\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[MAXIMUS logo](https://www.maximus.com/)

**Unit Test Case: CCO\_eCoaching\_Log\_Netsparker\_Findings\_Fix**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Prepared by: | Lili Huang |  | Date: | 8/11/2021 |
| Department / Location: |  |  |  |  |
| Approved by: |  |  | Date: |  |

**Change History Log**

| **Date** | **Change Description** | **Author** |
| --- | --- | --- |
| 8/11/2021 | TFS 22643 - eCoaching - resolve findings from security scan | Lili Huang |

|  |  |
| --- | --- |
| 1. PROJECT NAME: | eCoaching Log |
| 2. UNIT IDENTIFIER: | Web – Netsparker Findings Fix |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Test Case ID** | **Test Data Setup** | **Action** | **Expected Result** | **Pass/Fail** | **Netsparker Finding** |
| Wnff-1 |  | Launch eCL web app;  <https://uvaadadweb50cco.ad.local/ecl_dev/> | Response header contains the following:  Set-Cookie: ASP.NET\_SessionId=k2qlo0ltiartnjexlrvepr0j; path=/; **secure**; HttpOnly; SameSite=Lax | P | *1. Session Cookie Not Marked as Secure* |
| Wnff-2 |  | Launch eCL web app;  <http://uvaadadweb50cco.ad.local/ecl_dev/> | Redirected to https:  <https://uvaadadweb50cco.ad.local/ecl_dev/> | P | *2. Insecure HTTP Usage* |
| Wnff-3 |  | Same as Wnff-1 | *Szabo is working with Maximus Corporate on this because it is controlled by group policy* |  | *3. Insecure Transportation Security Protocol Supported (TLS 1.0)* |
| Wnff-4 |  | Same as Wnff-1 | The following is excluded in Response header:  **X-AspNetMvc-Version: 5.0** | P | *4. Version Disclosure (ASP.NET MVC)* |
| Wnff-5 |  | Same as Wnff-1 | The following is excluded in Response header:  **X-AspNet-Version: 4.0.30319** | P | *5. Version Disclosure (ASP.NET)* |
| Wnff-6 |  | Same as Wnff-1 | The following is excluded in Response header:  **Server: Microsoft-IIS/10.0** | P | *6. Version Disclosure (IIS)* |
| Wnff-7 |  | Same as Wnff-1 | Response header contains the following:  **Expect-CT: enforce, max-age=300, report-uri='https://UVAADADWEB50CCO.ad.local/ecl\_dev/'** | P | *7. Expect-CT Not Enabled* |
| Wnff-8 |  | Same as Wnff-1 | *Szabo is working with Maximus Corporate on this because it is controlled by group policy* |  | *8. Insecure Transportation Security Protocol*  *Supported (TLS 1.1)* |
| Wnff-9 |  | Same as Wnff-1 | Response header contains the following:  **X-XSS-Protection: 1** | P | *9. Missing X-XSS-Protection Header* |
| Wnff-10 |  | Same as Wnff-1 | The following is excluded in Response header:  **X-Powered-By: ASP.NET** | P | *10. ASP.NET Identified* |
| Wnff-11 |  |  | *Leave as it is.* |  | *11. Authorization Required* |
| Wnff-12 |  | Same as Wnff-2 | Same as Wnff-2. | P | *12. HTTP Strict Transport Security (HSTS) via*  *HTTP* |
| Wnff-13 |  | Same as Wnff-1 | Same as Wnff-6. | P | *13. IIS Identified* |
| Wnff-14 |  | Same as Wnff-1 | OPTIONS is disabled. | P | *14. OPTIONS Method Enabled* |

**Name of tester:** Lili Huang

**Date completed:** 08/11/2021