

**bulutklinik**

## **Cloud Sistemlerde Veri Güvenliđi**



**Ali Hulusi Ölmez**  
Bulutklinik  
co-Founder

# Genel Sayılar



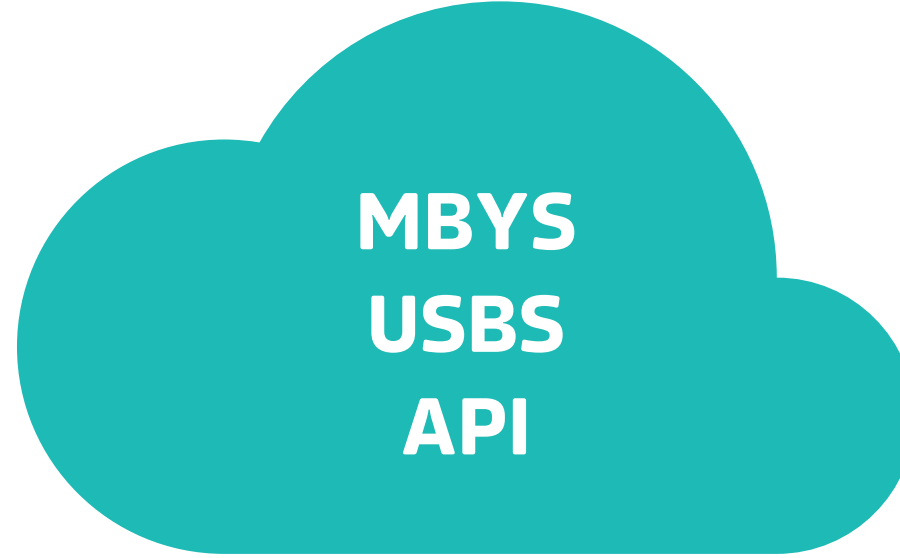
**12 Bin +**  
Doktor



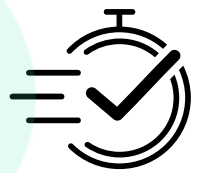
**4.4 Milyon +**  
Hasta



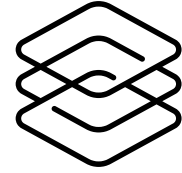
**290 Bin**  
Aylık Randevu



