



# **Hardening Project**

**a comprehensive security competition  
for website hardening**

<http://wasforum.jp/hardening-project/>

# FACT: 3000 people / 2 years attended OWASP Night Interest in Security in Japan is increasing greatly

---



# FACT: Guidelines, documents, tools, frameworks... “Knowhow” necessary for security in high demand

## e.g. OWASP Top 10

[https://www.owasp.org/index.php/Category:OWASP\\_Top\\_Ten\\_Project](https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project)

- **A1** Injection
- **A2** Broken Authentication and Session Management
- **A3** Cross-Site Scripting (XSS)
- **A4** Insecure Direct Object References
- **A5** Security Misconfiguration
- **A6** Sensitive Data Exposure
- **A7** Missing Function Level Access Control
- **A8** Cross-Site Request Forgery (CSRF)
- **A9** Using Components with Known Vulnerabilities
- **A10** Unvalidated Redirects and Forwards

日本語版  
Japanese version

**OWASP**  
The Open Web Application Security Project

**OWASP Top 10 - 2013**  
The Ten Most Critical Web Application Security Risks

+F
リスク因子に関する詳細

Top 10 リスク因子のまとめ

下の表は、2013 Top 10アプリケーションのセキュリティリスクと我々が各リスクに付けたリスク因子のまとめです。これらの因子は、OWASP Top 10チームが持つ統計資料と経験に基づいて決定しました。それぞれのアプリケーションや組織におけるリスクを理解するために、あなた自身にとっての「脅威となる人」と「ビジネスへの影響」を考慮しないといけません。ソフトウェアに基いたしい弱点があったとしても、攻撃をする「脅威となる人」がいない、或いは関連資産への「ビジネス的影響」が軽微な場合、重大なリスクにはなりません。

リスク	脅威となる人	攻撃手法 利用難易度	普及度	検出難易度	技術的影響	ビジネスへの影響
A1-インジェクション	アプリ依存	容易	中	普通	深刻	アプリ依存
A2-認証	アプリ依存	普通	高	普通	深刻	アプリ依存
A3-XSS	アプリ依存	普通	極高	容易	中程度	アプリ依存
A4-安全でないIDR	アプリ依存	容易	中	容易	中程度	アプリ依存
A5-設定ミス	アプリ依存	容易	中	容易	中程度	アプリ依存
A6-機密データ	アプリ依存	困難	低	普通	深刻	アプリ依存
A7-機密アクセス	アプリ依存	容易	中	普通	中程度	アプリ依存
A8-CSRF	アプリ依存	普通	中	容易	中程度	アプリ依存
A9-コンポーネント	アプリ依存	普通	高	困難	中程度	アプリ依存
A10-リダイレクト	アプリ依存	普通	低	容易	中程度	アプリ依存

その他の考慮すべきリスク

Top 10は、幅広く含めています。あなたの組織にとって考慮・評価すべきリスクは、他に多数あります。以前のTop 10に含まれていたリスクもありますが、まだ識別されていない新たな攻撃手法もあります。他に考慮すべき重要なアプリケーションのセキュリティリスクを以下に示します(アルファベット順)。

- クリックジャッキング
- 非正規の文法
- DoS攻撃 (2004 Top 10 だった - エントリー - 2004-A9)
- ELExpression Languageインジェクション (CVE-912)
- 情報流出と不適切なエラー処理 (2007 Top 10 の一部だった - エントリー - 2007-A6)
- 不十分な自動化防止 (CVE-799)
- 不十分なロギングと責任追及性 (2007 Top 10 に関連していた - エントリー - 2007-A6)
- 悪意ある検索と参照の欠陥
- 悪意あるファイルの実行 (2007 Top 10 だった - エントリー - 2007-A3)
- 大量読み込み (CVE-915)
- ユーザプライム

