A user friendly security framework for the protection of confidential information

Jawad Hussain Awan[†], Shahzad Memon[†], Shariq Mahmood Khan[††], Muhammad Usman[†††],Rahat Ali Khan[†],
Shazia Abbasi[†] , Abdul Qudoos Noonari[†] and Zahoor Hussain[†]
[†]Institute of Information and Communication Technology, University of Sindh, Jamshoro, Pakistan
[††]Department of Computer Science and Software Engineering, NED University of Engineering & Technology, Karachi, Pakistan
[†††]Department of Computer Software Engineering, UET Peshawar, Mardan Campus

Abstract

The term 'Cyber' is common in security discussions either international or national because increasing number of internet users had increased the growth of cyber-criminal activities. Critical systems of government, military, corporations, financial institutions, hospitals and other businesses are practicing security procedures, tools to tackle the growing level and complexity of cyber-attacks and protect sensitive information stored on databases, network and servers. Hence, a security technical framework is recommended which is helpful for national databases to design, monitor and manage its cyber policy to make sure that ID servers cannot be accessed or damaged by cyber terrorism activity. Proposed security framework detects vulnerabilities Such as: XSS (Cross-site scripting) attack, session riding, Full Path and information disclosure problems, misconfiguration error, injection attack, manipulation attack of protocol, file inclusion attack, automatically detect new URLs of the target website and observes the traffic between server and your browser, and also take control of the request and its response. This framework implemented advanced discovery and fuzzing technologies to detect above vulnerabilities. Moreover, this framework is developed to enhance the security of important national ID databases as well as identify possibilities and levels of cyber-attacks by scanning process while URL is open and its execution takes place that time. Therefore, this research has been carried out to recommend and develop a technical framework that defends national Identification databases as well as detect cyber terrorist attacks and their levelwhile monitoring its services and protect ID servers from unauthorized access or damage which may cause by cyber terrorism.

Keywords:
Cyber services, Cyber Security, IDs, Framework, Vulnerability, Cyber-threat. Cyber-attack, Protection.

1.Introduction

Nowadays, Internet has vital influence on national cyber security because Internet is common application and used in all over the world to access and uses various online services and applications. Simultaneously protecting IPR (Intellectual Property Rights), securing critical infrastructure and providing security to nations are creating double pressure to accelerate the financial remuneration of ICT (Information and Communication Technology) for the developing countries[1]. Various nations have designed legislative cyber capability and nearly about fifty nations have published cyber strategy policies, which defining what security resources should be recommended for upcoming national and economic security proposal. Relatively, it focuses on national cyber security demands also[2].Pakistan is the developing country, where huge numbers of organization are installing latest ICT tools and services into their infrastructures. In addition, governmental authorities are showing awareness to set up emerging technologies into their infrastructures[3]. NADRA (National Database and Registration Authority), eBanking, mobile networks are examples of offered services in Pakistan. But, the security of these organization/services is critical challenge for the researchers, technologists and government officials[4].

The use of Cyber services is universal practice and its security is emerging challenge for users[5]. Users can use these services to perform their activities on daily basis, such as eCommerce, online shopping and eBanking and other groups are dependent upon their IT infrastructure to guarantee business stability[6]. According to Eurostat's, 75% of users inside the European Union have access to computers as well as Internet in the year of 2014. Although the public enjoys the ease which is offered by IT, it also creates different cyber security threats such as spam, malware, DoS and more[7].

Stuxnet, a new kind of cyber-attack is also identified and discussed in this paper, which was target-oriented and complicated and its main objective was to target certain operations of Natanz nuclear of Iran. The categories of cyber threats have been classified according to the level of their target and actions which are against personnel, assets and government. There is a limited number of security frameworks existing for the security of cloud applications or cyber services. Therefore, few security frameworks Such as NVD (National Vulnerable Database), Web Scarab, W3af, Zed Attack Proxy, Web Securify and Web

Manuscript received April 5, 2017
Manuscript revised April 20, 2017

Defend have been discussed in this paper for the understanding of their security level and strategies[8]. Furthermore, prominent factors and barriers and five classes of Interruptive cyber measures have been classified which are foundation tactics for malicious actors as they can interrupt a targeted network. Such as: Message manipulation, exterior service interruption, interior communication interruption, information Attack and tools attack are interruptive cyber measure classes. The classification of these events enables to contrast events either existing in same class or different classes. Every interruptive event can be identified by characteristic of different strategies and procedures applied by cyber criminals or activists of a target network[9].

2. Aims And Objectives

In this section, few aims and objectives have been discussed and review the present mechanism of ID database protection and cyber security policy of national IDs. A technical security framework has been proposed which may help national IDs to monitor, revise, adopt, and ensures the protection of confidentiality of Identification data which is going to be stored on its computers. The development of protection policies may defend against internal and external threats created by network vulnerabilities, cyber-attacks, and events within the system and ability to act quickly to reduce these vulnerabilities and prevent intrusions[10][11]. It is also recommendation of internal and external measures to prevent the theft, damage and illegal use of ID by cyberterrorists.

