WEB APPLICATION SECURITY ANALYSIS USING THE KALI LINUX OPERATING SYSTEM

Ivan M. Babincev[a], *Dejan* V. Vuletić[b]
[a] Serbian Armed Forces, Technical test center,
Belgrade, Republic of Serbia,
e-mail: babincev1301@gmail.com,
ORCID iD: http://orcid.org/0000-0002-3994-9032
[b] Ministry of Defence of the Republic of Serbia, Defence Policy Sector,
Strategic Research Institute, Belgrade,
e-mail: dejan.vuletic@mod.gov.rs,
ORCID iD: http://orcid.org/0000-0001-9496-2259

DOI: 10.5937/vojtehg64-9231

FIELD: Computer Sciences
ARTICLE TYPE: Professional Paper
ARTICLE LANGUAGE: English

Abstract:

The Kali Linux operating system is described as well as its purpose and possibilities. There are listed groups of tools that Kali Linux has together with the methods of their functioning, as well as a possibility to install and use tools that are not an integral part of Kali. The final part shows a practical testing of web applications using the tools from the Kali Linux operating system. The paper thus shows a part of the posibilities of this operating system in analysing web applications security, which presents the goal of this work.

Key words: *security, web applications, Kali Linux.*

Introduction

Web applications contain many vulnerabilities that can compromise integrity of web pages, reveal confidential information and disrupt the operation of the application itself. Although there are different mechanisms of protection, new vulnerabilities are revealed dailly and attackers can use them for various attacks.

Due to the emergence of new security threats in the area of cyber security, the creators of the BackTrack operating system created a new, specialized Linux distribution intended for Penetration testing, called Kali Linux.

Kali Linux operating system

Born and released on March 13th, 2013, *Kali Linux* is based on Debian and an FHS-compliant filesystem. (Muniz, Lakhani, 2013). Debian was created in 1993 as a Linux distribution. It is completely democratically organized, in hands of community, and its users are generally enthusiasts and Linux experts, because Linux administration, in comparison to other operating systems, is more complicated. *Filesystem Hierarchy Standard (FHS)* defines the structure of folders and it is primarily intended for Unix programmers.

Kali has many updated tools, synchronized four times a day. This means that users have the latest package updates and security fixes. Kali Linux is essencially a Linux distribution intended for penetration testing. Kali Linux has many possibilities and different types of tools - it can test network security, security of operating systems, communications, applications, etc. It can be downloaded from the Internet in a few different ways.

Kali Linux can be used in a virtual environment, by installation on a virtual machine. Also, it can be run without installation software on the hard disk, accessing an external source such as a USB or DVD. However, this is not reliable, due to a negative effect on the setup and operations of some tools. Because of its speed, accuracy and other performances, it is highly recommended to install Kali Linux on a host hard drive.

There is a possibility of parallel existence and use of two operating systems on one computer, the *dual boot* method, which is desirable for Windows users and Linux beginners. It is recommended to install Kali Linux in a virtual machine. This paper uses the VMWare Workstation 10 virtualization software and the Kali Linux 1.0.7 operating system.

Kali Linux offers many customized tools designed for penetration testing, categorized in the following groups, (Muniz, Lakhani, 2013), as seen in Figure 1:

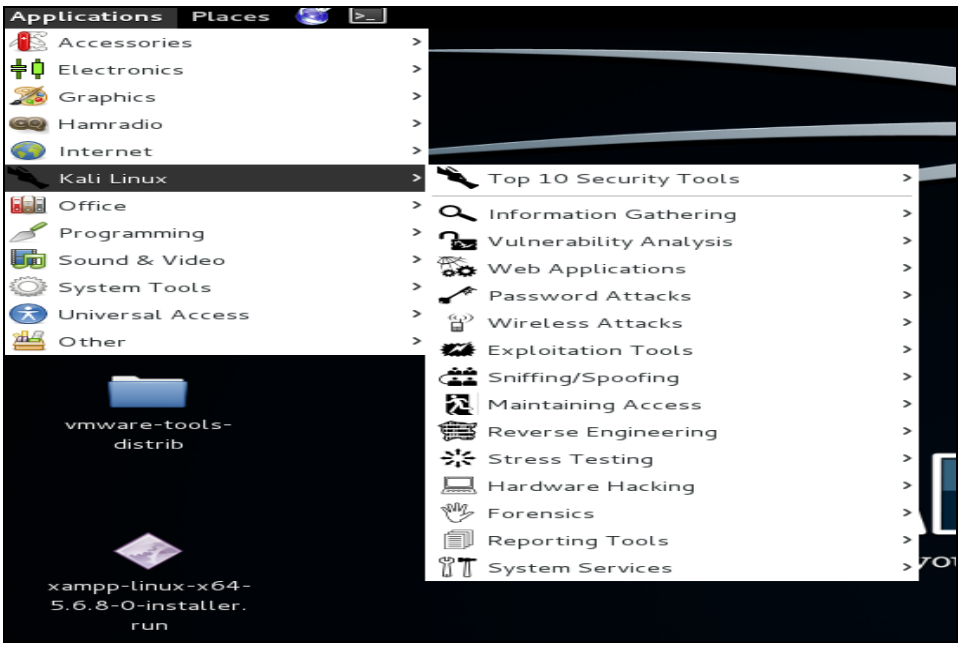


Figure 1 – Kali Linux group tools
Рис. 1 – список инструментов Kali Linux
Slika – 1 Grupa alata *Kali Linux-a*

- **Information Gathering:** these are reconnaissance tools, used to gather data on target networks and devices. Tools range from identifying devices to protocols used.
- **Vulnerability Analysis:** tools from this section focus on evaluating systems for vulnerabilities. Typically, these are run against systems found using the tools from the previous section.
- **Web Applications:** these are tools used to audit and exploit vulnerabilities in web servers. However, these tools do not always refer to attacks against web servers, they can be web-based tools for testing network services.
- **Password Attacks:** this section of tools is primarily used for perfoming Brute force attacks on passwords used for authentication.
- ***Wireless* Atacks:** these tools are used to exploit vulnerabilities found in wireless protocols. In most cases, tools from this section require a *wireless* adapter that can be configured by the Kali Linux operating system, to be put in a particular operation mode.

