



OWASP Egypt Chapter - Introduction

Mohamed Alfateh
Cairo Chapter Leader
Mohamed.alfateh@owasp.org

OWASP

21/4/2014

Copyright © The OWASP Foundation
Permission is granted to copy, distribute and/or modify this document
under the terms of the OWASP License.

The OWASP Foundation
<http://www.owasp.org>



What is OWASP

- Worldwide non-profitable charitable organization
- Focused on improving the security of software
- Founded: September 23, 2001

OWASP Resources and Community

Documentation (Wiki and Books)

- Code Review, Testing, Building, Legal, more ...

Code Projects

- Defensive, Offensive (Test tools), Education, Process, more ...

Chapters

- Over 270 and growing

Conferences

- Major and minor events all around the world

OWASP community

- Corporations
- Educational organizations
- Individuals from all over the world

OWASP community

- These communities work to create:
 - Articles,
 - Methodologies,
 - Documentation,
 - Tools & technologies
- Freely available to everyone

OWASP community

■ Vendor Neutral

- Does not endorse or recommend commercial products or services.

- All members are volunteers

■ All OWASP expenses are covered by:

- Conferences,
- Memberships,
- Corporate sponsors and
- Banner advertisements.

OWASP Mission

To make software security "visible" so that individuals and organizations worldwide can protect themselves and make informed decisions about software security risks.



