

How to lead better security
through our MINI Hardening Project

Kazuki Tsubo
Cloud Support Engineer
Amazon Web Services Ireland



OWASP
AppSec EU
Belfast

8th to 12th
of May
2017

Waterfront
Conference
Center





Kazuki Tsubo

- Mini Hardening Organizer
- OWASP Japan marketing team
- Job history
 - NIKKEI
 - Web Development Department
 - Amazon Web Services Japan
 - Amazon Web Services Ireland
 - Cloud Support Engineer





Compute

Amazon EC2
Amazon EC2 Container Registry
Amazon EC2 Container Service
Amazon Lightsail
Amazon VPC
AWS Batch
AWS Elastic Beanstalk
AWS Lambda
Auto Scaling
Elastic Load Balancing

Storage

Amazon Simple Storage Service (S3)
Amazon Elastic Block Storage (EBS)
Amazon Elastic File System (EFS)
Amazon Glacier
AWS Storage Gateway
AWS Snowball
AWS Snowball Edge
AWS Snowmobile

Database

Amazon Aurora
Amazon RDS
Amazon DynamoDB
Amazon DynamoDB Accelerator (DAX)
Amazon ElastiCache
Amazon Redshift
AWS Database Migration Service

Migration

AWS Application Discovery Service
AWS Database Migration Service
AWS Server Migration Service
AWS Snowball
AWS Snowball Edge
AWS Snowmobile

Networking & Content Delivery

Amazon VPC
Amazon CloudFront
Amazon Route 53
AWS Direct Connect
Elastic Load Balancing

Developer Tools

AWS CodeStar
AWS CodeCommit
AWS CodeBuild
AWS CodeDeploy
AWS CodePipeline
AWS X-Ray
AWS Command Line Interface

Management Tools

Amazon CloudWatch
Amazon EC2 Systems Manager
AWS CloudFormation
AWS CloudTrail
AWS Config
AWS OpsWorks
AWS Service Catalog
AWS Trusted Advisor
AWS Personal Health Dashboard
AWS Command Line Interface
AWS Management Console
AWS Managed Services

Artificial Intelligence

Amazon Lex
Amazon Polly
Amazon Rekognition
Amazon Machine Learning

Analytics

Amazon Athena
Amazon EMR
Amazon CloudSearch
Amazon Elasticsearch Service
Amazon Kinesis
Amazon Redshift
Amazon QuickSight
AWS Data Pipeline
AWS Glue

Security, Identity & Compliance

AWS Identity and Access Management (IAM)
Amazon Inspector
AWS Certificate Manager
AWS CloudHSM
AWS Directory Service
Amazon Cloud Directory
AWS Key Management Service
AWS Organizations
AWS Shield
AWS WAF
AWS Artifact

Mobile Services

AWS Mobile Hub
Amazon API Gateway
Amazon Cognito
Amazon Pinpoint
AWS Device Farm
AWS Mobile SDK

Application Services

AWS Step Functions
Amazon API Gateway
Amazon Elastic Transcoder
Amazon AppStream

Messaging

Amazon Simple Queue Service (SQS)
Amazon Simple Notification Service (SNS)
Amazon Pinpoint
Amazon Simple Email Service (SES)

Business Productivity

Amazon Chime
Amazon WorkDocs
Amazon WorkMail

Desktop & App Streaming

Amazon WorkSpaces
Amazon AppStream 2.0

Software

AWS Marketplace

Internet of Things

AWS IoT Platform
AWS Greengrass
AWS IoT Button

Contact Center

Amazon Connect

Game Development

Amazon GameLift
Amazon Lumberyard

Relationship with OWASP



OWASP Japan has branch

OWASPコミュニティとして、日本には以下のチャプター

- OWASP Japan Local Chapter 
- OWASP Kansai Local Chapter 
- OWASP Kyushu Local Chapter 
- OWASP Sendai Local Chapter 
- OWASP Fukushima Local Chapter 
- OWASP Okinawa Local Chapter 
- TOKYOならびに首都圏エリアは、OWASP Japan