# **FACT: Professionals in the following fields struggling with...**

---

■ **Systems operation**

■ **Security incident response**

■ **Web systems implementation**

■ **Customer support**

■ **Prospective workers in these fields  
(e.g. students, etc.)**

# ISSUE: Who's actually dealing with Security

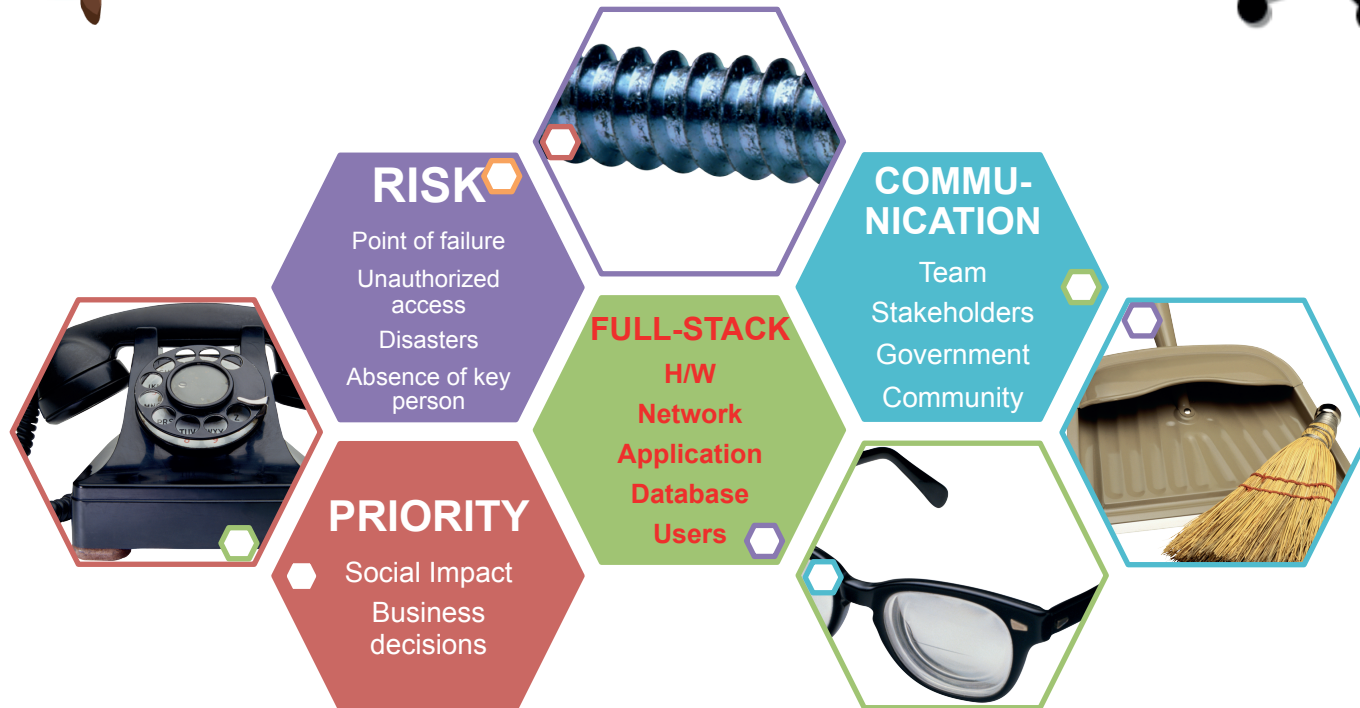
## What do you have to say about Defenders' skills?

