کارگاه آموزشی:حملات تحت وب، مقابله با آنها و برنامه نویسی امن در وب

سرفصل‌ها

- حمله SQL Injection
  - Union Based
  - Blind Based
  - روش‌های جلوگیری از حمله‌های SQL
- حمله XSS
  - Session and Cookies
  - Frame Options
  - XSS Reflected
  - XSS Stored
  - XSS Dom Based
  - XST
  - روش حمله و جلوگیری از XSS
  - Clickjacking
- LFI/RFI
  - خواندن داده
  - اجرای داده
  - Null Byte Poisoning
- روش‌های جلوگیری از LFI/RFI

پیش‌نیازها

- آشنایی با برنامه‌نویسی وب
- آشنایی با پایگاه داده ها در وب
- آشنایی با کانفیگ وب سرور
- آشنایی با WAFها

مدت پیشنهادی دوره

- ۶ ساعت

ابزارهای موردنیاز

- در صورت امکان لپ‌تاپ شخصی
- سیستم لینوکسی بصورت حقیقی یا مجازی در صورت امکان
- سیستم مجازی دارای وب سرور و زبان‌های برنامه‌نویسی سمت وب در صورت امکان

امکان برگزاری به صورت مجازی

- فعلا دوره به صورت حضوری برگزار می‌گردد.

مخاطبان دوره

- بخش آی تی و خدمات الکترونیکی ادارات، سازمان‌ها و نهادها
- بخش توسعه سمت وب شرکت‌های دولتی و خصوصی
- برنامه نویسان وب
- صاحبان سایت‌ها و خدمات در بستر وب
- دانشجویان و دانش‌آموزان علاقه‌مند به بحث برنامه نویسی وب

هزینه های دوره

- **شرکت برای عموم آزاد است.**
- **با توجه به محدودیت فضای سالن سمینار (۲۵ نفر) اولویت با کسانی است که زودتر ثبت نام نمایند.**

تاریخ برگزاری دوره

- **۲۲ بهمن تا ۲۹ بهمن روزهای فرد ساعت ۴ تا ۶ عصر**

مکان برگزاری دوره

- **سالن سمینار مرکز آپای دانشگاه ارومیه، واقع در پردیس شهر دانشگاه ارومیه، خیابان شهید بهشتی (دانشکده)، تلفن تماس: ۲-۳۳۴۸۸۲۳۰ ۰۴۴ و آدرس ایمیل:info@uucert.com**

نحوه ثبت نام

ثبت نام مشخصات در سایت uucert.com/workshops

مدرس دوره

- **میر سامان تاج بخش (سابقه ۸ سال کار در برنامه نویسی امن وب - دانشجوی دکتری رشته فناوری اطلاعات دانشگاه ارومیه)**

http://mstajbakhsh.ir

توضیحات

- در این دوره ابتداعا در ارتباط با نحوه عملکرد برنامه‌های سمت وب و مدل Client/Server و جایگاه پایگاه داده در این مدل صحبت خواهد شد. سپس به همراه مثال عملی، حمله SQL Injection تشریح شده و همزمان با تست بر روی برنامه آسیب پذیر از قبل تعبیه شده، حمله به نتیجه خواهد رسید. سپس در ارتباط با حمله سمت Client موسوم به XSS بحث خواهد شد. البته در این قسمت پیش‌نیازهای مربوطه نیز صحبت خواهد شد که مربوط به Session و Cookie است. زمان بیشتری

بر روی این مورد صرف خواهد شد چرا که جزء حملاتی است که کاربر را هدف گرفته و تشخیص سخت‌تری دارد. این در حالی است که در ماه گذشته (آذرماه ۱۳۹۵) از سیستم ایمیل شرکت یاهو، همین آسیب پذیری یافت شده است. در پایان این بخش در ارتباط با حمله ClickJacking نیز صحبت خواهد شد. در نهایت نیز در ارتباط با حمله LFI/RFI بحث شده و روش عملکرد این حمله تشریح خواهد شد. گفتنی است در انتهای هر بخش روش‌های جلوگیری از آسیب پذیری مربوطه تشریح خواهد شد. همچنین هریک از آسیب پذیری‌ها به همراه تست بر روی برنامه از قبل تعبیه شده، بصورت عملی تست و تشریح خواهد شد.