3. Background Study

In this section, a short literature has been discussed about Stuxnet, assassination of Hamas leader, cybercrimes and threats, existing security frameworks and common reasons of cyber-attacks which is given below:

3.1 Stuxnet

In the year of 2010 [12], a new kind of cyber-attack was noticed and identified which was target-oriented and complicated. This cyber-attack or worm was later known as Stuxnet and identified by A German team under the supervision of Ralph Langner. Stuxnet's main objective was to target certain operations of Natanz nuclear of Iran. Media had spread the reports about the effects and target of this worm around the globe. In this way, increasing number of cyber-attacks became interesting and challenging theme regarding the future of armed inconsistency. Furthermore, Stuxnet altered the nature of cyber-attacks where digital technology was known as robust for the laws of war. After the attack of this worm, industrial control and security of cyber services became the emerging issue[13]. Then, the concentration of cyber experts and Ralph Langner grew regarding this cyber worm that was scattering around the globe and self-implanted with control systems. Large number of computing devices has been infected from India, Iran and the USA. But the Iran was most infected country nearly 60% in 2010 because SCADA-related programs had poor cyber defense strategies, which made it more vulnerable[14].

From a report [15], most websites of Iran were infected and targeted by a virus and then cyber expert teams have started to dissect the malicious code of Stuxnet as well as its origin and target under discussions. Ralph Langner team was curious, and motivated to explore the code of Stuxnet. Furthermore, Stuxnet is a multifaceted piece of malicious code which was never seen or designed before and it comprises of new zero days, digital signatures and revised operating systems. In this cyber-attack, new zero days were identified which were unknown vulnerable, digital signatures had two stolen certificates of private keys designed by renowned companies and made it platform in dependable for windows operating systems as breach its security[16].

First time, cyber criminals designed a cyber-worm which had massive assets and required to be extremely target penetrating. Stuxnet had installed a component known as device driver which communicates with kernel and gain its access. These drivers were stolen and signed by two Taiwan companies indicated that author had access secret signing keys which were really powerful, well protected, and valuable in illegal market. The industrial firm's working experience of Langner proved helpful and he identified that "Stuxnet was only going after a specific industrial controller and a series of nuclear centrifuges" [12] which were working as configured and manufactured by Siemens. However, its nuclear centrifuge was not its target but it has targeted an assured size centrifuges and 984 nuclear centrifuges were linked together at the location of Natanz nuclear and the nuclear program ofIran[17].

After this cyber-attack, the relation of Iran with US and other states or international law has been infected because Stuxnet was a latest cyber weapon which had been used at Natanz nuclear facility. In past, cyber-attacks were carried for the purpose of stealing, interference and manipulation of information. But, Stuxnet surprised the cyber experts and enforced them to design new security strategies to overcome such type of cyber-attacks in future. Stuxnet was the first sovereign weapon and it was a latest type of weapon, designed to damage physically infrastructure via cyber way. Stuxnet target was to damage real world by doing an activity on digital networks. Stuxnet was also smaller as compared to traditional weapons but its physical impact was huge and its objective was to destroy a nuclear Lab which was previously the objective of political and economic sanctions (Chambers-Jones, 2013). They have justifiable answer regarding defensive act against the nuclear program of Iran because they have prohibited doing so. Stuxnet has breached nuclear centrifuges, which was illegally achieved for illegal research. It is also acknowledged that no one is injured and killed. While in 1981, Israel attempted to thwart nuclear research program of Iraq and dropped sixteen bombs having more than two thousands explosive matter on a research site where eleven were killed during Operation Opera [18].

Fig. 1 Seven of the 11 suspects [17]

3.2 Media report about cyberID theft

In the report[19], it is identified that eleven members team was created in the assassination operations of a Hamas Leader named Mahmoud al-Mabhouh, which comprises of six UK IDs, one Irish ID and 4 others which were stolen by Israeli agency MOSAD and used in the murder. Stolen IDs information was also used to make replicas of British passports of actual citizens to get legal entry at Dubai airport. Irish ID was titled as Evan Dennings and remaining six British passport holders were Paul Keeley, Melvyn Mildiner, James Clarke Michael Barney Jonathan Graham, and Stephen Hodes. These killers arrived in Dubai in the early hours of Jan 19, 2010 on flights from France, Germany, Italy and Switzerland [20].

3.3 Cyber Crimes and Threats

During literature review, we have figured out that cybercrimes which can be classified into three categories[21][22].
Category: 1Cyber-criminal activities against personnel
Category: 2Cyber-criminal activities against assets and
Category: 3 Cyber-criminal activities against Government.
Cyber-criminal activities against personnel in which cyber services are used to infect persons Such as child pornography, sexual harassment, spreading of obscene stuff or privacy breach. These cybercrimes puts negative impact on youth, societies and communities. So, it has to be controlled otherwise results bad impact in future.
Cyber-criminal activities against assets consist of computer sabotage, transmission of virus, bugs and spywares like Melissa virus and love bug. These crimes damages computer or business networks which is carried out through cyber services and these causes loss of millions dollars also.
Cyber-criminal activities against Government where cyber terrorist hacks or cracks or breeches the security measures of the government or military maintained website. Such as Hacking, unauthorized access and computer fraud are current emerging crimes.
Cyber Theft such as: identity theft or internet fraud, Cyber sabotage, Web Jacking attack, illegal copying, distribution of software, corporate spying, Cyber Terrorism, Child Pornography, Spamming, phishing, unauthorized online access, Logic bomb attack, Drive by Download, Cyber Assault by Threat, Script Kiddies and DoS (Denial of Service) are also cyber-attacks, which may stop the cyber services and results a large number of financial, economicallost.