**MBYS**  
**USBS**  
**API**



**1000**  
İstek /SN



**11 Milyon**  
Etkinlik / Ay



**7 Saat**  
Oturum Süresi / Gün

# Kullanılan Teknolojiler



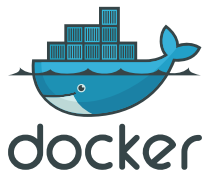
ubuntu

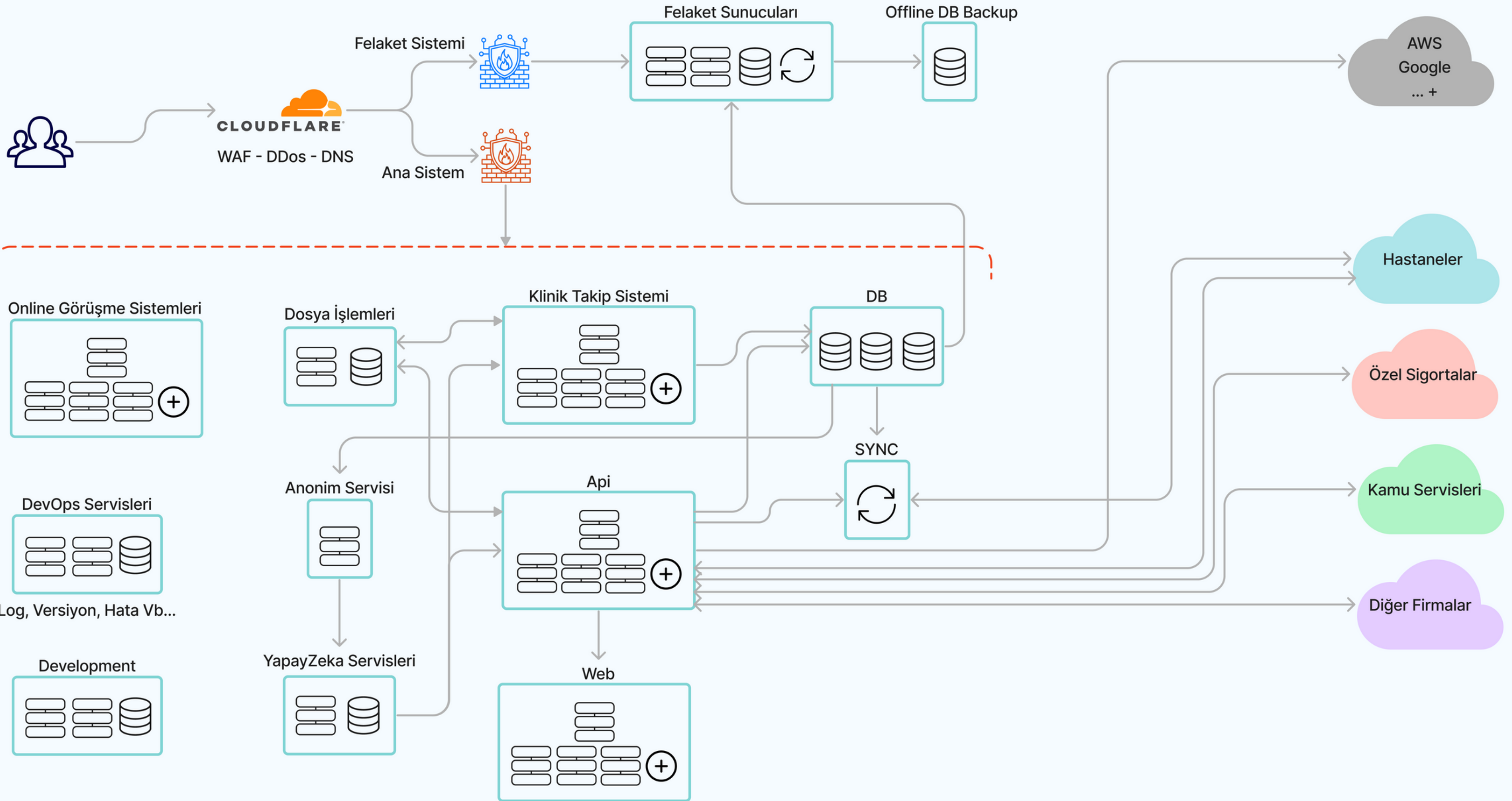


*php*



ZABBIX





# Saldırganların Yöntemleri

DDos

Sql injection

Code injection attacks

Social engineering (Phishing, Baiting)

