International Journal of Electronic Commerce Studies
Vol.10, No.2, pp.89-112, 2019
doi: 10.7903/ijecs.1536

NEW ATTACK POTENTIAL MEASUREMENT METHOD TO KAIZEN EVENT FOR WEB APPLICATION SECURITY VULNERABILITIES

Kuo-Sui Lin
Aletheia University
No.32, Zhenli St., Danshui Dist., New Taipei City 25103, Taiwan
au4234@mail.au.edu.tw

ABSTRACT

With recognition of the importance of web application security, there is a need for study on a conceptual Kaizen framework as a guide to initiate a series of Kaizen events for self-assessment of web application security vulnerabilities. Moreover, there is a need for study on a more effective attack potential measurement method to support the Kaizen event for stepwise measurement and incremental improvement of web application security vulnerabilities. As a result, a conceptual Kaizen framework to guide the Kaizen event was developed and a new attack potential measurement method was proposed in this study. A numerical example was given to demonstrate that the new attack potential measurement method is more suitable than the traditional attack potential measurement method to support the Kaizen event for measuring small but encouraging improvement of web application security vulnerabilities. Finally, conclusions are made and suggestions for future work are proposed.

Keywords: Attack Potential, Fuzzy Linguistic Decision Making, Fuzzy Pattern Recognition, Kaizen Event, OWASP Top Ten List

1. INTRODUCTION

Web application security is a branch of information security that deals specifically with security of websites, web applications and web services[1]. Due to varied nature of motivations, web applications are increasingly the preferred targets of hackers and/or adversaries. A quick hack of a vulnerable web application can give instant access to valuable data, looking to diversified motivations from data falsification, theft, fraud, espionage, defacement, phishing scams, denial of service attack, IT malfunction and dysfunction as well as other illegal activities. In an attempt to mitigate web

application vulnerabilities, web application administrators use web application security measures, such as firewalls and intrusion detection/prevention devices, but these web application security measures are not enough. Web applications introduce vulnerabilities, which can't be blocked by firewalls or by allowing access to an organization's data and information assets. As web applications have evolved and updated rapidly to different shapes, sizes, and complexities, the only way to achieve sustainable web application security is to spin continuous improvement mindset and actions into each phase of the web application's lifecycle.

Today, Kaizen is recognized worldwide as an important management philosophy to achieve incremental and continuous improvement over time through a series of well-structured Kaizen events[2,3,4,5,6]. In the Kaizen framework, a kaizen event would produce driving force that drives the PDCA wheel on the Kaizen track to the stepwise achievement of measurement and improvement of web application security vulnerabilities. Another issue in security evaluation is its subjectivity, uncertainties and incompleteness during acquisition and representation of qualitative evaluation knowledge in addition to quantitative evaluation knowledge. Therefore, the purpose of this study was to develop a Kaizen framework and a more effective attack potential measurement method for measuring the web application vulnerabilities of identified security scenarios.

With the background and purpose of this study, two questions that need to be addressed are: (1) What Kaizen framework is required to guide and initiate a series of Kaizen events for stepwise measurement and continuous improvement of the web application vulnerabilities? (2) What fuzzy logic based measurement method is required to support a Kaizen event for measuring small but encouraging improvement of web application security vulnerabilities? The results of this study would contribute to propose a more effective attack potential measurement method to support kaizen event for web application security vulnerabilities.

2. BACKGROUND AND RELATED WORKS

2.1 OWASP Most Critical Web Application Vulnerabilities

The Open Web Application Security Project (OWASP) is a worldwide open source community project, dedicated to finding and fighting the web application security vulnerabilities[7]. Its mission is to create freely-available articles, methodologies, documentation, tools, and technologies for mitigating the web application security vulnerabilities. OWASP has recommended a list of Ten Most Critical Web Application Security Vulnerabilities (OWASP Top Ten List) that make for a very useful security criterion compliance metrics (see Table 1)[8]. It represents a broad consensus

about the most critical security risks to web applications. The OWASP Top Ten List is also complemented by a set of secure coding and testing guidelines. In this study, the author recommends OWASP's Top Ten List as attack scenarios for measuring web application security vulnerabilities.

Table 1. OWASP ten most critical web application security vulnerabilities

AS_1- Code Injection	AS_6- Sensitive Data Exposure
AS_2- Broken Authentication and Session Management	AS_7- Missing Function Level Access Control
AS_3- Cross Site Scripting (XSS)	AS_8- Cross Site Request Forgery
AS_4- Insecure Direct Object References.	AS_9- Using Components with Known Vulnerabilities
AS_5- Security Misconfiguration	AS_{10}- Unvalidated Redirects and Forwards

2.2 Attack Potential Measurement Method

The attack potential of one specific security scenario is a numerically expressed attacker's potential that is required for executing attack to exploit/compromise the scenario[9].

Table 2. Factors and values for calculation of attack potential[2]

Factor	Value	Factor	Value
1.Elapsed Time		3. Knowledge of TOE	
<= one day	0	Public	0
<= one week	1	Restricted	3
<= two weeks	2	Sensitive	7
<= one month	4	Critical	11
<= two months	7	4.Window of Opportunity	
<= three months	10	Unnecessary / unlimited access	0
<= four months	13	Easy	1
<= five months	15	Moderate	4
<= six months	17	Difficult	10
> six months	19	5. Equipment	
2. Expertise		Standard	0
Layman	0	Specialized	4
Proficient	3	Bespoke	7
Expert	6	Multiple bespoke	9
Multiple experts	8		

Source: ISO/IEC 18045, Information technology – Security techniques – Evaluation criteria for IT security – CEM, September, 2012[11]

The Common Methodology for Information Technology Security

Evaluation (CEM) is a companion document to the Common Criteria (CC)[12]. Common Criteria is more formally called "Common Criteria for Information Technology Security Evaluation". CC is a widely recognized international scheme developed to assure security-enforcing products (applications, systems and products). It facilitates consistent evaluations of the security of ICT products, implemented either in hardware, software or firmware. CC is also published as ISO/IEC 15408[13]. CC evaluation employs the five factors discussed in the previous section and associates numeric values with the total value of each factor and applies following steps for the calculation and classification of attack potential vulnerabilities: (1) Defining the possible set of attack scenarios $AS=\{AS_1, AS_2, ..., AS_k\}$ for the TOE in the operational environment; (2) Performing a theoretical analysis and calculate the value of attack potential for each attack scenario by using Table 2; (3) Performing penetration tests to confirm or to disprove the theoretical analysis for each attack scenario, if necessary; (4) Mapping the security level of attack potential for each attack scenario and determining pass/fail verdict.

Table 3 describes different ranges of attack potential values and the mapped security levels of attack scenarios. The attack potential value of an attack scenario can be calculated following the summation formula given in the CEM[10]. It should be noted that a number of vulnerabilities rated individually may indicate high resistance to attack, collectively the combination of vulnerabilities may indicate that overall a lower rating is applicable. For example, attack potential required to exploit attack scenario is classified as "High (H)", if the five attack factors and their associated numeric values sum up to 20 points. Hence, the TOE is capable to resist attacks of this attack scenario, having attack potential of "Moderate".

