UDC 004.056.5 **doi: 10.20998/2522-9052.2018.4.19**

A. Tetskyi

National Aerospace University "Kharkiv Aviation Institute", Kharkiv, Ukraine

THE METHOD OF SELECTING MEASURES TO PROTECT THE WEB APPLICATION AGAINST ATTACKS

The **subject matter** of the paper is the process of ensuring the protection of Web applications against attacks aimed at obtaining unauthorized access to the functions of the content management system administrator. The **goal** is to create a method to select measures to protect the Web application against attacks. The **tasks** are: to determine a list of common Web application security measures, to develop a method of selection the most efficient protective measures within a limited budget. The **methods** used are: attacks trees analysis, expert assessment method, methods for solving nonlinear integer programming problems with Boolean variables. The following **results** were obtained. The method for selecting Web application security measures based on the success rate estimation of a Web application attack has been developed. Inasmuch as all protective measures differ in cost, effectiveness, and influence on various attack vectors, as a result of the choice an optimal set of countermeasures that will provide the maximal reduction level of attack success rate must be determined. That's why not only changing the parameters of countermeasures, but also changing the parameters of the attack tree can lead to changing the set of countermeasures. The problem of selecting protection measures is a nonlinear problem of integer programming with Boolean variables. **Conclusions.** The scientific novelty of the results is as follows: the method of selecting countermeasures by solving the optimization problem, which allows to select the most effective countermeasures in a limited budget, was improved. The minimization of the attack success rate is used as a target function; the budget of services is specified as a limitation. However, it is also possible to use a minimization of a budget level as a target function, wherein the maximum allowable value of the attack success rate is used as a limitation.

Keywords: attack; security; protection measure; Web application; cost minimization.

Introduction

Modern web applications provide opportunities for providing a wide range of services on the Internet. Owing to the development of content management systems, it is possible to create websites without writing code directly. Content management systems can be divided into classes, depending on the scope of their application. At the moment, content management systems are also used to run small and medium businesses in the World Wide Web. In this regard, the interest of intruders who can hack the site and, in any way, get a profit has increased in such systems. In the area of Web application security, there are a number of problems, normally being forgotten or missed by site owners. Moreover, site owners often do not understand the consequences of hacking the site by malicious users.

In general, there are two groups of reasons why hacking websites are possible. The first group of causes is associated with defects during creation a Web application [1]. The second group of causes is related to problems at the stage of exploitation. Causes from both groups arise from the low level of knowledge in the field of information security of those who develop the system and who use it. For example, if an attacker was able to bypass the authorization mechanism on the site and gain access to the control panel, this is the reason from the first group. If an attacker gained access to the control panel due to the usage of a weak password by the system administrator, then this is a problem from the second group.

Most of the problems from both groups are known for a long time and methods of protection against them are also known [2, 3]. Naturally, any method of protection can't guarantee one hundred percent effectiveness, but the usage of protection measures can significantly increase the site's resistance against malicious attacks [4, 5]. Insofar as the usage of protection measures is not ubiquitous and the protection measures have different efficiency levels, selecting protection measures for a particular Web application is the actual task.

The goal of the paper is to create a method for selecting the most effective measures for protecting a specific Web application.

Main results

This paper is based on the work [6], in which frequent attack scenarios of Web applications were visualized as an attack tree, and a method for estimation the attack success rate was proposed based on the tree. It is necessary to determine a variety of measures that can be applied to counter attacks in the attack tree. The attacks and countermeasures tree is shown in Fig. 1.

As an example, a site that implements the functionality of an online store, created using a content management system considered. Assume that no countermeasures from the list below have yet been applied to the site in question. Such security measures can be applied to the site (C_i):

1. Two-factor authentication usage to gain access to the control panel. Such a measure will not allow an attacker to log in to the system using compromised credentials of administrator.

2. Trainings for staff to improve the level of knowledge in the field of information security. Often the online store has several administrators who manage the processing of orders. Often, site managers do not know why they shouldn't set an easy password, why they shouldn't store the password, or use untrusted software on their computers. That is, this measure is used to reduce the number of hacks for the reasons of the second group, which was mentioned at the beginning of the paper.