Agenda

1. About Hardening Project
2. Original and Mini Hardening
3. What is Mini Hardening?
 - a. Our motivation
 - b. Passed competitions
 - c. Technical elements
4. Create own event
5. Conclusion

1. About Hardening Project



Hardening
Project 2016 



**Hardening
Project**



Lots of security risks in real business



#cloudbleed

CTF

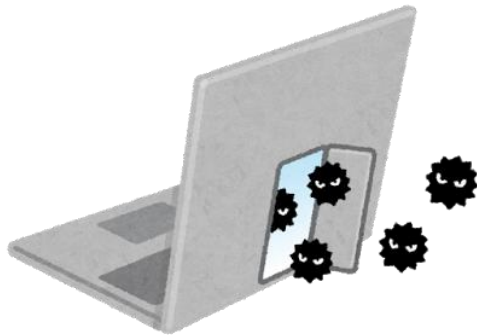


CTF ☑ TIME

Where is the profit?



Hardening Project is business focused



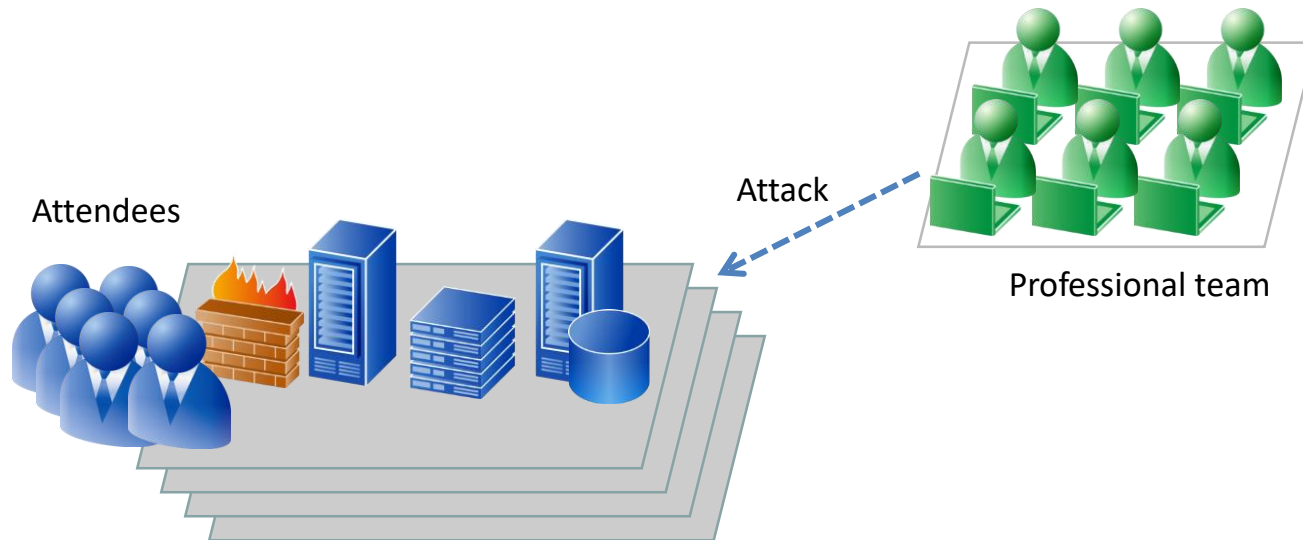
Rules



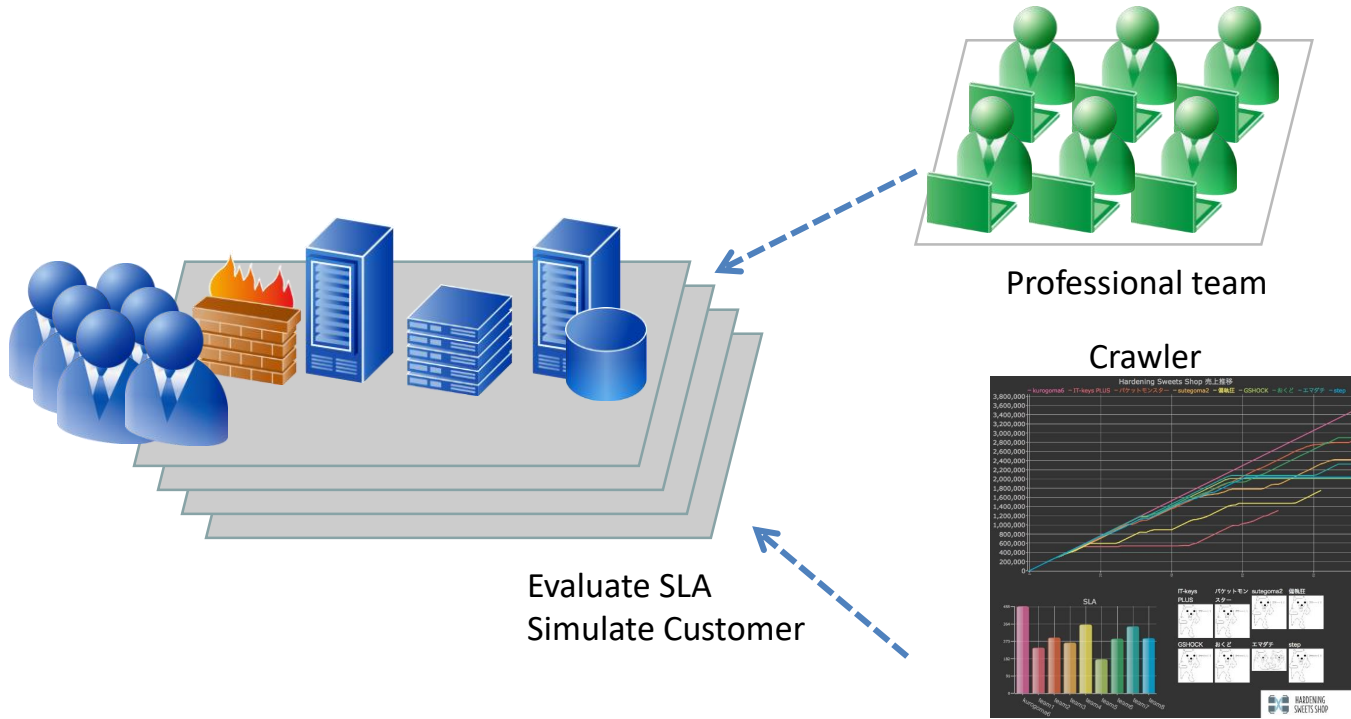
Expected investigation