Table 3. Rating of vulnerabilities and TOE resistance for CC[2]

Range of values	Attack potential required to exploit attack scenario:	TOE resistant to attackers with attack potential of:	Evaluation Assurance Level (EAL)
0~9	Basic (B)	No rating (N)	Undefined EAL
10~13	Enhanced-basic(EB)	Basic (B)	EAL1~EAL3
14~19	Moderate (M)	Enhanced-basic(EB)	EAL4
20~24	High (H)	Moderate (M)	EAL5
>= 25	Beyond-High (BH)	High (H)	EAL6~7

Source: ISO/IEC 15408, Information technology – Security techniques – Evaluation criteria for IT security– CC, 2012[13]

2.3 Kaizen and Continuous Improvement

Kaizen is a Japanese philosophy for "continuous improvement" that can be traced to the meaning of the two Japanese characters: "kai", meaning "to change"; and "zen", meaning "for the better"[14]. The core concept of Kaizen is that it is an on-going, never-ending improvement process. It seeks to achieve incremental and continuous improvement over time through standardizing processes with the involvement of entire workforce from the top management to middle managers and workers[15]. Today kaizen is recognized worldwide as an important pillar of an organization's long-term competitive strategy[2,3,4,5,6]. Certain guiding principles summarized for the Kaizen are that: (1) Kaizen speaks with data, manage by facts through standardizing processes to identify and solve problems, (2) Kaizen involves all levels of an organization, (3) Kaizen looks to improve every aspects and everywhere of an organization which improvements can be made, and (4) Kaizen seeks to achieve many continual aligned small improvements accumulated over time.

As mentioned in Petermann's book "The Kaizen Freeway: A High Speed Route to Process Improvement" [5], Kaizen has constructed a high speed route to process improvement. If kaizen has laid down a high speed route to process improvement, the kaizen event is accordingly a powerful driving force that drives the kaizen team on the kaizen track to stepwise achievement and continuous improvement. A Kaizen Event team, as a task force, is a team attended by a facilitator and the operators of a process area in which the kaizen event is being conducted plus cross-functional team members and even management. Although Kaizen events have been growing in popularity since the mid-1990s, there have been a multitude of research studies on incremental and continuous improvement activities seeking to achieve effectiveness of Kaizen events[16,17,18,19].

Kaizen events have evolved a large number of names, including "accelerated improvement workshop", "focused Improvement workshop", "rapid improvement event", "rapid improvement workshop", "kaizen blitz" and "Kaizen burst". Montabon defined Kaizen events as essentially well-structured, multi-day problem solving sessions involving a cross-functional team, who is empowered to use experimentation as they see fit to derive a solution[20]. Van et al's[21] defined a Kaizen event as a focused and structured improvement project, using a dedicated cross-functional team to improve a targeted work area, with specific goals, in an accelerated timeframe. These definitions of Kaizen event are similar in many points. Certain guiding principles summarized for the Kaizen are that: (1) A Kaizen event is a carefully planned and well-structured problem solving activity. (2) A Kaizen event is a relatively short-term, high-intensity effort focused on a specific problem area, (3) A Kaizen event uses the principles of Kaizen, (4)

Kaizen Events provide a series of small-step working sessions, and (5) A Kaizen event usually involves a cross-functional Kaizen team[21,22,23,24].

3. RESEARCH DESIGN AND METHODS

3.1 Cosine Similarity Measure for Triangular Fuzzy Numbers

Because it is easier for decision makers to express their vague and uncertain preferences by using fuzzy linguistic terms than by exact values, a linguistic approach is required to handle fuzzy linguistic decision making problems. In the fuzzy linguistic decision making process, the linguistic ratings of decision makers will be then transformed into fuzzy numbers for further processing. Triangular fuzzy numbers (TFNs) are able to express or approximate the decision maker's vague linguistic preferences because of its modeling capability and simple computational operations. In this study, TFNs are used in fuzzy linguistic decision making due to its popularity in specifying fuzzy sets[25,26].

A cosine similarity measure for trapezoidal fuzzy numbers is proposed in an analogous manner to the cosine similarity measure between fuzzy sets[27,28]. In which, the calculation results of the proposed cosine similarity was compared with the calculation results of different similarity measures and the results show that the proposed method is effective and reasonable[29]. The cosine similarity measure can also be used to measure TFNs which are considered to be special cases of trapezoidal fuzzy numbers. Let $\boldsymbol{A}= (a_1, a_2, a_3)$ and $\boldsymbol{B}= (b_1, b_2, b_3)$ be two triangular fuzzy numbers in the set of real numbers R. The three parameters in $\boldsymbol{A}$ and $\boldsymbol{B}$ can be considered as a vector representation with the three elements. Based on the extension of the cosine similarity measure for fuzzy sets, the cosine similarity measure between the two TFNs $\boldsymbol{A}$ and $\boldsymbol{B}$ can be defined as follows:

$$sim(\boldsymbol{A}, \boldsymbol{B}) = \mathrm{Dot}(\boldsymbol{A}, \boldsymbol{B}) / ||\boldsymbol{A}||||\boldsymbol{B}|| = (\boldsymbol{A} \bullet \boldsymbol{B}) / ||\boldsymbol{A}||||\boldsymbol{B}||$$
$$= \Sigma^3_{k=1} a_k * b_k / \mathrm{SQRT}(\Sigma^3_{k=1} a_k \text{^} 2) \times \mathrm{SQRT}(\Sigma^3_{k=1} b_k \text{^} 2)$$

It satisfies the following properties:

i) $0 \le sim(\boldsymbol{A}, \boldsymbol{B}) \le 1$

ii) $sim(\boldsymbol{A}, \boldsymbol{B}) = sim(\boldsymbol{B}, \boldsymbol{A})$

iii) $sim(\boldsymbol{A}, \boldsymbol{B}) = 1$ if $\boldsymbol{A} = \boldsymbol{B}$

Pattern recognition is an inductive process of gathering, grouping, and classification from data objects (measurements or observations) into a set of categories or classes (patterns) relying on the predefined criteria (features) of the data objects. In pattern recognition, an unknown data object can be classified on the basis of the knowledge of known patterns. The cosine

similarity measure is a simple and effective tool to solve pattern recognition problem[29]. In this study, the cosine similarity measure is used as a tool to classify security levels of attack potential value by measuring how close one data object is similar to another data object.

3.2 Developed Kaizen Framework and Its Kaizen Events

New threats to web applications are dynamically emerging and mutating over time. Thus, on-going web application security activities are critical for securing web application vulnerabilities, rather than a one-time large scale project. Today the kaizen philosophy has recognized and promoted worldwide as an important pillar seeking to achieve incremental and continuous improvement over time through standardizing processes, as well as searching for organizations' long-term competitive strategy[2,3,4,5].

Kaizen events are intense bursts of improvement activities conducted by a Kaizen team to periodically measure and incrementally improve the security vulnerability of attack scenarios and collectively for the security vulnerability of web application. In this study, the author developed a Kaizen framework as a guide to initiate a series of Kaizen events. The Kaizen event is disciplined in a Plan-Do-Check-Act cycle (PDCA wheel) to drive the iterative PDCA wheel on the Kaizen route for stepwise measurement and continuous improvement of web application security vulnerabilities. The contexts and the core concepts of the Kaizen framework and its initiated Kaizen events are outlined in Figure 1.

