ENPM809W - Introduction to Secure Coding

Lab - 11 – Fix Lab – Secure Deployment

Author: Syed Mohammad Ibrahim
UID: iamibi
Email: iamibi@umd.edu

Phase 1: Debug Code

a) Provide the URL of the WebGoat.NET application page where you are exercising the question. Do not include any query parameters or any other special characters in the answer.

NA

b) Provide the CWE-ID, Filename, Line Number of the weakness identified based on the question.

CWE-ID(s):
- CWE-489: Active Debug Code
- CWE-532: Insertion of Sensitive Information into Log File

Filename(s) & Line Number:
- WebGoat/App_Code/Settings.cs – 41,42
- WebGoat/App_Code/Util.cs - 67
- WebGoat/App_Code/WeakMessageDigest.cs – 26, 27
- WebGoat/WebGoatCoins/ChangePassword.aspx.cs – 31-34, 38-41
- WebGoat/WebGoatCoins/CustomerLogin.aspx.cs – 37, 40-46
- WebGoat/WebGoatCoins/Orders.aspx.cs – 24, 63-66

c) For the given identified weakness in the previous step, describe how you intend to fix the weakness. This can be as detailed as possible to explain how it will address the weakness.

The intended fix is to remove all the debug logs and debug control flows from the codebase.

d) Describe why your intended fix will address the weakness (either directly or indirectly) and whether to your knowledge it will prevent future attacks. This can be as detailed as possible to explain why it will address the weakness.

The fix will make sure that the application is production ready with no debug code present in it. This will also avoid any arbitrary code execution or DOS based attacks even if an attacker tries to disassemble the binary and try to reverse engineer it. The logs removed will make sure that no DOS attack takes place.

e) List all the paths with filenames you are changing to implement the fix for the weakness.
Filename(s) & Line Number:
- WebGoat/App_Code/Settings.cs
- WebGoat/App_Code/Util.cs
- WebGoat/App_Code/WeakMessageDigest.cs
- WebGoat/WebGoatCoins/ChangePassword.aspx.cs
- WebGoat/WebGoatCoins/CustomerLogin.aspx.cs
- WebGoat/WebGoatCoins/Orders.aspx.cs

f) Commit ID: 011441cbb1e93d38c64d9d0dbf37ebea7abc5b89

Phase 2: Debug Logging

a) Provide the URL of the WebGoat.NET application page where you are exercising the question. Do not include any query parameters or any other special characters in the answer.

http://localhost:52251/Content/LogInjection.aspx

b) Provide the CWE-ID, Filename, Line Number of the weakness identified based on the question.

CWE-ID(s):
- CWE-1295: Debug Messages Revealing Unnecessary Information
- CWE-532: Insertion of Sensitive Information into Log File

Filename & Line Number:
- WebGoat/Content/LogInjection.aspx.cs – 25, 26

c) For the given identified weakness in the previous step, describe how you intend to fix the weakness. This can be as detailed as possible to explain how it will address the weakness.

Remove the log from the functionality of the page.

d) Describe why your intended fix will address the weakness (either directly or indirectly) and whether to your knowledge it will prevent future attacks. This can be as detailed as possible to explain why it will address the weakness.

The fix makes sure that no sensitive information is passed on to logs and that an attacker doesn't flood the log system with irrelevant messages in any form of DoS based attack that may take up memory of the server.

e) List all the paths with filenames you are changing to implement the fix for the weakness.

- WebGoat/Content/LogInjection.aspx.cs

f) Commit ID: 7b141d3976de10acf62c97789a302b982d8d34c5

Phase 3: Release Build

a) Provide the URL of the WebGoat.NET application page where you are exercising the question. Do not include any query parameters or any other special characters in the answer.

NA

b) Provide the CWE-ID, Filename, Line Number of the weakness identified based on the question.

NA

c) For the given identified weakness in the previous step, describe how you intend to fix the weakness. This can be as detailed as possible to explain how it will address the weakness.

NA

d) Describe why your intended fix will address the weakness (either directly or indirectly) and whether to your knowledge it will prevent future attacks. This can be as detailed as possible to explain why it will address the weakness.

NA

e) List all the paths with filenames you are changing to implement the fix for the weakness.

- WebGoat/Resources/Master-Pages/Site.Master
- WebGoat/Global.asax.cs
- WebGoat/Web.config

f) Commit ID: c7b129be84e01a8627ae21d42248e4ec357beea6