# Credential Attack Protection

https://campus.barracuda.com/doc/98216623/

Credential Attack Protection uses the Advanced Bot Protection (ABP) internal service to protect your app against credential stuffing and credential spraying. The service requires the purchase of an ABP license.

## Credential Stuffing Protection

Credential stuffing is used to perform account takeover attacks through automated injection of breached username/password pairs. This method uses stolen email and password logins from other sources to gain unauthorized access to accounts. Attackers leverage large numbers of leaked credentials in an automated fashion against numerous websites in an attempt to take over user accounts with credential reuse. The attacker acquires these spilled usernames and passwords from a website breach, and uses an account checker (such as SentryMBA) to test the stolen credentials against many websites. Successful logins allow the attacker to take over the account matching the stolen credentials.

The Barracuda ABP system uses a database of breached credentials to validate incoming login requests. When a match for the incoming credentials is found, WAF-as-a-Service is configured to alert the admin and/or block such login requests. WAF-as-a-Service does not transmit the complete username or password to the Barracuda ABP for validation. The username/password is hashed, and only the first 16 characters of the hash is transmitted for validation.

## Credential Spraying Protection

In this type of protection, WAF-as-a-Service checks the incoming usernames and passwords independently on the databases. Since this is binded to the Brute Force Prevention feature, the Brute Force counter starts and identifies credential spraying attempts when either the username or the password matches the databases. However, if both the username and password match the databases, then the attack is detected immediately and a follow-up action is enforced.

## Enable Credential Attack Protection

1. From App Profiles, add Form Protection to the desired URL.
2. In the right side panel find Credential Account Protection and click on it.
   You must configure Login Form Information before using this feature.

3. Configure Credential Attack Protection:
   - **Credential Stuffing Protection** – Set to **Enable**.
     It is recommended to enable Brute Force Protection on the URL when Credential Stuffing Protection is enabled.
   - **Credential Spraying Protection** – Set to **Enable**.
     You must first enable Brute Force Protection before you can use Credential Spraying Protection.
   - **Credential Spraying Attack** – Set the number of credential spraying matches that need to occur in a short period of time before a client is blocked. Because any attempt with a compromised username *or* password will be detected as an attack, Credential Spraying is more prone to false positives. The default is 5.
4. Click **Save**.