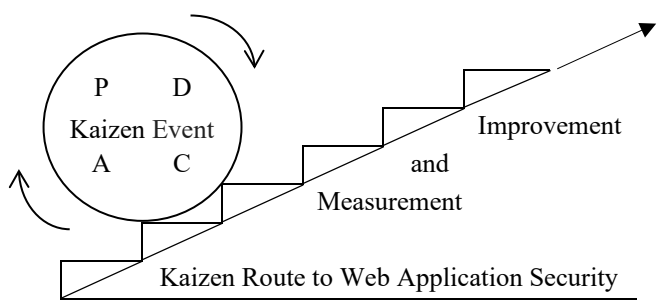

Figure 1. The Kaizen framework to web application security

A high-level flowchart for a Kaizen event disciplined in a Plan-Do-Check-Act cycle and initiated for conducting measurement and improvement of web application vulnerabilities is proposed and prescribed in Table 4.

Table 4. High-level flowchart for a Kaizen event

1.Plan stage
Step 1.1: Establishing a plan for a Kaizen event
Step 1.2: Measuring the "as-is" attack potential values of attack scenarios
Step 1.3: Analyzing the results
Step 1.4: Determining the "to-be" attack potential values and the security levels for the attack scenarios
Step 1.5: Identifying the "Whats" to improve from the evaluation results(root cause analysis)
Step 1.6: Identifying the "Hows" to improve from the evaluation results(countermeasure identification)
2.Do stage
Step 2.1: Taking actions to improve (countermeasure implementation)
3.Check stage
Step 3.1: Re-measuring the improved attack potential values of the attack scenarios
Step 3.2: Re-analyzing the results (effectiveness review)
4.Act stage
Step 4.1: Adjusting the "to-be" attack potential values
Step 4.2: Refining the plan and the SOPs
Step 4.3: Starting a new Kaizen event

The main purpose of the high-level flowchart for a Kaizen event was not intended for CC certification but for self-assessment and improvement to the security of each of the attack scenarios, and collectively to the security of web application security. To support a kaizen event, an effective attack potential measurement method is required for calculating the attack potential value and classifying the security level for each of the attack scenarios. Thus, a detailed flowchart for the proposed attack potential measurement method will be elaborated in the next section to provide a close-up view for the Step 1.2 of the high-level flowchart of a Kaizen event.

3.3 New Fuzzy Attack Potential Measurement Method for the Kaizen Event

In the process improvement route, if kaizen has laid down a high speed route[5], the kaizen event can be designed as a powerful driving force that drives the PDCA wheel on the kaizen track to stepwise and continuous improvement. Enabling a Kaizen event for the web application security requires the efforts of internal reviewers and external consulting experts' evaluation services. Thus an effective attack potential measurement method is required to support the Kaizen events for measuring small but

encouraging improvement of web application vulnerabilities. However, as further explained in Section 4, deficiencies remain evident when using traditional measurement method for attack potential measurement. The traditional attack potential measurement method uses crisp rating values and basic algebra operation for calculating each attack potential values. The crisp rating value of attack potentials are usually incomplete, insufficient or imprecise in nature; thus, it suffers from some information loss in the algebra calculation. Therefore, the traditional attack potential measurement method and its calculated crisp values are not appropriate for classifying security levels.

The proposed new attack potential measurement method is considered to be an umbrella under which several metrics and methods are included, such as OWASP's Top Ten List, ISO/IEC 18045 (CEM) attack potential calculation method, fuzzy linguistic decision making method, ISO/IEC 15408 (CC) attack potential classification method and fuzzy pattern recognition method. Figure 3 presents a detailed flowchart for the proposed new attack potential measurement method for calculating the attack potential values and classifying the level for each of the attack scenarios. This detailed flowchart provides a detailed description for the Step 1.2 of the high-level flowchart for a Kaizen event (see Figure 2).

Flowchart	Metrics and methods
Phase 1: Preparation phase:	
Step P1.1:Identifying possible attack scenarios Step P1.2:Preparing a measurement plan for the Kaizen event	*OWASP Top Ten List
↓	
Phase 2: Calculation phase:	
Step P2.1: Collecting linguistic rating values Step P2.2:Constructing fuzzy decision matrices	* ISO/IEC 18045(CEM) * Fuzzy linguistic decision making method
↓	
Phase 3: Classification phase:	
Classifying security level	*ISO/IEC 15408(CC) *Fuzzy pattern recognition method

Figure 2. Detailed flowchart for the new attack potential measurement method

The following paragraphs provide an overview of each of the phases, including Preparation Phase (Phase 1), Calculation Phase (Phase 2) and Classification Phase (Phase 3).

3.3.1 Preparation Phase

In the preparation phase, a measurement plan is prepared for supporting the Kaizen event. In the measurement plan, the "Target of Evaluation (TOE)" is selected as the "Target of Evaluation (TOE)". A possible set of attack scenarios for measuring the TOE are identified and a method for attack potential calculation and classification is prescribed. The author recommends OWASP's Top Ten List as attack scenarios for measuring web application security vulnerabilities based on the following reasons: (1) it represents a broad consensus from a wide variety of security experts about what the most critical web application security flaws are; (2) it has gained significant traction and is often looked to for guidance criteria when conducting web application vulnerability measurement; (3) it is an open source document and everybody can use it for developing, building, and testing secure web application system. The author recommends ISO/IEC 18045 and ISO/IEC 15408 as reference schemes for security evaluation of an attack scenario. As introduced in Subsection 2.2, ISO/IEC 18045 identifies five factors for attack potential calculation and ISO/IEC 15408 maps the calculated result of attack potential value for attack potential classification.

3.3.2 Calculation Phase

Because it is easier for decision makers to express their vague and uncertain ratings by using fuzzy linguistic terms than by exact values, a new method is required to employ fuzzy linguistic decision making approach for attack potential calculation. In the fuzzy linguistic decision making process, the linguistic terms will be then transformed into fuzzy numbers for further processing. Among the various shapes of fuzzy number, TFNs are used in this study due to its popularity in specifying fuzzy sets[28, 29].

In this study, the five factors of attack potential[2] defined in ISO/IEC 18045 are regarded as linguistic variables and the ranges of possible attack potential values are regarded as linguistic terms. By referring to several types of TFNs[30], the selected term set for each of the five linguistic variables can be transformed into their corresponding TFNs. As shown in Table 4 and Figure 3, the ranges of possible values of the five factors are predefined by linguistic terms and modeled by corresponding fuzzy numbers symmetrical and uniformly distributed in [0,1]. To measure the linguistic variables for factors (Expertise, Knowledge of TOE, Window of Opportunity and Equipment), defined linguistic terms and corresponding TFNs are shown in Table 2 and Table 5.

Table 5. Linguistic variables of factors, their linguistic terms and corresponding fuzzy numbers

Linguistic variable of factors	Defined linguistic terms	Corresponding TFNs
1.Elapsed Time	≤ one day (Very Short, *Vs*)	TFN(0, 0, 0.25)
	≤ one week (Short, *S*)	TFN(0, 0.25, 0.5)
	≤ two months (Moderate, *M*)	TFN(0.25, 0.5, 0.75)
	≤ four months (Long, *L*)	TFN(0.5, 0.75, 1)
	> six months (Very Long, *Vl*)	TFN(0.75, 1, 1)
2. Expertise	Layman (*L*)	TFN(0, 0, 0.25)
	Proficient (*P*)	TFN(0, 0.25, 0.5)
	Expert (*E*)	TFN(0.25, 0.5, 0.75)
	Multiple experts (*M*)	TFN(0.5, 0.75, 1)
	Stringent expertise (*Se*)	TFN(0.75, 1, 1)
3. Knowledge of TOE	Public (*P*)	TFN(0, 0, 0.25)
	Restricted (*R*)	TFN(0, 0.25, 0.5)
	Sensitive (*S*)	TFN(0.25, 0.5, 0.75)
	Critical (*C*)	TFN(0.5, 0.75, 1)
	Very Critical Design (*Vc*)	TFN(0.75, 1, 1)
4. Window of Opportunity	Unnecessary/unlimited access (*U*)	TFN(0, 0, 0.25)
	Easy (*E*)	TFN(0, 0.25, 0.5)
	Moderate (*M*)	TFN(0.25, 0.5, 0.75)
	Difficult (*D*)	TFN(0.5, 0.75, 1)
	Very Difficult (*Vd*)	TFN(0.75, 1, 1)
5. Equipment	Standard (*St*)	TFN(0, 0, 0.25)
	Specialized (*Sp*)	TFN(0, 0.25, 0.5)
	Bespoke (*P*)	TFN(0.25, 0.5, 0.75)
	Multiple bespoke (*M*)	TFN(0.5, 0.75, 1)
	Sophisticated (*So*)	TFN(0.75, 1, 1)

Source: Adapted from ISO/IEC 18045, Information technology – Security techniques – Evaluation criteria for IT security – CEM, September, 2012.

