Brute Force Protection

https://campus.barracuda.com/doc/98216232/

About Brute Force Attacks

Brute force attack is a technique used to explore an unknown value by systematically trying every key combination to gain access to the targeted resource. In the context of web applications, such attacks appear as a volley of HTTP requests that successively cycle through a user input value until finding the “right” value. This value could be a GET or POST parameter, usernames and passwords, URL paths, or header values. Such attacks are carried out using automated tools and scripts that try every possible character combination.

Attackers often make use of the fact that invalid inputs to web applications yield a different page than valid values. For example, an invalid username could yield one error message and an invalid password could yield another and a successful login yield a completely different page. An attacker can then write a script that cycles through username values where the error message generated is “invalid user”. When the error changes to “invalid password” the attacker can identify a valid username, and then proceed to cycle through passwords for that valid username, until the correct password is tried.

Another weakness that facilitates this type of attack is the lack of a policy to enforce a maximum number of attempts to access a particular resource.

In addition to targeting login credentials, a brute force attack could also be used for guessing hidden pages or content, session ID values, one time passcodes, credit card numbers, and even reversing cryptographic hash functions.

Because brute force attacks from a single client could be easy to spot and block, attackers frequently use multiple attack sources that try to attack the web application in concert. Therefore, a common by-product of brute force attacks is resource exhaustion on the target server that could degrade the quality of service to legitimate clients.

Indications of a Brute Force Attack

Since brute force attacks require trial and error with a large set of values, the most common indicator is an unusually large number of failed requests. When a parameter is being attacked (like username) then the requests are all to the same page. If the attacker is trying to find hidden pages, then each request would be different but the server response codes will be 404: Page Not Found.

Effects

A successful brute force attack can result in the following:

- Leaked confidential and private data (for example: user's profile data, bank details, financial status).
- Leaked hidden files or interfaces (for example: admin interface).
- It can disrupt the service if it is attacked to the point of causing a denial of service (DoS).

If the attackers succeed in gaining access to administrative panels, they can modify/delete/add web application content, modify user privileges, and more.

Barracuda WAF-as-a-Service allows you to restrict the maximum attempts to access resources in a given time window. The counting can be done per source IP or across all sources. When clients violate the access policy, they can be either presented with a CAPTCHA to prove they are humans and not scripts or locked out for a time period you specify.

Configure Brute Force Protection

To apply Brute Force Protection to all or a portion of your application, follow these steps:

1. From App Profiles, add Form Protection to the desired URL.
2. In the right-side panel find **Brute Force Protection** and click on it.
3. In the **Edit brute force prevention** panel, configure the following:
    1. Set **Brute force protection** to **Enabled** to enforce the brute force policy.
    2. **Block an IP Address** – Blocks requests from the IP address(es) that exceeds the configured threshold:
        1. **If it performs -- Valid Requests** - Specify the maximum number of valid requests to be allowed per IP address for the time specified in **Within _ Seconds**.
        2. **If it performs - - Invalid Requests** - Specify the maximum number of invalid requests to be allowed per IP address for the time specified in **Within _ Seconds**.
        3. **Or transfers- - Kilobytes** - Specify the maximum data to be transferred (in kilobytes) for the time specified in **Within _ Seconds**.
        4. **Within ... Seconds** - Specify the time in seconds within which the valid, invalid requests and data transferred by an IP address are evaluated.
        5. **IP Addresses to Never Block** – Add the IP address(es) that needs to be exempted from the brute force validation checks.
    3. **Block a client fingerprint** – Blocks the requests from devices based on their fingerprint(s) that exceeds the configured threshold.
        - I**f it performs -- Valid Requests** - Specify the maximum number of valid requests per client fingerprint to be allowed for the time specified in **Within _ Seconds**.
        - **If it performs -- Invalid Requests** - Specify the maximum number of invalid requests per client fingerprint to be allowed for the time specified in **Within _ Seconds**.

- **Or transfers- Kilobytes** - Specify the maximum data to be transferred (in kilobytes) for the time specified in **Within _ Seconds**.
- **Within ... Seconds** - Specify the time in seconds within which the valid, invalid requests and data transferred per client fingerprint are evaluated.
- **Client Fingerprints to Never Block** – Add the client fingerprints that needs to be exempted from the brute force validation checks.

```
-- Requests that receive 20x and 30x response status codes are considered valid requests.
-- Requests that receive 40x and 50x response status codes are considered invalid requests.
```

4. **Count Auth Responses** – Set to **Enabled** if you want auth responses to be counted.
   Configuration under **Block an IP Address** and **Block a Client Fingerprint** are applicable only when **Count Auth Responses** is set to **Enabled**.
5. **Auth Response Identifier** - Choose the auth response identifier type.
   1. **Auth Failure Response Codes** – The authentication status codes 401 and 407 will be considered invalid status codes, and not as exceptions. For example, When **If it performs ... Invalid Requests** is set to 10, and **Within _ Seconds** is set to 60, the Barracuda WAF-as-a-Service allows 10 invalid requests (4xx and 5xx codes including 401 and 407) for 60 seconds, after which the brute force action policy will be applied.
   2. **Response Text Message** - The text patterns which will be matched against the response page.
      1. **Text to match** - Provide the text patterns that needs to be matched against the response page and then click **Add**.
         You can add a maximum of 5 text patterns to match. If required, you can delete the existing patterns for adding new ones
6. Click **Save**.