- **Exploitation Tools:** these are tools used to exploit vulnerabilities found in systems.
- ***Sniffing and Spoofing*:** these are tools used for network packet captures and network packet manipulation.
- **Maintaining Access:** tools to be used after establishing access to the target network or system. They provide alternative paths and approaches, if the vulnerability used for access by attacker is found and removed.
- **Reverse Engineering:** the purpose of these tools is analyzing how a program was developed so it can be copied, modified, or so that it can lead to development of other programs. Reverse engingeering is also used for malware analysis or by researchers in discovering vulnerablities in software applications.
- **Stress Testing:** these tools are used to evaluate how much data a system can handle. Undesired outcomes could be obtained, such as causing a device controlling network communication to open all communication channels or a system shutting down (also known as a denial of service attack).
- **Hardware hacking:** this section contain Android tools, which could be classified as mobile, and Ardunio tools that are used for programming and controlling other small electronic devices.
- **Forensics:** forensics tools are used to monitor and analyze computer network traffic and applications.
- **Reporting Tools:** these tools serve to deliver information found during a penetration exercise.
- **System services:** this is where Kali Linux services can be enabled or disabled.

Using Kali Linux tools in Web application testing

A web application containing vulnerabilities threatens the security of a database and the entire computer system, because the web page must be constantly available to provide services to users. Firewall and other similar programs do not provide protection against malicious activities in such a case, because web applications often have direct access to user databases, but also must be available outside the local network, so it is difficult to ensure security. One of the main problems is to detect web application vulnerabilities before attackers exploit them. (CARNet, 2007), (CARNet, 2008).

Vulnerability scanning uses various tools, both commercial ones and those available on the Internet, which are free for using. The main

advantage of commercial tools is the automatization of the scanning proccess offered by almost all commercial versions. The efficiency of each tool depends on the content to be searched, but most tools can conduct basic vulnerability scanning. By studying the basic features of tools, it is easy to find a suitable scanner that should be used to search vulnerabilities of individual applications.

It is recommended to start the specific tools and test web applications to detect and correct security holes prior to its use. Kali Linux is an excellent solution that contains many tools intended for scanning vulnerabilities and web application security testing. This article covers tools: Burp Suite, XSSer, Nessus, Nikto and Vega. Damn Vulnerable Web Application and Mutillidae application are used as test applications.

Burp Suite

Burp Suite is an integrated platform for performing security testing of web applications (Burp Suite, nd). Its various tools support the entire testing process. It allows the combination of advanced manual techniques and automated attacks that accelerate the testing process and make it more effective. Burp Suite includes the following tools:

- *Proxy* – analyzes and modifies the traffic between the browser and the target application. It intercepts and modifies HTTP traffic, easily analyzes content and manipulates requests sent to the server by a client;
- *Spider* – analyzes the traffic that goes through the Proxy server and sends requested content to other Burp Suite tools. It keeps the entire work and allows the operation to continue where it stopped the last time;
- *Scanner* – scans web applications. It provides a complete control of the scanned content and displays the results of scanning;
- *Intruder* – allows performing improvized attacks that exploit vulnerabilities;
- *Repeater* – tool for modifying HTTP requests and analyzing the received responses;
- *Sequencer* – tool for testing randomness of session tokens of applications;
- *Decoder* –simple tool for encoding and decoding text strings;
- *Comparer* – this tool is used to compare data, for example to compare two or more HTTP responses;
- *Extender* – allows different extensions of the functionalities of the *Burp Suite* platform.

Burp Suite can be run in two ways:

- by typing the *burpsuite* command in the terminal,
- under *Applications* | *Kali Linux* | *Web Applications* | *Web Application Fuzzers* | *burpsuite.*

After launching *Burp Suite*, this launch dashboard will be presented: (Figure 2).

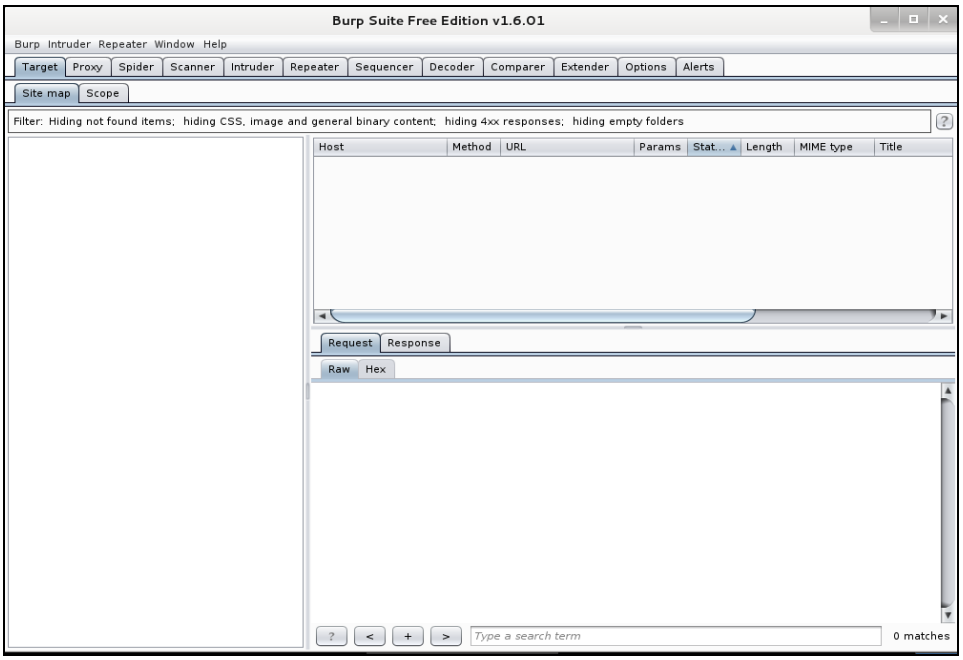


Figure 2 – Burp Suite – initial screen
Puc. 2 – Burp Suite – начальный экран
Slika 2 – Burp Suite – početni ekran

This paper describes a tool *Intruder*, which is used to perform an automated brute force attack on the *dvwa* (*damn vulnerable web application*) test application. Before performing the attack, it is necessary to configure *Proxy*. It is necessary to set the IP address and the port on which Proxy works, the localhost address and a specific port number. These settings should match the settings of the web browser (Figure 3).

