SEMATEC
IT Training Center

# API Security

## مقدمه

دوره "امنیت API" به منظور آشنایی عمیق با مفاهیم و تکنیک‌ها ی ضروری برای حفظ و تقویت امنیت APIها طراحی شده است. در دنیای امروز که بسیاری از سیستم‌ها و سرویس‌ها از APIها برای ارتباط و تبادل داده استفاده می‌کنند، تأمین امنیت این نقاط حیات ی امری ضروری است. این دوره با ترکیب تئوری و پروژههای عمل ی به دانشجویان کمک می‌کند تا اصول اولیه و پیشرفته امنیت API را درک کرده و در پروژههای واقعی به کار گیرند. همچنین، مباحثی مانند OAuth ۰,۲، OpenID Connect، و امنیت میکروسرویس‌ها به طور جامع پوشش داده می‌شود تا شرکت‌کنندگان بتوانند چالش‌های امنیتی در مقیاس بزرگ را مدیریت کنند. دوره همچنین به جدیدترین تکنولوژی‌ها و ابزارهای امنیتی می‌پردازد تا فراگیران با تهد یدات نوظهور نیز آشنا شوند.

## ضرورت

با گسترش روزافزون استفاده از APIها در ارتباطات بین سرویس‌ها و برنامه‌ها، اهمیت امنیت در این حوزه بیش از پیش نمایان شده است. APIها به عنوان دروازههای تبادل داده، هدف اصلی حملات سایبری هستند و هرگونه آسیب‌پذیری در آنها می‌تواند به نفوذ و سرقت اطلاعات حساس منجر شود. از طرفی، پیچیدگی معماری‌های مدرن مانند میکروسرویس‌ها، چالش‌های امنیتی جدیدی را به وجود آورده که نیازمند رویکردهای پیشرفته است. این دوره به شرکت‌کنندگان کمک می‌کند تا با تهد یدات متداول APIها آشنا شده و توانایی طراحی و پیادهسازی سیستم‌های امن را به دست آورند. تسلط بر ابزارها و پروتکل‌های امنیتی مانند OAuth ۰,۲ و OpenID Connect، به مد یران و توسعه‌دهندگان امکان می‌دهد تا APIهایی مقاوم در برابر حملات سایبری بسازند و امنیت دادهها را تضمین کنند.

## طول دوره :

**۴۲ ساعت**

SEMATEC
IT Training Center

# سرفصل ها :

## اصول پایه امنیتAPI

1. **مقدمه‌ای بر امنیتAPI ها**
   - اهمیت امنیت درAPI ها
   - اصول اولیه امنیت API و چالش‌های متداول
   - مفاهیم احراز هویت (Authentication) و مجوز( Authorization)
2. **حملات رایج درAPI ها**
   - Injection، XSS، حملات(o Man-in-the-Middle (MITM
     آسیب‌پذیری‌ها و راههای مقابله
3. **استانداردها و بهروشها**
   - معرفی استانداردها و ابزارهای مربوط به امنیتAPI

---

## مفاهیم و پیاده سازی OAuth 2.0

1. **مفاهیم پایهOAuth 2.0**
   - نحوه کار OAuth 2.0 و کاربردهای آن درAPI ها
   - نقش و مفاهیم کلیدی(Client) ، Resource Owner، Authorization Server)
2. **جریانهای مختلفOAuth 2.0**

   Owner Password Credentials Grant
   - نحوه انتخاب بهترین جریان برای کاربرد خاص
3. **توکن‌ها و مدیریت آنها**
   - Access Tokensو Refresh Tokens
     نحوه استفاده و مدیریت ایمن توکن‌ها

---

## امنیت پیشرفته OAuth 2.0 وOpenID Connect

1. **امنیت پیشرفتهOAuth 2.0**
   - استفاده ازJSON Web Signature
   - استفاده از(PKCE) Proof Key for Code Exchange

SEMATEC
IT Training Center

2. **OpenID Connect**
   - تفاوت OpenID Connect با OAuth 2.0
   - نحوه پیادهسازی OpenID Connect در API های مدرن
3. **پیادهسازی امنیت پیشرفته در معماری‌های پیچیده**
   - چالش‌ها و راهحل‌های امنیتی در پیادهسازی OAuth 2.0 در مقیاس بزرگ

---

## امنیتAPI ها در معماری میکروسرویس

1. **مقدمه بر امنیت میکروسرویس‌ها**
   - مفاهیم پایه میکروسرویس‌ها و چالش‌های امنیتی آنها
   - نحوه مدیریت و حفظ امنیتAPI ها در سیستم‌های میکروسرویس
2. **استفاده از OAuth 2.0 در معماری میکروسرویس** ○
   مدیریت هویت و مجوز میان سرویس‌ها
   - استفاده ازAPI Gateway ها وService Mesh ها برای امنیت ارتباطات
3. **امنیت ارتباطات داخلی میکروسرویس‌ها**
   - Transport Layer Security (TLS)و کنترل دسترسی در سطح میکروسرویس ○
   ابزارهای نظارت و مانیتورینگ امنیتی در سیستم‌های میکروسرویس

---

### ابزارهای تست و بررسی امنیتAPI ها

- OWASP ZAP، Postman، Burp Suite ○
  روشهای تست نفوذ برایAPI ها
- پیادهسازی گام به گام امنیت در○ API
  کار با ابزارهای امنیتی و تحلیل لاگها

---

## روندهای نوین در امنیت API و آینده آن

- بررسی روندهای نوین مثل GraphQL و○ gRPC
  چالش‌های امنیتی درAPI های مدرن و نسل آینده