

BMM CERTIFICATION REPORT

BMM Certification Number:	GRE.CATE-OL_CB.1001.01.01
Certification Term / Expiration Date	1 year, 11/06/2026
Report Issue Date:	11 June 2025
Issued by:	BMM Spain Testlabs s.l.u. Edificio Vinson del Parque Empresarial Vallsolana Camí de Can Camps, 17-19 – 08174 Sant Cugat del Vallés, Barcelona
Compliance Tested By:	BMM Spain Testlabs s.l.u.
Client:	CT INTERACTIVE EOOD
Client address:	7 Kukush str. 1345, Sofia Bulgaria
Compliance Certification for:	Vulnerability assessment and penetration test
Certification product scheme:	BMM Certification Product Scheme v.2.5 CB-26 Certification Procedure v.2.3 EURSAM-SPA-MO-225_Penetration Testing v.1.1 EURSAM-SPA-MO-102_Vulnerability Assessment v.1.7
The product conforms to certification criteria stated, subject to conditions product listed in the product certification details section. This certificate is granted subject to BMM certification body's rules on product certification. Conformity to specified criteria does not warrant product performance not complete bug free operation.	



bmm spain testlabs, s.l.u.

Edificio Vinson del Parque Empresarial Vallsolana - Camí de Can Camps, 17-19

08174 Sant Cugat del Vallés Barcelona (España)

t +34 93 143 3862

business no. B64622251

BMM CERTIFICATION REPORT

1. CRITERIA CERTIFICATION

Technical Standards and/or Jurisdiction used for the Criteria Certification

Decision of the Minister of Finance number 79841 EΞ 2020 (B' 3266) entitled "Adoption of Regulation on the Technical Specification (TEP) for the Organization and Operation of online games of chance" published on 05/08/2020 article 18 h,l,j

Based on the above listed standards or applicable jurisdiction, the BMM Testlabs Certification Body grants certification of the following products:

- Penetration testing and vulnerability assessment for CT INTERACTIVE EOOD.

The expiration date of this certification is for **one year** in compliance with the Article 24 of the Chapter 8.IT Structure Security of the Decision No:79841_2020 - Adoption of Regulation on the Technical Specification (TEP) for the Organization and Operation of online games of chance.

2. COMPLIANCE CERTIFICATION DETAILS

The following assets were included in the external scope:

- 3.72.44.64
- 31.13.228.87
- cdn5-bg.ctrqs.com
- rgs1.ctrqs.com

All discovered vulnerabilities are ranked based upon likelihood and impact to determine overall risk. BMM ranking is based on CVSS v3.1.

CVSS base score range	CVSS Severity
0.0	Informative
0.1-3.9	Low
4-6.9	Medium
7.0-8.9	High
9.0-10.0	Critical

BMM CERTIFICATION REPORT

3. AUDITOR TEAM

The following members of BMM Testlabs have been involved in the audit:

Name	Matiss Vlasseman
Role	Junior Penetration Tester
Certificates	-
Experience	More than 2 years in cybersecurity

Name	Javier Boned
Role	Senior Security Analyst / Project Leader
Certificates	Offsec Certified Professional (OSCP), PCI ASV, Certified Red Team Operator (CRTO)
Experience	More than 4 years working in Cybersecurity and Penetration Testing.

Name	Sara Queipo
Role	Global Director of Security Services/ Certification Reviewer
Certificates	PCI ASV, CEH, CISA, 27001 Lead Auditor
Experience	More than 8 year working in iGaming related Cybersecurity and Penetration Testing.

Name	Julien Pottiez
Role	Supervisor / PCCC Member
Certificates	NCQ L2 electrotechnics studies
Experience	More than 50 security audits related to iGaming. More than 3 years of experience in iGaming Cybersecurity. More than 10 years of experience in Information System Engineering.