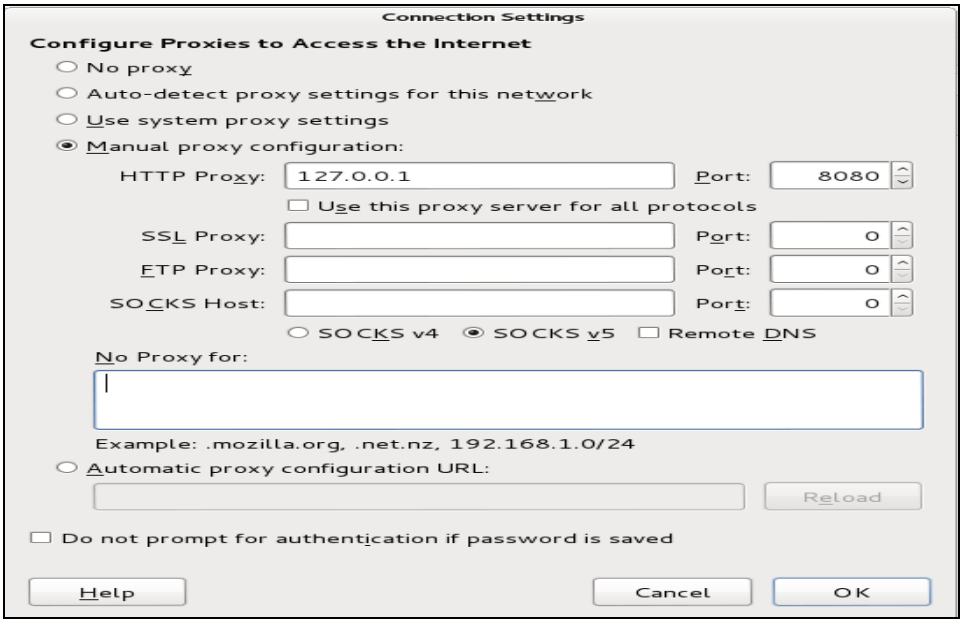


Figure 3 – Proxy server configuration
Рис. 3 – Настройки Proxy-сервера
Slika 3 – Podešavanje Proxy servera

As seen in Figure 3, Iceweasel uses the HTTP Proxy server active on port 8080 and the IP address of the localhost, 127.0.0.1. *Burp Suite Proxy* must be configured in the same way. It is necessary to select *Options* on the tab *Proxy* and enter the required parameters. After that, it is necessary to enable *Intercept* on the same tab, to intercept requests sent to the server. By a click on the *Brute Force* tab in the *dvwa* application, the authentification window shows up.

By a click on *login* after entering the username and the password, the authentification request will be sent to the server through *Burp Proxy*, and Proxy will intercept that request. As a result, the intercepted request will be displayed on the tab *Intercept* in the *Burp Suite* platform. In the next step, the request is sent to the *Intruder*. It is necessary to mark the areas over which the attack will be executed, and to select a type of attack .

After creating the list of possible usernames and passwords, the attack is launched (Figure 4).

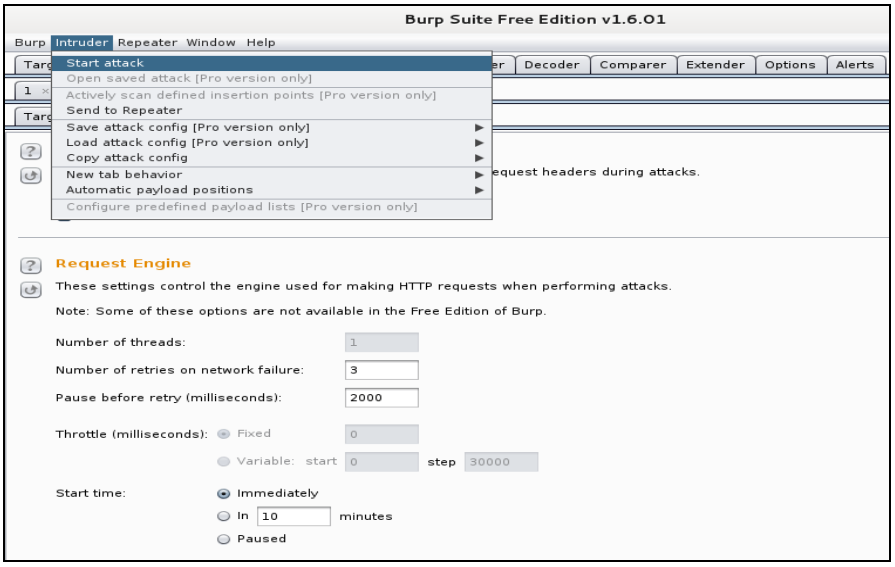


Figure 4 – Burp Suite - launch attack
Рис. 4 – Burp Suite – запуск атаки
Slika 4 – Burp Suite – realizacija napada

Figure 5 shows the results of an automated brute force attack. The attack was successfully executed, the username is *admin* and the password is *password*.

