• Networking, pizza and beer
• Welcome and OWASP Update
  Sam Stepanyan & Sherif Mansour
• CSP STS PKP ETC OMG WTF BBQ...
  Scott Helme
  ------------------------- short break -----------------------
• “Lightning” Talk - Jacks Tool Demo
  Lewis Arder
• Achieving Secure Continuous Delivery
  Lucian Corlan & Chris Rutter
• OWASP Roundup
  Sam Stepanyan
• Networking & Beer in the Brewhouse & Kitchen
Become a Member

We are all VOLUNTEERS!

OWASP
The Open Web Application Security Project

SUPPORTER
OWNP.ORG
2016
• Sam Stepanyan (@securestep9)
• Sherif Mansour (@kerberosmansour)
Software powers the world, but insecure software threatens safety, trust, and economic growth. The Open Web Application Security Project (OWASP) is dedicated to making application security visible by empowering individuals and organizations to make informed decisions about true application security risks.

OWASP boasts 46,000+ participants, more than 65 organizational supporters, and even more academic supporters.

As a 501(c)(3) not-for-profit worldwide charitable organization, OWASP does not endorse or recommend commercial products or services. Instead, we allow our community to remain vendor neutral with the collective wisdom of the best individual minds in application security worldwide. This simple rule is the key to our success since 2001.

Your individual and corporate membership powers the organization and helps us serve the mission. Please consider becoming an OWASP member today!

Not sure if you are a current member? Member Directory
Questions about OWASP Membership? MEMBERSHIP FAQ
Care to see our global membership demographics? Membership Demographics as of January 2014
Chapter Sponsors

The following are the list of OWASP Corporate Members who have generously aligned themselves with the London chapter, therefore contributing funds to our chapter:

- Gotham Digital Science
- Quotium
- Netsparker
- Veracode
- ThoughtWorks
- Intelligent Environments

Meeting Sponsors

The following is the list of organisations who have generously provided us with space for London chapter meetings:

- Skype
- Expedia
Contributing Members

These corporate members support OWASP at the $5,000 USD level annually.
Premier Members

These corporate members support OWASP at the $20,000 USD level annually.

Adobe, CONTRAST Security, Hewlett Packard Enterprise, Qualys, Salesforce
Application Security Verification Standard v3.01
Security knowledge framework

In order to provide you with accurate data about your application, the framework needs to know what processing functions are included in your application. Create a new project to get started if you haven't done so already.
HTTP strict transport security

Description:
HTTP Strict Transport Security (HSTS) is an opt-in security enhancement that is specified by a web application through the use of a special response header. Once a supported browser receives this header that browser will prevent any communications from being sent over HTTP to the specified domain and will instead send all communications over HTTPS. It also prevents HTTPS click through prompts on browsers.

Solution:
Simple example, using a long (1 year) max-age: Strict-Transport-Security: max-age=31536000

If all present and future subdomains will be HTTPS: Strict-Transport-Security: max-age=31536000; includeSubDomains

Recommended: If the site owner would like their domain to be included in the HSTS preload list maintained by Chrome (and used by Firefox and Safari), then use: Strict-Transport-Security: max-age=31536000; includeSubDomains; preload

The 'preload' flag indicates the site owner's consent to have their domain preloaded. The site owner still needs to then go and submit the domain to the list.

There is still a window where a user who has a fresh install, or who wipes out their local state, is vulnerable. This is due to the fact that the browser is not yet aware of the fact if the application the it is trying to connect to supports HSTS. Whenever you are added to the preload list, the application its preference is hard-coded into the browser and all first initial connections will always be made by HTTPS.

CAUTION Site owners can use HSTS to identify users without cookies. This can lead to a significant privacy leak.

Cookies can be manipulated from sub-domains, so omitting the include "includeSubDomains" option permits a broad range of cookie-related attacks that HSTS would otherwise prevent by requiring a valid certificate for a subdomain. Ensuring the "Secure Flag" is set on all cookies will also prevent, some, but not all, of the same attacks.
OWASP Top 10 - 2016 Data Call

The OWASP Top 10 project is launching its effort to update the Top 10 again. The current version was released in 2013, so this update is expected to be the 2016 or more likely 2017 release. This time around, we are making an open data call so anyone with application vulnerability statistics can contribute their data to the project. To make it easier for the project to consume this contributed data, we are requesting it be provided via this Google form.

DEADLINE: Data must be submitted by July 20, 2016.

As an OWASP project, we strive to make everything about every project as open as possible. For this release of the Top 10, we are going to publish all the contributed data so that anyone can review it to understand what input was considered to produce this update, and for other uses as well. We could imagine other groups/projects making use of this data for other reasons, so we believe publishing this data will have multiple benefits.

WARNING: You acknowledge that by contributing data to this update of the Top 10, that you authorize its publication. DO NOT CONTRIBUTE anything you don't want to become public.

