Sensitive Information
- CAPEC-117: Interception

7.1. https://global.qwikcast.tv/QwikCast/QwikCastEvent

Summary
Severity: Low
Confidence: Certain
Host: https://global.qwikcast.tv
Path: /QwikCast/QwikCastEvent

Issue Detail
The response is loaded over HTTPS, but loads other resources over an unencrypted connection. The following "passive" resource is loaded over HTTP. An attacker able to modify traffic could influence the application's appearance and behavior: http://piwik.qwikcast.tv/piwik.php?idsite=2

Request

```
GET /QwikCast/QwikCastEvent?eventKey=06f9ea1c-dd53-442c-ab8b-3f2e56e9d8c9 HTTP/1.1
Host: global.qwikcast.tv
Sec-Ch-Ua: "Chromium";v="97", " Not;A Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/97.0.4692.71 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applicatio
n/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Response

```
HTTP/1.1 200 OK
Cache-Control: public, no-store, max-age=0
Content-Length: 10159
Content-Type: text/html; charset=utf-8
Expires: Fri, 28 Jan 2022 17:35:58 GMT
Last-Modified: Fri, 28 Jan 2022 17:35:58 GMT
Vary: *
Server: Microsoft-IIS/10.0
customheader: value
X-Frame-Options: SAMEORIGIN
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: *
Access-Control-Allow-Methods: *
Set-Cookie:
ARRAffinity=327e34219519df25bedba7e0d77e23fac1d7c3ad5d9549029cf01e7a4117edac;Path=/;HttpOnly;
Secure;Domain=global.qwikcast.tv
Set-Cookie:
ARRAffinitySameSite=327e34219519df25bedba7e0d77e23fac1d7c3ad5d9549029cf01e7a4117edac;Path=/;
HttpOnly;SameSite=None;Secure;Domain=global.qwikcast.tv
Date: Fri, 28 Jan 2022 17:35:58 GMT
Connection: close
```

7.2. https://global.qwikcast.tv/QwikCast/QwikCastEventById

Summary
Severity: Low
Confidence: Certain
Host: https://global.qwikcast.tv
Path: /QwikCast/QwikCastEventById

Issue Detail
The response is loaded over HTTPS, but loads other resources over an unencrypted connection. The following "passive" resource is loaded over HTTP. An attacker able to modify traffic could influence the application's appearance and behavior: http://piwik.qwikcast.tv/piwik.php?idsite=2

Request

```
GET
/QwikCast/QwikCastEventById?eventKey=06f9ea1c-dd53-442c-ab8b-3f2e56e9d8c9&eventPageId=2833
HTTP/1.1
Host: global.qwikcast.tv
Cookie: qc4SessionId1275=1030260;
ARRAffinity=327e34219519df25bedba7e0d77e23fac1d7c3ad5d9549029cf01e7a4117edac;
ARRAffinitySameSite=327e34219519df25bedba7e0d77e23fac1d7c3ad5d9549029cf01e7a4117edac;
_ga=GA1.2.1788573453.1643391360; _gid=GA1.2.19972241.1643391360; _gat=1;
_pk_id.2.c6cf=4014f73af248e609.1643391360.1.1643391360.1643391360.; _pk_ses.2.c6cf=*;
.ASPXAUTH=175F2D521E5EABB48929639CA631AD5E02D2CC2050AA3D083074592FD3D864A4F09246
D5B1ECAF98E50D2D13B98AEA6678DCA50C66F3CB7D4A21F72748393DD41C170F398A2A91DB9DB09
A79BF209F54E6F0EBE779F5100C3B23AFB21A521AC5E70D920C3E367ED4B6EF542EDDFD366B0975
42E57A1DF6D674ECDB4650AD7FD6D1D40BFFBF2E198AEB2677692C82D5075C1448DB596F406765D
FD5F40A0F9A2F3A19BFDFF524CFB0E8AD4D0F116156A7358751845181E4461360EC6FD30DC3E2A0F
3EF5FB8C90FEC7DC8B3F9BE97F3467363ADC0C4F247F9E40985AB842CA2BE057201DA
Sec-Ch-Ua: "Chromium";v="97", " Not;A Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/97.0.4692.71 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applicatio
n/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer:
https://global.qwikcast.tv/QwikCast/QwikCastEvent?eventKey=06f9ea1c-dd53-442c-ab8b-3f2e56e9d8c9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Response

```
HTTP/1.1 200 OK
Cache-Control: public, no-store, max-age=0
Content-Length: 8686
Content-Type: text/html; charset=utf-8
Expires: Fri, 28 Jan 2022 17:36:15 GMT
Last-Modified: Fri, 28 Jan 2022 17:36:15 GMT
Vary: *
Server: Microsoft-IIS/10.0
customheader: value
X-Frame-Options: SAMEORIGIN
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: *
Access-Control-Allow-Methods: *
Date: Fri, 28 Jan 2022 17:36:15 GMT
Connection: close


<!DOCTYPE html>

<html lang="en" class="no-js" manifest="https://global.qwikcast.tv:443/QC4.manifest?eventPageId=2833"
style="background-color: #FFFFFF;">
<head>
<meta charset="utf-8" />
...[SNIP]...
<p><img src="http://piwik.qwikcast.tv/piwik.php?idsite=2" style="border:0;" alt="" /></p>
...[SNIP]...
```