- Improving vulnerable environment
- Avoid stopping
- Treating stakeholder

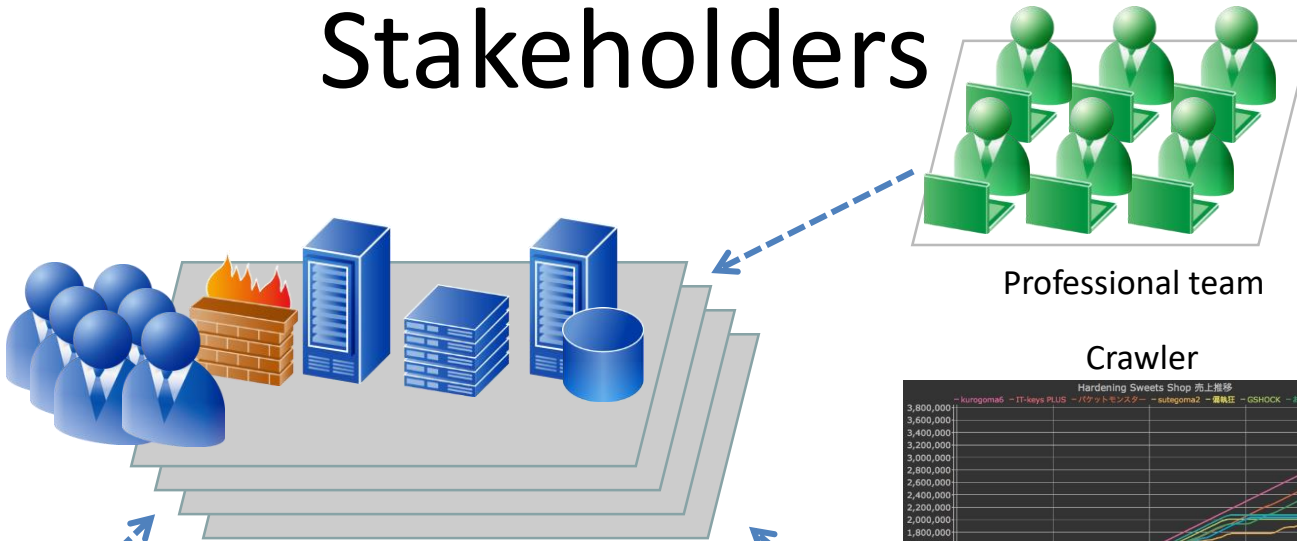
Attack from professional team



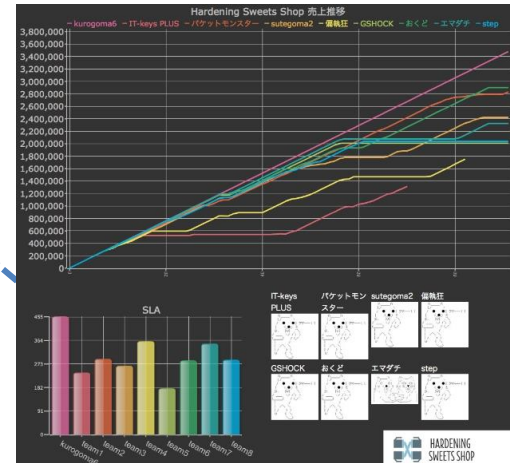
Evaluated by crawler



Stakeholders



Crawler





2. Original and Mini



Hardening Project

- Original
 - Since 2012
 - Business focused competition
- Mini
 - Very similar concept but smaller
 - Frequent

Difference

	 MINI Hardening	 Hardening Project
Team Member	3-4 person	6-8 person
Competition time	3 hours	8 hours
Feedback time	1 hours	8 hours
Nodes per team	2-3 nodes	20-30 nodes
Security issues	10-20 issues	50-60 issues
Attackers	3-4 person	Over 10 person
Frequency	Seasonal	Yearly

3. What is Mini Hardening?



a: Motivation to create “Mini”

- Experience
 - Attack from the other
- Easy to attend, easy to start
 - 1 day only
 - Common and simple security issues
 - Requirement is not team



b. Past 8 competitions

- Mini Hardening #1.x
 - 2015/03/07: #1.0
 - 2015/05/23: #1.1
 - 2015/08/29: #1.2
 - 2015/10/31: #1.3 at Osaka
 - 2016/02/27: Mini in OWASP DAY
- Mini Hardening #2.x
 - 2016/12/04: #2.0
 - 2017/03/26: #2.1
 - 2017/05/06: 078 Hardening at Kobe (Collaborated with “078” event)