---

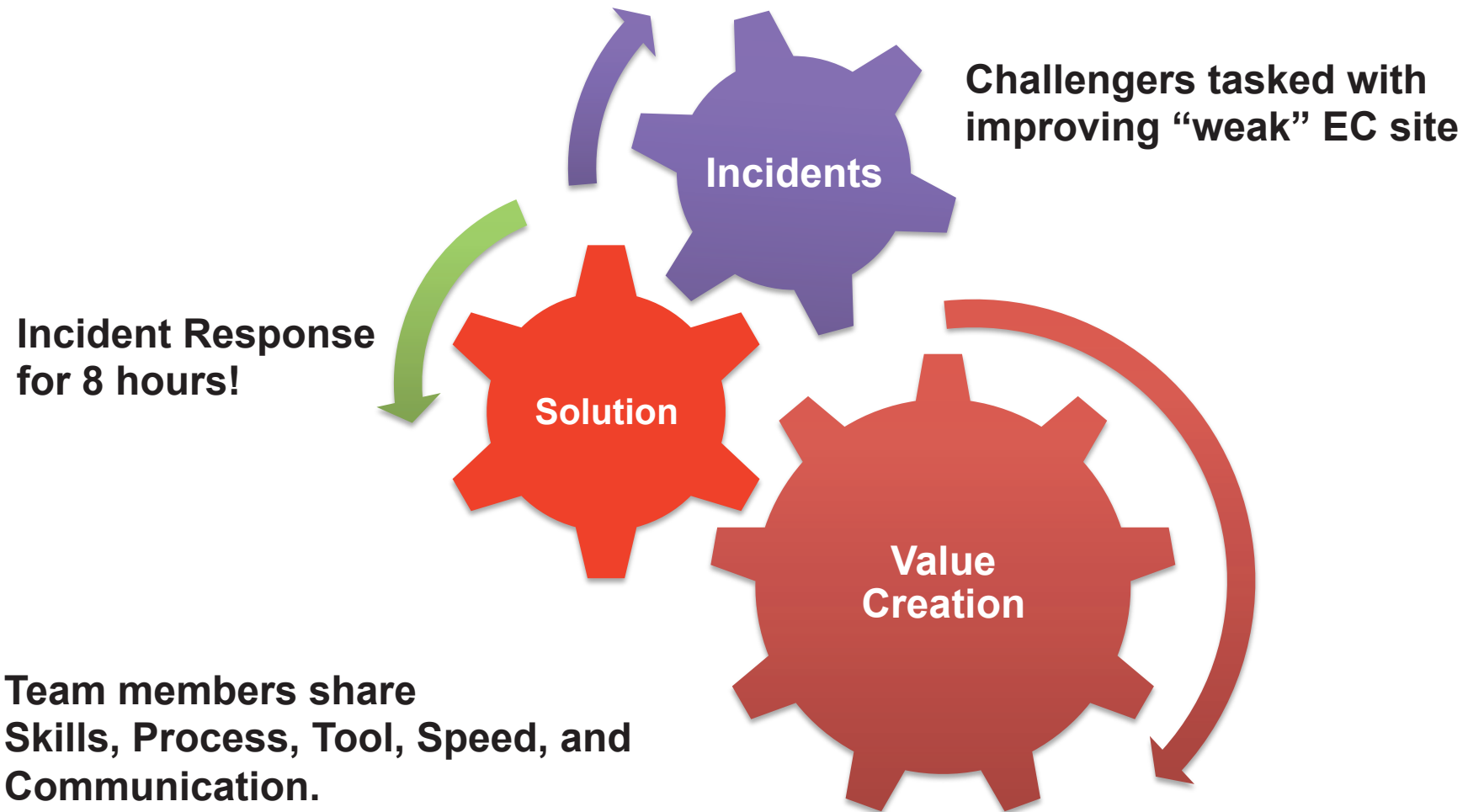
- Ability to correctly **understand the condition of the system environment**
- Ability to **detect irregularities in system operations** and security issues
- Ability to **predict future security incidents** and other potential risks
- Ability to quickly **detect and deal with security incidents**
- Ability to **detect security faults and vulnerabilities**
- Ability to **repair vulnerabilities and mitigate risk**
- Ability to **implement effective security incident triage**
- Ability to **efficiently and effectively deploy team resources**
- Overall ability and capabilities as well as **skill set of the team**
- Ability to effectively **communicate with users and other stakeholders**
- Ability to **coordination among various departments in the organization**
- **Strong mental power and spirit** to never give up no matter how difficult the challenge at hand is