3.4 Existing Security Frameworks

There is a limited number of security frameworks are available for the security of national confidential ID's database. Therefore, few security frameworks Such as NVD (National Vulnerable Database), Web Scarab, W3af, Zed Attack Proxy, Web Securify and Web Defend have been discussedbelow:

3.4.1 NVD (National VulnerabilityDatabase)

NVD [23] is a security framework, which is U.S. government content repository standard for the SCAP (Security Content Automation Protocol). It also supports ISAP (Information Security Automation Program) of the US government multi-agency such as NIST (National Institute of Standards and Technology). NVD offers four mailing lists publically. NVD includes content for monitoring and validating configuration of systems using the SCAP. NVD includes databases of security checklists, software flaws related to security, mix configurations and impact metrics. NVD uses vulnerability search engine, NCP (National Checklist Program), SCAP compatible tools,SCAP data feeds,product dictionary,common weakness enumeration and impact metrics as primary resource.

3.4.2 WebScarab

Web Scarab[24] is also security tool which monitors analyzing web applications. Web scarab in java enabled framework using HTTP (Hyper Text Transfer Protocol) or

HTTPS (Hyper Text Transfer Protocol Secure) protocols. This framework's functionality can be extended via plug-ins. It is also working as an intercepting proxy and assesses, observes the incoming and outgoing traffic from browser and to the server. Furthermore, traffic (Such as: request or response) can be modified prior to receive by server or browser. Web scarab helps penetration testers and works on a web application, discover vulnerabilities like SQL injection, XSS (Cross-Site Scripting), CRLF (Carriage Return Line Feed) and automatically discover new URL addresses of the targetwebsite.

3.4.3 W3af

W3af [25] is also web application framework, which intends to offer an enhanced penetration testing platform. This tool detects and identifies nearly about two hundred different web application vulnerabilities Such as Cross-Site Scripting. W3af possess both graphical and console interface, also developed by python. So, it's easy to use and understand. Authentication modules are used to scan the session-protected pages.

3.4.4 Zed AttackProxy

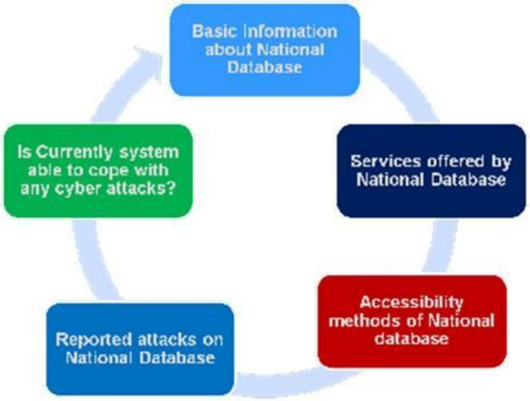

Basic Information about National Database
Services offered by National Database
Accessibility methods of National database
Reported attacks on National Database
Is Currently system able to cope with any cyber attacks?

Fig. 2Categories of Questionnaires

Zed Attack Proxy[26] is open source security framework and developed by AWASP (Advance Weapon Ammunition Support Point). It is used to observe and identify web applications vulnerabilities. This framework is supportive in penetration testing. Sometimes, Zed Attack Proxy is well-known as ZAP and accessible for Windows, Linux platforms. ZAP can be used as a scanner and a tool as an intercepting proxy. ZAP works as Intercepting Proxy, Automatic Scanner, Fuzzer, Plug-n-hack support, Authentication support, Smartcard and Client Digital Certificates support.

3.4.5 WebSecurify

Web securify [27] is one of web application security scanners, it is open source with extendibility feature. It supports diverse technologies and uses them as web workers. Such as: HTML5. This tool is cross- platform and accessible by Mac OS DMG (Disk Image) package. Web securify is also a dominant security testing environment which provides automatic and manual vulnerability testing technologies together.

3.4.6 WebDefend

Web Defend [28] is an application firewall that protects users and servers from cyber-attacks such as zero-day attacks by using Dynamic Profiling and SSL-based traffic. SSL (Secure Sockets Layer) is also known as UFAP (Universal Firewall Access Port). Collaboration detection engine is the protection mechanism of Web Defend, which is composed of a behavior analysis engine[29]. Behavior analysis engine assesses for anomalous practice patterns and signature analysis. Identified and indefinite web application attacks will be blocked by intelligent analysis. Exit control and application defect detection is the unique features of Web Defend. Exit control observes credit card and SSN (Social Security Number) patterns while application defect engine secure the system from programming errors[30].