Timeline

- 10:30 Door open
- 11:00 Opening - Start explanation & Ice break
- 12:00 Start competition
- 15:00 End competition
- 16:00 Feedback & Recognition
- 17:00 Ending
- 17:45 Start drinking
- 20:00 End of all activities



c. Technical Elements

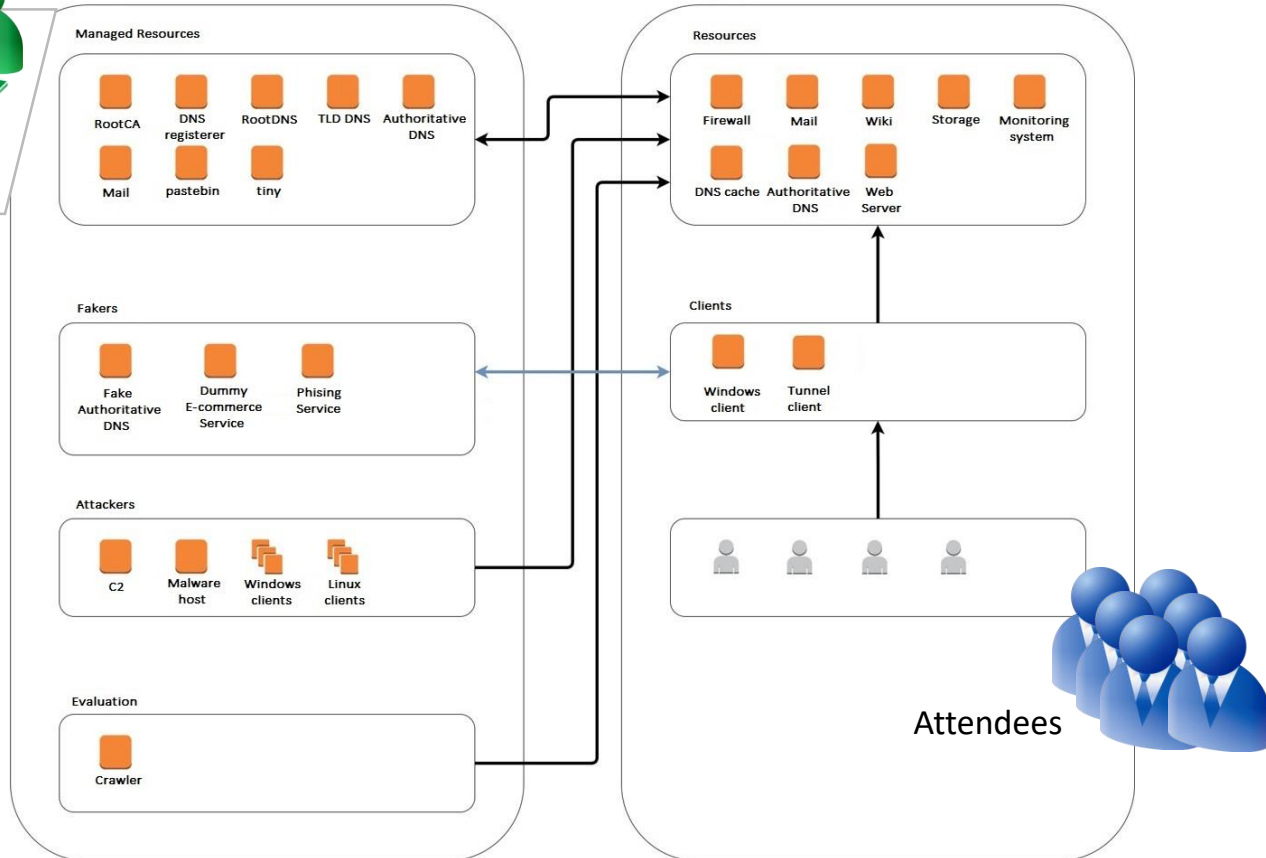


Infrastructure

- Using AWS
 - VPC / EC2
 - Send request of simulated events

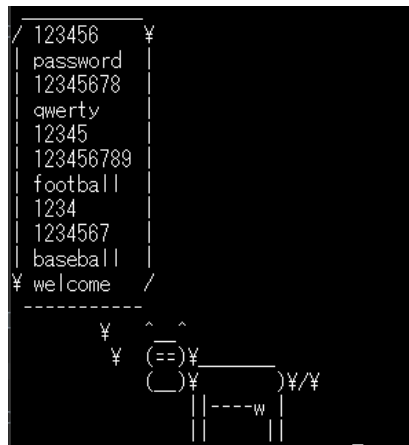


Professional team



Vulnerable environment

- Old versions
 - bash, httpd, openssl...
- Known issue
 - Weak password
 - Not tuned configuration
 - SSL certificate expiration