**How many people do you know with these skills?**

# Knowledge needed for solving problems in systems operation isn't “Breaker skills” it's “Builder skills”



**Challenge of technical decision making:**  
**Effective and solid collaboration on individual incidents**  
**leads to development of strong problem-solving skills**



# What is the purpose of Hardening Project?

Discover and award collaborative minds with **defending skills.**

All of challengers will try to work with:

- New Talent
- New Team
- New Methodology
- New Approach
- New Process
- New Communication

And will achieve a **New Hardening Sense.**



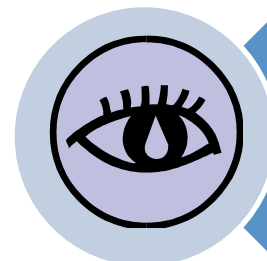
**Service-BCP**

Focus on prevention techniques and process



**Discover DEFENDERS!**

Engineering awards and talent discovery



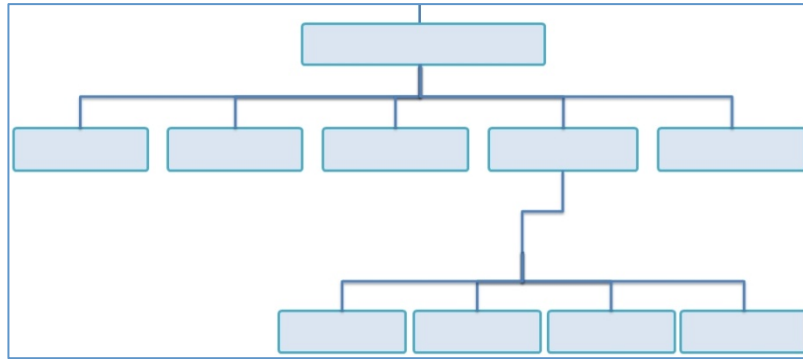
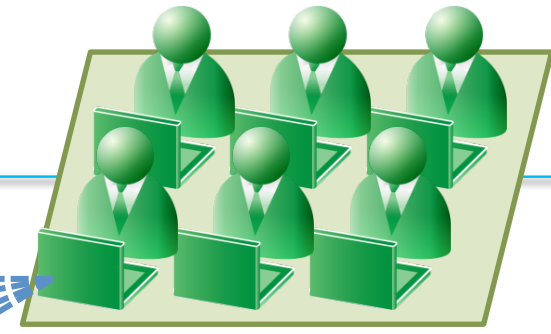
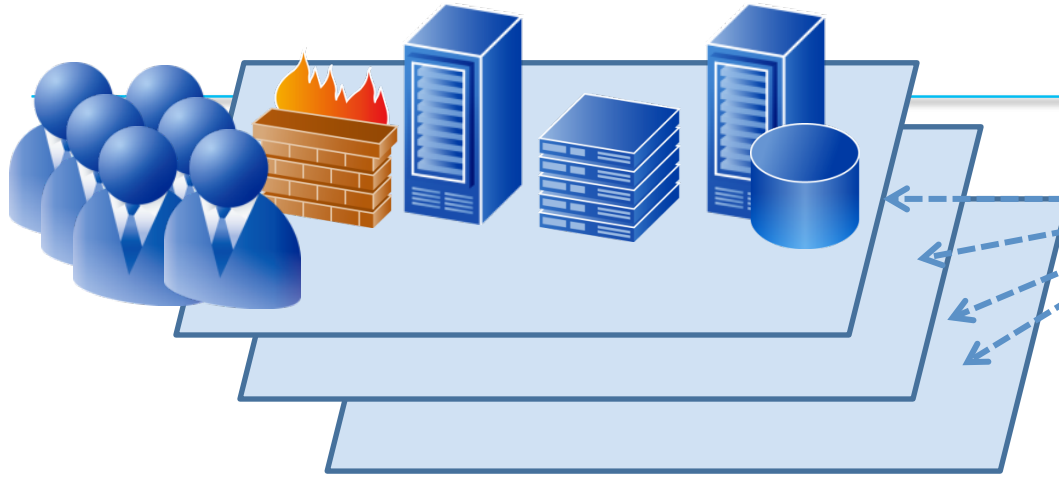
**From Users' point of view**