OWASP Core Values

INNOVATION

OPEN

**CORE
VALUES**

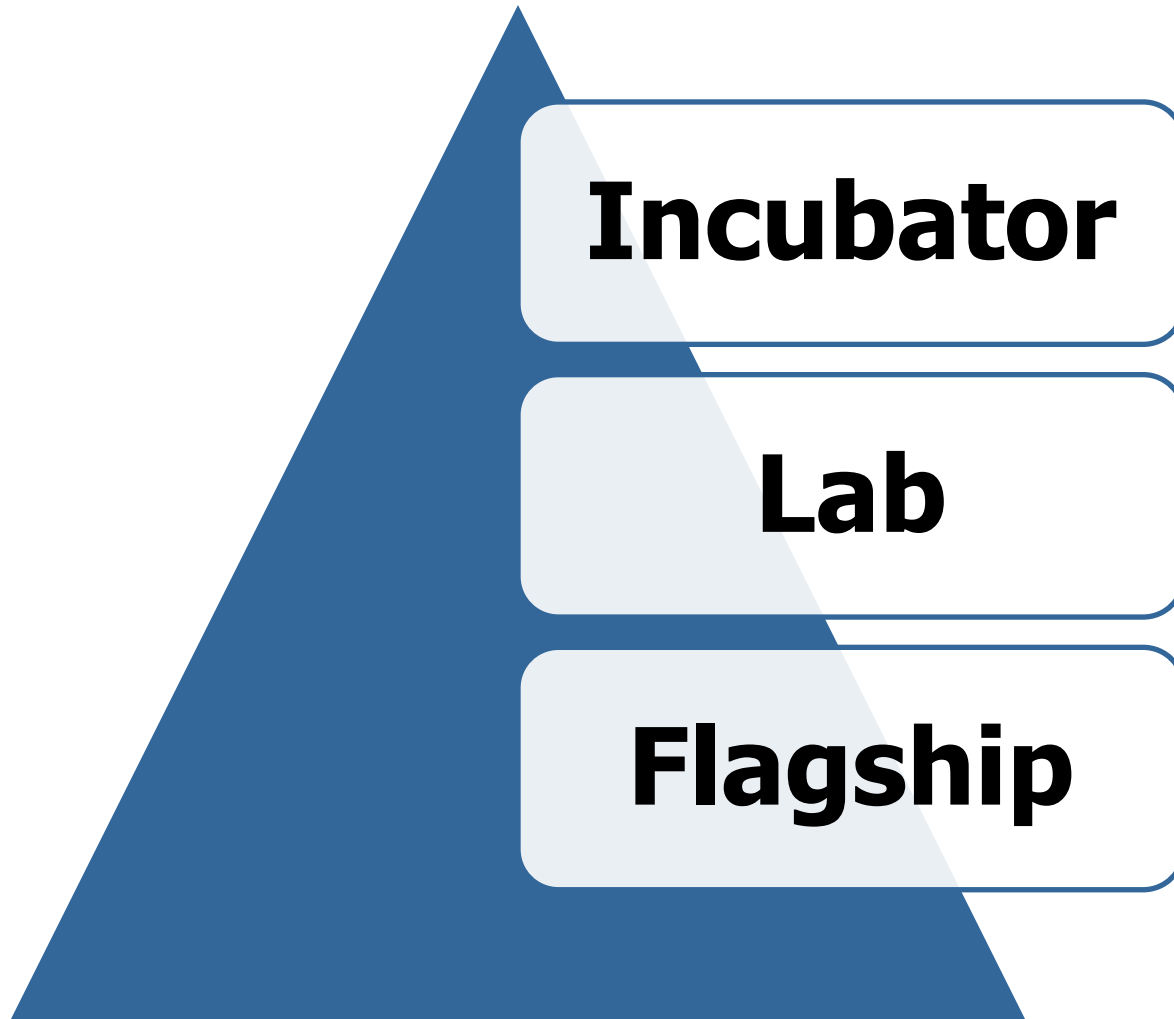
GLOBAL

INTEGRITY

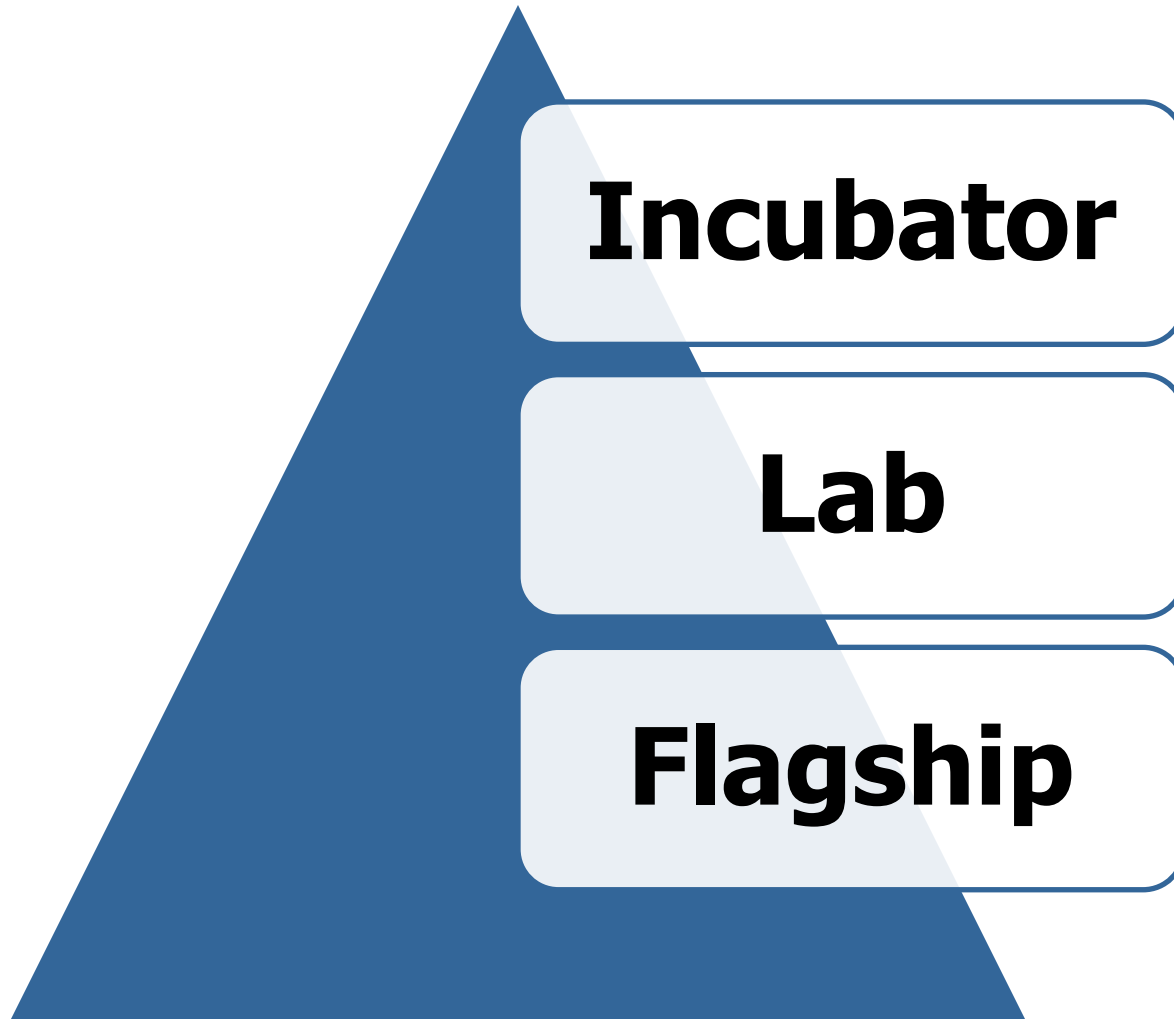
OWASP Projects

- Over 142 active projects,
- New project applications submitted every week
- Cover many aspects of application and software security
 - Documents
 - Tools
 - Teaching environments
 - Guidelines
 - Checklists

OWASP Projects



OWASP Projects



Education



The following courses either have been offered or are being offered free of charge courtesy of the trainers and the OWASP Foundation to anyone interested in learning about application security. Additionally, the training slides/coursework is available under an open source license and we encourage you to use it to set up your own training event!

- OWASP Conference Presentations
- Chapter Presentations
- OWASP Project Presentations
- OWASP Education Presentations
- Web Application Security Presentations

Heartbleed Bug (April 2014)



Page

[Discussion](#)

[Read](#)

Heartbleed Bug

Contents [\[hide\]](#)

- [1 Introduction](#)
- [2 About the Name](#)
- [3 Timing](#)
- [4 Severity](#)
 - [4.1 Session Hijacking with Heartbleed](#)
- [5 Explanation of the Bug](#)
- [6 The Fix](#)
- [7 Impact of the Vulnerability](#)
- [8 Defending against Vulnerability](#)
- [9 Exploit POCs](#)
- [10 Links for More Information](#)