XSS attacks

Brute force

DNS spoofing

Cookie theft

```
$ python sqlmap.py -u "http://debiandev/sqlmap/mysql/get_int.php?id=1" --batch
{1.0.5.63#dev}
http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting at 17:43:06

[17:43:06] [INFO] testing connection to the target URL
[17:43:06] [INFO] heuristics detected web page charset 'ascii'
[17:43:06] [INFO] testing if the target URL is stable
[17:43:07] [INFO] target URL is stable
[17:43:07] [INFO] testing if GET parameter 'id' is dynamic
[17:43:07] [INFO] confirming that GET parameter 'id' is dynamic
[17:43:07] [INFO] GET parameter 'id' is dynamic
[17:43:07] [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable (possible DBMS: 'MySQL')
```

```
89.179.247.168 - - [01/Dec/2023:11:10:59 +0300] GET /bin/zhttpd/${IFS}ping${IFS}-q${IFS}-c${IFS}2${IFS}-s${IFS}7${IFS}213.141.143.101; "400" 0 "-" "-" "-"

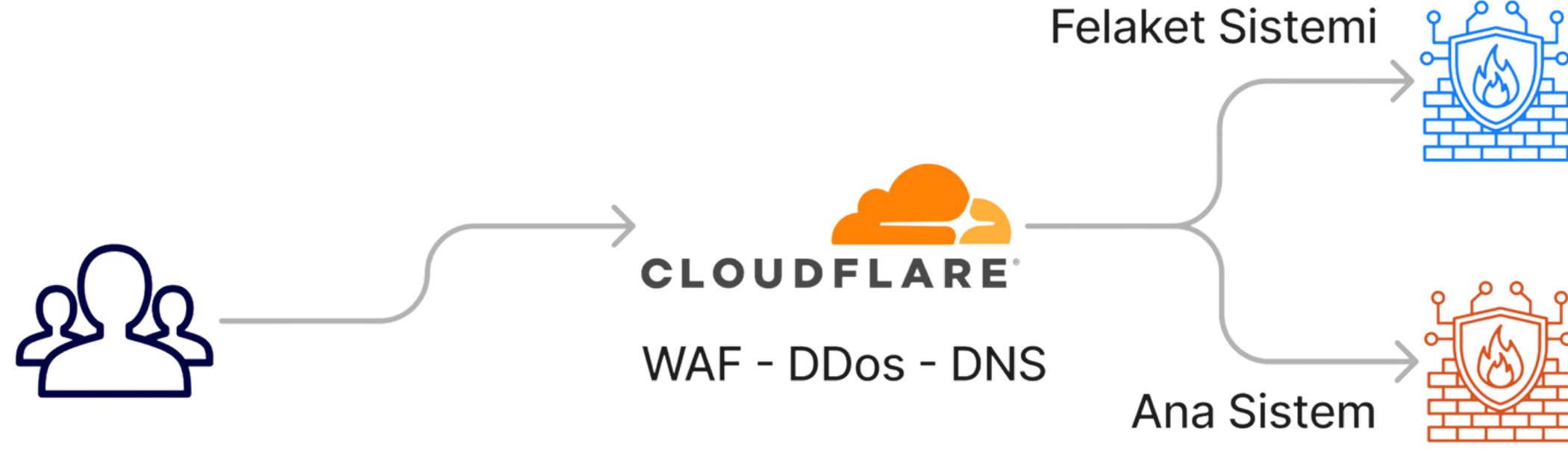
31.143.1.226 - - [01/Dec/2023:11:11:00 +0300] POST /setcookie HTTP/1.1 "302" 350 "https://bulutklinik.com/makale/karaciger-buyumesi-nedenleri-nelerdir-nasil-tedavi-edilir" "Mozilla/5.0 (iPhone; CPU iPhone OS 17_1_1 like Mac OS X)

167.235.65.146 - - [01/Dec/2023:06:16:51 +0300] \x16\x03\x01\x02\x00\x01\x00\x01\xFC\x03\x03p\x1A\x8C&\x115u9\xE1nf\x1B) f\xB4\xEF\xBE\x80\x17\xC10\xD8~\xBB\x8C\xC8'b\xD3\x7F\x83\xCD \x8DU\x7Fy\xA4\xAE\x84\x854\x9D\x9C\x0E\xB3c\xB3\x07!\xF0\x14~\x976u\xE1\x15Z\xE1\x92opo\x84\x00V\x13\x02\x13\x03\x13\x01\xC0,\xC00\xC0+\xC0/\xCC\xA9\xCC\xA8\x00\x9F\x00\x9E\xCC\xAA\xC0\xAF\xC0\xAD\xC0\xAE\xC0\xAC\xC0$\xC0(\xC0#\xC0'\xC0 "400" 150 "-" "-" "-"

167.235.65.146 - - [01/Dec/2023:06:16:55 +0300] GET /.env.www HTTP/1.1 "499" 0 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.129 Safari/537.36" "-"
```