3. Using encrypted HTTPS connections. Statistics shows that currently less than a half of sites in the net-

work use an encrypted protocol to transmit traffic [7]. This protection is extremely important, because when intercepting administrator credentials, password complexity does not matter.

4. Using VPN when working in the admin panel. This measure also protects traffic from interception.

5. Protection against busting usernames and passwords. Unfortunately, almost always the built-in brute force protection mechanisms are either missing or not effective. The usage of effective methods of protection against brute force will save the site even in the case of using dictionary logins and passwords.

6. Usage of complex passwords and non-standard logins. If there is no effective brute force protection, the brute force attack can continue infinitely. Using standard logins and weak passwords will lead to the fact that the attacker automatically selects a combination of a login and password that matches the credentials of one of the site administrators.

7. Install and configure the firewall. It will allow to restrict access to vulnerabilities for attackers that may be present in the source code of the application. The peculiarity of this protection measure is that its effectiveness depends on the setting, and if it is not configured correctly, such measure may completely obstruct the correct operation of the site.

Each protection measure is characterized by a cost and impact factor, which is determined by an expert. The list of countermeasures and events subject to countermeasures, as well as their impact coefficients and costs, are shown in Table 1. The cost is given for illustration on the assumption of there is a subject who is ready to provide services for the implementation of security measures at a specified cost.

