AppCheck
ACCURACY IS EVERYTHING

E: info@appcheck-ng.com
W: www.appcheck-ng.com
T: 0113 887 8380

Web Application Security Seminar

A Practical View of the Most Common Threats Facing Web Apps Today

Lord's Cricket Ground, St John's Wood, London, NW8 8QN

10am-4pm, Friday 8th November 2019

The Web Application Security seminar is a free event that presents a detailed analysis of the most common threats facing web applications today. We will review high profile examples and provide a technical breakdown of critical security flaws along with an introduction into emerging technologies such as HTML5.
Each delegate will receive a copy of the slides and exclusive tools and exploit code used in the live hacking demonstrations.

Seminar content includes:

Course Overview

Insecure web applications are among the greatest security threats to organisations today. To counter these threats AppCheck will host a web application security seminar to dissect these threats in detail and discuss how they impact organisations.

In the last year alone, AppCheck-NG completed over 11,000 web application vulnerability scans for some of the UK's leading organisations. Whilst carrying out these scans, we have uncovered a range of recurring, high risk vulnerabilities. This seminar presents a summary of our most recent findings, including live demonstrations of hacking techniques, and most importantly, best practice and remediation activities.

Key Benefits

This training module provides attendees with the following benefits: -

- Learn to protect your Web Applications from vulnerabilities that pose the greatest threat to organisations
- Gain an understanding of trends and changes in the threat landscape
- Confirmation of best practice and contemporary considerations
- Attain the skills required to test against the OWASP Top Ten
- Enjoy live hacking demonstrations
- Opportunity for detailed Q&A with one of the UK's leading pen testers, cyber researcher, and security innovator
- Insight into AppCheck's market leading technology
- Free Securing Web Applications Tool Kit
- Free use of the AppCheck Web Application and Infrastructure Scanner

Previous seminar attendee comments:

"I thoroughly enjoyed my day with AppCheck; the live hacking was a real eye opener. It showed how online tools are readily available for hackers to use, which has led me to take preventative steps to ensure this doesn't happen to our network. Overall an informative day which I would actively recommend to others… "

"Crammed a lot of content into a short time with practical and relatable real-world examples and testing methods"

"A fantastic and revealing insight into the world of hacking"

AppCheck
ACCURACY IS EVERYTHING

E: info@appcheck-ng.com
W: www.appcheck-ng.com
T: 0113 887 8380

The Days Agenda:

Introduction
- Brief introduction to AppCheck
- An overview of vulnerability types
- Recent high-profile vulnerability examples
- An introduction to security research and exploits development

Security Scanning
- Security scanning overview
- Information discovery techniques
- Introduction to parameter fuzzing

OWASP Top 10: Injection Vulnerabilities
- Overview of SQL Injection & high-profile examples
- SQL Injection 101
- Detecting and exploiting error-based SQL Injection
- Detecting and exploiting blind SQL Injection vulnerabilities
- Demo: Using content variance and time delays to extract database data
- Remote code execution via SQL Injection
- Watering hole attacks
- Demo: backdooring a CMS using SQL Injection
- Demo: Performing a watering hole attack to penetrate a secure network
- Defending against SQL Injection

AppCheck Demo
- Creating scans and reviewing results
- Using GoScript
- Q&A Session

Attacking the Supply Chain
- The modern web application supply chain
- Subdomain takeover attacks
- Demo: Performing a subdomain takeover attack against Azure
- Cloud storage misconfiguration
- Demo: Performing attacks against AWS S3
- Auditing third party JavaScript libraries

Attacking Users
- Cross-Site Scripting (XSS) attacks
- Detecting and exploiting reflected, stored and DOM based XSS
- Breaking parsers with obfuscation
- Demo: Cross-Site Scripting exploit frameworks

Additional Topics
Presented depending on time, otherwise presentations are provided for further reading

Upload Vulnerabilities
- Attacking upload components
- File path manipulation attacks
- The poison null byte
- Bypassing PHP mime type checking

HTML5 Vulnerabilities
- New features in HTML5
- Cross origin communication
- Attacking PostMessage
- CORS vulnerabilities

Q & A*
*The seminar is expected to finish at 4:30pm at the latest.

CALL OR EMAIL TO RESERVE YOUR COMPLIMENTARY PLACE:
LONDON WEB APPLICATION SECURITY SEMINAR
0113 887 8380 | info@appcheck-ng.com