3. EXTERNAL ASSESSMENT PARTICIPANTS

Name	Role
Lachezar Petrov	CEO

BMM CERTIFICATION REPORT

4. BMM RESULTS

4.1. VULNERABILITIES SUMMARY

NAME OF VULNERABILITY	OCCURRENCES
Ext.M.1 - Vulnerable jQuery JavaScript dependency	1
Ext.M.2 - Session token in URL	1
Ext.L.1 - Strict Transport Security Misconfiguration	8
Ext.L.2 - SSL Certificate Cannot Be Trusted	1
Ext.L.3 - Potential TLS/SSL Timing Side-Channel Attacks (LUCKY13)	8
Ext.L.4 - Potential BREACH attack against HTTP compression	1
Ext.L.5 - Cross-origin resource sharing: arbitrary origin trusted	1
Ext.L.6 - Account screen name disclosed	1
Ext.L.7 - Cacheable HTTPS response	10
Ext.L.8 - Content Sniffing not disabled	8

4.2. BMM EVALUATION PERFORMED.

4.2.1. CRITICAL VULNERABILITIES

Extreme risk of security controls being compromised with the possibility of catastrophic financial losses occurring as a result.

No critical vulnerabilities have been identified.

4.2.2. HIGH VULNERABILITIES:

High risk of security controls being compromised with the potential for significant financial losses occurring as a result.

No high vulnerabilities have been identified.

4.2.3. MEDIUM VULNERABILITIES:

Medium risk of security controls being compromised with the potential for a likelihood to affect to the flow of the functionalities and, from here, to the impact of the business.

BMM CERTIFICATION REPORT

Ext.M.1 - Vulnerable jQuery JavaScript dependency	
Affected System:	cdn5-bg.ctrqs.com:443
CVSS:	6.1 (AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)
Description:	The JavaScript library jQuery has been detected. The version detected of this library has several vulnerabilities that can lead to cross site scripting (XSS) and prototype pollution. Some library vulnerabilities affect every application that imports that library, but others only affect applications that use certain features of the library. For some applications might be difficult to distinguish if the vulnerabilities affect to it or not. This library is used on the games hosted on the webapp.
Recommendation:	Update jQuery to its latest version or to a one without known vulnerabilities. Develop a patch-management strategy to ensure that security updates are promptly applied to all third-party libraries in your application. Also, consider reducing your attack surface by removing any libraries that are no longer in use.
References:	https://cwe.mitre.org/data/definitions/1104.html https://security.snyk.io/package/npm/jquery/2.2.4 https://owasp.org/www-project-top-ten/2017/A9_2017-Using_Components_with_Known_Vulnerabilities CVE-2019-11358, CVE-2020-11022, CVE-2020-11023
Additional Information:	Version detected by BMM: JQuery 2.2.4 Example affected paths: /html-20200413-stable/jquery-2.2.4.min.js
Remediation:	Yes, included in mitigation plan.

Ext.M.2 - Session token in URL	
Affected System:	cdn5-bg.ctrqs.com:443
CVSS:	5.3 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)
Description:	Sensitive information as session tokens 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. 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. It is also easier to inadvertently share the URL with the sensitive information with an accidental copy-paste or by sharing the URL in a social application. Also, URLs may also be displayed on-screen or bookmarked. In this case when a game is launched through palmsbet.com, a link with the game is generated with parameter in the URL including session token
Recommendation:	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.
References:	https://cwe.mitre.org/data/definitions/200.html https://cwe.mitre.org/data/definitions/384.html

BMM CERTIFICATION REPORT

Ext.M.2 - Session token in URL	
	https://cwe.mitre.org/data/definitions/598.html https://capec.mitre.org/data/definitions/593.html
Additional Information:	This issue was tested only on some games but according to the structure of the webapp, all the games launched through palmsbet.com include session token in URL Example affected paths: /html-20200413-stable/BookOfPower/app.html /html-20200413-stable/BrilliantsHot/app.html /html-20200413-stable/KingOfClovers/app.html /html-20200413-stable/KingOfClovers/app.html
Remediation:	Yes, included in mitigation plan.

4.2.4. LOW VULNERABILITIES:

Low risk of security controls being compromised with measurable negative impacts as a result.