Introduction

Heartbleed is a catastrophic bug in OpenSSL, anno

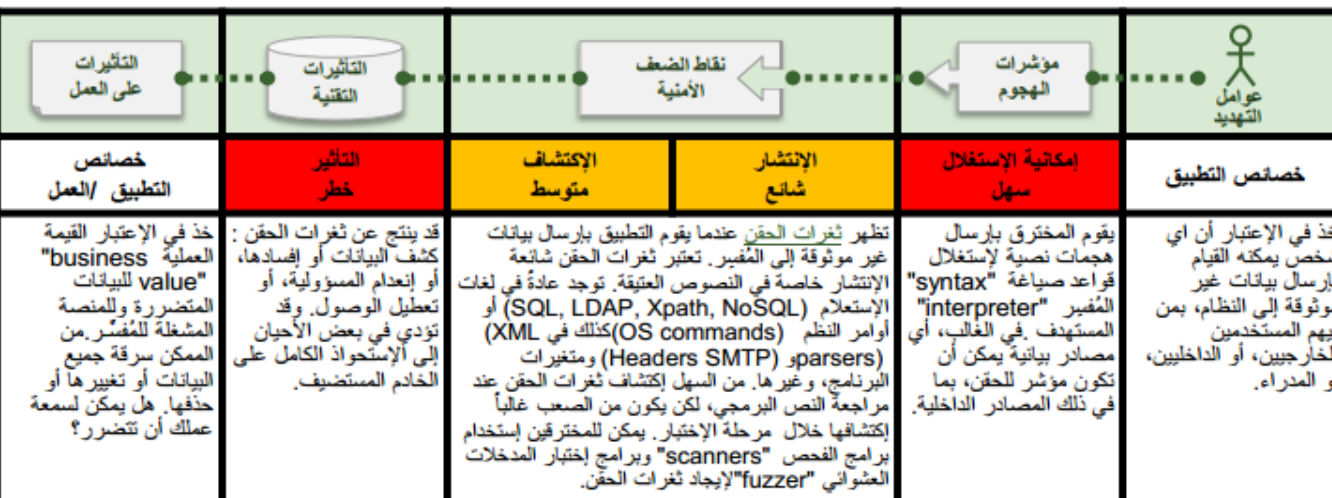


Navigation

- [Home](#)
- [About OWASP](#)
- [Acknowledgements](#)
- [Advertising](#)
- [AppSec Conferences](#)
- [Brand Resources](#)
- [Chapters](#)
- [Donate to OWASP](#)
- [Downloads](#)
- [Governance](#)
- [Funding](#)
- [Mailing Lists](#)
- [Membership](#)
- [News](#)

OWASP





OWASP Top 10 Arabic

كيف أمنع هذه الثغرة؟

منع ثغرات الحقن تتطلب عزل البيانات الغير موثوقة عن الأوامر والإستعلامات:

1. الخيار المفضل هو بإستخدام واجهة التطبيق البرمجية "API" والتي تتجنب استخدام المُفسر بشكل كامل، أو مخاطبتها عبر واجهة المعاملات "parameterized interface". يجب الحذر عن استخدام واجهات التطبيق البرمجية، مثل الإجراءات المخزنة التي تتعامل بالمعاملات حيث يمكن أن تتسبب في ثغرات الحقن.

2. في حال عدم توفر واجهة التطبيق البرمجية التي تتعامل بالمعاملات "parameterized API" فعليك استخدام -وبحذر- صياغات تخطي مناسبة لتخطي بعض الرموز الخاصة «special character». مشروع (OWASP's ESAPI) يقدم الكثير من أساليب التخطي.

3. التحقق من المدخلات عبر القوائم البيضاء من الإجراءات التي ينصح بها، لكن لا يعتبر هذا الأسلوب دفاعي كامل، حيث أن كثير من التطبيقات تتطلب استخدام الرموز الخاصة كمدخلات. في حال وجوب استخدام الرموز الخاصة، فالأسلوبان أعلاه (رقم 1 و 2) هما الأفضل استخداماً. يقدم مشروع (OWASP's ESAPI) مكتبة شاملة من أساليب التحقق من المدخلات عبر القوائم البيضاء.

هل أنا معرض لهذه الثغرة؟

أفضل طريقة لمعرفة ما إذا كان التطبيق يعاني من ثغرات الحقن هو بالتحقق من أن جميع استخدامات المُفسر يتم فيها عزل البيانات الغير موثوقة عن الأوامر والإستعلامات. بالنسبة لطليات لغة الإستعلام (SQL)، فهذا يعني ضرورة استخدام متغيرات مرتبطة "bind variables" في جميع الجمل المُعدّة مسبقاً والإجراءات المخزنة "stored procedures"، وتجنب إستخدام الإستعلامات التفاعلية «dynamic queries».

إن عملية فحص النص البرمجي هي أسرع وأدق طريقة لإكتشاف ما إذا كان التطبيق يستخدم المُفسر بطريقة سليمة. تساعد أدوات (أو برامج) تحليل النص البرمجي إكتشاف استخدامات المُفسر ومتابعة تدفق البيانات خلال التطبيق. مختبري الإختراق يمكن لهم التحقق من وجود هذه الثغرات عبر تطوير استغلالات مناسبة لذلك.

قد تتمكن برامج الفحص التفاعلية الآلية "dynamic scanner" من إختبار التطبيق وبيان ما إذا كان يعاني من وجود أي ثغرات حقن يمكن إستغلالها. قد لا تتمكن برامج الفحص دائماً من الوصول إلى المُفسر وبهذا ستواجه صعوبة في تحديد نجاح الإستغلال من فشله. سوء معالجة الأخطاء "error handling" بشكل صحيح يجعل من السهل جداً إكتشاف وجود ثغرات الحقن.