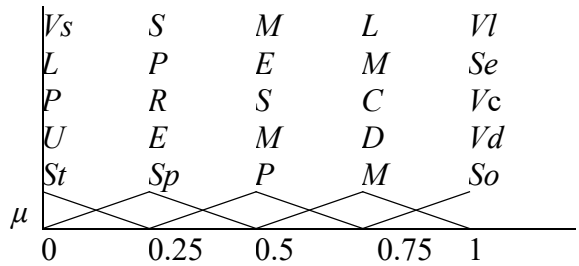

Figure 3. Membership functions for linguistic terms of factors

The following steps are proposed for performing the calculation phase of the new fuzzy attack potential measurement method (see Figure 2, Phase 2: Calculation phase).

Step P2.1: Collecting linguistic rating values

Kaizen team's ratings against the set of feature space $\boldsymbol{C}=\{C_1,C_2,\ldots,C_n\}(1\leq j\leq n)$ are solicited and fused to obtain a set of data object $\boldsymbol{A_i}$ represented as following rating vectors: $\boldsymbol{A_i}=\{(C_1, r_{i1}),(C_2, r_{i2}),\ldots,(C_n, r_{in})\}(1\leq i\leq m; 1\leq j\leq n)$. The ratings $r_{ij}\,(1\leq i\leq m; 1\leq j\leq n)$ of the data object $\boldsymbol{A_i}$ against feature C_j are expressed by TFNs. Suppose that there exist a set of t patterns represented as following rating vectors: $\boldsymbol{B}_s=\{(C_1, r_{s1}),(C_2, r_{s2}),\ldots,(C_n, r_{sn})\}(1\leq s\leq t; 1\leq j\leq n)$. The ratings $\boldsymbol{r_{sj}}\,(1\leq s\leq t; 1\leq j\leq n)$ of the pattern B_s against feature C_j are expressed by TFNs.

Step P2.2: Constructing fuzzy decision matrices

A fuzzy pattern recognition problem can be expressed in a fuzzy decision matrix $\boldsymbol{R}_A$ for a set of evaluated data objects $\boldsymbol{A}=\{A_1, A_2,\ldots, A_m\}(1\leq i\leq m)$ and a fuzzy decision matrix $\boldsymbol{R}_B$ for patterns $\boldsymbol{B}=\{B_1, B_2,\ldots, B_t\}(1\leq s\leq t)$. Given m unknown pattern vectors $\boldsymbol{A}_i(1\leq i\leq m)$ and n criteria $\boldsymbol{C}=\{C_1,C_2,\ldots,C_n\}$ $(1\leq j\leq n)$, the fuzzy decision matrix for the evaluated data objects $\boldsymbol{A}_i$ can be expressed in a fuzzy decision matrix $\boldsymbol{R}_A=[\boldsymbol{r}_{ij}]_{m\times n}$. As shown in Figure 4, the elements $\boldsymbol{r}_{ij}(1\leq i\leq m;1\leq j\leq n)$ describe the ratings of evaluated data object $\boldsymbol{A}_i$ against criterion C_j and can be expressed by TFNs.

$$\boldsymbol{R}_A = \begin{array}{c|cccccc} & C_1 & C_2 & \ldots & C_j & \ldots & C_n \\ A_1 & r_{11} & r_{12} & \ldots & r_{1j} & \ldots & r_{1n} \\ A_2 & r_{21} & r_{22} & \ldots & r_{2j} & \ldots & r_{2n} \\ \vdots & \vdots & \vdots & \ldots & \vdots & \ldots & \vdots \\ A_i & r_{i1} & r_{i2} & \ldots & r_{ij} & \ldots & r_{in} \\ \vdots & \vdots & \vdots & \ldots & \ldots & \ldots & \vdots \\ A_m & r_{m1} & r_{m2} & \ldots & r_{mj} & \ldots & r_{mn} \end{array}$$

Figure 4. Fuzzy decision matrix for the ratings of evaluated data objects

Given t classified pattern vectors $\boldsymbol{B}_s(1\leq s\leq t)$ and n criteria $\boldsymbol{C}_j(1\leq j\leq n)$,

the fuzzy decision matrix for the ratings of patterns B_s can be expressed in a fuzzy decision matrix $\boldsymbol{R}_B=[\boldsymbol{r}_{sj}]_{t\times n}$. As shown in Figure 5, the elements $\boldsymbol{r}_{sj}(1\le s\le t;1\le j\le n)$ describe the ratings of pattern B_s against criterion C_j and can be expressed by TFNs.

$$\boldsymbol{R_B}=\begin{array}{c|cccccc} & C_1 & C_2 & \dots & C_j & \dots & C_n \\ B_1 & r_{11} & r_{12} & \dots & r_{1j} & \dots & r_{1n} \\ B_2 & r_{21} & r_{22} & \dots & r_{2j} & \dots & r_{2n} \\ \vdots & \vdots & \vdots & \dots & \vdots & \dots & \vdots \\ B_s & r_{s1} & r_{s2} & \dots & r_{sj} & \dots & r_{sn} \\ \vdots & \vdots & \vdots & \dots & \dots & \dots & \vdots \\ B_t & r_{t1} & r_{t2} & \dots & r_{tj} & \dots & r_{tn} \end{array}$$

Figure 5. Fuzzy decision matrix for the ratings of patterns

3.3.3 Classification Phase

In the calculation phase, attack potential values of attack scenarios are collected and calculated; in the classification phase, attack potential values of attack scenarios are recognized and classified. To classify different ranges of attack potential values, levels of attack potential required to exploit attack scenario are defined as linguistic terms. Corresponding TFNs for possible measurement of these linguistic terms are shown in Table 6 and Figure 6.