Ext.L.1 - Strict Transport Security Misconfiguration	
Affected System:	31.13.228.87:443 cdn5-bg.ctrgs.com:443 rgs1.ctrgs.com:2053 rgs1.ctrgs.com:2083 rgs1.ctrgs.com:2087 rgs1.ctrgs.com:2096 rgs1.ctrgs.com:8443 rgs1.ctrgs.com:8020
CVSS:	3.7 (AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N)
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.
Recommendation:	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.
References:	https://github.com/moxie0/sslstrip https://hstspreload.org/ https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html
Additional Information:	This template identifies if the Strict-Transport-Security header is missing or misconfigured on a web server.
Remediation:	Yes, included in mitigation plan.

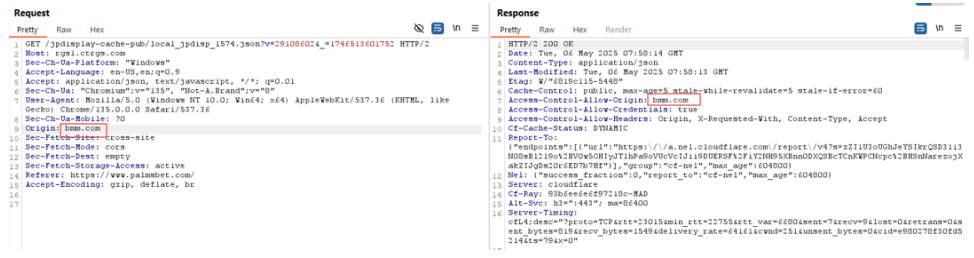
BMM CERTIFICATION REPORT

Ext.L.2 - SSL Certificate Cannot Be Trusted	
Affected System:	31.13.228.87:443
CVSS:	3.7 (AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N)
Description:	The issue occurs because the SSL certificate is issued for a hostname (e.g.,) but not for the IP address (e.g.,). During the security assessment, it was identified that the SSL/TLS certificate used by the application is not fully trusted. Specifically, the certificate is only valid for the hostname (e.g., cdn5-bg.ctrigs.com) but not for direct IP access (e.g., 31.13.228.87). This can lead to security warnings, failed HTTPS connections, when users attempt to access the site via IP instead of the hostname.
Recommendation:	Obtain a certificate that includes both the wild card domain and the IP address, if IP access is required, if not disable direct IP access.
References:	https://www.itu.int/rec/T-REC-X.509/en https://en.wikipedia.org/wiki/X.509
Additional Information:	N/A
Remediation:	No

Ext.L.3 - Potential TLS/SSL Timing Side-Channel Attacks (LUCKY13)	
Affected System:	31.13.228.87:443 cdn5-bg.ctrigs.com:443 rgs1.ctrigs.com:2053 rgs1.ctrigs.com:2083 rgs1.ctrigs.com:2087 rgs1.ctrigs.com:2096 rgs1.ctrigs.com:443 rgs1.ctrigs.com:8443
CVSS:	3.7 (AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N)
Description:	The SSL LUCKY13 is a cryptographic timing attack that can be used against implementations of the Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) protocols using the Cipher Block Chaining (CBC) mode of operation. This can also be considered a type of man-in-the-middle attack. The TLS protocol, the successor of the Secure Sockets Layer (SSL) protocol, provides privacy, data integrity, and secure traffic between communicating networks or applications. The vulnerability that makes the SSL LUCKY 13 possible affects the TLS 1.1 and 1.2 and DTLS 1.0 or 1.2 implementations. It also affects previous versions such as SSL 3.0 and TLS 1.0.
Recommendation:	Apply vendor patches or apply one of the following mitigation techniques: - Add random time delays - Switch to using RC4 cipher suites (not recommended by BMM) - Switch to authenticated encryption - Careful implementation of MEE-TLS-CBC decryption
References:	https://en.wikipedia.org/wiki/Lucky_Thirteen_attack https://crashtest-security.com/prevent-ssl-lucky13/
Additional Information:	N/A
Remediation:	No

