**BRUTE FORCE**

Password cracking is the process of recovering passwords from data that has been stored in or transmitted by a computer system. A common approach is to repeatedly try guesses for the password.

Users often choose weak passwords. Examples of insecure choices include single words found in dictionaries, given and family names, any too short password (usually thought to be 6 or 7 characters or less), or any password meeting a too restrictive and so predictable, pattern (eg, alternating vowels and consonants).

A last resort is to try every possible password, known as a brute force attack. In theory, if there is no limit to the number of attempts, a brute force attack will always be successful since the rules for acceptable passwords must be publicly known; but as the length of the password increases, so does the number of possible passwords.

**Description**

Brute force attack is the type of attack in which the concept of trial and error is used by the hacker to figure out the user login credentials. DVWA is subject to the brute force attack which can be done with the help of a tool name burp suite which can intercept the request by integrating with the web browser and further use payloads to input the list.

**Impact:**

An attacker can take over the victim’s account by finding the correct username and password through brute force.

**Prevention:**

1. Limit login fail Attempts – This must be initiated so that anyone attempting brute force can be stopped after 2-3 failed attempts.
2. Monitor server Logs – Be sure to monitor the Logs because an attacker will make many attempts using different ways to get into your data.
3. Send alert on email for each login attempt and turn on 2fa, so that even if password is cracked, OTP is needed for login.

**LOW**

**Steps to reproduce:**

1. Configure your web browser and burp suite.
2. Go to the dvwa page and enter the random credentials.
3. Now capture the request in the tool like burp suite.
4. Brute force the username and password parameter.
5. Correct username and password will show http status ‘200’ and length ‘4948’.

**Vulnerable request:**

GET /dvwa/vulnerabilities/brute/?username=XXXXXX&password=XXXXXX&Login=Login HTTP/1.1

Host: 192.168.80.130

User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:78.0) Gecko/20100101 Firefox/78.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8