Perspective for stakeholder communication

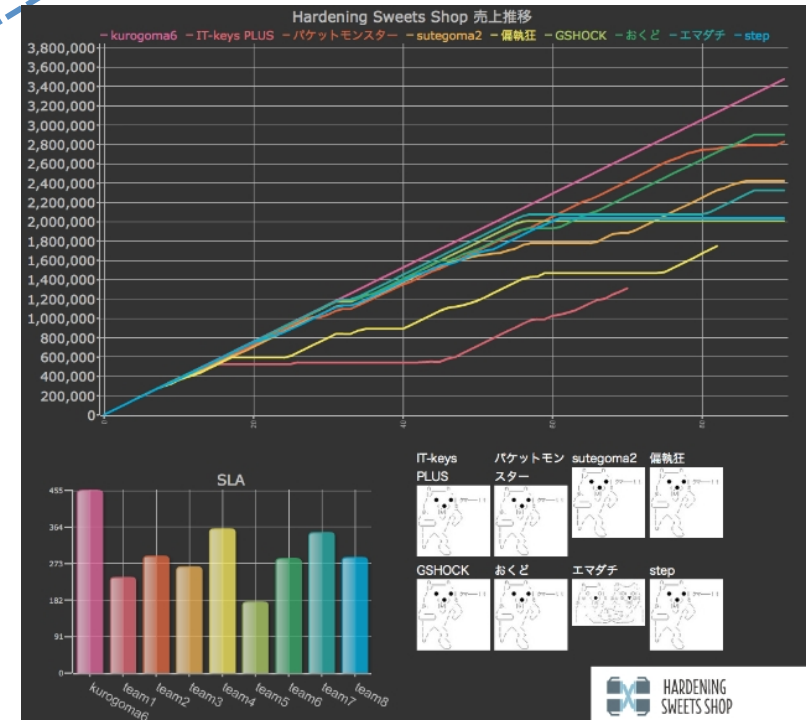


# 8 Challenger Teams

# Attackers: kuromame6

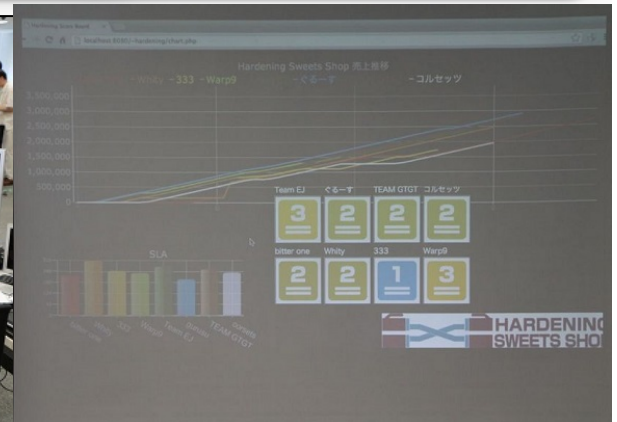


Virtual E-Commerce Site and administration environment on StarBED (NICT)



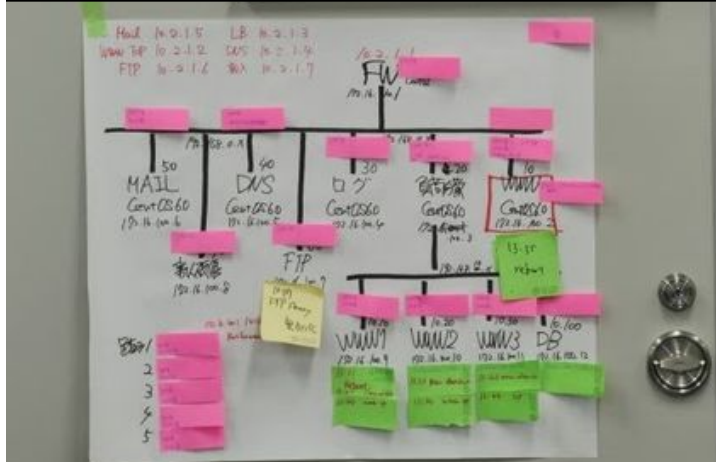
Sales Competition for 8 hours

2012/4 Hardening Zero  
 2012/10 Hardening One  
 2013/7 Hardening One Remix  
 2014/6 Hardening 10 APAC  
 ...