Rushing

- Reboot infected nodes
- Stopping daemons
- DDoS attack
- Ransomware



Scoring

- Reading reports
- Verifying nodes



Score sheet

模範解答		MINI Hardening #1			A	B		C		D		E		F		G		H
脆弱性		模範解答	確認観点(具体的な確認項目)	得点	Script	Report	Script	Report	Script	Report	Script	Report	Script	Report	Script	Report	Script	Report
パスワードが脆弱:ken	パスワード変更。報告書にパスワードを記載		hardmini でログイン後、su - hoge して構築時のパスワードでログインできないこと。	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0
パスワードが脆弱:yasuhiro				3	0	0	0	0	0	0	0	0	0	0	0	0	0	0
パスワードが脆弱:ayaka			パスワードの変更が報告書に書かれていること。(報告されていない場合で構築時のパスワードでログインできない場合は減点(-3))	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0
パスワードが脆弱:sunyou			ログインが無効化されていないこと(無効化の場合は減点(-3))	3	0	0	0	3	3	3								
パスワードが脆弱:wwwadmin				3	0	0	3	3	3									
バックドアアカウント作成		"vnyou" ユーザを削除。 "/etc/passwd" 内に "vnyou" がいないこと。	\$ grep vnyou /etc/passwd	5	5	5	5	5	0									
FTP: root でログイン可能		FTPでrootのログインを制限する。 "/etc/vsftpd/ftpusers", "/etc/vsftpd/ftpusers" で root を指定する (コメントアウトを外す)。	\$ grep root /etc/vsftpd/ftpusers /etc/vsftpd/user_list	5	0	0	0	0	0	0								
FTP: root が chroot() 対象外		"/etc/vsftpd/chroot_list" から root を削除する。	\$ grep root /etc/vsftpd/chroot_list	5	0	0	0	0	0	0								
FTP: wwwadmin が chroot() 対象外		wwwadmin を削除する。	\$ grep wwwadmin /etc/vsftpd/chroot_list	5	0	0	0	0	0	0								
FTP: バックドアアカウントが chroot() 対象外			\$ grep vnyou /etc/vsftpd/chroot_list	5	0	0	0	0	0	0								
FTP: アクセス制限			\$ iptables -L の結果からFTPにインターネットからアクセス制限されていること。 または、\$ grep vsftpd hosts.deny hosts.allow が以下になっていること。 - hosts.deny vsftpd: ALL - hosts.allow vsftpd: 172.31.10X.0/255.255.255.0	1	0	0	0	0	0	0								
webshell設置: /var/www/html/ass/vp-muth/webshell削除			wp-mytheme-setup.php が削除されていること。	4	0	0	0	0	0	1	4	0	0	0	0	0	0	0
webshell設置: /var/www/html/ass/vp-muth/webshell削除			test2.php が削除されていること。	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
bot設置: /var/www/html/ass/vp-muth/webshell削除			healthcheck が削除されていること。	0	0	5	5	0	1	5	5	0	0	0	0	0	0	0
bot設置: /var/www/html/ass/vp-muth/webshell削除			\$ sudo crontab -u root -l で healthcheck のジョブが設定されていること。	0	0	5	5	0	0	5	5	0	0	0	0	0	0	0
bot設置: /var/www/html/ass/vp-muth/webshell削除			\$対策を行う。 トリから、 mod_security-2.7.3-3.el6.x86_64.rpm, mod_security-crs-2.2.6-3.el6.noarch.rpm を ダウンロードしてインストールする。															
			/etc/httpd/modsecurity.d/ 以下に、下記を含むディレクトリであればよい。設定値は、httpd.conf内のMaxClientsより十分に小さい値であればよい。 SecReadStateLimit 20															