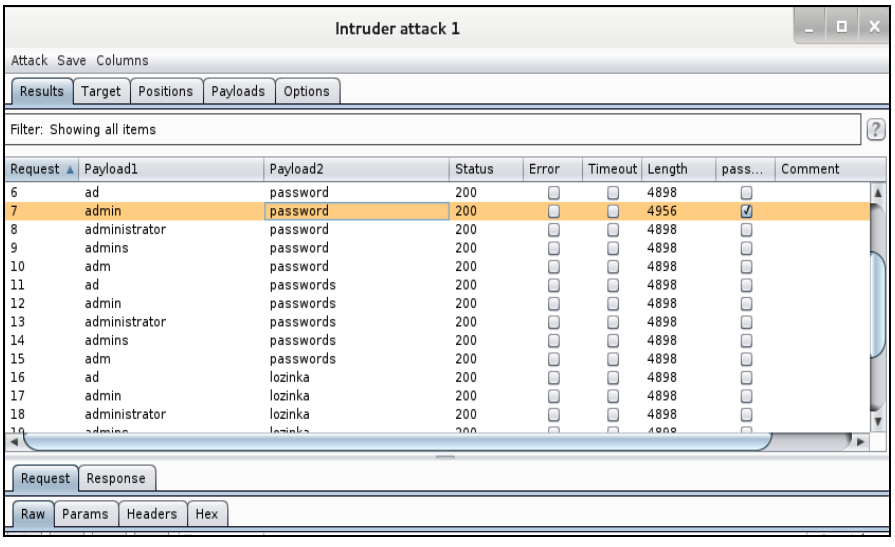


Figure 5 – Burp Suite – results shown
Рис. 5 – Burp Suite – отчет результатов
Slika 5 – Burp Suite – prikaz rezultata

XSSer

XSSer is an open source tool used for penetration testing. (http://xsser.03c8.net/). It automates the process of detection and exploitation of XSS vulnerability on a web site or application (XSSer, nd). By typing the *xsser --gtk* command into the terminal, the initial XSSer screen shows up (Figure 6). It can also be accessed without typing commands, by clicking on the tab Applications | Kali Linux | Web Applications | Web Application Fuzzers | xsser.

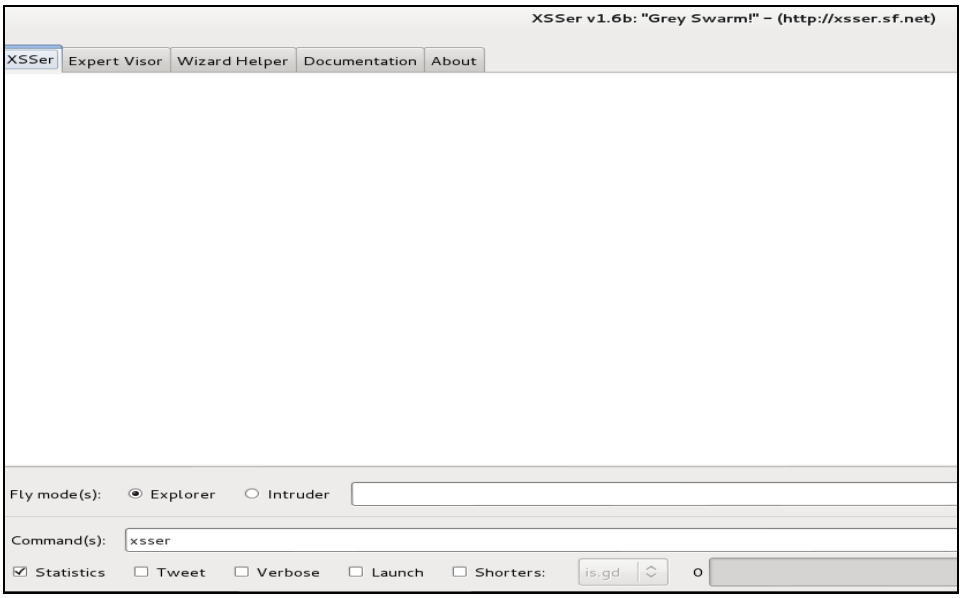


Figure 6 – XSSer – initial screen
Puc. 6 – XSSer – Начальный экран
Slika 6 – XSSer – početni ekran

Before starting the attack, it is necessary to set certain parameters in the URL of the site or the tested application. After displaying the startup screen, it is necessary to click on the Expert Visor tab, choose Visor (s) and set the Connect option to ON (include connection). Then, mark the Intruder, enter the target URL and mark the Automatic.

After that, click on the button Aim!, then the button FLY!!! and XSSer will begin attack. As a result of the attack, a list of possible XSS injections will be displayed after certain time (Figure 7).

Figure 7 – XSSer – overview of a possible injection
Рис. 7 – XSSer – отчет о возможных XSS инъекциях
Slika – XSSer – prikaz mogućih XSS injekcija

Nessus

Nessus is a free tool for scanning and finding vulnerabilities in computer systems. Nessus supports over 50,000 plugins for detection of various types of vulnerabilities. A plugin typically contains information about the vulnerabilities, guides the user to confirm the existence of certain vulnerabilities and gives instructions for their removal.

Using the Nessus tool on the Kali Linux operating system requires an additional installation of Nessus, because Nessus does not belong to the set of tools contained in Kali Linux. After downloading the installation file, the installation is launched from the terminal (Figure 8), by typing the command *dpkg-i* in front of the file name.

Nessus operates using the Web server and the Nessusd server. The web server communicates with the Nessusd server and it is used for configurating and monitoring the scanning process, while the Nessusd server contains a plugins database and realizes the scanning process (Chuming, Manton, 2004).

