## Using Hashcat to Target testphp.vulnweb.com



**Objective:**

This document aims to demonstrate the use of Hashcat and John the Ripper, industry-standard tools, in the context of password cracking. The procedure will be carried out against a known vulnerable website.

**Target:**

testphp.vulnweb.com

**Tools:**

* Hashcat
* Standard web browser with developer tools

**Procedure:**

1. **Password Hash Identification:**
   * Employ a web browser to navigate to the designated website: testphp.vulnweb.com.
   * Identify a page that implements user authentication. A typical example is a login page.
   * Utilize the browser's developer tools. These tools are commonly accessed by pressing the F12 key. The developer tools will be used to inspect network traffic. Specifically, the process involves submitting a login form with a known username (e.g., "testuser") and an intentionally incorrect password.
   * Examine the network request generated by the login attempt.
   * Within the request data, locate the password. It is expected that the password will not be in plaintext but rather in a hashed format.
   * Copy the password hash. The hash is typically a long string of seemingly random characters.
2. **Hash Preparation for Cracking:**
   * Create a plain text file. For organizational purposes, this file may be named "hash.txt". Paste the copied password hash into this file.
   * It is crucial to ensure that the text file contains only the hash string and no extraneous characters or formatting.
3. **Password Cracking with Hashcat:**
   * Open a terminal or command prompt.
   * Execute the following Hashcat command:  
     hashcat -m <hash\_type> hash.txt <wordlist\_path>  
     + Replace the placeholder <hash\_type> with the appropriate Hashcat hash mode identifier.
     + Replace <wordlist\_path> with the correct path to a wordlist file. A wordlist is a text file containing a collection of potential passwords. A commonly used wordlist is "rockyou.txt," which is often found in penetration testing distributions.
   * If Hashcat successfully cracks the hash, the corresponding plaintext password will be displayed on the terminal.

**Important Considerations:**

* **Wordlist Quality and Size:** The efficacy of password cracking is directly related to the quality and size of the wordlist employed. A more extensive and comprehensive wordlist increases the probability of finding the correct password but also increases the processing time.
* **Hash Type Identification:** Accurate identification of the hash type is paramount. If an incorrect hash type is specified, the cracking process will fail.
* **Rules:** Both Hashcat and John the Ripper support the use of rules. Rules are sets of transformations applied to words from the wordlist (e.g., converting words to uppercase, appending numerical characters). The application of rules can significantly enhance the effectiveness of a cracking attack.
* **Time Considerations:** Password cracking can be a time-intensive process. The duration depends on several factors, including the complexity of the password, the hash type, the size of the wordlist, and the computational resources available.
* **Ethical and Legal Use:** It is imperative to emphasize that password cracking should only be conducted with explicit and unequivocal authorization. Unauthorized attempts to crack passwords on systems or networks are illegal and unethical. The testphp.vulnweb.com website is provided solely for authorized security testing and educational purposes.