Accept-Language: en-US,en;q=0.5

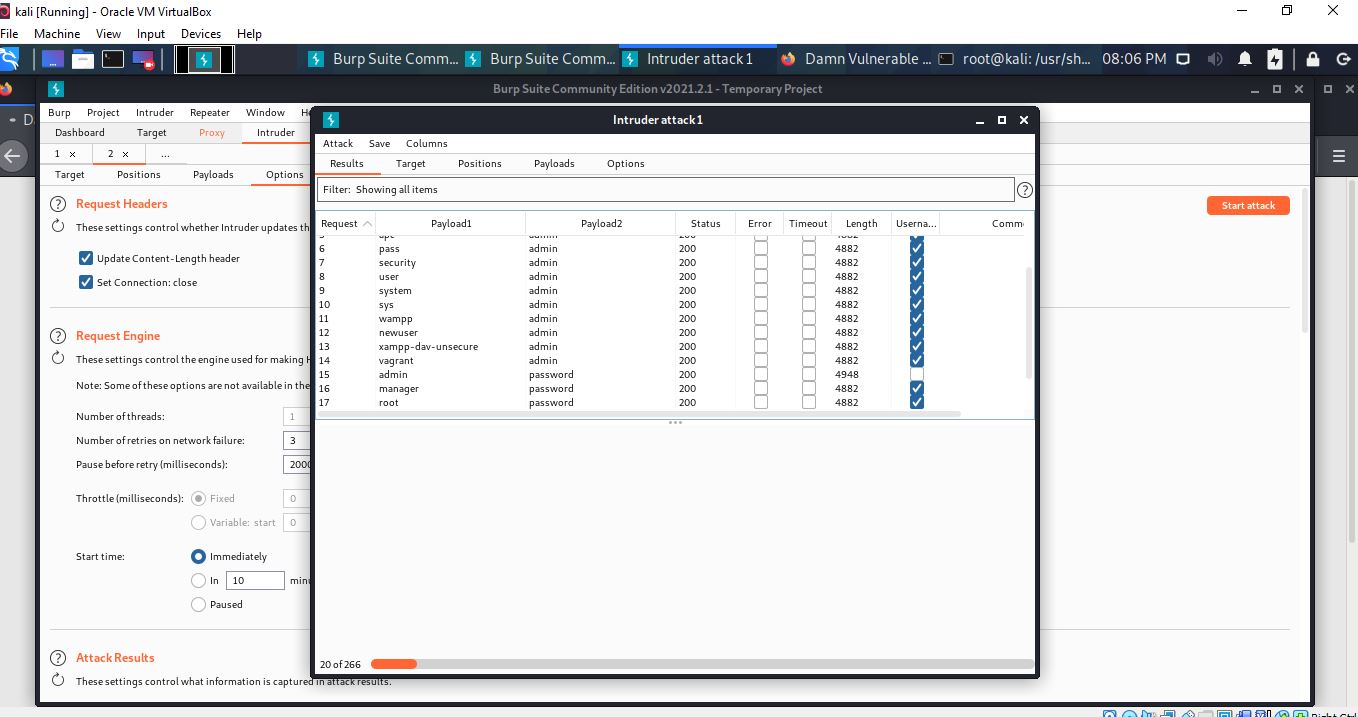
Accept-Encoding: gzip, deflate

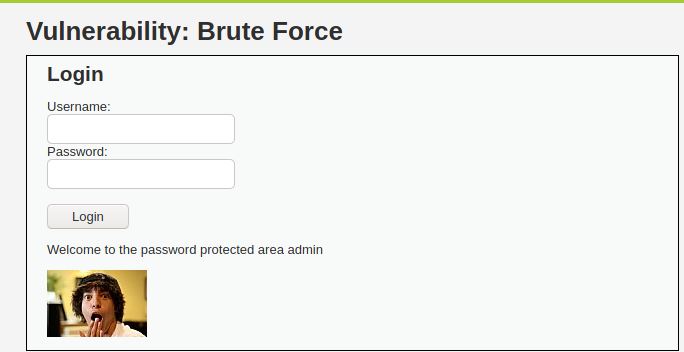
Connection: close

Referer: http://192.168.80.130/dvwa/vulnerabilities/brute/

Cookie: security=low; PHPSESSID=aca0fa66057d675e1e6e050de40138a1

Upgrade-Insecure-Requests: 1





**MEDIUM**

**Steps to reproduce:**

1. Configure your web browser and burp suite.
2. Go to the dvwa page and enter the random credentials.
3. Now capture the request in the tool like burp suite.
4. Brute force the username and password parameter.
5. Correct username and password will show http status ‘200’ and length ‘4948’.

**Vulnerable request:**

GET /dvwa/vulnerabilities/brute/?username=XXXXXX&password=XXXXXX&Login=Login HTTP/1.1

Host: 192.168.80.130

User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:78.0) Gecko/20100101 Firefox/78.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8

