



به نام خدا

**استقرار، پیاده سازی و راه اندازی فورتی وب**

# **FortiWeb**

**امنیت سامانه های تحت وب**

مؤلف:

**احسان امجدی**



مؤسسه فرهنگی هنری  
دیباجران تهران

هرگونه چاپ و تکثیر از محتویات این کتاب بدون اجازه کتبی ناشر ممنوع است. متخلفان به موجب قانون حمایت حقوق مؤلفان، مصنفان و هنرمندان تحت پیگرد قانونی قرار می گیرند.

## ◀ عنوان کتاب: **استقرار، پیاده سازی و راه اندازی فورتی وب** **FortiWeb امنیت سامانه های تحت وب**

◀ مولف: **احسان امجدی**

◀ ناشر: **مؤسسه فرهنگی هنری دیباجران تهران**

◀ ویراستار: **نرگس مهربد**

◀ صفحه آرای: **نازنین نصیری**

◀ طراح جلد: **داریوش فرسایی**

◀ نوبت چاپ: **اول**

◀ تاریخ نشر: **۱۴۰۱**

◀ چاپ و صحافی: **صدف**

◀ تیراژ: **۱۰۰ جلد**

◀ قیمت: **۱۴۰۰۰۰۰ ریال**

◀ شابک: **۹۷۸-۶۲۲-۲۱۸-۶۴۰-۱**

**نشانی واحد فروش:** تهران، خیابان انقلاب، خیابان دانشگاه

-تقاطع شهدای ژاندارمری-پلاک ۱۵۸ ساختمان دانشگاه-

طبقه دوم-واحد ۴ تلفن ها: ۶۶۴۹۸۱۶۸-۲۲۰۸۵۱۱۱

**فروشگاههای اینترنتی دیباجران تهران :**

**WWW.MFTBOOK.IR**

**www.dibagarantehran.com**

سرشناسه: امجدی بیگونند، احسان، ۱۳۶۴-

عنوان و نام پدیدآور: استقرار، پیاده سازی و راه اندازی فورتی

وب FortiWeb : امنیت سامانه های تحت وب / مولف:

احسان امجدی؛

ویراستار: نرگس مهربد.

مشخصات نشر: تهران: دیباجران تهران: ۱۴۰۱

مشخصات ظاهری: ۱۸۲ ص: مصور،

شابک: ۹۷۸-۶۲۲-۲۱۸-۶۴۰-۱

وضعیت فهرست نویسی: فیپا

عنوان دیگر: امنیت سامانه های تحت وب

موضوع: فورتی وب FortiWeb

موضوع: فایروال (ایمن سازی کامپیوتر)

موضوع: (computer security) firewalls

موضوع: شبکه های کامپیوتری-تدابیر ایمنی

موضوع: computer networks-security measures

رده بندی کنگره: ۵۹/۵۱۰۵ TK

رده بندی دیویی: ۰۵/۸۰۰

شماره کتابشناسی ملی: ۹۰۶۰۸۰۹

نشانی اینستاگرام دیبا **dibagaran\_publishing** نشانی تلگرام: **@mftbook**

هر کتاب دیباجران، یک فرصت جدید علمی و شغلی.

هر گونشی همراه، یک فروشگاه کتاب دیباجران تهران.

از طریق سایتهای دیباجران، در هر جای ایران به کتابهای ما دسترسی دارید.

