



WEB PenTEST



مقدمه

سرفصل دوره ی آموزشی:

- **Module 1 Introduction To Web Application Pentest**
- WEB app Architecture
- HTTP Protocol
- Web Application Framework
- Web Application Assessment Methodology
- OWASP
- **Module 2 Reconnaissance & Mapping**
- Search Engine
- DNS Enumeration
- Subdomains
- Service Enumeration
- Framework Enumeration
- WAF Detection
- Vhost & Dhost
- Mapping
- Automate Reconnaissance
- **Module 3 Client Side Attack**
- HTML & CSS Comment
- JS Control Bypass
- Js framework control bypass

تست نفوذ (Penetration Testing) به فرآیند هک اخلاقی گفته می‌شود که شامل ارزیابی برنامه یا زیرساخت یک سازمان در برابر انواع مختلف تهدیدات می‌شود. این تست کمک می‌کند تا از آسیب پذیری‌های مختلف سیستم جلوگیری شود و دلایل احتمالی این آسیب پذیری‌ها مانند تنظیمات نادرست و طراحی ضعیف تشخیص داده شود.

اهداف دوره:

در تعریفی ساده تست نفوذ، penetration testing یا pen testing یک حمله سایبری شبیه سازی شده علیه سیستم کامپیوتری شما است. این حمله شبیه سازی شده برای بررسی آسیب پذیری‌های قابل بهره برداری می‌باشد. تست نفوذ در واقع تلاشی برای ارزیابی سطح امنیت زیرساخت‌های فناوری اطلاعات، توسط آزمایش و اجرا آسیب پذیری‌های موجود به صورت امن است.

مدت زمان دوره:

30 ساعت – حضوری / آنلاین

WEB PenTEST

پیش نیازهای دوره

پیش نیاز ضروری برای این دوره ی آموزشی وجود ندارد.

درباره ی مدرک

به شرکت کنندگان در این دوره ی آموزشی گواهی حضور از سوی موسسه ITHOUSE اعطا خواهد شد.

- Automated bypass Control
- **Module 4 XSS**
- Types of XSS
- Discovery XSS
- Exploitation XSS
- **Module 5 Command & Code Injection**
- OS Command Injection
- OS Command Injection Code Execution
- **Module 6 XXE**
- XXE to FI
- XXE to command Injection
- XXE Xinclude
- XXE shell upload
- **Module 7 SQL Injection**
- Types of SQLI
- SQLI Discovery
- SQLI Discovery
- SQLI Exploitation
- **Module 8 Broken access control**
- IDOR
- Missing functional Level Access Control
- File Inclusion
- Shell Upload
- **Module 9 Identification and Authentication Failures**
- User Enumeration
- Disctionary Attack
- Rule base Attack
- Captcha Bypass
- **Module 10 Security Misconfiguration**
- Common weakness Enumeration (CWE)
- Unnecessary features
- Error handling
- **Module 11 Ajax Pentest**
- XML
- Json
- Html
- **Module 12 Business Logic Pentest**



درباره ی IT HOUSE

تیم مدیریتی IT House از سال ۱۳۸۷ به صورت جدی به منظور ارائه ی خدمات مشاوره ای و آموزشی در حوزه ی چارچوب های مدیریتی فناوری اطلاعات پا به عرصه ی ظهور گذاشت. این گروه در ابتدا تحت نام های تجاری دیگری همچون NIS ICT شروع به فعالیت نموده که در سال ۱۳۹۸ به منظور ارائه ی خدمات جدید و متفاوت برند IT House را ایجاد نموده اند. IT House با اتکا به توانمندی نیروهای متخصص داخلی و همینطور حمایت شبکه ای گسترده از شرکای بین المللی، همچون گذشته آمادگی دارد سبد کاملی از خدمات مورد نیاز سازمان ها را در حوزه های استاندارد ها و چارچوب های مدیریت فناوری اطلاعات و امنیت اطلاعات، ارائه نماید. حوزه های اصلی فعالیت این شرکت چارچوب ها و استانداردها و به روش های مدیریتی فناوری اطلاعات از جمله و نه محدود به موارد مندرج در دیاگرام های ذیل است که در هر یک از چارچوب های درج شده خدمات مرتبط با:

- آموزش
 - مشاوره
 - نرم افزار
 - ممیزی و مدورگواهینامه
 - ارزیابی
- بسته به نوع محصول، ارائه می شود.

تماس با IT HOUSE

آدرس:

تهران، سهروردی شمالی، کوچه تهمتن، پلاک 6 واحد 7

تلفن: + 98 (0) 21 88731466

فکس: + 98 (0) 21 86031447

وبسایت: www.it-house.me

ایمیل: info@it-house.me