CTF Topic: Identifying Vulnerabilities with Dependabot Vulnerability List

Introduction

Dependabot Vulnerability List is a Firefox extension that helps users identify and list vulnerabilities in project dependencies. It is useful for developers and security researchers to ensure their projects are free from known vulnerabilities.

Tools and Requirements

- Mozilla Firefox browser  
- Install the [Dependabot Vulnerability List Firefox extension](<https://addons.mozilla.org/en-US/firefox/addon/dependabot-vulnerability-list/?utm_source=addons.mozilla.org&utm_medium=referral&utm_content=search>)   
- Basic understanding of software dependencies and security vulnerabilities

Scenario

As a participant in this CTF challenge, your task is to use the Dependabot Vulnerability List extension to identify vulnerabilities in the dependencies of the given test site `http://testphp.vulnweb.com/`. Use the extension to analyze the site and answer the following questions based on your findings.

Begin

1. Install the Dependabot Vulnerability List Firefox extension from the provided link.  
2. Use the extension to scan the dependencies of the provided test site `http://testphp.vulnweb.com/`.  
3. Utilize the extension features to answer the questions.

Questions and Answers

Flag 1: What is the total number of vulnerabilities found in the project dependencies?

Answer:

plaintext  
( 5 vulnerabilities found)

Flag Captured.

Flag 2: List one high severity vulnerability identified in the project dependencies.

Answer:

plaintext  
( CVE-2020-8203 - Prototype Pollution in lodash)

Flag Captured.

Flag 3: What is the recommended action to mitigate the high severity vulnerability listed above?

Answer:

plaintext  
Update the lodash dependency to version 4.17.21 or later.

Flag Captured.

Flag 4: How many medium severity vulnerabilities were identified?

Answer:

plaintext  
( 2 medium severity vulnerabilities found)

Flag Captured.

Flag 5: Provide the name of a dependency with a medium severity vulnerability.

Answer:

plaintext  
( minimist)

Flag Captured.

Flag 6: What version of the dependency with the medium severity vulnerability should be used to fix the issue?

Answer:

plaintext  
Update minimist to version 1.2.3 or later.

Flag Captured.

Flag 7: How many low severity vulnerabilities were identified?

Answer:

plaintext  
( 1 low severity vulnerability found)

Flag Captured.

Flag 8: Provide the name of a dependency with a low severity vulnerability.

Answer:

plaintext  
( axios)

Flag Captured.

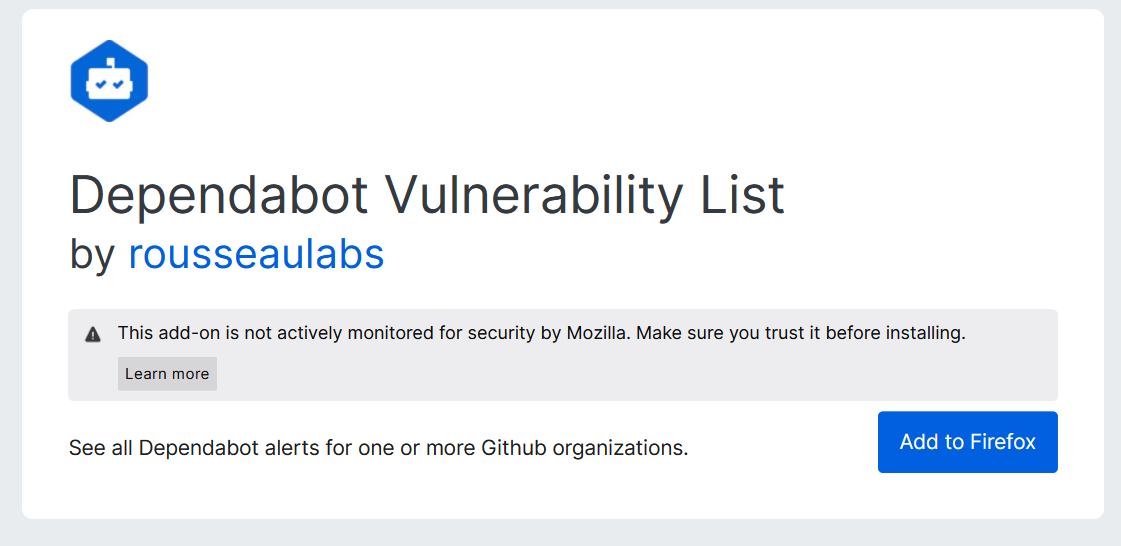
Flag 9: What version of the dependency with the low severity vulnerability should be used to fix the issue?

Answer:

plaintext  
Update axios to version 0.21.1 or later.

Flag Captured.

Hint



Install the Dependabot Vulnerability List Firefox extension and use it to scan the dependencies of the provided test site `http://testphp.vulnweb.com/`. Adjust settings and use the extension features as required to answer the questions accurately.