2012/4 Hardening Zero  
2012/10 Hardening One  
2013/7 Hardening One Remix  
2014/6 Hardening 10 APAC

...



# Thoughts and impressions from participants

## Participant A

“Even with the same environment, same product and same attacks, there was a **gap of 300% in revenue based on operational differences**. This demonstrated the need for and importance of secure operations.”

## Participant B

“I gained a deeper insight into the **importance of choosing which problem to prioritize** and focus on given only a limited amount of time.”

**Privacy data**

**Attached files??**

**Claims from Customers**

**DoS**

**WHY REBOOT??**

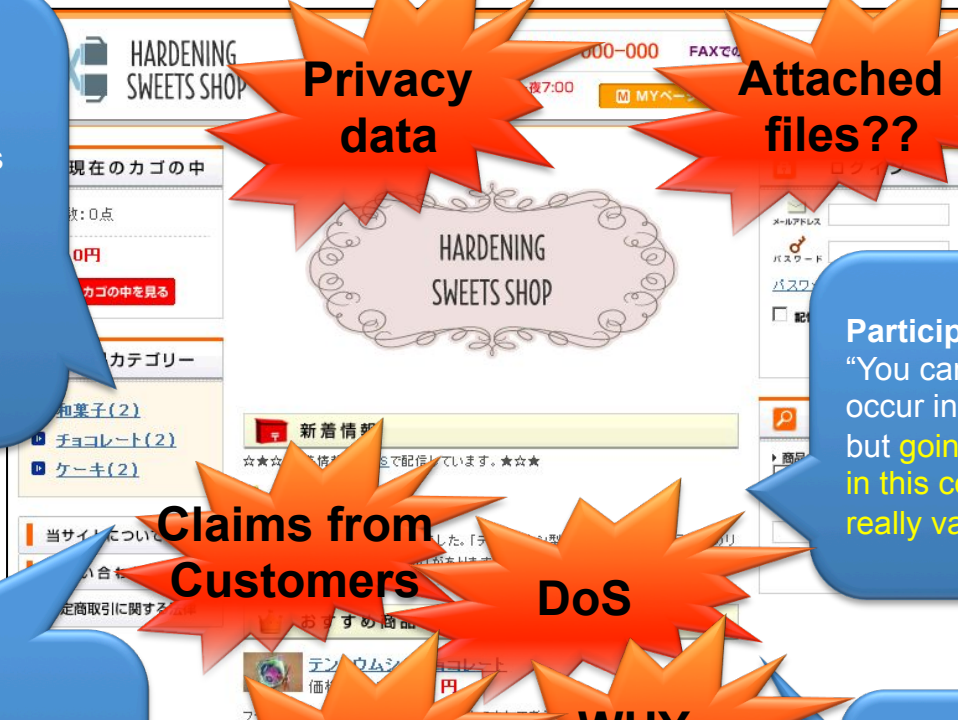
**WHY STOP??**

## Participant C

“You can’t allow a system error to occur in the production environment but **going through bitter experiences in this controlled environment is a really valuable experience.**”

## Participant D

“In addition to the competition on Hardening Day, the **reflection on Softening Day is also very important.**”



# Hardening 2 Days Framework

---

## 1<sup>st</sup> Hardening Day

- **8 Hour Competition**
  - “**Kuromame 6**” with more incidents vs. **8 defender teams**
- **Live stream** with Online Conference

## Networking

- Enjoy **cross-border communications** & unwinding

## 2<sup>nd</sup> Softening Day

- All teams present their **approach and challenges**
- Presentation from “**Attacker**”