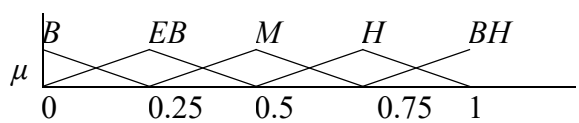

Figure 6. Membership functions for the linguistic terms of security levels

In this classification phase, a similarity based pattern recognition approach is proposed to recognize patterns against a set of criteria. Given a set of t classified patterns $\boldsymbol{B}=\{B_1, B_2,\dots, B_t\}(1\le s\le t)$, suppose that there is a set of m evaluated data objects $\boldsymbol{A}=\{A_1, A_2,\dots,A_m\}(1\le i\le m)$ to be recognized against a feature space $\boldsymbol{C}=\{C_1, C_2,\dots,C_n\}$. The evaluated data object A_i can be represented by the following fuzzy set: $\boldsymbol{A}_i=\{(C_j, r_{ij})|C_j\in C;\ 1\le j\le n\}$. The pattern B_s can be represented by the following fuzzy set: $\boldsymbol{B}_s=\{(C_j, r_{sj})|C_j\in C;1\le j\le n\}$. Two kinds of similarity measures used in this similarity based pattern recognition approach are local similarity measure $sim(r_{ij}, r_{sj})$ and global similarity measure $Sim(A_i, B_s)$ introduced by Lin[31]. Local similarity is similarity on criteria (features); global similarity is similarity on data objects. A local similarity measure is computed by comparing each criteria value and a global similarity measure is obtained as a weighted

calculation of the local similarity measures. The following steps are proposed for performing the classification phase of the new fuzzy attack potential measurement method (see Figure 3, Phase 3: Classification phase).

Table 6. Linguistic terms for the ranges of attack potential values and their corresponding fuzzy numbers

Range of values	Corresponding TFNs	Level of attack potential required to exploit attack scenario:	TOE resistant to attackers with attack potential of:	Evaluation Assurance Level (EAL)
0~9	TFN (0, 0, 0.25)	Basic (B)	No rating (N)	Undefined EAL
10~13	TFN (0, 0.25, 0.5)	Enhanced-basic (EB)	Basic (B)	EAL1~3
14~19	TFN (0.25, 0.5, 0.75)	Moderate (M)	Enhanced-basic (EB)	EAL4
20~24	TFN (0.5, 0.75, 1)	High (H)	Moderate (M)	EAL5
>= 25	TFN (0.75, 1, 1)	Beyond-High (BH)	High (H)	EAL6~7

Step P 3.1: Computing local similarity measure
The local similarity (criterion similarity) is the similarity measure on each criterion of the evaluated data object vector $\boldsymbol{A_i}$ and the pattern vector $\boldsymbol{B}_s$. Let $sim(r_{ij},r_{sj})$ denote the local similarity measure between the data object vector A_i and the pattern vector $\boldsymbol{B}_s$ with regard to criteria $\boldsymbol{C}_j$. r_{ij} and r_{sj} are the rating against $\boldsymbol{C}_j$ in the data object vector $\boldsymbol{A}_i$ and the pattern vector $\boldsymbol{B}_s$, respectively. $sim(r_{ij},r_{sj})=\mathrm{Dot}(r_{ij},r_{sj})/||r_{ij}||||r_{sj}||=r_{ij}\cdot r_{sj}/||r_{ij}||||r_{sj}||$ is a general equation to calculate the cosine similarity of the two ratings against $\boldsymbol{C}_j$. In this study, the two ratings against $\boldsymbol{C}_j$ are expressed by TFNs due to its popularity in specifying fuzzy sets[25,26]. Thus, a cosine similarity measure for TFNs is introduced in an analogous manner to the cosine similarity measure between fuzzy sets[29]. Assume that there are two triangular fuzzy numbers: $\boldsymbol{r}_{ij}=(\mu_{Ai}(x_1), \mu_{Ai}(x_2), \mu_{Ai}(x_3))$ and $r_{sj}=(\mu_{Bs}(x_1), \mu_{Bs}(x_2), \mu_{Bs}(x_3))$, in the set of real numbers R, the three parameters in r_{ij} and r_{sj} can be considered as a vector representation with the three elements. Based on the extension of the cosine similarity measure for fuzzy sets, a local similarity measure between in r_{ij} and r_{sj} is presented as:

$sim(r_{ij},r_{sj})=\Sigma^3_{k=1}(\mu_{ij}(x_k)\times\mu_{sj}(x_k))/(\text{SQRT}(\Sigma^3_{k=1}\mu_{ij}(x_k)\text{^}2)\times\text{SQRT}(\Sigma^3_{k=1}\mu_{sj}(x_k)\text{^}2))$
$= (\mu_{ij}(x_1)\times\mu_{sj}(x_1)+\mu_{ij}(x_2)\times\mu_{sj}(x_2)+\mu_{ij}(x_3)\times\mu_{sj}(x_3))/(\text{sqrt}(\mu_{ij}(x_1)\text{^}2+\mu_{ij}(x_2)\text{^}2$
$+\mu_{ij}(x_3)\text{^}2)\times\text{SQRT}(\mu_{sj}(x_1)\text{^}2+\mu_{sj}(x_2)\text{^}2+\mu_{sj}(x_3)\text{^}2))$ (1)

Step P 3.2: Computing global similarity measure
Let $Sim(\boldsymbol{A}_i, \boldsymbol{B}_s)$ denote the global similarity between the evaluated data object vector $\boldsymbol{A}_i$ and the pattern vector $\boldsymbol{B}_s$, then a global similarity measure can be derived by the weighted summation of the local similarity measures:

$$Sim(\boldsymbol{A}_i, \boldsymbol{B}_s)= (\Sigma^n_{j=1} w_j\times sim(r_{ij},r_{sj}))/\Sigma^n_{j=1} w_j, \quad (2)$$

where w_j is the local weights allocated to each feature(criterion) reflecting importance of the corresponding feature. In this study, the weightings are equally weighted and the weightings are represented as a weighting vector, $\boldsymbol{W}=\{1,1,\ldots,1\}$.

Step P 3.3: Comparing $Sim(\boldsymbol{A}_i, \boldsymbol{B}_s)$ for $s=1,2,\ldots,t$ and selecting the largest one denoted by $Sim(\boldsymbol{A}_i, \boldsymbol{B}_s^*)$.

Step P 3.4: Getting a pattern $\boldsymbol{B}_s^*$ such that $Sim(\boldsymbol{A}_i, \boldsymbol{B}_s^*)= max\{Sim(\boldsymbol{A}_i, \boldsymbol{B}_s)| 1\le s\le t\}$. Then the evaluated data object $\boldsymbol{A}_i$ belongs to the pattern $\boldsymbol{B}_s^*$.

Step P 3.5: Selecting the next data object to proceed until all data objects have been classified.

4. THE NEW MEASUREMENT METHOD TO SUPPORT KAIZEN EVENT FOR WEB APPLICATION SECURITY: A NUMERICAL EXAMPLE

The developed Kaizen framework could guide the Kaizen team to initiate a series of Kaizen events that drive the PDCA wheel on the Kaizen track to stepwise achievement of continuous measurement and improvement of the web application security vulnerabilities. Furthermore, the proposed new fuzzy based attack potential measurement method could support the Kaizen event for attack potential calculation and security level classification of web application security vulnerabilities.

In this numerical example, the TOE is the web application itself. OWASP Top Ten Web Application Vulnerabilities is the set of attack scenarios $\boldsymbol{AS}=\{AS_1, AS_2,...,AS_{10}\}$ for the web application in the operational environment. Take attack scenario "AS_1-Code Injection" as illustration for attack potential calculation and security level classification. By using traditional attack potential measurement method presented in Section 2.2, the rating values of "Initial Attack Potential" and "Improved Attack Potential" for the specific attack scenario "AS_1-Code Injection" are calculated respectively. However, the calculated total rating values are crisp

values. Because crisp values suffer from some information loss during data analysis, the comparison of their relative mapped security levels is sometimes unreasonable and meaningless. As shown in Table 7, the values of "Initial Attack Potential" and "Improved Attack Potential" required to exploit this attack scenario are 1 and 9 respectively. The calculation results showed that the values for both "Initial Attack Potential" and "Improved Attack Potential" for "AS_1-Code Injection" are all classified as "Basic (B)". This means that the security improvement efforts to the subject attack scenario AS_1 have resulted in an evaluation of "Undefined EAL". It can be easily concluded that the classified security levels of the values of "Initial Attack Potential" and "Improved Attack Potential" for "AS_1-Code Injection" are indistinguishable.