مراجع

أواسب:

• OWASP SQL Injection Prevention Cheat Sheet

أمثلة لكيفية الإختراق

المثال الأول: التطبيق يستخدم بيانات غير موثوقة لتكوين جملة إستعلام (SQL) مصابة:

String query = "SELECT * FROM accounts WHERE



OWASP University or Educational Membership

Be recognized as a supporter by posting your university logo on the OWASP

OWASP and the University can jointly publicize season of code events which provide funding for students or faculty to perform security based research

Host security seminars

Provide introductory training sessions for students

NO COST!!

OWASP University or Educational Membership

Provide meeting space 2x per year

Include OWASP in the education, awareness, and curriculum to students.

Encourage students to apply and work on OWASP projects

OWASP University or Educational Membership



How to Participate

- Everyone is free to participate in OWASP
- All of the materials are available under a free and open software license.
- OWASP global group of volunteers are over 36,000 participants.

How to Participate

■ Join a project

- Freely test theories and ideas with the professional advice and support of the OWASP community

■ Edit a page

- Thousands of active wiki users around the globe who review the changes to ensure quality

■ Global Initiatives

- Program was established to provide easy access for volunteers interested in contributing in OWASP

■ Local Chapters

OWASP Egypt Chapter

Egypt AppSec Sample Qualified Professionals



SANS Advanced Penetration Testing Instructor
DEFCON 21 speaker

SANS best performance Award