## فهرست مطالب

مقدمه ناشر ..... ۷

مقدمه مؤلف ..... ۸

### فصل اول

چرا وف؟! چرا فورتی وب؟! ..... ۹

توضیحات اولیه و ضروری درباره چرایی استفاده از وف ..... ۱۱

چرا استفاده از وف برای سازمان‌ها حیاتی است؟ ..... ۱۳

مزیت‌ها ..... ۱۷

قابلیت‌ها و طراحی خاص برای وب‌سرورها و وب‌سرویس‌ها ..... ۱۷

معماری ..... ۱۹

### فصل دوم

استقرار اولیه فورتی وب ..... ۲۰

تجهیز سخت‌افزاری یا VMWare؟ ..... ۲۱

رجیستر کردن فورتی وب ..... ۲۱

طرح‌ریزی توپولوژی شبکه ..... ۲۲

نحوه انتخاب مود عملکرد ..... ۲۸

مود Reverse Proxy ..... ۳۳

مودهای Transparent ..... ۳۵

مود Offline Protection ..... ۳۸

مود WCCP ..... ۴۰

سناریو ..... ۴۲

ساختار High Availability Clustering ..... ۴۳

سناریوی اول ..... ۴۵

سناریوی دوم ..... ۴۶

رابط کاربری وب / رابط خط فرمان ..... ۵۰

به‌روزرسانی فریم‌ور ..... ۵۵

تست فریم‌ور جدید ..... ۵۹

چطور تست کنیم؟ ..... ۶۱

نصب فریم‌ور ..... ۶۳

۶۸	تغییر پسورد اکانت admin
۷۰	تنظیم زمان و تاریخ
۷۳	پیکربندی مودهای عملکردی
۷۶	پیکربندی تنظیمات شبکه
۷۹	اضافه کردن VLAN Subinterface ها
۸۲	پیکربندی Bridge
۸۶	پیکربندی IP مجازی
۸۸	تعریف وب سرورها و لودبالانسرها
۸۹	وب سرورهای محافظت شده / Hostname های محافظت شده (مجاز)
۹۱	پیکربندی Protected Hostname
۹۳	تعریف Web Server ها در فورتی وب
۹۳	پیکربندی Health check سرور
۹۸	ایجاد یک Server Pool
۱۰۵	مسیریابی بر اساس محتوای HTTP
۱۰۷	پیکربندی HTTP content routing
۱۰۷	تعریف پروکسی ها، کلاینت ها و X-Header ها
۱۰۸	ارسال IP اصلی کلاینت به سرورهای بک اند
۱۰۹	پیکربندی فورتی وب برای فعال کردن X-Forwarded-For و/یا X-Real-IP
۱۱۱	عکس العمل نسبت به IP مهاجم نه نسبت به IP لود بالانس
۱۱۱	برای آنکه فورتی وب بتواند IP اصلی کلاینت را از هدر پکت HTTP به دست بیاورد
۱۱۳	پیکربندی سرورهای مجازی روی فورتی وب
۱۱۴	پیکربندی یک سرور مجازی
۱۱۵	پیکربندی پالیسی های اصلی و مورد نیاز
۱۱۶	مثال ۱: پیکربندی یک پالیسی برای ترافیک HTTP
۱۱۷	مثال ۲: پیکربندی مثال قبل بر پایه پروتکل HTTPS
۱۱۸	مثال ۳: پیکربندی یک پالیسی، با در نظر گرفتن لودبالانسینگ
۱۱۹	تست پیکربندی های انجام شده
۱۱۹	کاهش اشتباهات پیکربندی

## فصل سوم

### سیاست ها ..... ۱۲۰

۱۲۰	تأثیر Operation Mode ها بر رفتار Server Policy
۱۲۱	پیکربندی Global Object Allow List
۱۲۳	پیکربندی یک Protection Profile برای توپولوژی های Inline
۱۳۱	مدیریت کلاینت

۱۳۲.....	Threat Weight	پیکربندی
۱۳۳.....	Client Management	پیکربندی
۱۳۴.....	Server Policy	یک پیکربندی

## فصل چهارم

### ارتباطات امن ..... ۱۳۸

۱۳۸.....	Inspection یا Offloading	؟
۱۴۰.....	CA	سرتیفیکیت‌های
۱۴۰.....	CA	وارد کردن فایل‌های سرتیفیکیت به صورت لوکال
۱۴۱.....	CA	آپلود یک سرتیفیکیت
۱۴۱.....	CA certificate group	پیکربندی یک
۱۴۲.....	inspection یا offloading	از چه سرتیفیکیت‌هایی باید برای استفاده کرد؟

## فصل پنجم

### کاربران ..... ۱۴۴

۱۴۴.....	مدل‌های احراز هویت	
۱۴۷.....	لوکال	پیکربندی اکانت‌های
۱۴۸.....	ریموت	پیکربندی ارسال کوئری برای اکانت‌های
۱۵۰.....	Radius	پیکربندی یک سرور

## فصل ششم

### امنیت ..... ۱۵۲

۱۵۲.....	مسدود کردن حملات شناخته‌شده	
۱۵۳.....	سیگنچر	پیکربندی
۱۵۳.....	signature policy	استفاده از wizard برای ایجاد یک
۱۵۴.....	Signature Rule	برای پیکربندی یک

## فصل هفتم

### کاهش (حملات) ربات ..... ۱۵۸

۱۵۸.....	Threshold	پیکربندی «تشخیص بات بر اساس
۱۶۴.....	بیومتریکی»	پیکربندی رول «تشخیص بات بر اساس پارامترهای
۱۶۶.....	«فریب بات»	پیکربندی
۱۶۸.....	شناخته‌شده	پیکربندی بات‌های
۱۶۹.....	Bot Mitigation Policy	پیکربندی

## فصل هشتم

### مدیران ..... ۱۷۱

- ۱۷۱..... پیکربندی پروفایل‌های دسترسی
- ۱۷۳..... تغییر پسورد اکانت Administrator
- ۱۷۵..... ایجاد یک اکانت لوکال Administrator

