*www.Soda-Machines.com*

Analysis of Password Cracking Attacks.

**Jack Napolitano**

**Abstract.** Security is extremely important in the protection of data and performance of certain services. Soda-Machines.com provides customers with a source for information in the field of vintage soda antiquities. We will see what steps Soda-Machines.com takes to provide their customers with maximum security.

1. Introduction

Security is receiving more and more attention today due to the advancement in technology and mass amounts of data that is stored online. Although Soda-Machines.com does not provide a service that would cause major problems if taken down by an attack, it could be a major weakness in protecting user's data. Soda-machines.com is a fairly low traffic not well know website. Due to this, it may not have the advancements in security other popular websites do. The main concern here in that people may be using their same email and password on Soda-Machines.com as they are on more critical websites, say their banking site. If the information is compromised on Soda-Machines.com, they could be putting their users at risk and putting themselves at risk legally.

2. Password Cracking

Password cracking has become more prevalent in the modern computing era. With the power of machines increasing, the ability to test millions of passwords becomes less of a challenge. Programs like John The Ripper use many different techniques to crack passwords faster than ever. Rather than actually trying to crack users passwords, I tested to see if the website would be vulnerable to these password cracking techniques or if they take any measures to prevent such an attack.

3. Approach

To test whether Soda-Machines.com takes precautions against brute-force password cracking attacks, I wrote a simple Selenium IDE test (found on github). pwTest.html is a test case which makes use of Selenium IDE's ability to add extensions which allow for while loops within the test. The extension sideflow.js gave me the ability to loop over a login attempt and by creating a simple file containing passwords in a list (credentials.js), I was able to sit back and watch as Selenium entered password after password. Although my test was simple an only iterated 11 times until it hit the right password, it revealed some major security holes in Soda-Machines.com's login process. There was nothing stopping my program from entering as many passwords as I wanted, which, if taken advantage of by a malicious user, could prove to be bad.

4. Results

Through the tests that were run, it is apparent that no measures were being taken to prevent against brute-force login attempts. This is a huge risk for Soda-Machines.com and I would recommend implementing some, if not all, of the following measures.

1. Locking out account.
   1. Simply block an account or IP address from trying to log in after failing to enter a correct password after a number of times.
2. Adding captcha field
   1. Make the user enter a captcha field that is difficult for a program to be able to do.
3. Adding a timer between login attempts.
   1. Make the user wait for 60 seconds between login attempts. This will kill brute-force performance and make it not worth attacking.

5. Conclusion

Currently, Soda-Machines.com suffers from critical faults in the prevention of brute-force password cracking attacks. However, due to their small footprint in terms of popularity, they should not be overly concerned with attacks. That being said, with the simple implementation of some of the countermeasures seen above, security on Soda-Machines.com will significantly increase.