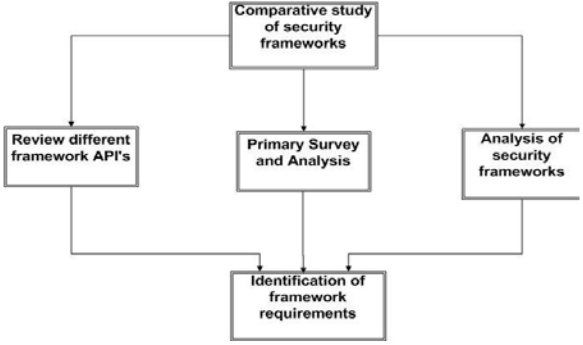

Comparative study of security frameworks
Review different framework API's
Primary Survey and Analysis
Analysis of security frameworks
Identification of framework requirements

Fig. 3Requirement analysis

4. Data Collection

This section illustrates the data analysis of primary survey which was conducted to collect data and analysis to gather relevant information for the proposed research. During this survey, we have designed 31 questionnaires and divided them into five categories, which are mentioned below and shown in fig 2:

1. Basic Information about National Database
2. Services offered by National Database
3. Accessibility methods of National database
4. Reported attacks on National Database
5. Currently system is able to cope with any cyber attacks

Basic Information about National Database section describes the latest information of national database such as NADRA (National Database and Registration Authority). Services offered by National Database section illustrates that which services are offered to registered organizations of Pakistan (such as: mobile companies, banking) by national database. Accessibility methods of National database section discuses that which accessibility methods are used and which rights are allotted to employee and registered organizations in national database. Reported attacks on National Database sections elaborated that any attack or threat has been targeted to national database till now or not. Currently system is able to cope with any cyber-attacks section illustrates that in future this system will protect confidential information and it is or will be secure framework. Furthermore, some general instructions along with questionnaires are also defined in Appendix-I which have given to responders while filling the primary survey questionnaire.

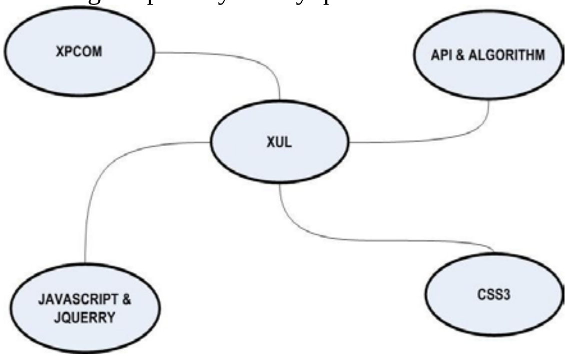


Fig. 4 Tools for the development of proposed framework

5. Development of Framework

In this section, development of security framework has been illustrated and presented. During the development of security framework, following sub sections are required and illustrated:-

5.1 Requirements

This section includes Requirement Analysis of security framework, which is comprised on three steps which are illustrated and discussed in fig 3.Step 1 is comparative study of existing security frameworks, which is further categorized into three parts review of different framework API's, Primary survey analysis and analysis of security frameworks and finally identifies the frameworks requirements in step 3.

5.2 Services of SecurityFramework

Framework offers the services to detect following vulnerabilities: Such as: XSS (Cross-site scripting) attack, session riding, Full Path and information disclosure problems, misconfiguration error, injection attack, manipulation attack of protocol, file inclusion attack, automatically detect new URLs of the target website and observes the traffic between server and your browser, and you can take control of the request and response. Observes the traffic between server and your browser, and you can take control of the request andresponse.

5.3 Tools of SecurityFramework

In this sub section, XUL, XPCOM, JavaScript & jQuery, CSS3 and different API's and algorithm have been discussed and shown in fig 4.

5.4 Internal workingmechanism

In this subsection, internal working mechanism has been discussed and shown in fig 5 and which is comprised of 6 steps. Step 1 loads the framework, Step 2 starts the scanning test, Step 3 sets the URL target, step 4 loads the applications for security purpose in its browser, step 5 monitors the existing workspace for vulnerabilities, and step 6 displays the detected vulnerabilities andthreats.

5.5 Testingmechanism

This section includes testing process flow of framework, which is divided into four stages which are illustrated and discussed in fig 6. Enumeration stage comprises of server and client technologies, software versions, application structure and common configuration practices. Assessment stage is finding vulnerabilities by brute force, fuzzing or manually. Exploitation stage proves that the target is vulnerable, measures attack effectiveness, ease of exploitability and attack likelihood and mitigation controls. Deliverable stage helps in document findings, discuss mitigations and provide examples.