Table 7. Classified security level for attack scenario "AS_1-Code Injection" using traditional method

Factor	Initial Attack Potential required to exploit Attack scenario		Improved Attack Potential required to exploit Attack scenario	
1.Elapsed Time	One week	1	Two weeks	2
2.Expertise	Layman	0	Proficient	3
3.Knowledge of the TOE	Public	0	Restricted	3
4.Window of Opportunity	Unnecessary/ Unlimited access	0	Easy	1
5.Equipment	Standard	0	Standard	0
Total numeric rating values		1		9
Classified security level		Basic (B)		Basic (B)
Evaluation Assurance Level(EAL)		Undefined EAL		Undefined EAL

The comparison deficiencies of the traditional attack potential classification method can be avoided by applying a fuzzy linguistic decision making approach to the attack potential calculation and classification. Due to its ability to deal with uncertainties, vagueness and incompleteness, fuzzy linguistic decision making approach provides a number of suitable properties for the proposed fuzzy based attack potential measurement method. It can use linguistic terms and fuzzy numbers to represent uncertain and vague ratings and use fuzzy logic to calculating and reasoning attack potential values.

By using the same collected data set presented in Table 6, applying the proposed new measurement method introduced in subsection 3.3, the

advantages of the new measurement method can be demonstrated. In this example, the set of five factors defined in ISO/IEC 158045[11] are defined as a criteria set: $\boldsymbol{C}$={C_1:Time, C_2: Specialist Expertise, C_3: Knowledge of the TOE, C_4: Window of Opportunity, C_5: Equipment}. Let $\boldsymbol{A}$ represent a set of two evaluated data objects $\boldsymbol{A}_i$(i=1,2); then the set of evaluated data objects $\boldsymbol{A}$ could be defined as: $\boldsymbol{A}$={⟨$\boldsymbol{A}_1$:Initial Attack Potential⟩, ⟨$\boldsymbol{A}_2$:Improved Attack Potential⟩}. The five ranges of attack potential values defined in ISO/IEC 15408[13] can be regarded as five patterns. Assume that $\boldsymbol{B}$ is a set of five patterns $\boldsymbol{B}_s$($1\leq s\leq 5$); then the set of patterns $\boldsymbol{B}$ could be defined as: $\boldsymbol{B}$={⟨B_1:Basic(B)⟩, ⟨B_2:Enhanced-basic(EB)⟩, ⟨B_3:Moderate(M)⟩, ⟨B_4:High(H), ⟨B_5:Beyond-High(BH)⟩}. The linguistic terms of the five given patterns are transformed into TFNs. Thus the five patterns can be represented by the following fuzzy sets in the given five criteria:

$\boldsymbol{B}_1$={⟨C_1,(0,0,0.25)⟩, ⟨C_2, (0,0,0.25)⟩, ⟨C_3, (0,0,0.25)⟩, ⟨C_4, (0,0,0.25)⟩, ⟨C_5, (0,0,0.25)⟩},
$\boldsymbol{B}_2$={⟨C_1,(0, 0.25,0.5)⟩,⟨C_2,(0, 0.25,0.5)⟩,⟨C_3,(0, 0.25,0.5)⟩,⟨C_4, (0, 0.25,0.5)⟩, ⟨C_5, (0, 0.25,0.5)⟩},
$\boldsymbol{B}_3$={⟨C_1,(0.25,0.5,0.75)⟩,⟨C_2,(0.25,0.5,0.75)⟩,⟨C_3,(0.25,0.5,0.75)⟩,⟨C_4, (0.25,0.5,0.75)⟩, ⟨C_5, (0.25,0.5,0.75)⟩},
$\boldsymbol{B}_4$={⟨C_1,(0.5,0.75,1)⟩,⟨C_2,(0.5,0.75,1)⟩,⟨C_3,(0.5,0.75,1)⟩,⟨C_4,(0.5,0.75,1)⟩, ⟨C_5, (0.5,0.75,1)⟩},
$\boldsymbol{B}_5$={⟨C_1, (0.75,1,1)⟩, ⟨C_2, (0.75,1,1)⟩, ⟨C_3, (0.75,1,1)⟩, ⟨C_4, (0.75,1,1)⟩, ⟨C_5, (0.75,1,1)⟩}.

The five patterns $\boldsymbol{B}_s$($1\leq s\leq 5$) can be expressed in a fuzzy decision matrix $\boldsymbol{R}_B$=$[r_{sj}]_{5\times 5}$. As shown in Table 7, the elements r_{sj}($1\leq s\leq 5$;$1\leq j\leq 5$) describe the ratings of pattern $\boldsymbol{B}_s$ against criterion C_j and can be expressed by TFNs.

Given two evaluated data objects $\boldsymbol{A}$={⟨$\boldsymbol{A}_1$: Initial Attack Potential⟩, ⟨$\boldsymbol{A}_2$: Improved Attack Potential⟩}, they are represented by TFNs for further processing through multi-criteria decision making approach. The two evaluated data objects can be represented by the following fuzzy sets in the given five criteria:

$\boldsymbol{A}_1$={⟨C_1,(0,0,0.25)⟩,⟨C_2,(0,0,0.25)⟩,⟨C_3,(0,0,0.25)⟩,⟨C_4,(0,0,0.25)⟩,⟨C_5,(0,0, 0.25)⟩},
$\boldsymbol{A}_2$={⟨C_1,(0,0.25,0.5)⟩,⟨C_2,(0,0.25,0.5)⟩,⟨C_3,(0,0.25,0.5)⟩,⟨C_4,(0,0.25,0.5)⟩, ⟨C_5,(0, 0.25, 0.5)⟩}.

The two evaluated data objects $\boldsymbol{A}_i$ (i =1,2) can be expressed in a fuzzy decision matrix $\boldsymbol{R}_A$=$[r_{ij}]_{2\times 5}$. As shown in Table 8, the elements r_{ij} ($1\leq i\leq m$,$1\leq j\leq n$) describe the ratings of evaluated data object $\boldsymbol{A}_i$ against criterion $\boldsymbol{C}_j$ and can be expressed by TFNs.

