A Review on 0-day Vulnerability Testing in Web Application

Pratap Kumar
Raksha Shakti University
Ahmedabad, India
pratapkumar105@gmail.com

Ravi K Sheth
Raksha Shakti University
Ahmedabad, India
rks.it@rsu.ac.in

ABSTRACT
In recent year a lot of web applications have been released in the world. At the same time, Zero-Day attacks against web application vulnerabilities have also increased. In such a scenario, it is necessary to make web applications more secure. However checking all web vulnerabilities by manually is very difficult and time-consuming. Therefore, we need a web application vulnerability scanner which is used for detecting security vulnerabilities in web services by underlining the service from the attacker's point of view. Web Application Penetration Testing (WAPT) plays an important role in every modern organization but, if an organization web apps does not properly test and secure then adversaries can compromise your applications, steal organization data and. damage business performance. Unfortunately, many organizations are under an illusion that a web application scanner which they are using will sincerely discover loopholes in their systems. According to research and study, there are different penetration testing tools have provide different performance on vulnerabilities detection. In this paper we have analyze and take survey of the different Zero-day vulnerability, how we can help organizations in testing their web applications in order to build reliable and secure applications.

Keywords
Remote Command Execution; Zero-day; vulnerability; Pen testing; Web Application;

1. INTRODUCTION
Zero-day exploits are generally difficult to prevent because information is usually only available for analysis after the attack has been completed. The vulnerabilities which are found are highly desired by the governmental agencies, cyber criminals and software companies who pay huge amount of money to get access to that exploit, it can be as a worm, Trojans, viruses and other malware, for avoiding this attack we need proper penetration testing also known as a pen testing. In this method of testing the areas of weakness in web application systems in terms of security are put to test to determine, if any weak-point is found that can be broken and access is possible or not. [2][3]

ICTCS '16, March 04-05, 2016, Udaipur, India
© 2016 ACM. ISBN 978-1-4503-3962-9/16/03…$15.00
DOI: http://dx.doi.org/10.1145/2905055.2905357

In some cases, it is very difficult to discover all the vulnerability simultaneously. Even if every security protocol was used to at the time of launch, it is still possible for hackers in the various types of security exploits to take advantage if something is left behind in the code by a code-developer. [1]

2. ZERO DAYS PHENOMENON
Zero-day attack, it refers to the undefined security loopholes in any website, software and any other application that are present but yet to be discovered at the time of its launch. It means that the developers have zero days to address and patch the vulnerability. The attacker shares the Zero-day exploit before the developer of the target software knows about that same vulnerability. These vulnerabilities are found in any software or website [6].the pen-tester should have the proper knowledge of these vulnerabilities and fix them before the hackers use this exploit. Zero-day vulnerabilities are commonly present in CMS scripts such as Joomla, WordPress, Drupal and also plain HTML. They are also found in plenty when it comes to modern day website plugins.

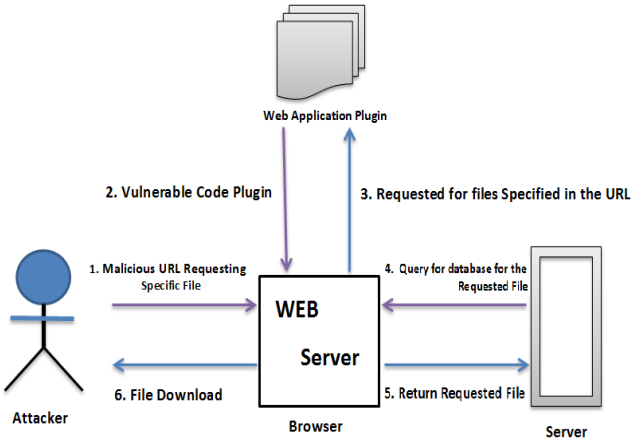


Figure 1. Working flow of Zero-day Vulnerability [12]

According to figure 1, when web Application plugin into web server at that time attacker try to send malicious code if application is vulnerable than that can be executed and attacker access to sensitive files and information of the system like database information and configuration files may cause critical damage and loss when incorporated with higher risk attacks. Even though they are just add-on modules, they almost take with full privileges, thus exploiting these components could also affect even the server running it.

3. CLASSIFICATION
By the research and study Zero-day is has broadly classified against exploits as a statistical-based, signature-based, behavior-

based, and hybrid techniques [8]. The main goal of each of these techniques are to identify the exploits in real time and try to eliminate in real time as possible and separation of the specific attack or minimize the damage induce by the attack. Other challenge of these methods face is making sure the victim's machine threshold delay for analysis and quarantine is not exceeded. This may be cause undermine of the attacked machine.