## فصل نهم

### پایش ..... ۱۷۶

- ۱۷۶..... لاگ
- ۱۷۶..... لاگ‌ها و فرآیند ثبت آن‌ها
- ۱۷۷..... انواع لاگ
- ۱۷۷..... شدت لاگ
- ۱۷۸..... محدودیت نرخ ثبت لاگ
- ۱۷۹..... پیکربندی ثبت لاگ
- ۱۷۹..... برای پیکربندی ثبت لاگ

خط‌مشی انتشارات مؤسسه فرهنگی هنری دیباگران تهران در عرصه کتاب‌هایی با کیفیت عالی است که تواند  
خواسته‌های به روز جامعه فرهنگی و علمی کشور را تا حد امکان پوشش دهد.  
هر کتاب دیباگران تهران، یک فرصت جدید شغلی و علمی

حمد و سپاس ایزد منان را که با الطاف بی‌کران خود این توفیق را به ما ارزانی داشت تا بتوانیم در راه ارتقای دانش عمومی و فرهنگی این مرز و بوم در زمینه چاپ و نشر کتب علمی و آموزشی گام‌هایی هرچند کوچک برداشته و در انجام رسالتی که بر عهده داریم، مؤثر واقع شویم.

گسترده‌گی علوم و سرعت توسعه روزافزون آن، شرایطی را به وجود آورده که هر روز شاهد تحولات اساسی چشمگیری در سطح جهان هستیم. این گسترش و توسعه، نیاز به منابع مختلف از جمله کتاب را به عنوان قدیمی‌ترین و راحت‌ترین راه دستیابی به اطلاعات و اطلاع‌رسانی، بیش از پیش برجسته نموده است.

در این راستا، واحد انتشارات مؤسسه فرهنگی هنری دیباگران تهران با همکاری اساتید، مؤلفان، مترجمان، متخصصان، پژوهشگران و محققان در زمینه‌های گوناگون و مورد نیاز جامعه تلاش نموده برای رفع کمبودها و نیازهای موجود، منابعی پُر بار، معتبر و با کیفیت مناسب در اختیار علاقمندان قرار دهد.

کتابی که در دست دارید تألیف "جناب آقای احسان امجدی" است که با تلاش همکاران ما در نشر دیباگران تهران منتشر گشته و شایسته است از یکایک این گرامیان تشکر و قدردانی کنیم.

**با نظرات خود مشوق و راهنمای ما باشید**

با ارائه نظرات و پیشنهادات و خواسته‌های خود، به ما کمک کنید تا بهتر و دقیق‌تر در جهت رفع نیازهای علمی و آموزشی کشورمان قدم برداریم. برای رساندن پیام‌هایتان به ما از رسانه‌های دیباگران تهران شامل سایتهای فروشگاهی و صفحه اینستاگرام و شماره‌های تماس که در صفحه شناسنامه کتاب آمده استفاده نمایید.

مدیر انتشارات

مؤسسه فرهنگی هنری دیباگران تهران  
dibagaran@mftplus.com

## مقدمه مؤلف

کتابی که هم اکنون تقدیم نگاهتان می‌شود، حاصل تجمیع مقالات و استانداردهای منتشرشده و همچنین تجربه ۸ ساله بنده در مدیریت و راهبری فایروال‌های موسوم به وف است. هدف از نگارش این کتاب، نظم دادن به دانسته‌ها و تجارب خواننده‌های عزیز در حوزه فایروال‌های فورتی‌وب است.

قطعاً بخش عظیمی از مخاطبان اصلی این کتاب، متخصصان و کارشناسان باتجربه در زمینه شبکه و امنیت هستند، که چه بسا در برخی موارد تخصص و تجربه بیشتری نسبت به من داشته باشند؛ اما از آنجا که گستردگی حوزه فناوری اطلاعات و زیرشاخه‌های آن اجازه نمی‌دهد هر کسی به تنهایی به کل دامنه و عمق آن دسترسی یابد و تلاش برای رسیدن به این هدف جز با به اشتراک‌گذاری اطلاعات تک‌تک دوستان میسر نیست؛ لذا بر آن شدم تا بخشی از تجارب و دانسته‌های خود در زمینه فایروال‌های فورتی‌وب را با شما عزیزان به اشتراک بگذارم.

این کتاب با زبانی ساده و در عین حال رویکردی تخصصی، استقرار، نصب و راه‌اندازی اولیه فورتی‌وب را در دستور کار خود قرار داده‌است و امید بر آن است که اگر عمری باقی باشد، بررسی قابلیت‌ها و سناریوهای پیشرفته فورتی‌وب در آینده خدمت شما عزیزان تقدیم شود.

امیدوارم جوانه‌های شادی و امید در دل تک‌تک شما خوبان همیشه پاینده و در حال رشد باشد.

**این کتاب را به همسر و فرزند عزیزم و تک‌تک عزیزانی که با تمام وجود پشتیبان بنده هستند، تقدیم می‌کنم.**

احسان امجدی

آبان ۱۴۰۱