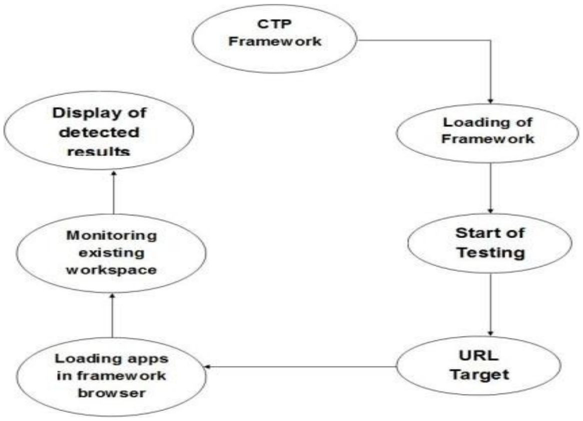

CTP Framework
Loading of Framework
Start of Testing
URL Target
Loading apps in framework browser
Monitoring existing workspace
Display of detected results

Fig. 5. Internal working mechanisms

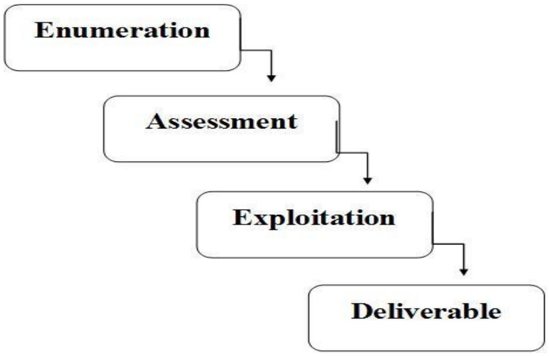
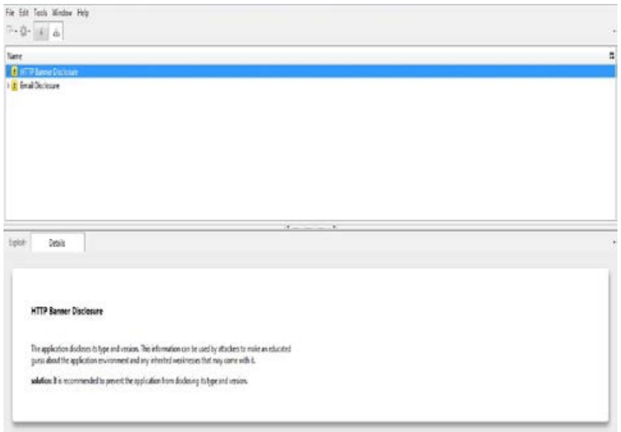


Fig.6. Testing process Flow of proposed framework



HTTP Banner Disclosure

The application discloses its type and version. This information can be used by attackers to make an educated guess about the application environment and any inherited weaknesses that may come with it.

solution: It is recommended to prevent the application from disclosing its type and version.

Fig. 7. Issue Tab of HTTP banner disclosure

6. Results

Result section is main core of research which illustrates and highlights it's working. In this connection, results of proposed framework have been discussed and this section comprises of two sub sections such as Issue Tab and Result Tab.

6.1 Issue Tab

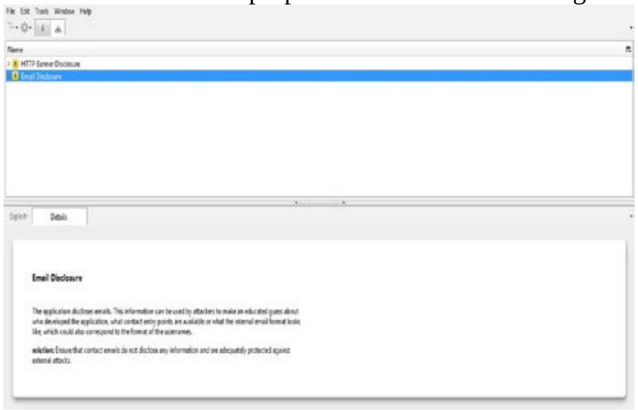
Issue tab only lists the existing vulnerabilities of URL. In this section, different results of Issue tab have been illustrated and shown in following figures.

6.1.1. Http Banner Disclosure

HTTP banner disclosure is vulnerability existing in URLs. HTTP banner disclosure contains the information such as the operating system and its version, web server and its modules shown in Fig7.

6.1.2 Email Disclosure

An email disclosure is vulnerability existing in URLs. Email disclosure contains confidential information and used for informational purposes which is shown in Fig 8.



Email Disclosure

The application discloses emails. This information can be used by attackers to make an educated guess about who developed the application, what contact entry points are available or what the internal email format looks like, which could also correspond to the format of the usernames.

solution: Ensure that contact emails do not disclose any information and are adequately protected against external attacks.

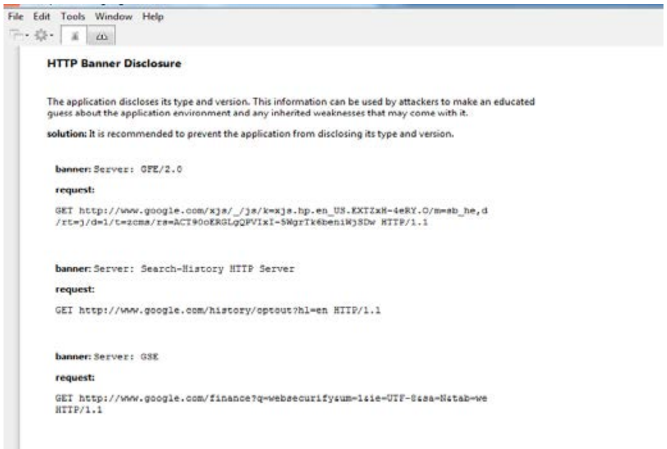
Fig. 8 Issue Tab of Email disclosure

6.2 Result Tab

Result tab displays a result report of selected vulnerability have been illustrated and shown in following figures.