## Awards

- **Awards ceremony** for the Winner and MVPs

# 2014 expansion to APAC region

---



Hosting events in **Naha, Okinawa**

- strategically located as a **hub in the Asia Pacific region**

**Hardening 10 APAC** Jun. 2014

6 hour competition & presentations

**Hardening 10 Evolutions** Nov. 2014

2 day conference & workshops

idea-thon, hack-a-thon

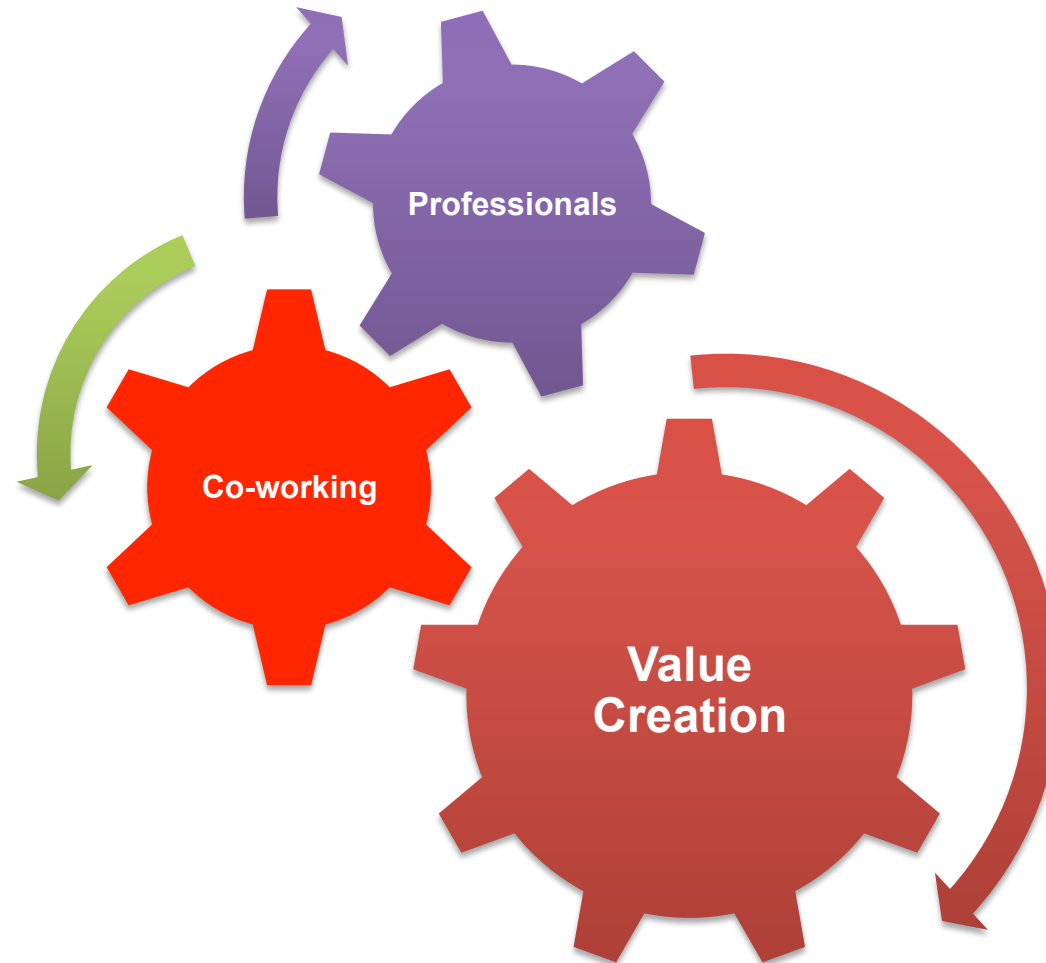
& presentations

**DETAILED INFORMATION**

<http://wasforum.jp>

# Competition meets Collaboration

---





Web Application Security Forum  
**Hardening Project**

riotaro@wasforum.jp

<http://wasforum.jp>