Table 8. Corresponding triangular fuzzy numbers of patterns and evaluated data objects for attack scenario "AS_1−Code Injection"

	C_1 : Elapsed Time	C_2 : Expertise	C_3 : Knowledge of the TOE	C_4 : Window of Opportunity	C_5: Equipment
$\boldsymbol{B_1}$	TFN (0, 0, 0.25)	TFN (0, 0, 0.25)	TFN (0, 0, 0.25)	TFN (0, 0, 0.25)	TFN (0, 0, 0.25)
$\boldsymbol{B_2}$	TFN (0, 0.25, 0.5)	TFN (0, 0.25, 0.5)	TFN (0, 0.25, 0.5)	TFN (0, 0.25, 0.5)	TFN (0, 0.25, 0.5)
$\boldsymbol{B_3}$	TFN (0.25,0.5,0.75)	TFN (0.25,0.5,0.75)	TFN (0.25,0.5,0.75)	TFN (0.25,0.5,0.75)	TFN (0.25,0.5,0.75)
$\boldsymbol{B_4}$	TFN (0.5, 0.75, 1)	TFN (0.5, 0.75, 1)	TFN (0.5, 0.75, 1)	TFN (0.5, 0.75, 1)	TFN (0.5, 0.75, 1)
$\boldsymbol{B_5}$	TFN (0.75, 1, 1)	TFN (0.75, 1, 1)	TFN (0.75, 1, 1)	TFN (0.75, 1, 1)	TFN (0.75, 1, 1)
$\boldsymbol{A_1}$	TFN (0, 0, 0.25)	TFN (0, 0, 0.25)	TFN (0, 0, 0.25)	TFN (0, 0, 0.25)	TFN (0, 0, 0.25)
$\boldsymbol{A_2}$	TFN (0, 0.25, 0.5)	TFN (0, 0.25, 0.5)	TFN (0, 0.25, 0.5)	TFN (0, 0.25, 0.5)	TFN (0, 0.25, 0.5)

In order to classify the two data objects $\boldsymbol{A}_i(i=1,2)$ to the five patterns $\boldsymbol{B}_s(1\leq s\leq 5)$, the local similarity measures $sim(r^A_{ij}, r^B_{sj})$ between the data object vector $\boldsymbol{A_i}$ and the patterns vector $\boldsymbol{B}_s$ with regard to five criteria $\boldsymbol{C}_j(1\leq j\leq 5)$ are calculated first and then aggregated into the global similarity measures $Sim(\boldsymbol{A}_i, \boldsymbol{B}_s)$. For example, Eq. (1) is used to calculate local similarity measure between the data object vector $\boldsymbol{A}_1$ and the pattern vector $\boldsymbol{B}_1$ with regard to criteria $\boldsymbol{C}_j(1\leq j\leq 5)$. The calculation results of the local similarity measure $sim(r^A_{1j},r^B_{1j})(1\leq j\leq 5)$ for attack scenario "AS_1-Code Injection" are as follows: $sim(r^A_{11},r^B_{11})=1$,$sim(r^A_{12}, r^B_{12})=0.894$, $sim(r^A_{13}, r^B_{13}) =0.801$, $sim(r^A_{14},r^B_{14})=0.743$,$sim(r^A_{15}, r^B_{15})=0.625$.

Suppose the weightings are equally weighted for each criteria; using Eq. (2), each of the global similarity measures between the data object vector $\boldsymbol{A}_1$ and each of the five pattern vector $\boldsymbol{B}_s(1\leq s\leq 5)$ can be calculated, representing the aggregated result of local similarity measures with regard to criteria $\boldsymbol{C}_j(1\leq j\leq 5)$ for evaluated data object $\boldsymbol{A}_1$. The calculation results of the global similarity measure $Sim(A_1, B_s)(1\leq s\leq 5)$ for attack scenario "AS_1−Code Injection" are as follows: $Sim(\boldsymbol{A_1}, \boldsymbol{B_1}) =1$, $Sim(\boldsymbol{A_1}, \boldsymbol{B_2}) = 0.894$, $Sim(\boldsymbol{A_1}, \boldsymbol{B_3}) = 0.801$, $Sim(\boldsymbol{A_1}, \boldsymbol{B_4}) = 0.743$, $Sim(\boldsymbol{A_1}, \boldsymbol{B_5}) = 0.625$.

The results indicate that the data object vector $\boldsymbol{A_1}$ is recognized and classified as "B_1 pattern". Similarly, the local similarity measure $sim(r^A_{ij},r^B_{sj})$ $(1\leq i\leq 5;1\leq j\leq 5;1\leq s\leq 5)$ is used to calculate local measure between the data object vector $\boldsymbol{A_2}$ and each of the pattern vector $\boldsymbol{B}_s(1\leq s\leq 5)$ with regard to

criteria $\boldsymbol{C_j}$. The data object vector $\boldsymbol{A}_2$ is recognized and classified as "B_2 pattern".

By the proposed fuzzy based attack potential measurement method, it can be easily seen that the "A_1-Initial Attack Potential" and the "A_2-Improved Attack Potential" for attack scenario "AS_1-Code Injection" can be classified into different Evaluation Assurance Levels. Table 9 indicates that the value of "A_2-Improved Attack Potential" required to exploit the attack scenario is classified as "Enhance Basic (EB)". It means that the security improvement efforts to the attack scenario AS_1 have resulted in an evaluation of "Evaluation Assurance Level of EAL1~EAL3." It can be easily concluded that the classified security levels of the value of "A_1- Initial Attack Potential" and "A_2-Improved Attack Potential" for attack scenario "AS_1-Code Injection" are distinguishable. The numerical results showed that the proposed fuzzy based attack potential measurement method performs better than the existing method.

Table 9. Classified security level for attack scenario "AS_1-Code Injection" using new method

Factor	Initial Attack Potential required to exploit attack scenario		Improved Attack Potential required to exploit attack scenario	
Elapsed Time	1 week	TFN (0,0.2,0.4)	two weeks	TFN (0.2,0.4,0.6)
Specialist Expertise	Layman	TFN (0,0.2,0.4)	Proficient	TFN (0.2,0.4,0.6)
Knowledge of the TOE	Public	TFN (0,0.2,0.4)	Restricted	TFN (0.2,0.4,0.6)
Window of Opportunity	Unnecessary /Unlimited access	TFN (0,0.2,0.4)	Easy	TFN (0.2,0.4,0.6)
Equipment	Standard	TFN (0,0.2,0.4)	Standard	TFN (0,0.2,0.4)
Classified security level		Basic(B)		Enhance Basic(EB)
Evaluation Assurance Level(EAL)		Undefined EAL		EAL1~EAL3

The numerical results of the illustrative example demonstrate that the proposed fuzzy based attack potential measurement method is more practical, efficient and advantageous than the traditional method:
(1) Results reveal that the proposed fuzzy based attack potential measurement method is able to support the Kaizen event for measuring small but encouraging improvement of web application vulnerabilities.
(2) Results show that the proposed fuzzy based attack potential measurement method has the advantage that the deficiencies existed in

traditional measurement method is no longer existed for calculation of attack potential values and classification of security levels.
(3) Results demonstrate that the fuzzy linguistic decision making approach in the proposed fuzzy based attack potential measurement method is suitable to represent, handle impreciseness and uncertainties in the data, information and knowledge under fuzzy environment.

5. CONCLUSIONS

This study developed a Kaizen framework to guide and initiate a series of Kaizen events. Following the steps of the Kaizen framework, a new fuzzy based attack potential measurement method was proposed to support the Kaizen events to the stepwise achievement of measurement and improvement of web application security vulnerabilities. A numerical example was applied in examining how the new measurement method is useful in supporting the Kaizen event. The results of the illustrative example show that the proposed fuzzy based attack potential measurement method is more practical, efficient and advantageous than the traditional method to support the Kaizen events for measuring small but encouraging improvement of web application vulnerabilities. This research provides new insights into the use of Kaizen philosophy to initiate Kaizen events that can be of use to those working in the areas related to web application security vulnerabilities. Practitioners and researchers can easily apply the proposed new measurement method to gather and analyze data, as well as to support the Kaizen events for their own research goal and objectives.