6.2.1 Http Banner Disclosure

HTTP banner disclosure information can be used by attackers to make an educated guess about the application environment and existing weaknesses shown in Fig 9.



HTTP Banner Disclosure

The application discloses its type and version. This information can be used by attackers to make an educated guess about the application environment and any inherited weaknesses that may come with it.

solution: It is recommended to prevent the application from disclosing its type and version.

banner: `Server: GFE/2.0`

request:

```
GET http://www.google.com/xjs/_/js/k=xjs.hp.en_US.EXTZxH-4eRY.O/m=sb_he,d
/rt=j/d=1/t=zcms/rs=ACT90oERGLgQPVIxI-5WgrTk6beniWj3SDw HTTP/1.1
```

banner: `Server: Search-History HTTP Server`

request:

```
GET http://www.google.com/history/optout?hl=en HTTP/1.1
```

banner: `Server: GSE`

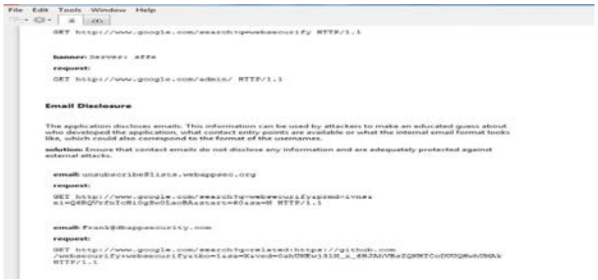
request:

```
GET http://www.google.com/finance?q=websecurify&um=1&ie=UTF-8&sa=N&tab=we
HTTP/1.1
```

Fig. 9 Result Tab of HTTP banner disclosures

6.2.2 Email Disclosure

Email disclosure contains the information of what contact entry points are available or what the internal email format looks like, which could also correspond to the format of the usernames shown in Fig 10.



```
GET http://www.google.com/search?q=websecurify HTTP/1.1

banner: Server: sffe
request:
GET http://www.google.com/admin/ HTTP/1.1

Email Disclosure

The application discloses emails. This information can be used by attackers to make an educated guess about
who developed the application, what contact entry points are available or what the internal email format looks
like, which could also correspond to the format of the usernames.
solution: Ensure that contact emails do not disclose any information and are adequately protected against
external attacks.

email: unsubscribe@lists.webappsec.org
request:
GET http://www.google.com/search?q=websecurify&prmd=ivns&
ei=Q4RQVrfnIcMi0gSw0LacBA&start=80&sa=N HTTP/1.1

email: frank@webappsecurity.com
request:
GET http://www.google.com/search?q=related:https://github.com
/websecurify/websecurify&tbo=1&sa=X&ved=0ahUKEwj31H_s_4MJAhVBaZQKHTCoDUUQHwhSMAk
HTTP/1.1
```

Fig. 10Result Tab of Email disclosure

7. Conclusion

At this cyber age, global cyber laws do not give tolerable official mechanisms to govern cyber combat. Nations should become independent to protect their public and significant infrastructure from cyber-attacks. To overcome these types of criminal activities and cyber-attacks or threats, a security technical framework is proposed, which is helpful for national databases which are offering services via internet. It takes input as URL of database then creates a workspace for inserted URL then scanning technique is applied to identify and detect the vulnerabilities. Proposed framework detects vulnerabilities Such as: Such as: XSS (Cross-site scripting) attack, session riding, Full Path and information disclosure problems, misconfiguration error, injection attack, manipulation attack of protocol, file inclusion attack, automatically detect new URLs of the target website and observes the traffic between server and your browser, and you can take control of the request and response. Framework implemented advanced discovery and fuzzing technologies to detect above vulnerabilities. It is only defined for Windows operating systems. This tool takes nearly 3 hour to complete the scanning process for application URL. Furthermore, this framework is developed to enhance the security of important national ID databases as well as identify possibilities and levels of cyber-attacks by scanning process while database URL is open and execution takes place. Security framework may help the national IDs to design, monitor and manage its cyber policy to make sure that ID servers cannot accessed or damaged by cyber terrorism.

Future Work

Proposed security framework is only capable for Windows Operating System and works on Mozilla Firefox browser. In future, proposed framework may be designed for other browsers such as: Google chrome and for different operating system such as: Linux.

References

[1] R. M. Clark and S. Hakim, “Cyber-Physical Security,” pp. 1–17, 2017.

[2] A. Klimburg, “National Cyber Security Framework Manual,” NATO CCD COE, 2012. [Online]. Available: https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf. [Accessed: 25-Oct-2015].