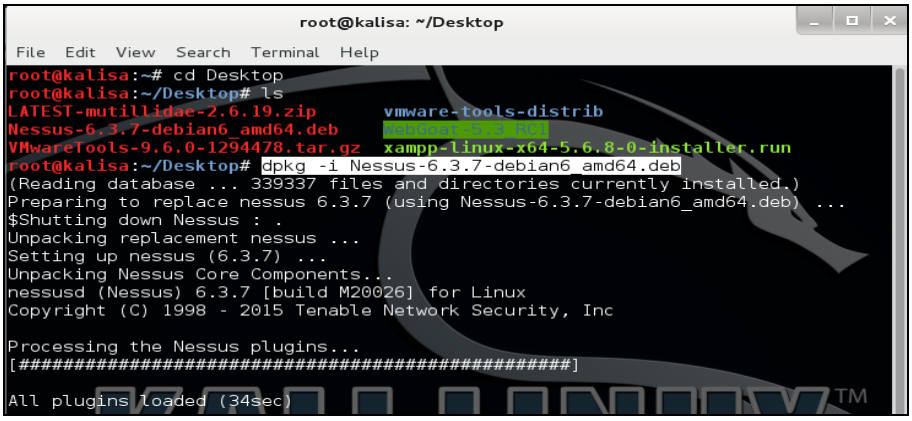


Figure 8 – Nessus – installation
Puc. 8 – Nessus –установка
Slika 8 – Nessus – instalacija

A click on the New Scan displays a page with different types of scans that Nessus can realize (Figure 9), which shows a wide range of its capabilities. As shown in Figure 9, Nessus supports web application testing.

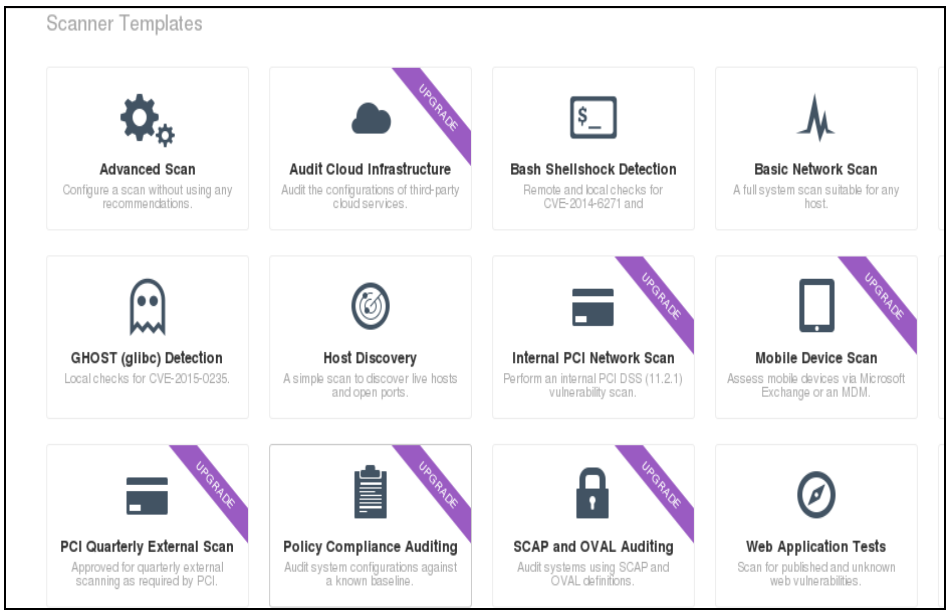


Figure 9 – Nessus – some of the possibilities
Puc. 9 – Nessus – некоторые возможности
Slika 9 – Nessus – neke od mogućnosti

A click on the Web Application Tests displays a page where the user has to set certain parameters and perform settings (Figure 10). The BASIC card allows entering the name of scanning, the description and the targeted URL address. The Mutillidae application is used as a test application. Using Schedule options and Email Notifications, Nessus allows periodical scanning and reporting via e-mail.

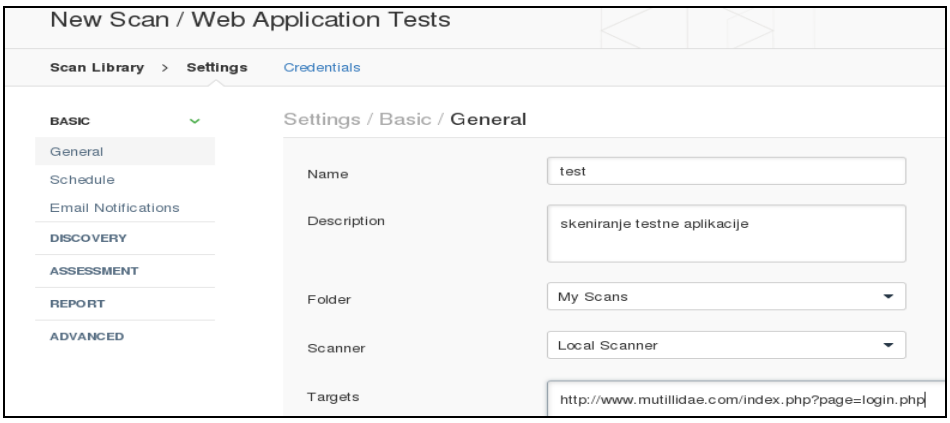


Figure 10 – Nessus – data entry
Puc. 10 – Nessus – ввод данных
Slika 10 – Nessus – unos podataka

Nikto

Nikto is a very popular open source tool for testing web application security. It is written in the *Perl* programming language. Nikto is platform independent, so it can work on both Windows and Linux. Nikto's tools are based on a Perl module called *libwhisker* that allows finding *CGI* scripts on web servers. The Libwhisker module is included in the standard Nikto software package, but it is advisable to regularly update it with new versions (CARNet, 2003).

Although it can be treated as deficiency, Nikto uses the CLI, which is suitable for the remote start of the tool, using an SSH connection. There is no graphical user interface. It is designed so that it does not require a graphical access to the system to install and run. During the scan, Nikto sends a large number of requests to the server and then analyzes the received responses. Nikto is capable of sending data in the form of HTTP requests so it can test the XSS (Cross Site Scripting) and SQL Injection vulnerabilities.

After starting, Nikto will begin scanning and results will be displayed in the terminal (Figure 11).