7.3. https://global.qwikcast.tv/public/QwikCast/QwikCastEventById

Summary
Severity: Low
Confidence: Certain
Host: https://global.qwikcast.tv
Path: /public/QwikCast/QwikCastEventById

Issue Detail
The response is loaded over HTTPS, but loads other resources over an unencrypted connection. The following "passive" resource is loaded over HTTP. An attacker able to modify traffic could influence the application's appearance and behavior: http://piwik.qwikcast.tv/piwik.php?idsite=2

Request

```
GET
/public/QwikCast/QwikCastEventById?eventKey=06f9ea1c-dd53-442c-ab8b-3f2e56e9d8c9&eventPageId=2
834 HTTP/1.1
Host: global.qwikcast.tv
Cookie: ARRAffinity=327e34219519df25bedba7e0d77e23fac1d7c3ad5d9549029cf01e7a4117edac;
ARRAffinitySameSite=327e34219519df25bedba7e0d77e23fac1d7c3ad5d9549029cf01e7a4117edac;
_ga=GA1.2.1788573453.1643391360; _gid=GA1.2.19972241.1643391360; _gat=1; _pk_ses.2.c6cf=*;
.ASPXAUTH=175F2D521E5EABB48929639CA631AD5E02D2CC2050AA3D083074592FD3D864A4F09246
D5B1ECAF98E50D2D13B98AEA6678DCA50C66F3CB7D4A21F72748393DD41C170F398A2A91DB9DB09
A79BF209F54E6F0EBE779F5100C3B23AFB21A521AC5E70D920C3E367ED4B6EF542EDDFD366B0975
42E57A1DF6D674ECDB4650AD7FD6D1D40BFFBF2E198AEB2677692C82D5075C1448DB596F406765D
FD5F40A0F9A2F3A19BFDFF524CFB0E8AD4D0F116156A7358751845181E4461360EC6FD30DC3E2A0F
3EF5FB8C90FEC7DC8B3F9BE97F3467363ADC0C4F247F9E40985AB842CA2BE057201DA;
_pk_id.2.c6cf=4014f73af248e609.1643391360.1.1643391376.1643391360.
Sec-Ch-Ua: "Chromium";v="97", " Not;A Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/97.0.4692.71 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applicatio
n/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer:
https://global.qwikcast.tv/QwikCast/QwikCastEventById?eventKey=06f9ea1c-dd53-442c-ab8b-3f2e56e9d8c
9&eventPageId=2833
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Response

```
HTTP/1.1 200 OK
Cache-Control: public, no-store, max-age=0
Content-Length: 12258
Content-Type: text/html; charset=utf-8
Expires: Fri, 28 Jan 2022 17:36:22 GMT
Last-Modified: Fri, 28 Jan 2022 17:36:22 GMT
Vary: *
Server: Microsoft-IIS/10.0
customheader: value
X-Frame-Options: SAMEORIGIN
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: *
Access-Control-Allow-Methods: *
Date: Fri, 28 Jan 2022 17:36:22 GMT
Connection: close


<!DOCTYPE html>

<html lang="en" class="no-js" manifest="https://global.qwikcast.tv:443/QC4.manifest?eventPageId=2834"
style="background-color: #FFFFFF;">
<head>
<meta charset="utf-8" />
...[SNIP]...
<p><img src="http://piwik.qwikcast.tv/piwik.php?idsite=2" style="border:0;" alt="" /></p>
...[SNIP]...
```

5. Remediation

A. Retesting

CPG does offer free retesting up to 30 days after the completion and submission of the assessment and corresponding reports.

If the client has made any remediation attempts to fix the identified vulnerabilities outlined in the technical reports, CPG is able to retest the systems.

The client is responsible for contacting CPG for retesting services. If the client proceeds with retesting, CPG will schedule and then retest the previously tested systems for the client.

Once retesting is completed, CPG will confirm vulnerability status to the client.

6. Business Profile

A. Profile

The Cyber Protection Group was founded by a team with nearly two decades of Information Technology / Information Security experience. At Cyber Protection Group, technology is what we love. Because we enjoy what we do, we work with all types of clients. We have experience serving small businesses as well as enterprise level clients.

Our team has experience in all aspects of information security including defensive (intrusion detection), offensive (ethical hacking), network penetration testing, wireless security testing, application penetration testing, and vulnerability assessments.

Cyber Protection Group also brings years of PCI experience to provide you with GAP assessments, risk assessments, and an overall security assessment surrounding your network environment. Cyber Protection Group has the experience your company requires, but we are small enough that we can serve every single client on a personal level.

Cyber Protection Group is located in the countryside of Loysburg, in Central Pennsylvania. Due to the fact that Cyber Protection Group is not located in a large city, this company is competitive with their pricing and services. This allows Cyber Protection Group to bring top notch penetration testing to companies, municipalities and other entities for a fraction of the price of their competitors.