Duke Clinical Research Institute

Cyber Application Security Testing Team

PENETRATION TEST

Application Name: Collective 4.0

Penetration Test Report

February 1, 2023

DCRI performs periodic testing of their applications that store or transmit confidential customer data. To fulfill these requirements the Information Security Team performs regularly scheduled Security Testing of DCRI applications.

The private and intellectual information contained herein are exclusively owned by DCRI and therefore should not be disclosed to anyone that is not authorized or that does not have a specific business need to know of this information. When in doubt or when dealing with third party non DCRI business partners contact DCRI Information Security for assistance, and remember to always utilize secure transport methods when communicating confidential information.

Table of Contents

Document History

Paper copies are valid only on the day that they are printed. Contact the author if you are in any doubt about the accuracy of this document.

Revision History

Version	Date	Author/Reviewer	Change
1.	2/1/2023	Charles Baxter	Final Report

1 Executive Summary

The DCRI Cyber Security Testing Team performed a two week Penetration Test against the Collective 4.0 web application beginning on January 19, 2023 through February 1, 2023. We analyzed the web application and its' dependencies and identified three Medium security issues associated with the Collective 4.0 application residing in the DCRI Test Environment environment. The results of this security test and the risk findings are depicted in (*Figure 1*) below from the highest to the lowest severity ratings.

1.1 Qualitative Vulnerability Statistics

This section provides a qualitative representation of the security issue finding (s) for this particular Penetration Test .

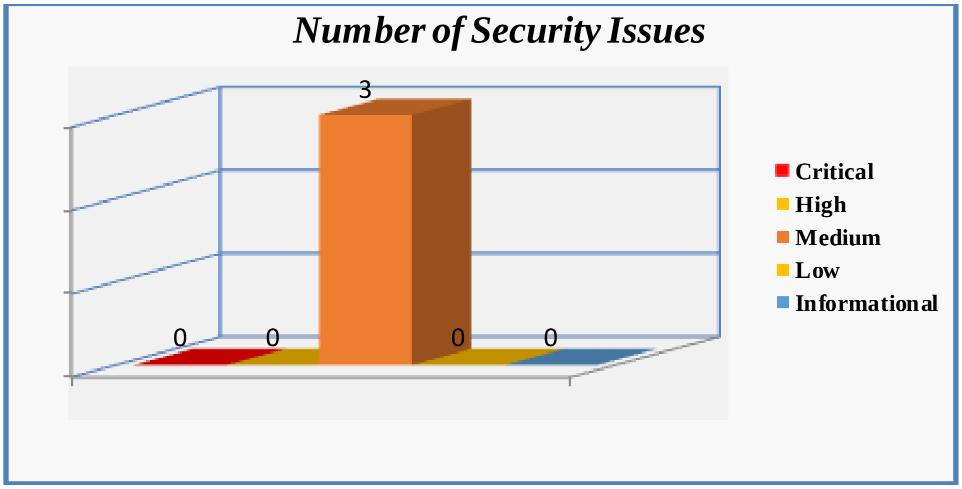
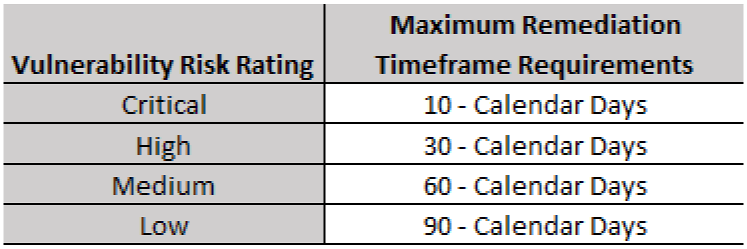


Figure 1 ***DCRI Test Environment***

Best practices advise that remediation of higher level issues often resolve lower level security issues. Therefore, we recommend that you consider this practice when determining the priority in which to address or remediate any security issues. Other consideration for prioritizing vulnerability remediation efforts is that it is a DCRI requirement that all critical, high, and medium level risks are addressed and either remediated or mitigated.