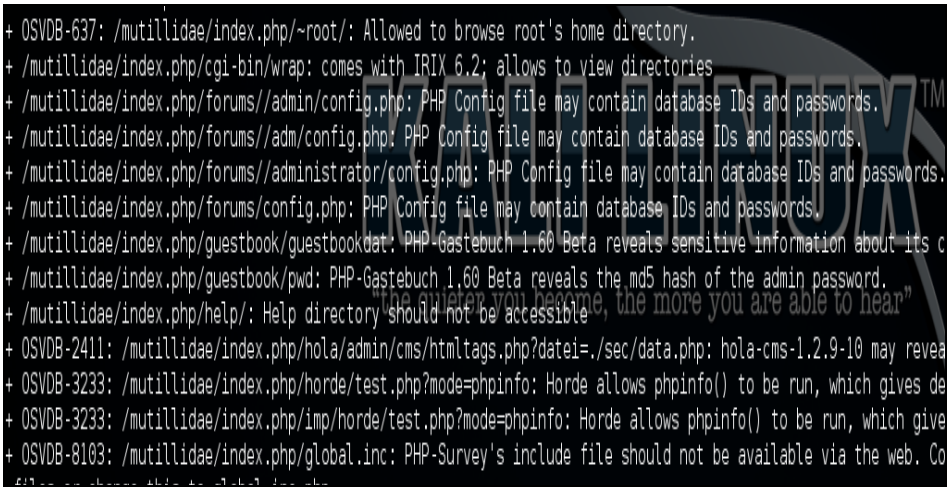


Figure 11 – Nikto - results shown in the terminal
Puc. 11 – Nikto – отчет выявленных результатов
Slika 11 – Nikto – prikaz rezultata u terminalu

Based on the displayed results, the application is vulnerable. If the user uses the command -o (output) and determines the output file, the results will be saved in the output file. In this case, the results are stored in the file testic.html. Opening the testic.html file using the web browser allows an access to the scan results, which are presented in the form of web pages (Figure 12).

localhost / 127.0.0.1 port 80	
Target IP	127.0.0.1
Target hostname	localhost
Target Port	80
HTTP Server	Apache/2.2.22 (Debian)
Site Link (Name)	http://localhost:80/mutillidae/index.php/
Site Link (IP)	http://127.0.0.1:80/mutillidae/index.php/
URI	/mutillidae/index.php/
HTTP Method	GET
Description	Retrieved x-powered-by header: PHP/5.4.41-0+deb7u1
Test Links	http://localhost:80/mutillidae/index.php/ http://127.0.0.1:80/mutillidae/index.php/
OSVDB Entries	OSVDB-0
URI	/mutillidae/index.php/
HTTP Method	GET
Description	The anti-clickjacking X-Frame-Options header is not present.
Test Links	http://localhost:80/mutillidae/index.php/ http://127.0.0.1:80/mutillidae/index.php/
OSVDB Entries	OSVDB-0
URI	/mutillidae/index.php/
HTTP Method	GET
Description	Uncommon header 'logged-in-user' found, with contents:

Figure 12 – Nikto – presentation of the report in the Iceweasel browser
Puc. 12 – Nikto – отчет в браузере Iceweasel
Slika 12 – Nikto – prikaz izveštaja u Iceweasel pretraživaču

Vega

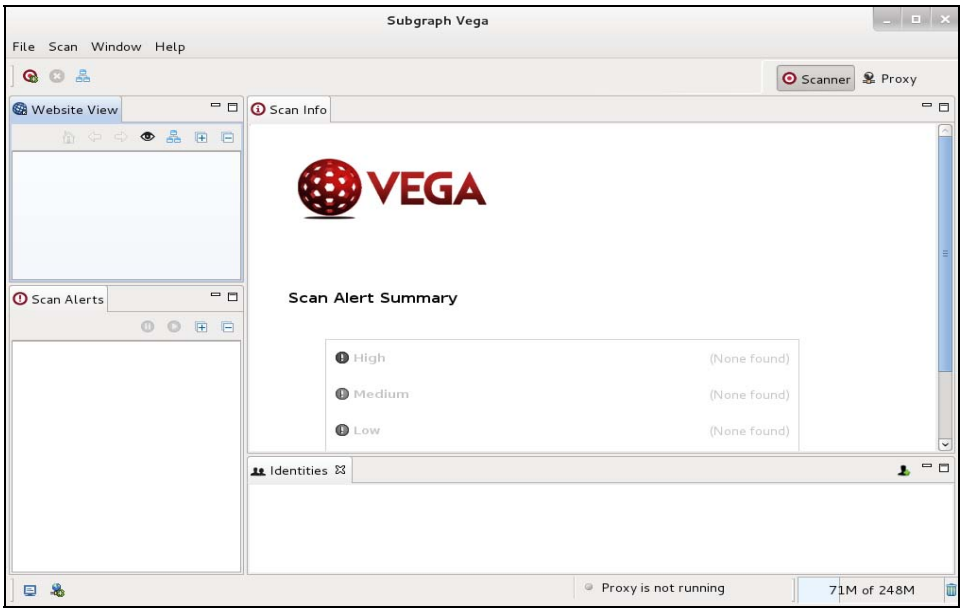
Vega is a free tool designed to test the security of web applications. It is used to check the vulnerability of web applications such as SQL Injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF) and many others. It is written in the programming language Java, contains a graphical environment and runs on various operating systems (https://subgraph.com/vega/).

Vega contains an automated scanner that conducts vulnerability testing. According to many sources, this is one of the best free tools for vulnerability assessment.

Vega has a very simple graphical environment. With the launch of the new scanning and entering the target URL, the preparation for web applications scanning is completed. Vega can be run in one of two ways:

- typing the *vega* command into the terminal,
- clicking on Applications | Kali Linux | Web Applications | Web Vulnerability Scanners | Vega,

The initial screen is displayed after start (Figure 13).



Slika 13 – Vega – početni ekran
Figure 13 – Vega – initial screen
Рис. 13 – Vega – начальный экран

Vega contains *Scanner* and *Proxy* buttons in the upper right corner of the initial screen. Clicking on the Scanner button in the upper right corner and then clicking on the Scan button in the upper left corner will display a window to enter the targeted URL address (Figure 14).