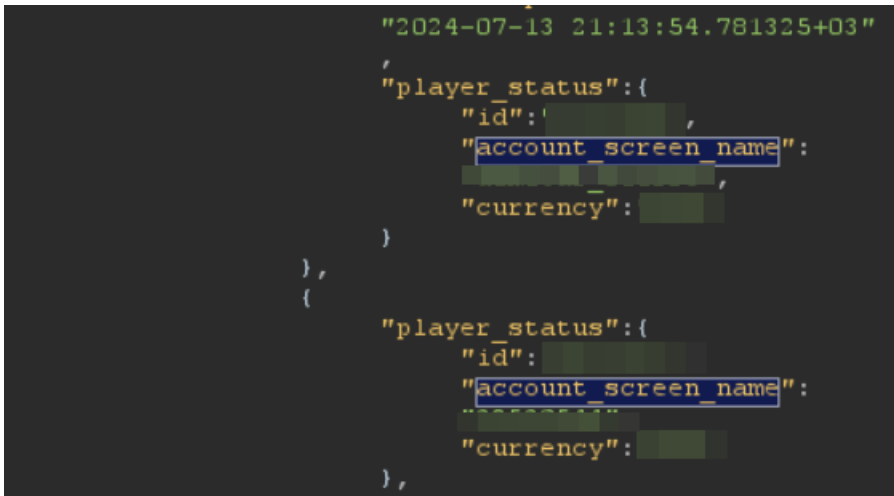
BMM CERTIFICATION REPORT

Ext.L.4 - Potential BREACH attack against HTTP compression	
Affected System:	rgs1.ctrigs.com:443
CVSS:	3.7 (AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N)
Description:	This vulnerability targets the compression ratio of HTTPS responses in TLS/SSL. By manipulating the size of compressed responses, an attacker can infer the content of encrypted data, potentially compromising sensitive information.
Recommendation:	Disable HTTP compression, implement randomized padding, separate secrets from user-controlled input, enable Strict Transport Security (HSTS), use encryption at the application level, keep software and libraries updated, and monitor for any suspicious activities.
References:	https://bugzilla.redhat.com/show_bug.cgi?id=995168 https://www.breachattack.com/ https://docs.digicert.com/en/certcentral/certificate-tools/discovery-user-guide/tls-ssl-endpoint-vulnerabilities/breach.html
Additional Information:	N/A
Remediation:	No

Ext.L.5 - Cross-origin resource sharing: arbitrary origin trusted	
Affected System:	rgs1.ctrigs.com:443
CVSS:	3.7 (AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N)
Description:	The application implements an HTML5 cross-origin resource sharing (CORS) policy for this request that allows access from any domain. The application allowed access from the requested origin http://evildomain.com If the application relies on network firewalls or other IP-based access controls, this policy is likely to present a security risk.
Recommendation:	Rather than using a wildcard or programmatically verifying supplied origins, use a whitelist of trusted domains.
References:	https://cwe.mitre.org/data/definitions/942.html https://portswigger.net/web-security/cors
Additional Information:	See evidence in the following screenshot:  Example affected paths: <code>/jpdisplay-cache-pub/local_jpdisp_1574.json</code> <code>/jpdisplay-cache-pub/local_jpdisp_24.json</code>

BMM CERTIFICATION REPORT

Ext.L.5 - Cross-origin resource sharing: arbitrary origin trusted	
	/jpdisplay-cache-pub/local_jpdisp_2764.json /pjpdisplay-cache-pub/local_pjpdisp_44_2265.json
Remediation:	No

Ext.L.6 - Account screen name disclosed	
Affected System:	rgs1.ctrgrs.com:443
CVSS:	3.7 (AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N)
Description:	Account name and one email address are disclosed into a .json file, this can be a security flaws as it can permit to an attacker to have an username list of the user on the platform for example to prepare a bruteforce attack.
Recommendation:	Restrict access of this information, remove it if not needed.
References:	https://portswigger.net/web-security/information-disclosure
Additional Information:	"account_screen_name" is line that display account name or email.  Example affected paths: /jpdisplay-cache-pub/local_jpdisp_1574.json
Remediation:	No