Measurement and improvement are two basic approaches to implement an initiated Kaizen event under the Kaizen framework. This study focuses on proposing a new measurement method to support the initiated Kaizen events. The improvement actions taken to implement the Kaizen event are not explored in further detail. In the future work, a case study focused on the improvement actions will be taken to implement the Kaizen event will be conducted. The new measurement method will be used to the case study and the measurement result is expected to lead the Kaizen team for continuous improvement of web application security vulnerabilities. With the release of the upcoming version of OWASP Top Ten List, a new update will be made to further evolve a new attack potential measurement method and to support Kaizen events for the developed Kaizen framework.

6. REFERENCES

[1] Microsoft, Improve web application security: Threats and countermeasures. Chapter 1: Web application security fundamentals. Retrieved on September 28, 2019. https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff648636(v=pandp.10)?redirectedfrom=MSDN.

[2] J. I. Ker, Y. Wang, and H. Y. Lee, Applying Kaizen methods to improve voltage regulator subassembly area. *Lecture Notes in Electrical Engineering*, 293, 667-674, 2014. https://doi.org/10.1007/978-3-319-04573-3_83

[3] I. Kato, and A. Smalley, *Toyota Kaizen methods: Six steps to improvement*. New York: Taylor & Francis Group, 2011.

[4] J. Miller, M. Wroblewski, and J. Villafuerte, *Creating a Kaizen culture: Align the organization, achieve breakthrough results, and sustain the gains*. New York: McGraw-Hill, 2014.

[5] R. A. Petermann, *The Kaizen freeway: A high speed route to process improvement*. CreateSpace, Independent Publishing Platform, 2014.

[6] K. A. Ramírez, and V. P. Álvaro, Continuous improvement practices with Kaizen approach in companies of the metropolitan district of Quito: An exploratory study. *Intangible Capital*, 13(2), 479-497, 2017.

[7] OWASP, Category: OWASP top ten project. Retrieved on June 16, 2017. http://www.owasp.org./index.php/Top10#OWASP_Top_10_for_2013.

[8] Eugene Lebanidze, Securing enterprise web applications at the source: An application security perspective. Retrieved on January 16, 2017. https://www.owasp.org/images/8/83/Securing_Enterprise_Web_Applications_at_the_Source.pdf.

[9] Information-Technology Promotion Agency (IPA), Vulnerability assessment guide for developers, March 4, 2013. http://www.ipa.go.jp/security/jisec/jisec_e/reference.html.

[10] CEM, *Common methodology for information technology security evaluation-evaluation methodology*, Version 3.1 Revision 5, CCMB-2017-04-004, Common Criteria Member Organizations, April 2017.

[11] ISO/IEC 18045, Information technology – Security techniques – Evaluation criteria for IT security – CEM, September, 2012.

[12] CC, *Common criteria for information technology security evaluation,* Version 3.1 Revision 5,
Part 1: Introduction and general model, CCMB-2017-04-001,
Part 2: Security functional components, CCMB-2017-04-002,
Part 3: Security assurance components, CCMB-2017-04-003,
Common Criteria member organizations, April 2017.

[13] ISO/IEC 15408, Information technology – Security techniques – Evaluation criteria for IT security – ISO/IEC 15408-1, 15408-2 and 15408-3– Common Criteria Part 1, 2, 3, September, 2012.
[14] M. Imai, *Kaizen*: *The key to Japan's competitive success*. New York: Random House Business Division, 1986.
[15] R. Maurer, *The spirit of Kaizen*: *Creating lasting excellence one small step at a time*, USA: McGraw-Hill Professional Publishing, 2012.
[16] C. Baril, V. Gascon, J. Miller, and N. Côté, Use of a discrete-event simulation in a Kaizen event: A case study in healthcare. *European Journal of Operational Research*, 249(1), 327-339, 2016. *https://doi.org/10.1016/j.ejor.2015.08.036*
[17] W. J. Glover, J. A. Farris, and E. M. Van Aken, Kaizen Events: Assessing the existing literature and convergence of practices. *Engineering Management Journal*, 26(1), 39-61, 2014. https://doi.org/10.1080/10429247.2014.11432003
[18] N. H. A. Halim, A. N. Adnan, and N. S. Khusaini, Kaizen event assessment through performance and economic investment analysis. *International Journal of Business and Administrative Studies*, 3(1), 1-7, 2017. https://doi.org/10.20469/ijbas.3.10001-1
[19] W. Glover, W. H. Liu, J. Farris, and E. M. Van Aken, Characteristics of established Kaizen event programs: An empirical study. *International Journal of Operations & Production Management*, 33 (9), 1166-1201, 2013. https://doi.org/10.1108/IJOPM-03-2011-0119
[20] F. Montabon, Using Kaizen events for back office processes: The recruitment of frontline supervisor co-ops. *Total Quality Management & Business Excellence*, 16(10), 1139-1147, 2005. https://doi.org/10.1080/14783360500235876
[21] E. M. Van Aken, J. A. Farris, W. J. Glover, and G. Letens, A framework for designing, managing, and improving Kaizen event programs. *International Journal of Productivity and Performance Management*, 59(7), 641-667, 2010. https://doi.org/10.1108/17410401011075648
[22] J. A. Farris, E. M. Van Aken, T. L. Doolen, and J. M. Worley, Learning from less successful Kaizen events: A case study. *Engineering Management Journal*, 20(3), 10-20, 2008. https://doi.org/10.1080/10429247.2008.11431772
[23] J. A. Farris, E. M. Van Aken, T. L. Doolen, and J. M. Worley, Critical success factors for human resource outcomes in Kaizen events: An empirical study. *International Journal of Production Economics*, 117(1), 42-65, 2009. https://doi.org/10.1016/j.ijpe.2008.08.051
[24] J. A. Marin-Garcia, J. J. Garcia-Sabater, and T. Bonavia, The impact of Kaizen events on improving the performance of automotive components' first-tier suppliers. *International Journal of Automotive*

Technology and Management, 9(4), 362-376, 2009. https://doi.org/10.1504/ijatm.2009.028524

[25] U. Y. Nahm, M. Bilenko, and R. J. Mooney, Two approaches to handling noisy variation in text mining. In *Proceedings of the ICML-2002*, *Workshop on Text Learning* (pp. 18-27). Sydney, Australia, 2002.

[26] V. Novák, Základy fuzzy modelování. Praha: BEN–technická literatura, 2000.

[27] S. A. Melnyk, R. J. Calantone, F. L. Montabon, and R. T. Smith, Short-term action in pursuit of long-term improvements: Introducing Kaizen events. *Production and Inventory Management Journal*, 39(4), 69-76, 1998.

[28] K. Martin, and M. Osterling, *The Kaizen Event Planner*. New York: Productivity Press, 2007.

[29] J. Ye, Multicriteria decision-making method based on a cosine similarity measure between trapezoidal fuzzy numbers. *International Journal of Engineering*, *Science and Technology*, 3(1), 272-278, 2011. https://doi.org/10.4314/ijest.v3i1.67654

[30] T. Y. Chen, and T.C. Ku, Importance-assessing method with fuzzy number-valued fuzzy measures and discussions on TFNs and TrFNs. *International Journal of Fuzzy Systems*, 10(2), 92-103, 2008.

[31] K. S. Lin, and J. C. Pan, Modeling a multi-criteria decision support system for capital budgeting project selection. In N. Nguyen, S. Tojo, L. Nguyen, and B. Trawiński (Eds.), *Lecture Notes in Computer Science*, 10192, 137-147, 2017. https://doi.org/10.1007/978-3-319-54430-4_14