Guidance on what data we are looking for:

We are looking for web application vulnerability statistics collected by your organization: external, internal, or a cross-section.
The OWASP AppSec Rugged DevOps Pipeline Project

The OWASP AppSec Rugged DevOps Pipeline Project is the place to find the information you need to increase the speed and automation of your AppSec program. Using the documentation and references of this project will allow you to setup your own AppSec Pipeline.

Description

The AppSec pipeline project is a place to gather together information, techniques and tools to create your own

What is the OWASP AppSec Pipeline Project?

The AppSec Pipeline project is a place to gather together information, techniques and tools to create your own AppSec Pipeline.

Project Leaders

Matt Tesauro 🗂️
Aaron Weaver 🗂️
Matt Konda 🗂️

Quick Download

Bag of Holding 🗂️

News and Events

AppSec EU June 2016 🗂️

In Print

Building an AppSec Pipeline 🗂️
Taking DevOps practices into your AppSec Life 🗂️
GAME OF HACKS

SEE HOW GOOD YOU ARE

This game was designed to test your application hacking skills. You will be presented with vulnerable pieces of code and your mission if you choose to accept it is to find which vulnerability exists in that code as quickly as possible.

SINGLE PLAYER

CHALLENGE YOUR FRIEND

Add your own code to the game
What vulnerability is exposed in this code?

- Reflected Cross-Site Scripting
- Command Injection
- A & B are correct
- None of the above

```python
from django.http import HttpResponse, HttpResponseRedirect
from django.template import loader, Context
import os;

def addressValidator(request):
    fullName = request.GET.get('fullName', None)
    address = request.GET.get('address', None)
    zipCode = request.GET.get('zip', None)
    zipValid = os.system('zipvalidator "" + zipCode + "\"\"" + address + "\\"")

    u = User(name=fullName, address=address, zipCode=zipCode, validZip=zipValid)

    t = loader.get_template('registration-form.html')
    return HttpResponse(t.render(Context(
        {'user': u}
    ), autoescape=False)))
```
Mobile-Security-Framework (MobSF)

Version: v0.9.2 beta

Mobile Security Framework (MobSF) is an intelligent, all-in-one open source mobile application (Android/iOS) automated pen-testing framework capable of performing static and dynamic analysis. It can be used for effective and fast security analysis of Android and iOS Applications and supports both binaries (APK & IPA) and zipped source code. MobSF can also perform Web API Security testing with it's API Fuzzer that can do Information Gathering, analyze Security Headers, identify Mobile API specific vulnerabilities like XXE, SSRF, Path Traversal, IDOR, and other logical issues related to Session and API Rate Limiting.

Made with ❤️ in India
Chapter Activity

• Sherif Mansour - CyberSecurity Challenge
• Scott Helme
Main Talks

- CSP STS PKP ETC OMG WTF BBQ...
  Scott Helme

- short break

- “Lightning” Talk - Jacks Tool Demo
  Lewis Ardem

- Achieving Secure Continuous Delivery
  Lucian Corlan & Chris Rutter
APPSECUSA 2016

Oct 11-14, 2016 in Washington DC, USA

OWASP’s 13th Annual AppSecUSA Security Conference is the premier application security conference for developers and security experts. Come hear an amazing group of inspirational speakers—including YouTube’s Favorite Hacker, Former DHS NCSD Director of Software Assurance, and Assistant Professor & Cryptographer—who are challenging traditions. You’ll be inspired by fresh ideas, start rethinking the status quo, and leave ready to tackle your challenges in innovative ways.

REGISTER NOW

11 - 14 October 2016
Washington DC, USA
Chapter Sponsors

The following are the list of OWASP Corporate Members who have generously aligned themselves with the London chapter, therefore contributing funds to our chapter:

- Gotham Digital Science
- Quotium
- Netsparker
- Veracode
- ThoughtWorks
- Intelligent Environments

Meeting Sponsors

The following is the list of organisations who have generously provided us with space for London chapter meetings:

- Skype
- Expedia
Thank You

Speakers:

- Scott Helme
- Lewis Ardern
- Lucian Corlan
- Chris Rutter

London Chapter Leaders:

- Sam Stepanyan
- Sherif Mansour

Hosts for this event

- Expedia

- Attendees (you!)
Keep in Touch – get informed about future events:

Join The OWASP London Mailing List
http://lists.owasp.org/mailman/listinfo/owasp-london

Follow us on Twitter
@owasplondon

“Like” us on Facebook
https://www.facebook.com/OWASPLondon

Visit OWASP London Chapter webpage
https://www.owasp.org/index.php/London

OWASP London
Save The Dates of Future meetings:
29th September 2016
24th November 2016
Call For Speakers For Future Events

Do you have a great Web Application Security Related Talk?

3 Tracks:

• Breakers
• Defenders
• Builders

Submit the abstract of your talk and your bio to:

owasplondon (at) owasp.org
Drinks and Networking
“Brewhouse and Kitchen”