



OWASP Software Secure Coding



OWASP

Open Web Application
Security Project

مقدمه

خود در این زمینه را براساس رهنمودهای OWASP و یا سایر خطوط راهنمای کدنویسی امن تولید نمایند.

برنامه نویسی حوزه بسیار وسیعی می باشد و متدها و خطوط راهنما و زبان های برنامه نویسی متنوعی وجود دارد. دوره ی حاضر با تمرکز بر نامه نویسی JAVA و تحت وب، براساس خطوط راهنمای OWASP طراحی گردیده است.

سرفصل های دوره

- Architecture of PC and mobile devices. x86, x64 and ARM.
- Java Virtual Machine (JVM) and Java Runtime Environment (JRE).
- ByteCode Verifier and Classloader;
- Security Manager and Access Controller, managing permissions policy.
- Java Native Interface (JNI).
- Secure Sockets Layer (SSL).
- Code signing.
- Buffer overflow.
- Format string attacks.
- Heap overflow.
- Return oriented programming.
- Defenses: stack canaries, DEP, ASLR.
- Thread safety and race conditions.

کلمه OWASP مخفف شده Open Web Application Security Protocol Project است و یک متدولوژی یا بهتر بگوییم یک پروژه غیر دولتی است که در آن به شما به عنوان یک کارشناس برنامه نویس تحت وب ، معیارهایی که بایستی برای امن تر شدن نرم افزار خود بکار ببرید تشریح شده است. OWASP یک متدولوژی است ، یعنی راهکار را به ما نشان می دهد ، این متدولوژی منحصر به شرکت یا فرد یا سازمان خاصی نبوده و نیست و یک پروژه کاملا متن باز (Open Source) است که هر کسی در هر جای دنیا می تواند به آن بپیوندد و در آن شرکت کند. جامعه آماری که برای پروژه OWASP فعالیت می کنند در زمینه های مختلفی از جمله تولید مقالات ، شرکت در تالارهای گفتمان ، معرفی و تولید نرم افزارهای امنیتی وب ، تولید مستندات و متدولوژی های امنیتی بصورت کاملا رایگان فعالیت می کنند و نتیجه فعالیت خود را در مستند نهایی این پروژه مشاهده می کنند. پروژه OWASP در ابتدا به عنوان یک استاندارد مطرح نشد اما امروزه به عنوان معیار یا بهتر بگوییم Baseline امنیتی طراحی و تولید امنیت در نرم افزارهای تحت وب استفاده می شود. این استاندارد به عنوان یکی از اصول کدنویسی امن در سایر استانداردها در صنایع مختلف مانند PCI DSS و PA DSS در صنعت پرداخت، توصیه گردیده است. بدین معنا که استاندارد PCI DSS ، از فعالان صنعت پرداخت میخواهد که نرم افزارهای

تیم مدیریتی IT House از سال ۱۳۸۷ به صورت جدی به منظور ارائه 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 خدمات جدید و متفاوت برند IT House را ایجاد نموده اند. 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 استانداردها 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 متدرج در دیاگرام های ذیل است که در هر یک از چارچوب های درج شده خدمات مرتبط با:

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

مدت زمان دوره

3 روز (24 ساعت)

تعداد شرکت کنندگان

15 الی 22 نفر

درباره ی مدرک

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

- SQL Injection
- Cross-site scripting.
- Cross-site request forgery.
- Broken authentication and session management.
- Insecure direct object reference.
- Invalidated Redirects.
- XML injection.
- Integer overflow. CVE-2013-1493.
- Unsafe deserialization CVE 2008-5353.
- Unsafe reflection CVE-2004-2331.
- Unsafe inner classes.
- Insecure cryptography.
- Secure Systems Development Lifecycle (Secure SDLC).
- Secure requirements definition.
- Application risk management and threat modeling.
- Application secure design principles.
- Static code analysis.
- Penetration testing and vulnerability assessment.
- Fuzzing.
- OWASP TOP 10, ASVS, Testing guide, Developers guide.

مخاطبان دوره

تمامی متخصصان و علاقمندان در حوزه امنیت اطلاعات بخصوص:

- کارشناسان امنیت و شبکه سازمانها
- برنامه نویسان JAVA
- تولید کنندگان نرم افزارهای صنایع پرداخت
- سازمان هایی که علاقمند به پیاده سازی PCIDSS و یا PADSS می باشند.

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