GIAC's GSSP-JAVA and GSSP-NET Exams Steering

Committee Member

OWASP Project Leader



Bug Hunters

Google™



at&t

Yandex
Яндекс



github
SOCIAL CODING

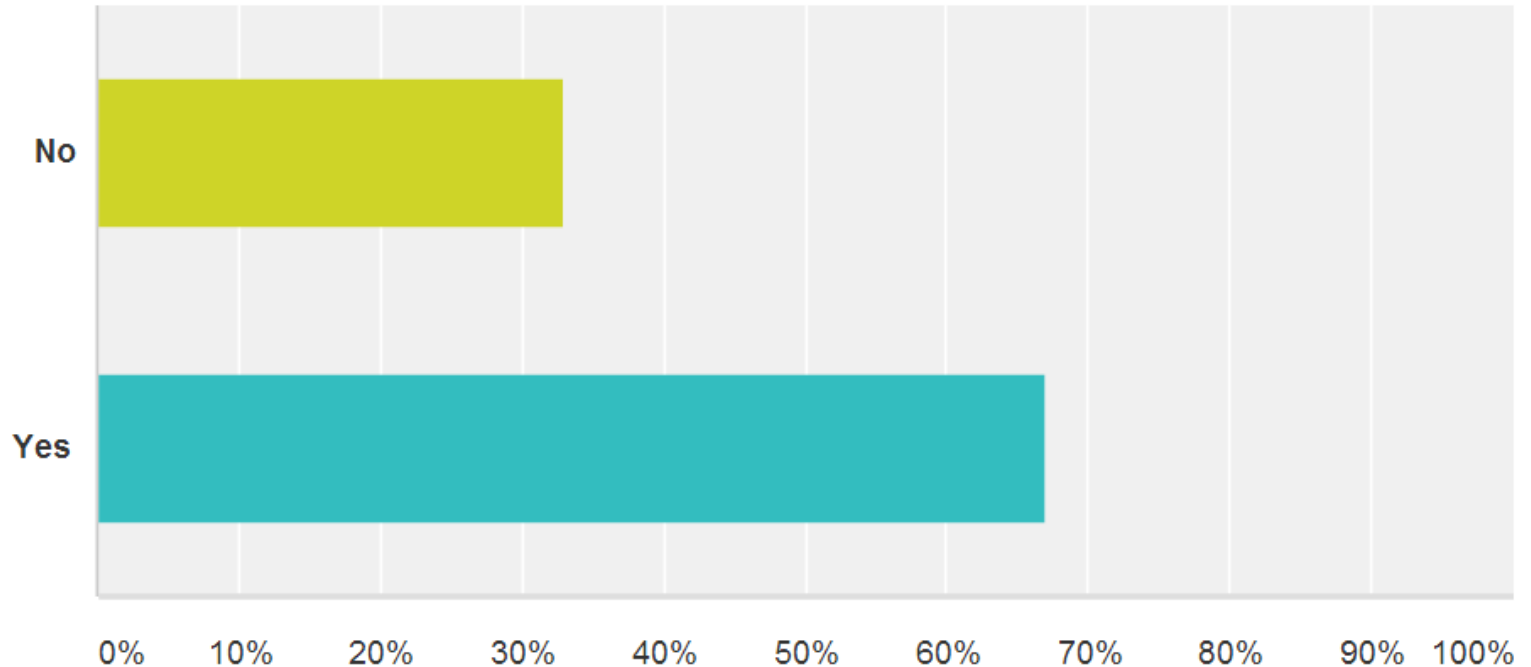


Adobe



Pre-Event Survey

Would you be willing to participate in an awareness program to increase the application security know-how for Egyptian governments?



Answer Choices	Responses	
No	33.09%	45
Yes	66.91%	91

Security In Egypt



Date	Notifier
2014/04/11	AKINCILAR
2014/04/03	ErHaBi HAIL
2014/04/03	ErHaBi HAIL
2014/03/31	ymh
2014/03/23	ymh
2014/03/10	fallag_gassrini
2014/01/27	ErHaBi HAIL
2013/11/24	ymh
2013/11/24	ymh
2013/11/24	ymh
2013/11/21	Algeriano
2013/11/20	AKINCILAR
2013/11/13	AKINCILAR
2013/11/12	AKINCILAR
2013/10/31	MoroccanGhosts
2013/10/02	AKINCILAR
2013/10/02	CapoO_TunisiAnoO
2013/10/02	CapoO_TunisiAnoO
2013/09/28	Watchful Eye Hacker
2013/09/25	MrWanz
2013/09/22	MR.KADEROU
2013/09/21	ayyildiztim
2013/09/21	MrWanz
2013/09/13	mosh3
2013/09/13	AnonyMOus-Jo


H	M	R	L			
	M	R			Date : <input type="text" value="ALL"/>	<input type="button" value="Apply filter"/>
	M					
	M				★	Linux
	M				★	Win 2008
	R				★	Win 2008
H					★	Win 2008
H	R				★	Linux
	M	R			★	Win 2003
	M				★	Win 2003
	M				★	Win 2003
	R				★	Win 2008
	M				★	Win 2000
					★	Win 2003
					★	Linux
	R				★	Win 2003
H					★	Win 2003
					★	Win 2003
H					★	Win 2003
	M				★	Win 2008
H					★	Linux
H					★	Win 2008
					★	Win 2008
					★	Linux
	R				★	Win 2003
H	R				★	Linux



Security In Egypt

改善

BLUE KAIZEN

CONNECTING MINDS  IMPROVING LIVES

CSCAMP2012

THE MILESTONE



IS EGYPT HACKED !

