Ethical Hacker 9 – Password cracking

* **What is password cracking?**

Password cracking is the process of recovering passwordsfrom data that has been stored in or transmitted by a computer system in scrambled form. A common approach (brute-force attack) is to repeatedly try guesses for the password and to check them against an available cryptographic hash of the password or a list of passwords.

* **How does password cracking work?**

I began by logging in on DVWA and went to the **Brute Force** page. I typed my username and a wrong password on purpose, then pressed the submit button. After this, I opened Burp Suite and went to the proxy tab.

I looked at the request and response for this specific request and sent this line to the intruder:

A screenshot of a computer

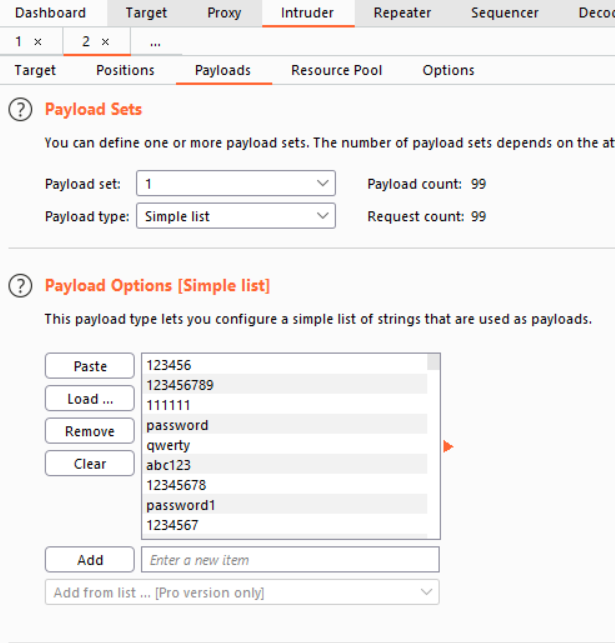
Description automatically generated

Adding a payload marker on the password field:

Graphical user interface, text, application, email

Description automatically generated

Adding the most common 100 passwords on the simple list:



I went back to DVWA and intentionally typed a wrong password so I can copy the message received.

A screenshot of a computer

Description automatically generated

I have pasted the message in the grep section so that the incorrect passwords, which will generate this message, will be flagged:Graphical user interface, text, application

Description automatically generated

I then went to the attack section, with this part automatically filled in, and began the attack.

Graphical user interface

Description automatically generated with medium confidence

The attack tries all the passwords, and if the **Username and/or password incorrect** is displayed, the box will be ticked. The only unchecked password in this case will be the correct one.

Table

Description automatically generated

There are many alternatives to this. For instance, the message generated by typing the correct password can be copied and pasted, and then only the correct password will be checked.

* **Give examples of famous password cracking attacks.**

On June 5th, 2012, LinkedIn has been hacked and the passwords for nearly 6.5 million user accounts have been stolen by cyber criminals. As a result, a United States grand jury indicted Nikulin and three unnamed co-conspirators on charges of aggravated identity theft and computer intrusion.

In 2013, Tumblr has been attacked by hackers. 65,469,298 unique emails and passwords were leaked from Tumblr. The data breach's legitimacy is confirmed by computer security researcher Troy Hunt.

* **How to make password cracking harder for an attacker?**

The easiest way to make password cracking harder for an attacker is to use a long password which contains lowercase and uppercase letters, numbers, and special characters. This makes the password cracking process extremely lengthy and difficult.

* **Resources**
* [**https://en.wikipedia.org/wiki/Password\_cracking**](https://en.wikipedia.org/wiki/Password_cracking)
* [**https://en.wikipedia.org/wiki/List\_of\_security\_hacking\_incidents**](https://en.wikipedia.org/wiki/List_of_security_hacking_incidents)