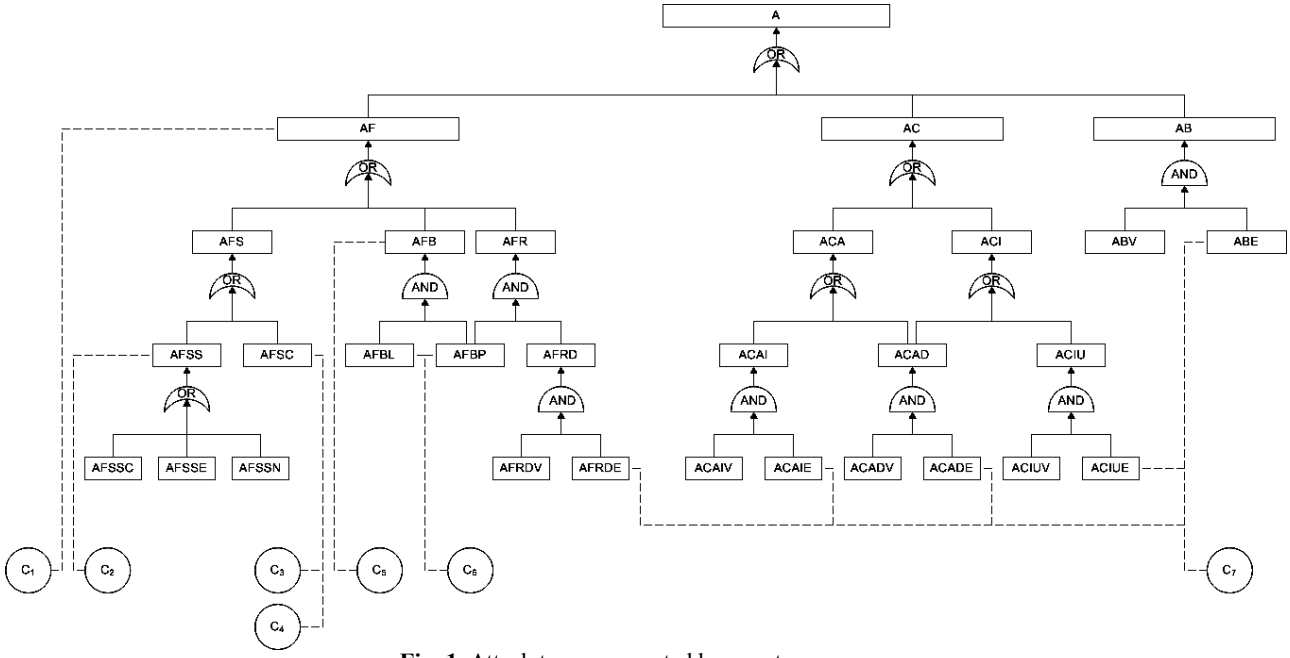

Fig. 1. Attack tree, augmented by countermeasures

Table 1 – **The list of countermeasures**

Countermeasure	Events affected by countermeasure	Impact coefficient	Cost (cu)
C_1 – Two-factor authentication usage	AF	0.8	120
C_2 – Staff training	AFSS	0.5	300
C_3 – HTTPS usage	AFSC	0.7	50
C_4 – VPN usage	AFSC	0.8	80
C_5 – Protection against brute forcing usernames and passwords	AFB	0.9	60
C_6 – Setting complex passwords and non-standard logins	AFBL, AFBP	0.6	20
C_7 – Installing and configuring the firewall	AFRDE, ACAIE, ACADE, ACIUE, ABE	0.75	220

The full names of the events are given in Table 2. The main event is event «A» – a successful attack of a Web application that managed to gain access to the administrator's functions.

Selection of protection measures being held by solving an optimization problem. For calculations, a spreadsheet MS Excel is used, the function of calculating the attack success rate is implemented in VBA, the add-in "Solver" is used for solving the optimization problem [8]. The fragment of the document in which the success rate is calculated is shown in Fig. 2. The values used for evaluations, coefficients and costs for calculations are test values and they intended to demonstrate how the methods for evaluating the attack success rate and the selection of security measures for a Web application work.

Another sheet of the document contains information about countermeasures. The target function is to

minimize the success rate of an attack; the limitation is the total amount of services cost. A fragment of the document, reflecting the source data for the selection of countermeasures, is shown in Fig. 3.

Table 2 – **Event names**

Abbreviation	Full name of the event
A	Get access to control panel functions
AF	Find out the login and password of the current administrator
AC	Create a new administrator account
AB	Bypass authorization
AFS	Steal login and password
AFB	Find login and password using brute force
AFR	Find a password using a known hash
ACA	Add a new account with privileges directly to the database
ACI	Increase standard user privileges
ABV	Vulnerabilities to bypass authorization are found
ABE	Exploit vulnerabilities to bypass authorization
AFSS	Credentials stolen from storage
AFSC	Credentials stolen during unencrypted transmission
AFBL	The attacker has a dictionary that includes the desired login
AFBP	The attacker has a dictionary that includes the desired password
AFRD	Retrieve username and password from database
ACAI	Usage of appropriate vulnerabilities (for example, SQL injection on insert)
ACAD	The credentials for connecting to the database are known
ACIU	Usage of appropriate vulnerabilities (for example, SQL injection on update)
AFSSC	Credentials stolen from PC
AFSSE	Credentials stolen from email or any cloud storage
AFSSN	Credentials stolen from non-digital storage
AFRDV	Appropriate vulnerabilities have been discovered that allow retrieving username and password from database
AFRDE	Exploiting vulnerabilities that allows to retrieve username and password from the database
ACAIV	Appropriate vulnerabilities found (for example, SQL injection on insert)
ACAIE	Exploit vulnerabilities (for example, SQL injection on insert)
ACADV	Appropriate database connection vulnerabilities found
ACADE	Exploiting database connectivity vulnerabilities
ACIUV	Appropriate vulnerabilities found (for example, SQL injection on update)
ACIUE	Exploiting vulnerabilities (for example, SQL injection on update)

Event name	ABV	ABE	AFSC	AFBL	AFBP	AFSSC	AFSSE	AFSSN	AFRDV	AFRDE	ACAIV	ACAIE	ACADV	ACADE	ACIUV	ACIUE
Attack difficulty	4	4	4	4	5	5	5	5	4	4	4	4	4	4	4	4
Attack cost	2	3	2	3	3	5	5	5	2	3	2	3	2	3	2	3
Detection difficulty	4	3	1	1	1	1	1	1	4	3	4	3	4	3	4	3
Coefficient w_1	0.33															
Coefficient w_2	0.33															
Coefficient w_3	0.33															
Coefficient c	0.30															
Attack success rate	0.512															