Ext.L.7 - Cacheable HTTPS response	
Affected System:	rgs1.ctrgrs.com:8020 rgs1.ctrgrs.com:2053 cdn5-bg.ctrgrs.com:80 rgs1.ctrgrs.com:2096 rgs1.ctrgrs.com:2087 rgs1.ctrgrs.com:2083 31.13.228.87:443 rgs1.ctrgrs.com:443 cdn5-bg.ctrgrs.com:443 31.13.228.87:80
CVSS:	3.3 (AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N)
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,

BMM CERTIFICATION REPORT

Ext.L.7 - Cacheable HTTPS response	
	then this may be retrieved by other users who have access to the same computer at a future time.
Recommendation:	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:	https://cwe.mitre.org/data/definitions/525.html https://cwe.mitre.org/data/definitions/524.html https://portswigger.net/web-security/information-disclosure
Additional Information:	N/A
Remediation:	No

Ext.L.8 - Content Sniffing not disabled	
Affected System:	rgs1.ctrgrs.com:2053 cdn5-bg.ctrgrs.com:80 rgs1.ctrgrs.com:2096 rgs1.ctrgrs.com:2087 rgs1.ctrgrs.com:2083 31.13.228.87:443 cdn5-bg.ctrgrs.com:443 31.13.228.87:80
CVSS:	3.1 (AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N)
Description:	There was no "X-Content-Type-Options" HTTP header with the value nosniff set in the response. The lack of this header causes that, certain browsers, try to determine the content type and encoding of the response even when these properties are defined correctly. This can make the web application vulnerable against Cross-Site Scripting (XSS) attacks. E.g., the Internet Explorer and Safari treat responses with the content type text/plain as HTML, if they contain HTML tags.
Recommendation:	Set the following HTTP header at least in all responses which contain user input: - X-Content-Type-Options: nosniff
References:	https://developer.mozilla.org/es/docs/Web/HTTP/Headers/X-Content-Type-Options
Additional Information:	N/A
Remediation:	Yes, included in mitigation plan.

4.2.5. REMEDIATION PLAN

Ext.M.1 - Vulnerable jQuery JavaScript dependency:

- This vulnerability has been sent to the frontend team to replace the vulnerable jQuery version with newer non-vulnerable version.
- DATE FOR FIX: 2025-10-01

BMM CERTIFICATION REPORT

Ext.M.2 - Session token in URL:

- The session token found in URL will be fixed by transmitting this sensitive information in HTTP cookie.
- DATE FOR FIX: 2025-10-01

Ext.L.1 - Strict Transport Security Misconfiguration

- Client is going to add HTTP header Strict-Transport-Security "max-age=63072000; includeSubDomains; preload" to the specified domains and ports.
- DATE FOR FIX: 15-07-2025

Ext.L.8 - Content Sniffing not disabled

- Client is going to add HTTP header X-Content-Type-Options "nosniff" to the specified domains and ports.
- DATE FOR FIX: 15-07-2025

5. TERMS AND CONDITIONS

Client shall not use or make reference of the BMM Certification or refer to BMM in any manner, in advertising, promotional, or other material that implies endorsement or approval of any Product by BMM beyond a determination of compliance with the certified Technical Standards. Client shall not use or make reference to its Product certification in such a manner as to bring BMM into disrepute and shall not make any statement regarding its certification which BMM may consider misleading or unauthorized. Client shall only use or make reference to the certification to indicate the Product certified is in conformity with the specified Certification Technical Standards.

Client must not use under any circumstances the ENAC accreditation mark.

If Client applies the certification to Products that do not comply with the certification Technical Standards or otherwise uses the Certification not in accordance with this Agreement, Client acknowledges that this certification may be withdrawn or suspended by BMM.

Client shall upon suspension or withdrawal of certification, discontinue its use of all advertising material that contains reference to the certification.

If the Certification Technical Standards for a Product are modified, BMM shall notify the Client of the date beyond which the Certification may no longer be applied to the Product in the absence of recertification of the Product to the modified Certified Technical Standards.

In instances where certification documentation will be distributed, Client agrees to reproduce certification documentation only in its entirety.

Please feel free to contact BMM Testlabs if you have any questions in regards to this certification report.

Yours sincerely,

PCCC Member:

Julien Pottiez

VP Security Services