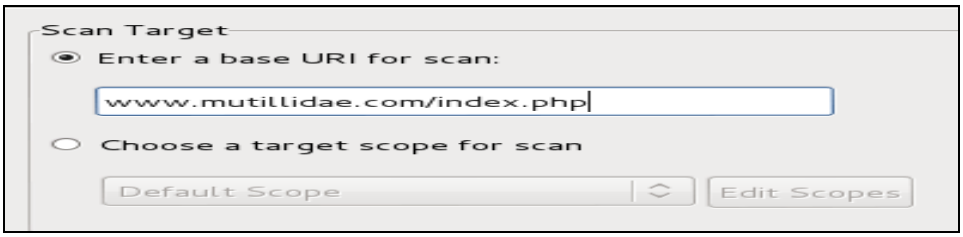


Figure 14 – Vega – entry of the targeted URL
Рис. 14 – Vega – ввод целевого URL
Slika 14 – Vega – unos ciljanog URL-a

The next step is to select a specific scanning mode so that vulnerability can be tested (Figure 15).

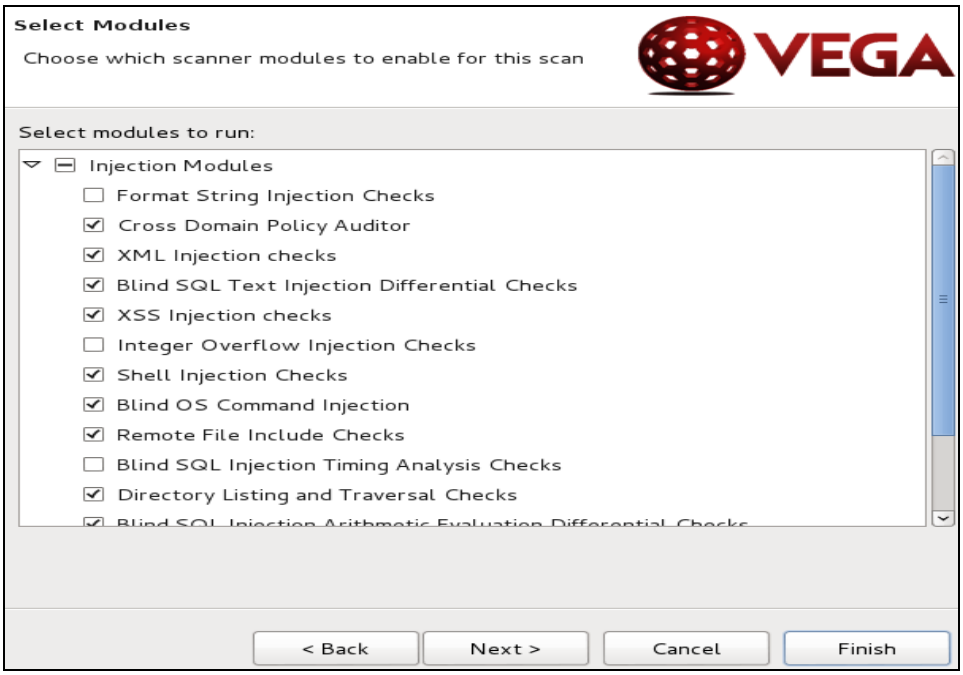


Figure 15 – Vega - ways of scanning
Рис. 15 – Vega – способы сканирования
Slika 15 – Vega – načini skeniranja

During scanning, the Vega groups discovered vulnerabilities according to the level of risk. Website View in the upper left corner shows the tested applications and other URL addresses associated with the tested applications (Figure 16). The Scan Alerts window in the lower left corner displays the categories of the discovered vulnerabilities (Figure 16).

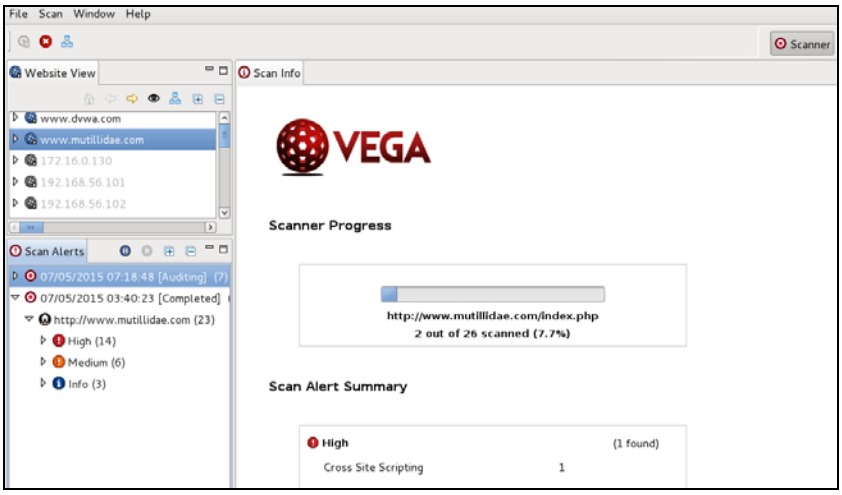


Figure 16 – Vega – scanning
Рис. 16 – Vega – сканирование
Slika 16 – Vega – skeniranje

As a scanning result, Vega will present a report on the discovered vulnerabilities. The vulnerabilities are grouped according to the level of risk to the tested application (Figure 17).