Fig. 2. Calculation of attack success rate

	A	B	C	D	E	F	G	H
1	Countermeasure name	C_1	C_2	C_3	C_4	C_5	C_6	C_7
2	Cost	120	300	50	80	60	20	220
3	Coefficient of reducing	0.8	0.5	0.7	0.8	0.9	0.6	0.75
4	Usage	0	0	0	0	0	0	0
5								
6								
7	The objective function is to minimize P	0.511721						
8	Cost of services	0						

Fig. 3. Initial data for selecting countermeasures

The objective function is contained in cell B7, the total cost of services is contained in cell B8. In the example shown in Fig. 4, the restriction B8 <= 450 is used. In the process of solving an optimization problem, the values of the B4:H4 cells change, conditional formatting is applied to them for greater clarity. The restriction for these cells is that they can contain an integer value not greater than one, i.e. two values are

possible, 1 – a countermeasure is used, 0 – a countermeasure is not used. If a countermeasure is used, the probabilities of the events affected by this countermeasure are multiplied by the impact coefficient of the countermeasure.

Fig. 5 shows the graph of the attack success rate dependence on budget. Indeed, the value of the indicator is minimal, subject to a limited budget of 450 conventional units. Fragments of the graph, going only up, are dead-end and they are caused by the fact that the cost of different combinations of countermeasures is the same, but their total impact on the success rate of an attack can vary greatly.

Of the total set of possible combinations of measures, sets were selected that provide a greater reduction of the attack success rate at the same total cost. The optimized graph of attack success rate dependence on budget is shown in Fig. 6.

Figure 6 shows that even a small budget can significantly increase the security of the site. For example, with a budget of 120 conventional units, the attack success rate is approximately 0.138, with a total cost of services of 440 conventional units, this value is 0.088. A significant increase in the total cost of services leads to a slight decrease of the attack success rate.

That's why the customer must determine the feasibility of purchasing the proposed set of protection measures.

	A	B	C	D	E	F	G	H
1	Countermeasure name	C_1	C_2	C_3	C_4	C_5	C_6	C_7
2	Cost	120	300	50	80	60	20	220
3	Coefficient of reducing	0.8	0.5	0.7	0.8	0.9	0.6	0.75
4	Usage	1	0	0	1	0	1	1
5								
6								
7	The objective function is to minimize P	0.088255						
8	Cost of services	440						