[3] J. H. Awan, S. A. Memon, N. A. Memon, R. Shah, Z. Bhutto, and R. A. Bhatti, “Conceptual Model for WWBAN (Wearable Wireless Body Area Network),” Int. J. Adv. Comput. Sci. Appl., vol. 8, no. 1, pp. 377–381, 2017.

[4] M. Sommer, O. Njå, K. Lussand, S. Haugesund, and N.-Haugesund, “International Journal of Disaster Risk Reduction,” vol. 21, no. November 2016, pp. 70–84, 2017.

[5] J. H. Awan, S. Memon, M. Shah, and F. H. Awan, “eGovernment Services Security and Challenges in Pakistan,” in SAI Computing, 2016, pp. 1082–1085, 2016.

[6] S. A. Memon and J. H. Awan, “Transformation towards Cyber Democracy: A study on Contemporary Policies, Practices and Adoption Challenges for Pakistan,” in Handbook of Cyber-Development, Cyber-Democracy and Cyber-Defense, 2017, pp. 50–1, 2017.

[7] Eurostat, “INFORMATION SOCIETY,” 2014. [Online]. Available: http://ec.europa.eu/eurostat/cache/metadata/en/isoc_bde15c_esms.htm. [Accessed: 27-Jun-2016].

[8] N. Vithanwattana, G. Mapp, and C. George, “mHealth - Investigating an information security framework for mHealth data: Challenges and possible solutions,” Proc. - 12th Int. Conf. Intell. Environ. IE 2016, no. September, pp. 258–261, 2016.

[9] K. Transactions, I. Systems, K. Lee, S. Policy, and S. Korea, “Lightweight Acknowledgement-Based Method to Detect Misbehavior in MANETs,” KSII Trans. Internet Inf. Syst., vol. 10, no. 2, 2016.

[10] H. Debar, M. Becker, and D. Siboni, “A neural network component for an intrusion detection system,” Proc. 1992 IEEE Comput. Soc. Symp. Res. Secur. Priv., pp. 240–250, 1992.

[11] J. Wolff, “Perverse Effects in Defense of Computer Systems: When More Is Less,” J. Manag. Inf. Syst., vol. 33, no. 2, pp. 597–620, 2016.

[12] M. Kenney, “Cyber-Terrorism in a Post-Stuxnet World,” Orbis, vol. 59, no. 1, pp. 111–128, 2015.

[13] S. Editors, S. Hakim, E. A. Blackstone, R. M. Clark, and R. M. Clark, Cyber- Physical Security, 2015.

[14] D. Bamrara, G. Singh, M. Bhatt, and others, “Cyber Attacks and Defense Strategies in India: An Empirical Assessment of Banking Sector,” Gajendra Bhatt, Mamta, Cyber Attacks Def. Strateg. India An Empir. Assess. Bank. Sect. (January 1, 2013), 2013.

[15] P. W. Singer, “Stuxnet and Its Hidden Lessons on the Ethics of Cyberweapons,” Case West. Reserve J. Int. Law, vol. 47, 2015.

[16] M. Schumacher, E. Fernandez-Buglioni, D. Hybertson, F. Buschmann, and P. Sommerlad, Security Patterns: Integrating security and systems engineering. John Wiley & Sons, 2013.

[17] S. Halpern, “US Cyber Weapons : Our ‘ Demon Pinball ,’” pp. 1–6, 2016.

[18] P. Aggarwal, "Review on cyber crime and security," Int. J. Res. Eng. Appl. Sci., vol. 02, no. 01, pp. 48–51, 2014.

[19] "Dubai Hamas assassination: how it was planned." [Online]. Available: http://www.telegraph.co.uk/news/worldnews/middleeast/dubai/7251960/Dubai-Hamas-assassination-how-it-was-planned.html. [Accessed: 25-Oct-2015].

[20] "Dubai murder: fake identities, disguised faces and a clinical assassination | World news | The Guardian." [Online]. Available: http://www.theguardian.com/world/2010/feb/16/dubai-murder-fake-identities-hamas. [Accessed: 25-Oct-2015].

[21] R. N. Mehta and R. E. Whitlark, "Unpacking the Iranian Nuclear Deal: Nuclear Latency and U.S. Foreign Policy," Wash. Q., vol. 39, no. 4, pp. 45–61, Oct. 2016.

[22] J. H. Awan, S. Memon, R. A. Khan, A. Q. Noonari, Z. Hussain, and C. Technology, "Security strategies to overcome cyber measures, factors and barriers," Eng. Sci. Technol. Int. Res. J., vol. 1, no. 1, pp. 51–58, 2017.

[23] J. Awan and S. Memon, "Threats of Cyber Security and Challenges for Pakistan," in 11th International Conference on Cyber Warfare and Security: ICCWS - 2016, Boston USA, 2016, p. 425, 2016.

[24] A. Christidis, "Network/Application Vulnerability Assessment Tools." TEI Πειραιά, pp. 48–51, 01-Jul-2011.

[25] D. Jagli and A. Joy, "Rational Unified Treatment for Web application Vulnerability Assessment," in 2014 International Conference on Circuits, Systems, Communication and Information Technology Applications (CSCITA), 2014, pp. 336–340.