2 Vulnerability Analysis

This section provides analysis and remediation recommendations for the vulnerabilities identified during the Penetration Test performed on the Collective 4.0 application. Risk ratings are derived by utilizing the National Vulnerability Databases' Common Vulnerability Scoring System Version 3.1 (CVSSv3.1) Calculator found at this link. The high level security issues should be addressed as soon as possible, while any Low and Informational Risk items should be considered for increased security and implemented if they can be feasibly performed.



Vulnerability Risk Rating	Maximum Remediation Timeframe Requirements
Critical	10 - Calendar Days
High	30 - Calendar Days
Medium	60 - Calendar Days
Low	90 - Calendar Days

Remediation tasks with identical priority numbers may be performed simultaneously or as separate events. Remediation feedback should be communicated with Information Security at least one week subsequent to receipt of this report. Information Security will validate the remediation once fixes have been implemented and report the follow up findings. If the remediation testing is successful the particular item(s) will be appropriately recorded with a closure date.

2.1 *Vulnerability Finding:* Cross-domain Referer Leakage

Vulnerability Category *OWASP Top Ten***:** A5. Security Misconfiguration

References # (s)	CWE-200

Technical Analysis

Exposure	*Host / Path*	*Severity Level*
Internet	**https://radxup-cde-dev.duhs.duke.edu/**	**Medium**

Security Analysis

The page was loaded from a URL containing a query string:

- https://radxup-cde-test.duhs.duke.edu/

The response contains the following link to another domain:

- https://radx-up.org/colectiv/

Remediation

Priority	*Recommendation* (s)	*Remediation Timeframe*
1	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.	60 Days (Medium)

2.2 *Vulnerability Finding:* Cacheable HTTPS Response

Vulnerability Category OWASP Top Ten: A5. Security Misconfiguration

References # (s)	CWE-524, CWE-525

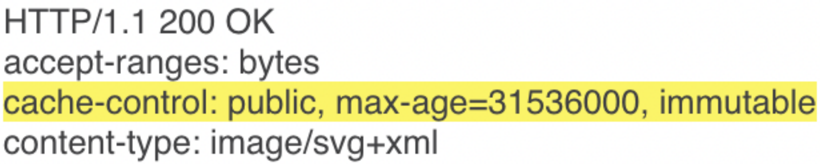
Technical Analysis

Exposure	*Host / Path*	*Severity Level*
Internet	**https://radxup-cde-dev.duhs.duke.edu /_next/static/media/logoWatermark.b4c86413.svg**	**Medium**

Security Analysis

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.

Applications should return caching directives instructing browsers not to store local copies of any sensitive data.



```
HTTP/1.1 200 OK
accept-ranges: bytes
cache-control: public, max-age=31536000, immutable
content-type: image/svg+xml
```

Remediation

Priority	*Recommendation* (s)	*Remediation Timeframe*
2	The web server should return the following HTTP headers in all responses containing sensitive content: • Cache-control: no-store • Pragma: no-cache	60 Days (Medium)

2.3 *Vulnerability Finding:* Frameable response (potential Clickjacking)

Vulnerability Category *OWASP Top Ten***:** A5. Security Misconfiguration

References # (s)	CWE-524, CWE-525

Technical Analysis

Exposure	*Host / Path*	*Severity Level*
Internet	**https://radxup-cde-dev.duhs.duke.edu**	**Medium**

Security Analysis

3 instances of this issue were identified, at the following locations:

- /
- /library-management
- /login

If a page fails to set an appropriate X-Frame-Options or Content-Security-Policy HTTP header, it might be possible for a page controlled by an attacker to load it within an iframe. This may enable a clickjacking attack, in which the attacker's page overlays the target application's interface with a different interface provided by the attacker.

Remediation

Priority	*Recommendation* (s)	*Remediation Timeframe*
3	To effectively prevent framing attacks, the application should return a response header with the name **X-Frame-Options** and the value **DENY** to prevent framing altogether, or the value **SAMEORIGIN** to allow framing only by pages on the same origin as the response itself.	60 Days (Medium)

3 Conclusions

The Penetration Test conducted against the Collective 4.0 web application performed by the DCRI Cyber Security Testing Team beginning on January 19, 2023 identified three Medium risk security issues.

The Cyber Security Testing Team recommends remediation of the highest issue firsts, as they tend to be more well known, and when fixed often reduces the risk of other lower level security issues.