Fig. 4. The result of the countermeasures selection

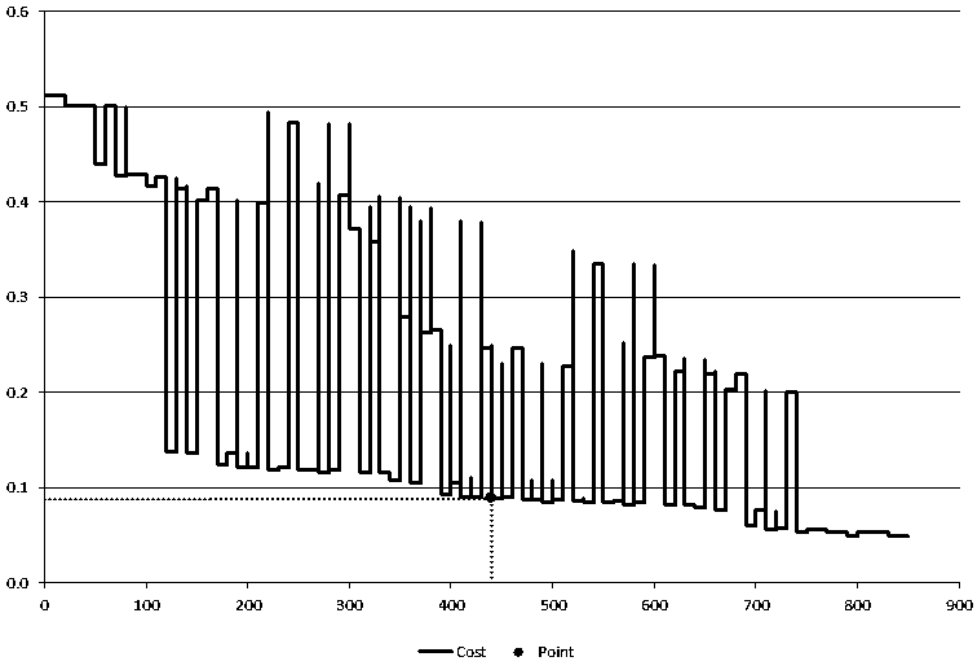

Fig. 5. The graph of the attack success rate dependence on budget

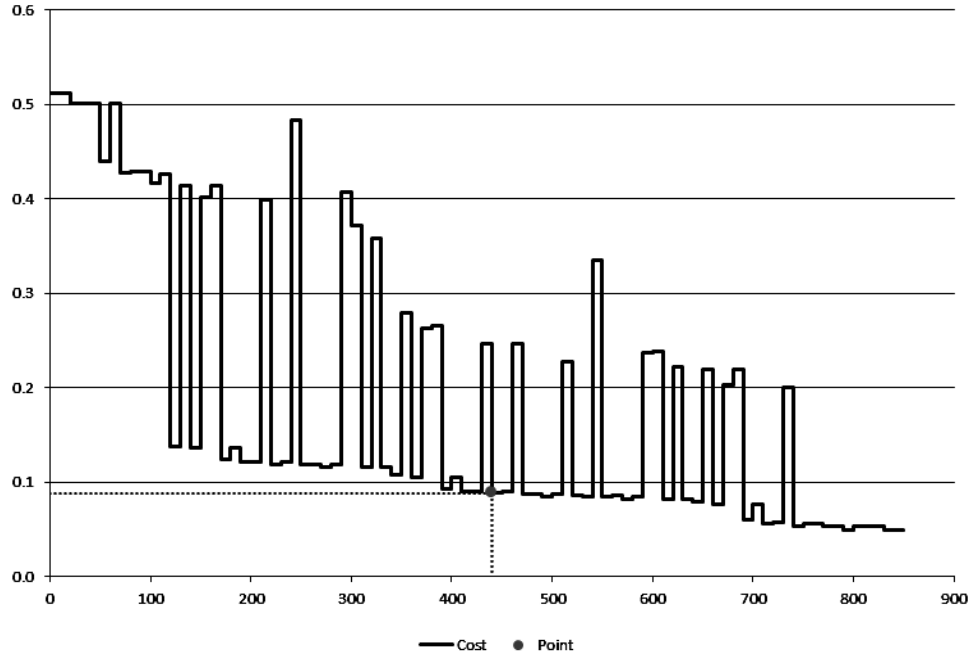

Fig. 6. The optimized graph of the attack success rate dependence on budget

Conclusions

The developed method allows to select the most effective protection measures for each individual Web application.

A set of countermeasures that provides the greatest decrease of attack success rate is selected.

The minimization of the attack success rate is used as the target function; the budget of services is used as a limitation. However, it is also possible to use budget minimization as a target function, and to set the maximum allowable value of the attack success rate as a limitation.

References

1. Atashzar, H., Torkaman, A., Bahrololum, M. and Tadayon, M.H. (2011), "A survey on web application vulnerabilities and countermeasures", *Proc. of the 2011 6th Int.Conf. on Computer Sciences and Convergence Information Technology*, pp. 647-652.
2. Lepofsky, R. (2014), *The manager's guide to web application security: a concise guide to the weaker side of the web*, Apress, 232 p., DOI: https://doi.org/10.1007/978-1-4842-0148-0.
3. Shah, S. and Mehtre, B. M. (2015), "An overview of vulnerability assessment and penetration testing techniques", *Journal of Computer Virology and Hacking Techniques*, vol. 11, no. 1, pp. 27-49, DOI: https://doi.org/10.1007/s11416-014-0231-x.
4. Han, Y., Sakai, A., Hori, Y. and Sakurai, K. (2009), "Improving the Quality of Protection of Web Application Firewalls by a Simplified Taxonomy of Web Attacks", *Advances in Information Security and Its Application. ISA 2009. Communications in Computer and Inf. Science*, Vol. 36, Springer, Berlin, Heidelberg, pp. 105-110, DOI: https://doi.org/10.1007/978-3-642-02633-1_14.
5. McClure, S., Shah, S. and Shah, S. (2002), *Web hacking: Attacks and defense*, Addison-Wesley Professional, 528 p.
6. Tetskyi, A.G. (2018), "Applying of attack trees for estimation the probability of a successful attack of the web-application", *Radioelektronni i komp'uterni sistemi*, no. 3, pp. 74-79, DOI: https://doi.org/10.32620/reks.2018.3.08.
7. *Usage of Default protocol https for websites*, available at: https://w3techs.com/technologies/details/ce-httpsdefault/all/all.
8. *Solver in Excel*, available at: https://www.excel-easy.com/data-analysis/solver.html.