[26] A. Hameurlain, J. Küng, R. Wagner, T. K. Dang, and N. Thoai, Eds., Transactions on Large-Scale Data- and Knowledge-Centered Systems XVI, vol. 8960. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014.

[27] A. Razzaq, A. Hur, H. F. Ahmad, and M. Masood, "Cyber security: Threats, reasons, challenges, methodologies and state of the art solutions for industrial applications," 2013 IEEE Elev. Int. Symp. Auton. Decentralized Syst., pp. 1–6, 2013.

[28] [28] J. Garcia-Alfaro, G. Lioudakis, N. Cuppens-Boulahia, S. Foley, and W. M. Fitzgerald, Eds., Data Privacy Management and Autonomous Spontaneous Security, vol. 8247. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014.

[29] Y. Zou and G. Wang, "Intercept Behavior Analysis of Industrial Wireless Sensor Networks in the Presence of Eavesdropping Attack," Ind. Informatics, IEEE Trans., vol. PP, no. 99, p. 1, 2015.

[30] M. Alenezi, "Developer Companion : A Framework to Produce Secure Web Applications," vol. 14, no. 7, p. 2016, 2016.

About authors

Jawad Hussain Awan is a member of IFIP WG 9.10 - ICT Uses in Peace and War. He is PhD Research Fellow, in Institute of Information and Communication Technology at University of Sindh, Pakistan. His research interests are Cyber security, Information Security, e-Governance, e- Democracy, Security challenges in Information Systems and Wireless Body Area Networks. He published his research in several national and international research journals. Mr. Awan attended and presented his research in national and international conferences. He is the reviewer of various reputable HEC recognized national and international journals such as IJACSA, IJCSNS. He is also Microsoft Certified Professional in Web Programming.

Shahzad Memon is a member of IEEE. He is working as an Associate Professor, in Institute of Information and Communication Technology at University of Sindh, Pakistan. He completed his doctorate in Livens issues with fingerprint sensors technology from Brunel University, London, UK. His research interests are fingerprint Sensors, multimodal biometrics, Cyber security, Micro and Nanosensors for security applications, Simulation of Micro and Nano-systems, Security challenges in Information Systems. He published his research in several national and international research journals. Dr. Memon attended and presented his research in national and international conferences. He is also member of Institution of Engineering and Technology UK, and IAENG, USA.

Shariq Mahmood Khan received his Bachelor and Master Degrees with distinction in Computer Science from NED University of Engineering and Technology, Pakistan, in 2005 and 2007, respectively. He did Ph.D from Brunel University, London, UK in 2015. His career started in NED University from 2005 and since 2009 he is an Assistant Professor in Department of Computer Science and Software Engineering. His research focuses on various aspects of networking that include Quality of Service (QoS) of wireless networks, protocol design for Mobile Ad-Hoc network (MANET) and Vehicular Ad-Hoc Network (VANET).

Muhammad Usman received the B.Sc. degree in Computer Information Systems Engineering from the University of Engineering and Technology (UET) Peshawar, Pakistan, in 2004, and the M.Sc. degree in Computer Engineering from the Center of Advanced Studies in Engineering, Islamabad (CASE), Pakistan, in 2007. He Completed his Ph.D. from the University of Ulsan, South Korea in 2016. His is associated with the UET Peshawar (Mardan Campus) as Assistant Professor since 2007. His research interests include security and energy efficiency in wireless networks, next-generation networks, and wireless sensor networks. In 2015, he received best SCI(E) paper award from the Korean Government through BK21+ project. He is the reviewer of various reputable international journals such as IEEE Transactions on Wireless Communications, IEEE Transactions on Cognitive Communication and Networking, IEEE Sensors Journal, IEEE Systems Journal, Applied Mathematics & Information Sciences, The Computer Journal.

Rahat Ali Khan received his BS Electronics, MBA Finance and M.Phil Telecommunications from University of Sindh Jamshoro in 2005, 2012 and 2016 respectively. He is enrolled in Ph.D. in Information Technology at the Institute of Information and communication Technology University of Sindh Jamshoro, Pakistan. He is working as a Teaching Assistant at the Institute of Information and Communication Technology University of Sindh Jamshoro, Pakistan since 2007. His research interests include Wireless Sensor Networks, Wireless Body Area Sensor Networks and Underwater Acoustic Sensor Networks.

Shazia Abbasi is an Assistant Professor, in Institute of Information and Communication Technology at University of Sindh, Pakistan and currently pursuing doctor of philosophy in Information Technology. Her research interests are wireless communication; wireless networks and wireless mesh networks.

Abdul Qudoos Noonari is an MPhil Research Student, in Institute of Information and Communication Technology at University of Sindh, Pakistan. His research interests are Cyber security, Information Security.

Zahoor Hussain is PhD scholar at Institute of Information and Communication technology since January 2015. The research area of interest is, Smart Energy Management system, Telecommunication Networks, Smart Grid, Smart Environment and Renewable Energy. He is also performing his duties in ISP, IICT as a Network Staff. He has additional Charge of Warden for Postgraduate Boys Hostel, University of Sindh, and Jamshoro.