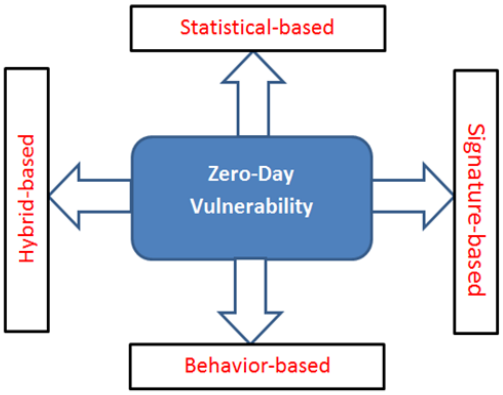


Figure 2. Classified against zero-day exploits

3.1 Statistical-based

Statistical-based techniques for the quality of the detection is directly related to threshold limits set by the vendor or security professional this technique determines the normal activity and anything is happening from outside of normal is blocked or flagged. The longer the system is utilizing this technique is online. The more accurate of the system is determining existing techniques in this approach perform static analysis or dynamic analysis on the packet payloads to detect the invariant aspect reflecting semantics of malicious and it attempts to detect the exploit prior to the execution of the actual code.

3.2 Signature-based

Signature-based detection is used by virus software vendors that can compile a library of different malware signatures. They will also cross reference of these signatures with application, local files, network files, email or web downloads depending on settings of web browser. These libraries are regularly being updated for new signatures that often represent on new exploited vulnerabilities. This technique is one step behind a zero-day exploit because it requires a signature to be in the signature library for the detection.

The first type of signature-based technique is content-based. Content-based signatures compare the content of packets with known malicious signatures. Polygraph is an example of a content signature-based technique that will produce signatures to match and detect polymorphic worms.

The second type of signature is semantic-based. Semantic signature-based techniques are computationally expensive to generate as compare to approaches that is based on substrings. Moreover, they cannot be implemented in existing Intrusion Detection system.

The third type of signature is vulnerability-based. A vulnerability-based signature has to identify the vulnerability point reachability (VPRP) , it denotes whether an input message will make the program execution reach the vulnerability point. Weakness of vulnerability based signatures is the limited library of known.

3.3 Behavior-based

Behavior-based techniques actually it's a characteristics of worms. The goal of these techniques is to predict the future behavior of a web server, victim machine in order to deny any behaviors that are not expected. In this technique relies on the ability to predict the flaw of network traffic.

3.4 Hybrid-based

Hybrid-based techniques are an advance technique which is a combination of previous techniques i.e. statistical-based, signature-based, and behavior based techniques. Hybrid-based techniques overthrow the weakness in any Suspicious Traffic Filter (STF), for detecting zero-day polymorphic worms. There are various advantages of hybrid based detection such as:

- It furnishes sensitivity and specificity to identifying zero-day attacks from the data which is collected automatically from the high interaction honeypots.
- It increases the advantages of already existing techniques and minimizing their disadvantages.
- In this technique prior knowledge of zero-day attacks is not required because it uses the Honeynet as an anomaly detector.
- In this technique zero-day attacks can easily be detect in its early phase and even, it can store the attack initializations before its real occurrence.

4. Vulnerability Assessment

According to CVE survey details [7], we analyze the different vulnerability in current scenario from 2012 to 2016, as per classified against zero-day exploit there are different vulnerability which is shown in Table 1. According to Table 2: we can see most of the attack is happen due to remote execution code (RCE) and denial of service (DOS) attack, generally zero day attack is happen due RCE vulnerability because it provides an attacker to take complete access and execute malicious code of an affected system with the privileges of the user running of the application [11]. Due to security flaws in different application vulnerability are increasing day by day these are the listed current vulnerability based on classified zero day exploits in Table 2. data breaches are increasing more and more. An attacker gains the user information and takes full control over it [1][9][10].

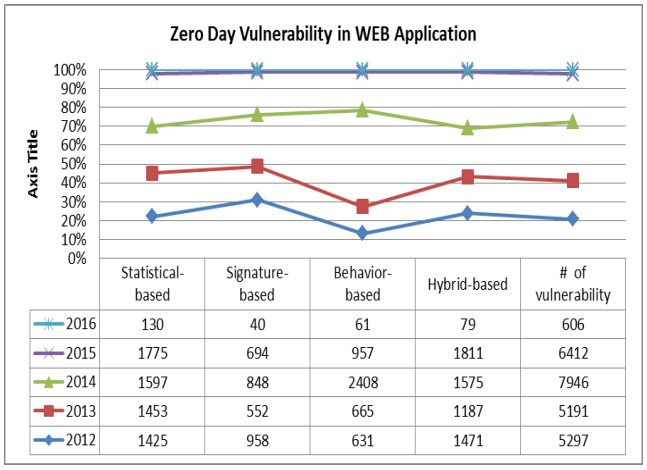
TABLE I. Classified Zero-day Attack with Vulnerability