Team scores

- fix
- Report

Expected investigation

Base score

Vulnerabilities

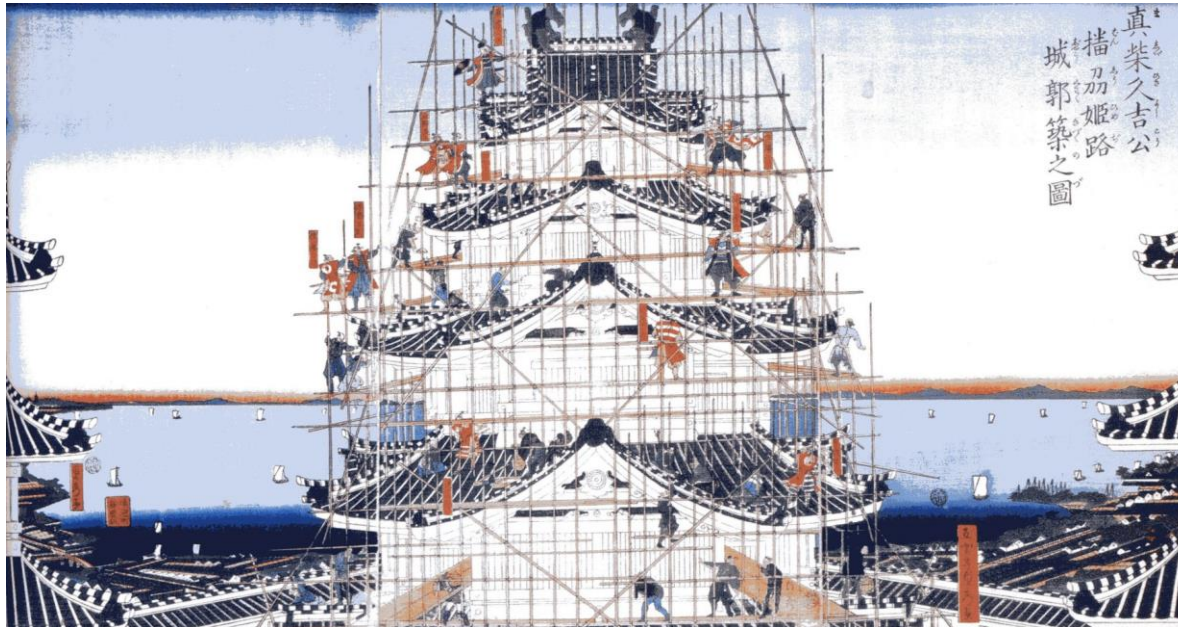
Checkpoint

Crawler

- Simulating customer
- Crawling
 - Connection
 - Content
 - Latency
 - Port



4. Create own event



Our case

- Sponsored by WASForum
- Online meeting every Wednesday
 - Slack
 - Google doc / Hang out

Is it easy? No.

- Tasks
 - Organize
 - Implement vulnerabilities
 - Ready to evaluate
 - Attack
 - Evaluate&Feedback

Core members

- 4 core members at start
 - Easy to talk
 - High context
- Today 7 members except me
 - Splitted role



Benefits

— For me

- Networking opportunity
- Feeling my growth
- Enjoyable with others



5. Conclusion

First small steps

- We can start training by using some tools
 - Broken Web Application Project
 - Easy to break
 - Try to fix
 - OWASP Zed Attack Proxy Project
 - Handful tool for evaluating



Thank you for listening today!



twitter: @TSB_KZK

Facebook/LinkedIn: Kazuki Tsubo