After Two Years

Case Studies

Publications

Contact

You Just Viewed

Oil & Gas - Brief

Industries

Power - Case Studies

Power - Case Studies

Of Further Interest

Oil & Gas - Brief

Industries

Power - Case Studies

Power - Case Studies

Case Studies

All Industries

All Solutions

Shabab 1000 MW and Damietta 500 MW Simple Cycle Pow

SCADA System for Great Cairo – DCS

Al-Hassa Irrigation and Drainage Project

Water Management System Project

Telecom Egypt Hardware Maintenance

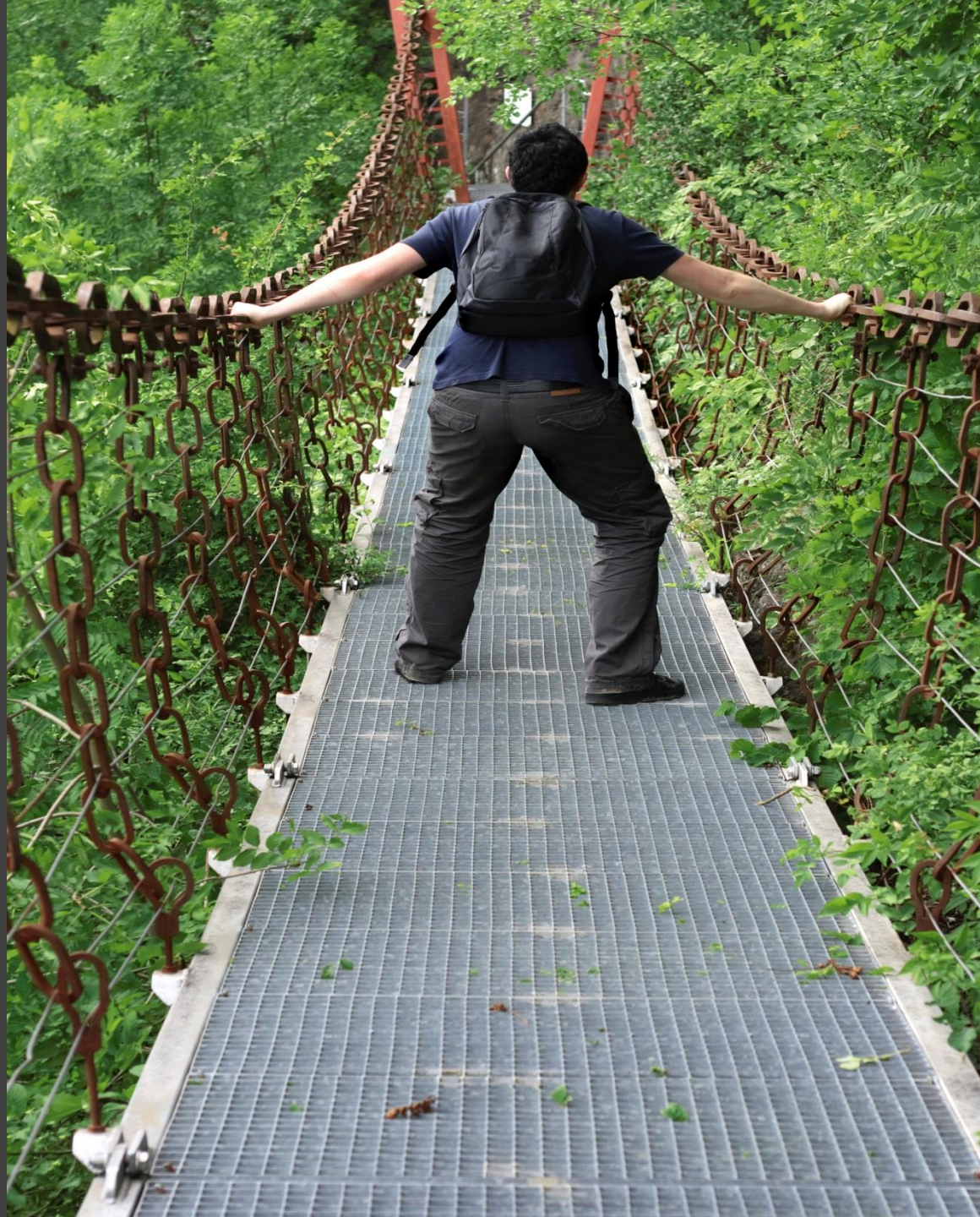
Telecom Egypt Data Collection

Telecom Egypt Data Center Installation

Upgrading CX700 to CX4

Kafr El Dawar Thermal Power Plant Rehabilitation Project





OWASP Egypt Chapter

- Attending our chapter meetings is FREE and OPEN to anyone
- Chapter mailing list
 - Address all questions pertaining to application security, of any level of technical ability
- Focus Groups
- Vendor Neutral Environments
- Educational workshops

2014 Pain

- Application Security Awareness Program (ASAP)
- Bi-Monthly Meeting
- OWASP Project Day

OWASP membership

Membership category	Annual membership fee
Individual Supporters	\$50
Organization Supporters	Starting by \$5,000
Accredited University Supporters	FREE

- Funds OWASP Speakers via OWASP On the Move
- Funds Season of Code projects
- Helps Support Local Chapters

Event Sessions

Egypt Cert Security Awareness Program

Effective Bug Hunting for Open Source Applications



OWASP Security Research and Development Framework



Facebook Zero-Day Vulnerability - Code Point of View



OWASP Projects - Overview



**Open Discussion: Information Security Challenges, from Individual
Privacy to National Security.**

That's it...

Any questions or comments?

Presentation will be online:

Thank you!