

I mrt

WEB APPLICATION Firewall

Agenda

ATTACKING WEB APP
WEB APP Firewall
DIFF WAF and IPS/IDS
WAF Consideration

* Web APP Attack

- SQLi, XSS, Command injection

- Altered hidden form input, Long query string, Brute force and etc.....

* WAF

E.g. ModSecurity, Azure

WAF and IPS/IDS DIFF

OSI Layer

- 7 Application
- 6 Presentation
- 5 Session
- 4 Transport
- 3 Network
- 2 Data Link
- 1 Physical

WAF Consider

OWASP method

Alert mode or Block mode

TLS Termination

Rules set