Accept-Language: en-US,en;q=0.5

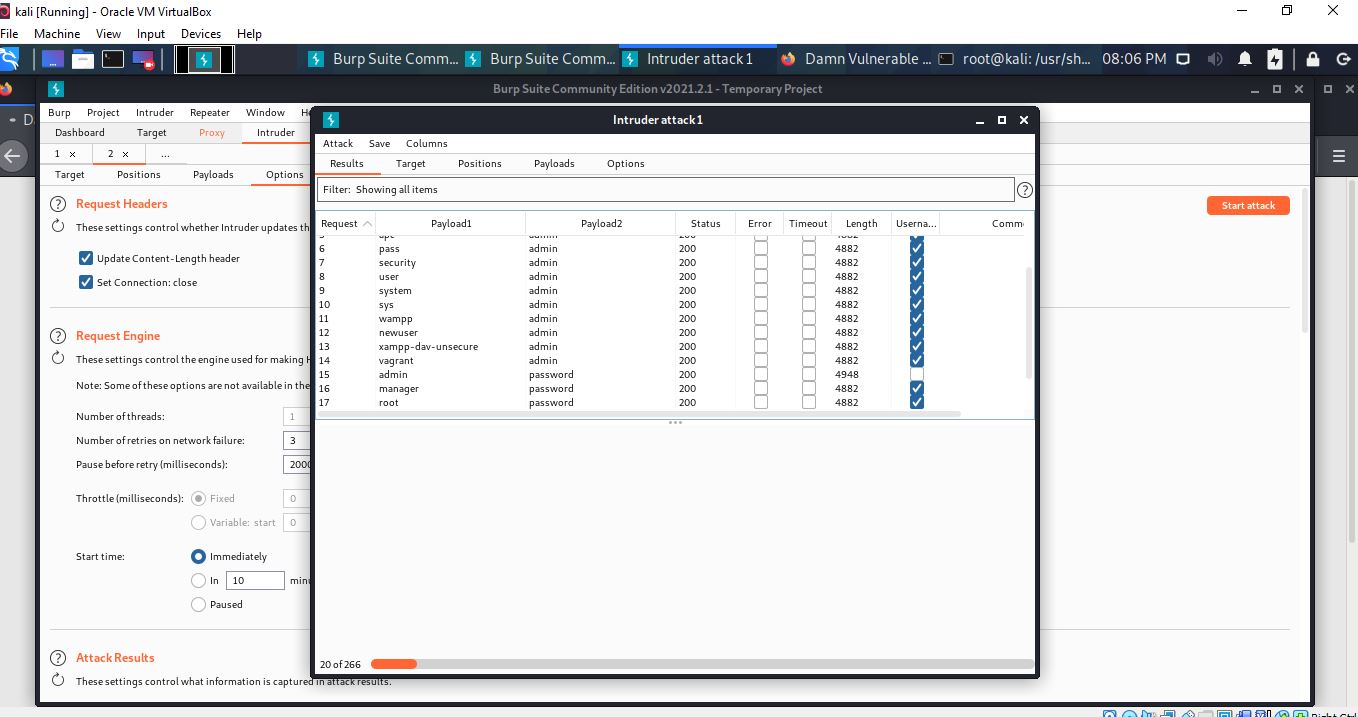
Accept-Encoding: gzip, deflate

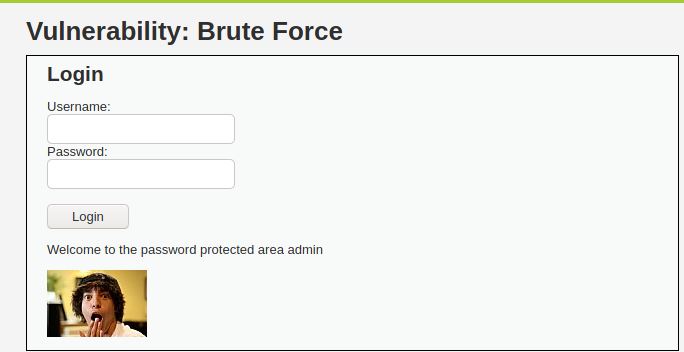
Connection: close

Referer: http://192.168.80.130/dvwa/vulnerabilities/brute/

Cookie: security=medium; PHPSESSID=aca0fa66057d675e1e6e050de40138a1

Upgrade-Insecure-Requests: 1





**HIGH**

**Description:**

We will first understand what is different in this level.Go to the brute force tab in the DVWA dashboard and click on view source code.Here we see the website is generating Anti-CSRF Tokens which is a combination of Numbers and alphabets randomly generated by the website and they are unique for every Session.

So, when we enter our credentials and click on login, first the Anti-CSRF Token will bechecked and verified then our username and password details will be checked.Also, in the code there is a line which says if login is failed sleep for 0-4 seconds.

So now if we perform a normal brute force attack the Anti-CSRF token will change after theevery attempt and even if we have the correct username and password it would not matter asthe Anti-CSRF token is verified first and it would be wrong and also the login page would sleep for 0-4 seconds.

**Steps to reproduce:**

1. Configure your web browser and burp suite.
2. Go to the dvwa page and set level of brute force to the high level
3. Enter the random credentials and capture the request in the tool like burp suite.
4. Now set a new rule in burp suite to pass same csrf token with each brute force attempt.
5. Brute force the username and password parameter.
6. Correct username and password will show http status ‘200’ and length ‘4659’.

**Vulnerable request:**

GET /DVWA/vulnerabilities/brute/?username=XXX&password=XXX&Login=Login&user\_token=418ce1652460d8f1d1cc481ca64c6089 HTTP/1.1

Host: 127.0.0.1

User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:78.0) Gecko/20100101 Firefox/78.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,/;q=0.8

Accept-Language: en-US,en;q=0.5

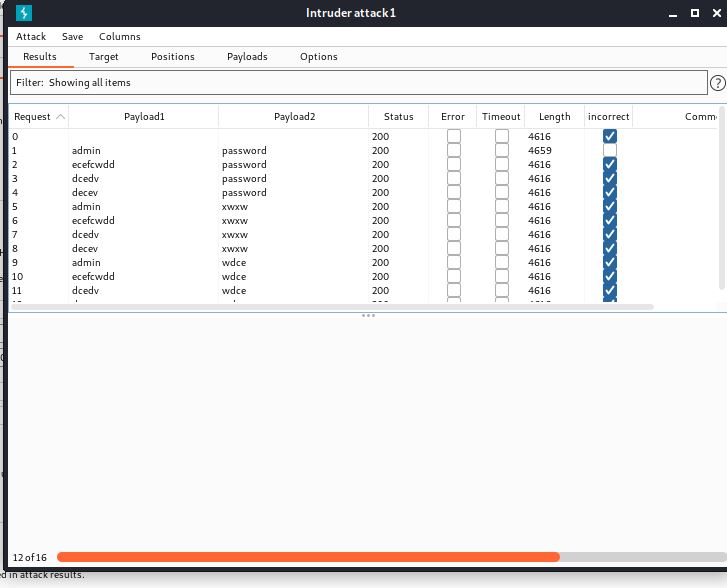
Accept-Encoding: gzip, deflate

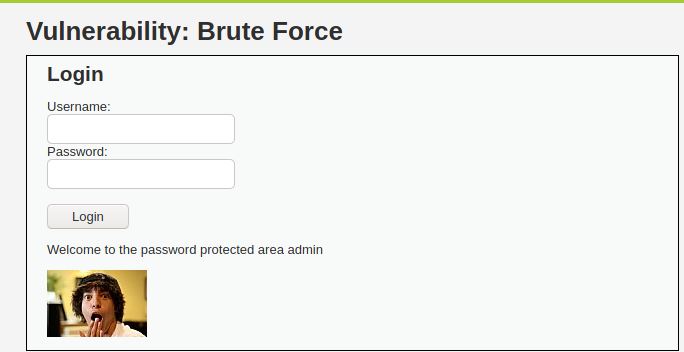
Connection: close

Referer: http://127.0.0.1/DVWA/vulnerabilities/brute/

Cookie: security=high; PHPSESSID=ko3ju9oaj7svq8homk2lb4082a

Upgrade-Insecure-Requests: 1

****

****