

## دوره NSE۶ فورتی وب | Fortinet FortiWeb

### مروری بر دوره

مروری بر دوره

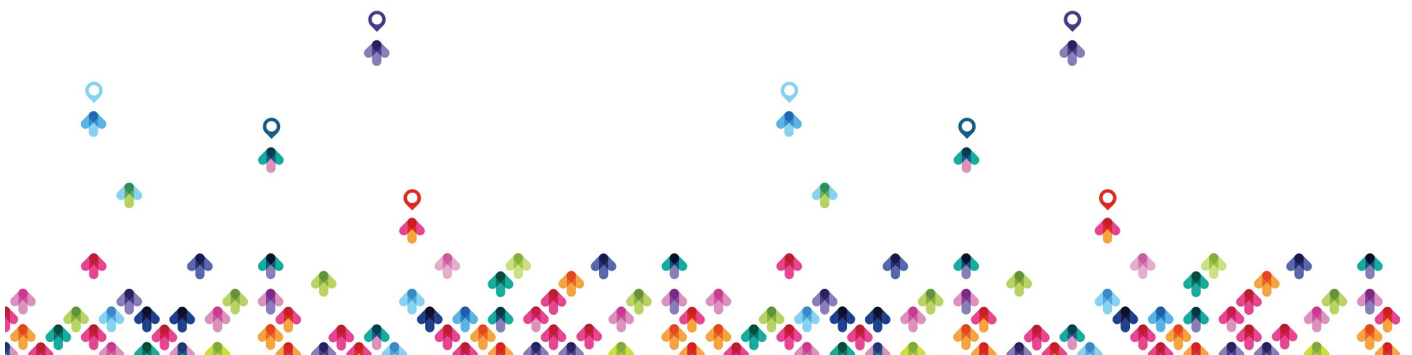
در این دوره شما نحوه پیاده سازی، پیکربندی و عیب یابی فایروال وب اپلیکیشن FortiWeb موسوم به FortiWeb را خواهید آموخت. مدرسان این دوره سعی دارند تا با پرداختن به مفاهیم کلیدی مربوط به امنیت در وب اپلیکیشن و پیاده سازی لابراتورهای متنوع شما را با قابلیت های امنیتی و عملکرد این سیستم آشنا سازند.

لابراتورهای این دوره به شما این امکان را خواهد داد تا به بهترین شکل ممکن در محیطی شبیه سازی شده و با استفاده از وب اپلیکیشن واقعی عبور ترافیک و بروز حملات را تجربه کنید. کار با این شبیه سازها به شما کمک خواهد نمود تا در عین حفظ پارامترهای منطقی، بازرسی جریان ترافیک و ایمن نگه داشتن کوکی های مربوط به HTTP session، نحوه توزیع بار از سرورهای مجازی به سرورهای واقعی را نیز بیاموزید.

### آنچه در این دوره خواهید آموخت

آنچه خواهید آموخت

- درک تهدیدات در سطح Application Layer
- مقابله با DoS و Defacement
- جلوگیری از حملات Zero-day بدون بروز اختلال در ترافیک Live
- مطابق سازی Application ها با OWASP top ۱۰ و PCI-DSS
- کشف آسیب پذیری بر روی سرور ها و Web App های میزبانی شده به منظور حفاظت بهینه
- پیکربندی FortiGate به همراه FortiWeb با هدف امنیت بیشتر Application های مبتنی بر HTTP و XML
- جلوگیری از دور خوردن اتفاقی اسکن در حالیکه FTP و SSH اجازه برقراری ارتباط دارند.



- پیکربندی Blocking و گزارش گیری برای یک FortiGate، FortiADC و یا FortiAnalyzer
- انتخاب Mode عملیاتی مناسب
- Load Balance کردن ترافیک میان سرورهای یک Pool
- پیاده سازی SSL/TLS، Authentication، و ابزارهای کنترل دسترسی برای Application های غیر ایمن
- آموزش FortiWeb برای دفاع از Application های خاص شما
- Blacklist نمودن موارد مشکوک به هک، کامپیوترهای مشکوک به شرکت در یک حمله DDoS و دیگر موارد content scraper ها
- انجام Troubleshoot مربوط به Traffic flow شامل Flow مربوط به FTP/SSH
- تشخیص False Positive ها و سفارشی کردن Signature ها
- بهینه سازی عملکرد

## سرفصل ها (حضور)

سرفصل ها

۱. Introduction
۲. Basic Setup
۳. Integrating Front-End SNAT and Load Balancers
۴. DoS and Defacement
۵. Signatures, Sanitization, and Auto-Learning
۶. SSL/TLS
۷. Authentication and Access Control



۸. PCI DSS ۳.۰ Compliance

۹. Caching and Compression

۱۰. HTTP Routing, Rewriting, and Redirects

۱۱. Troubleshooting

## مخاطبان دوره

مخاطبان دوره

- متخصصان امنیت و شبکه که در زمینه مدیریت و پشتیبانی از FortiWeb فعالیت دارند.

## پیش نیازها

پیش نیازها

- Knowledge of OSI layers and the HTTP protocol
- Basic knowledge of HTML, JavaScript, and server-side dynamic page languages, such as PHP
- Basic experience using FortiGate port forwarding