Browser inspect ile veri değiştirmek

# Sistemsel Önlemler Nelerdir ?



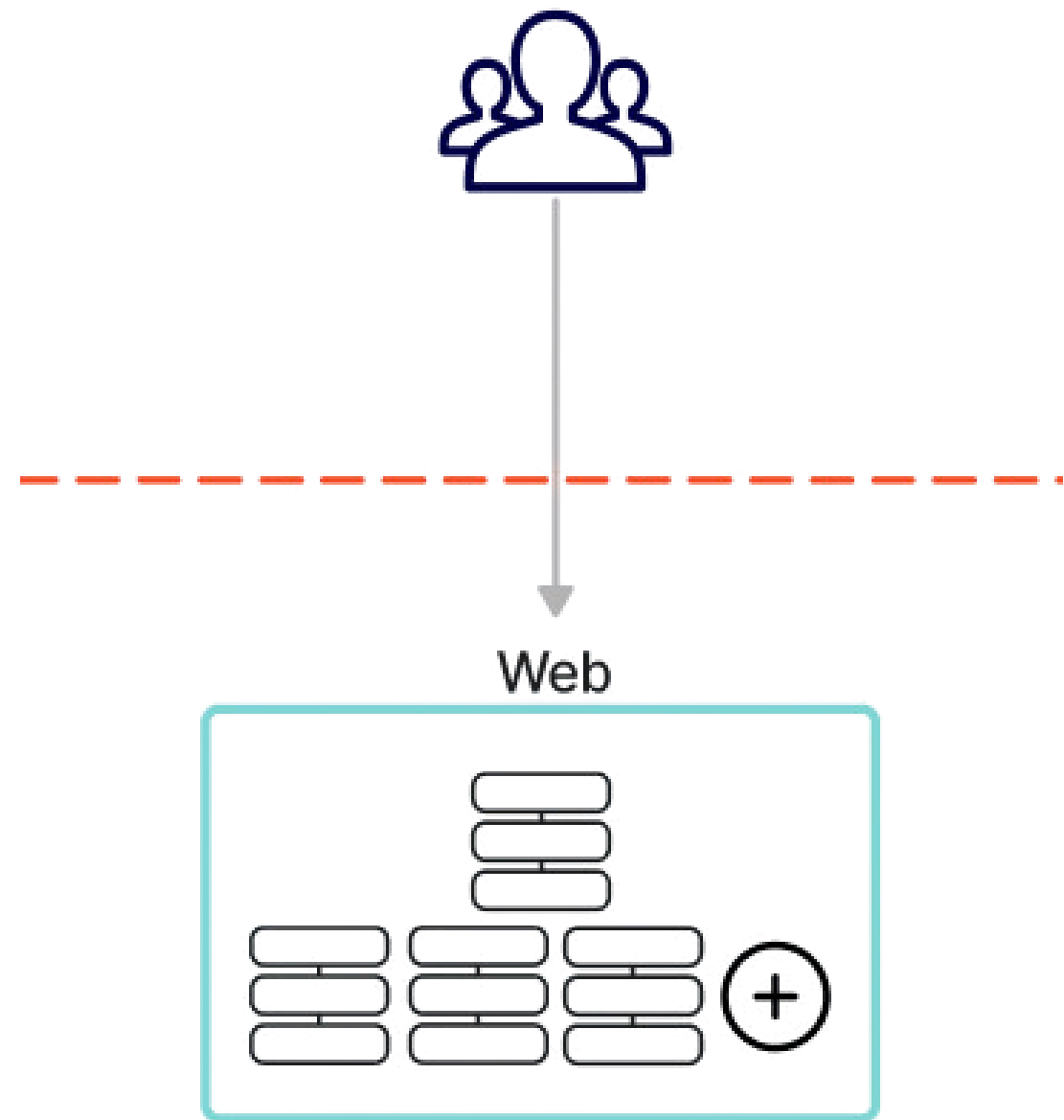
## Cloudflare

- Waf
- DDos
- Page shield
- Bots
- Rate limiter

## Firewall

- Firewall rules
- DDos
- Port kısıtlamaları
- Veri giriş çıkış kontrolleri
- Sunucu grup izolasyonları

# Sistemsel Önlemler Nelerdir ?



## Rules

- Rate Limiter (30+)
- Captha
- 2FA
- Ülke kısıtları
- İstemci kısıtları

## Code Level

- Data type
- Lenght
- InArray
- Format
- ...

```
public function rules()
{
    return [
        "appointmentDate" => "required|date_format:Y-m-d H:i|after_or_equal:".Carbon::now()->format("Y-m-d").
        "appointmentType" => "nullable|in:interview,appointment",
        "doctorId"        => "required|numeric",
    ];
}
```



# bulutklinik

Doktorunuza erişmenin **en kolay yolu!**

Ali Hulusi Ölmez  
aliolmez@bulutklinik.com

