CTF Topic: Vulnerabilities with Dorkish



Introduction



Dorkish is a Firefox extension that helps in using Google Dorks to find potential vulnerabilities and sensitive information exposed on websites. Google Dorks are advanced search queries used to locate specific types of information or vulnerabilities on the internet. Participants will use this extension to discover vulnerabilities on the test site `http://testphp.vulnweb.com/`.

Tools and Requirements

- Mozilla Firefox browser  
- Install the [Dorkish Firefox extension](<https://addons.mozilla.org/en-US/firefox/addon/dorkish/?utm_source=addons.mozilla.org&utm_medium=referral&utm_content=search>)   
- Basic understanding of Google Dorks and web vulnerabilities

Scenario



As a participant in this CTF challenge, your task is to use the Dorkish extension to identify potential vulnerabilities on the provided test site `http://testphp.vulnweb.com /`. Use Google Dorks via the extension to analyze the site and answer the following questions based on your findings.

Steps

1. Install the Dorkish Firefox Extension  
   - Open Mozilla Firefox.  
   - Go to the [Dorkish Firefox extension](<https://addons.mozilla.org/en-US/firefox/addon/dorkish/?utm_source=addons.mozilla.org&utm_medium=referral&utm_content=search>) link.  
   - Click "Add to Firefox" and complete the installation process.

2. Open the Test Site  
   - Navigate to the test site: <http://testphp.vulnweb.com/>

3. Use Dorkish to Perform Google Dorks Search  
   - Open the Dorkish extension from the Firefox toolbar.  
   - Enter relevant Google Dorks queries to search for potential vulnerabilities and sensitive information on the test site. For example, `site:testphp.vulnweb.com filetype:php` or `site:testphp.vulnweb.com inurl:admin`.

4. Analyze the Results  
   - Review the search results provided by Google Dorks.  
   - Identify potential vulnerabilities or sensitive information exposed on the site.

5. Answer the Questions  
   - Use the information from the search results to answer the following questions.

Questions and Answers

Flag 1: What files can be found using the Google Dork `site:testphp.vulnweb.com filetype:php`?

Answer:

Flag Captured. PHP Version 5.1.6 file can be Found .

Flag 2: What does the Google Dork `site:testphp.vulnweb.com ext:sql` reveal?

Answer: No Result Were Found.

Flag Captured.

Hint

Install the Dorkish Firefox extension and use it to perform Google Dorks searches on the provided test site `<http://testphp.vulnweb.com/>` . Adjust your queries to discover different types of vulnerabilities and sensitive information.

A screenshot of a computer

Description automatically generated