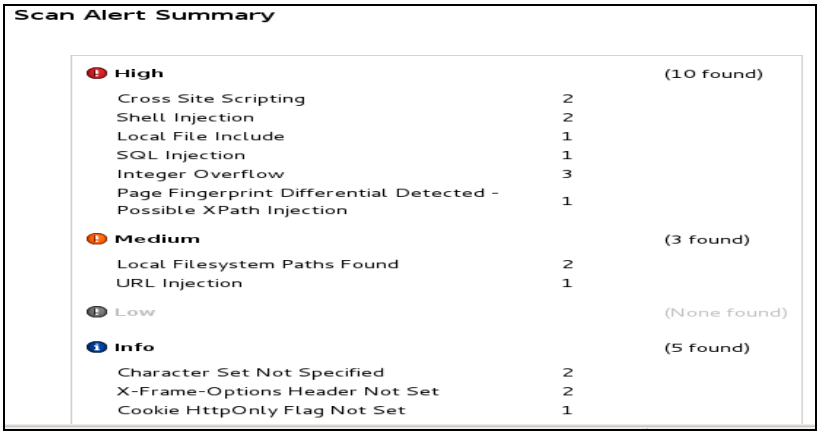


Figure 17 – Vega – report
Рис. 17 – Vega – отчет
Slika 17 – Vega – izveštaj

Conclusion

The paper describes different tools used for security testing and finding vulnerabilities in web applications. All tools are an integral part of the Kali Linux operating system, except Nessus, which is additionally installed thus showing a possibility of upgrading Kali Linux with new tools. This article shows how the tools operate, demonstrates practically how to configure and use different tools, and which vulnerabilities were discovered using these tools. This paper presents only a part of the Kali Linux operating system possibilities in the analysis of the web application security. It is shown that the Kali Linux operating system is very efficient, considering the fact that it contains enough tools to implement a complete web application test. Although this paper describes only five, it should be noted that Kali Linux contains over thirty tools for testing web applications.

For a detailed web application test, it is necessary to use all the tools available. Detecting XSS, SQL injection and other vulnerabilities is a laborious and time-consuming job. Therefore, it is useful to have several automated scanners which will conduct an analysis of the application and prepare a report for a relatively short period of time. The number of vulnerabilities will be higher or lower, depending on the tools. Discovered vulnerabilities should be manually checked.

Although automated scanners facilitate the work of conducting web application tests, they have a deficiency since they are not able to independently decide on the appropriate action to be taken on the basis of the semantics of the content viewed and analyzed. For now, this can be performed only by the user, but tools with this ability are being developed.

It is important to emphasize that it is not advisable to use only one tool in the analysis of web application security. Scans show a lot of fake vulnerabilities and some of them are not detected. The experience and knowledge of the person who conducts testing is a crucial factor for quality and a complete analysis of web applications.

References

Burp Suite. . . Preuzeto sa https://portswigger.net/burp/

CARNet. 2003. *Analiza Nikto CGI Skenera*.Zagreb: Hrvatska akademska istrazivacka mreza., str. 2-9.

CARNet. 2007. *Analiza Nessus alata*.Zagreb: Hrvatska akademska istrazivacka mreza., str. 5-25.

CARNet. 2008. *Usporedba besplatnih alata za ispitivanje sigurnosti Web aplikacija*. Zagreb: Hrvatska akademska istrazivacka mreza., str. 5-20.

Chuming, C., & Manton, M. 2004. A Web Interface for Nessus Network Security Scanner. U: International Conference on Internet Computing, Las Vegas, Nevada, USA, str. 383-389 p. 383-389.

Muniz, J., & Lakhani, A.(2013). *Web Penetration Testing with Kali Linux*. Preuzeto sa https: //www. packtpub. com/networking-and-servers/web-penetration-testing-kali-linux

Vega Preuzeto sa https://subgraph.com/vega/

XSSer Preuzeto sa http://xsser.03c8.net/

АНАЛИЗ БЕЗОПАСНОСТИ ВЕБ-ПРИЛОЖЕНИЙ ОПЕРЦИОННОЙ СИСТЕМОЙ KALI LINUX

Иван В. Бабинцев[а], *Дејан* В. Вулетич[б]
[а] ВСРС, Центр технического тестирования, Белград, Республика Сербия,
[б] Министерство обороны Республики Сербия,
Институт стратегических иследованний, Белград

ОБЛАСТЬ: компьютерные науки
ВИД СТАТЬИ: профессиональная статья
ЯЗЫК СТАТЬИ: английский

Резюме:

В статье дается описание операционной системы Kali Linux, включая цели и возможности ее использования. Приведен список инструментов системы Kali Linux, способ работы ее конкретных инструментов, а также возможность установки и использования инструментов, которые не являются частью операционной системы Kali Linux. В заключительной части статьи, наглядно представлено тестирование веб-приложений с применением инструментов операционной системы Linux Кали. Таким образом, представлена часть возможностей Кали Linux операционной системы, применяемой для анализа безопасности веб-приложений, что являлось целью данной работы.

Ключевые слова: *безопасность, Веб-приложения, Kali Linux.*

ANALIZA BEZBEDNOSTI *WEB* APLIKACIJA OPERATIVNIM SISTEMOM *KALI LINUX*

Ivan M. Babincev[a], *Dejan* V. Vuletić[b]
[a] Vojska Srbije, Tehnički opitni centar, Beograd, Republika Srbija,
[b] Ministarstvo odbrane Republike Srbije, Sektor za politiku odbrane,
Institut za strategijska istraživanja, Beograd

OBLAST: računarske nauke
VRSTA ČLANKA: stručni članak
JEZIK ČLANKA: engleski
Sažetak:

U radu je opisan operativni sistem Kali Linux , njegove namene i mogućnosti. Navedene su grupe alata kojima Kali Linux raspolaže, način rada određenih alata koje ovaj sistem sadrži, kao i mogućnost instalacije i korišćenja alata koji nisu njegov sastavni deo. U završnom delu rada praktično je prikazano testiranje web aplikacija korišćenjem alata iz operativnog sistema Kali Linux. Time je prikazan deo mogućnosti ovog operativnog sistema u analizi bezbednosti web aplikacija, što predstavlja cilj ovog rada.

Ključne reči: *bezbednost, web aplikacija, Kali Linux.*

Paper received on / Дата получения работы / Datum prijema članka: 08. 10. 2015.
Manuscript corrections submitted on / Дата получения исправленной версии работы / Datum dostavljanja ispravki rukopisa: 30. 10. 2015.
Paper accepted for publishing on / Дата окончательного согласования работы / Datum konačnog prihvatanja članka za objavljivanje: 02. 11. 2015.