Received (Надійшла) 27.09.2018
Accepted for publication (Прийнята до друку) 28.11.2018

Метод вибору заходів захисту WEB-застосунка від атак

А. Г. Тецький

Предметом дослідження є процеси забезпечення захисту Web-застосунка від атак, спрямованих на отримання несанкціонованого доступу до функцій адміністратора системи управління контентом. **Метою** є створення методу вибору заходів захисту Web-застосунка від атак. **Завдання**: визначити перелік найбільш поширених заходів захисту Web-застосунка, розробити метод вибору найбільш ефективних заходів захисту за умови обмеженого бюджету. Використовуваними **методами** є: аналіз дерев атак, метод експертних оцінок, методи розв'язання нелінійних задач цілочисельного програмування з булевими змінними. Отримані наступні **результати**. Розроблено метод вибору заходів захисту Web-застосунка, заснований на методі оцінювання показника успішності атаки Web-застосунка. Оскільки всі заходи захисту відрізняються вартістю, ефективністю і впливом на різні вектора атак, в результаті вибору визначається набір контрзаходів, який надає максимальне зниження показника успішності атаки. Тому до зміни набору контрзаходів призводить не тільки зміна параметрів контрзаходів, а й зміна параметрів дерева атак. Завдання вибору заходів захисту є нелінійним завданням цілочисельного програмування з булевими змінними. **Висновки**. Наукова новизна отриманих результатів полягає в наступному: удосконалено метод вибору контрзаходів шляхом розв'язання оптимізаційної задачі, що дозволяє вибрати найбільш ефективні контрзаходи в умовах обмеженого бюджету. В якості цільової функції використовується мінімізація показника успішності атаки, бюджет послуг вказується в якості обмеження. Однак також можливо використовувати в якості цільової функції мінімізацію бюджету, а в якості обмеження встановити максимально допустиме значення показника успішності атаки.

Ключові слова: атака; безпека; захід захисту; Web-застосунок; мінімізація витрат.

Метод выбора мер защиты Web-приложения от атак

А. Г. Тецкий

Предметом изучения являются процессы обеспечения защиты Web-приложения от атак, направленных на получение несанкционированного доступа к функциям администратора системы управления контентом. **Целью** является создание метода выбора мер защиты Web-приложения от атак. **Задачи**: определить перечень наиболее распространенных мер защиты Web-приложения, разработать метод выбора наиболее эффективных мер защиты при условии ограниченного бюджета. Используемыми **методами** являются: анализ деревьев атак, метод экспертных оценок, методы решения нелинейных задач целочисленного программирования с булевыми переменными. Получены следующие **результаты**. Разработан метод выбора мер защиты Web-приложения, основанный на методе оценивания показателя успешности атаки Web-приложения. Поскольку все меры защиты отличаются стоимостью, эффективностью и влиянием на различные вектора атак, в результате выбора определяется набор контрмер, оказывающий максимальное снижение показателя успешности атаки. Поэтому к изменению набора контрмер приводит не только изменение параметров контрмер, но и изменение параметров дерева атак. Задача выбора мер защиты является нелинейной задачей целочисленного программирования с булевыми переменными. **Выводы**. Научная новизна полученных результатов состоит в следующем: усовершенствован метод выбора контрмер путем решения оптимизационной задачи, что позволяет выбрать наиболее эффективные контрмеры в условиях ограниченного бюджета. В качестве целевой функции используется минимизация показателя успешности атаки, бюджет услуг указывается в качестве ограничения. Однако также возможно использовать в качестве целевой функции минимизацию бюджета, а в качестве ограничения установить максимально допустимое значение показателя успешности атаки.

Ключевые слова: атака; безопасность; мера защиты; Web-приложение; минимизация затрат.