Classified zero-day attack	Classification based on vulnerability
Statistical-based	Denial of service
Signature-based	Bypass security, exploitation
Behavior-based	Gain information, Sql injection
Hybrid-based	Remote code execution, File inclusion

TABLE II. Current Vulnerability Report of Web Application [7]

Vulnerability in Web Application	2012	2013	2014	2015	2016
Statistical-based	1425	1453	1597	1775	130
Signature-based	958	552	848	694	40

Behavior-based	631	665	2408	957	61
Hybrid-based	1471	1187	1575	1811	79
# of vulnerability	5297	5191	7946	6412	606



	Statistical-based	Signature-based	Behavior-based	Hybrid-based	# of vulnerability
2016	130	40	61	79	606
2015	1775	694	957	1811	6412
2014	1597	848	2408	1575	7946
2013	1453	552	665	1187	5191
2012	1425	958	631	1471	5297

Figure 3. Chart based on classified Zero-day vulnerability [7]

5. RELATED WORK

After literature survey on zero-day attacks which is publicly available information on vulnerabilities disclosed between 2012 to 2016.Following conclusion comes at last that, 35% of vulnerabilities are open for and 43% of vulnerabilities are patched. After disclosure of vulnerabilities around 94% exploits are generated within a month. The exploits covered in public achieves are proofs-of-concept. Real world attacks are [7][9][10] are not generally used by this type of concept. Lifespan of Zero-day vulnerabilities are analyzed by McQueen et al [13]. So, that we can able to calculate the real number of zero-day vulnerabilities endured in before. Here, we investigate the collected data on real hosts targeted by cyber-attacks. Before publishing the vulnerabilities, the analysis of attacks are defined for understanding the prevalence and lifespan of zero day. Here, we concentrate on real time analysis compare to statistic information because this type of zero day vulnerabilities do not understand as a thoroughly. Exploitation of such vulnerabilities is a portable activity.

6. CASE STUDIES

If vulnerability is discovered by the adversary first, and by exploiting that vulnerability to perform malicious activities, then the moment of these malicious activities are discovered, it is known as a zero-day attack.

6.1 Zero-day attack

Vulnerability found in large number of WordPress websites that it could be compromised due to exploitable loophole within popular plug-in In April 2015. If that vulnerability of plug in abused then malicious code can be run in the comments field of the site [16]. When the zero-day vulnerability exploited and code injection done into comment after that viewed as a site administrator and it could change passwords, create new users or anything else that would normally require for admin rights. The flaw is a rare stealthy in that it modify the core part of the CMS script rather than some badly-coded third-party plugin. If logged-in administrator activates then it run in default settings so adversary can take advantage of vulnerability to execute arbitrary malicious code on the web server by plugin and theme editors.

Adobe Flash Player attacked by a zero-day where hackers exploited unpatched vulnerability in Flash Player In February 2015 which was undetected till two months. In that users redirected to advert linked to malicious sites. Trend micro stats about popular website dailymotion.com of sharing video which became victim of malvertisement attack that exploited through the vulnerability elaborated in previous case. It was observed that Dailymotion website was not only the victim but also that infection was spread from the advertising platform not from web data itself [15].

6.2 Ways to avoid Zero-day Attacks

6.2.1 Host Intrusion Protection Software (HIPS)

HIPS do not depend upon signatures created by hash of file to detect or remove viruses. Counterpart HIPS detect infection by monitoring activity on the machine, and it incorporate rules-based identification to prevent adversary from making unwanted action [14].

6.2.2 Use good antivirus

Authenticated AV zero-day attacks are due to Signature identifiable attacks that were unaware of just one day earlier. So when antivirus software choice occur, it must protect from both known and unknown attacks [14][17].

6.2.3 Update Application

Updating of software periodically can prevent Zero-day attacks. If software notification occurs then update it accordingly. If the update elaborates that it is necessary to include a patch to a recently identified vulnerability. By updating your software, you create safe environment against possible future attack through that vulnerability [14].

6.2.4 Use only updated browsers

All browsers push out automatic periodic updates of timely basis. It adds patches to recently identified exploitable vulnerabilities which occur in the background processes [17].

7. COUNTERMEASURE

The best idea to avoid against zero day exploits is to pursue best security practices, keeping updated time to time with the current hotfixes and patches are very important. Importantly it should be a dedicated teams to antithetical such attacks. Another plan of this action should be in place so that the organizational work does not stall due to any incident of zero-day attacks and employees should be educated of any potential threats in web application. Another security measures are: Block E-mail file attachment, Employ hardware as well software firewall and enable heuristic scanning used to bock virus or worm which is not identified by antivirus [14].

8. COMPARISON TABLE

Table III. Comparison table classified against zero-day exploit

Classified zero-day attack	Classification based on vulnerability	Problem	Solution
Statistical-based	Denial of service	Inaccessible data	State full Firewall
Signature-based	Bypass security, exploitation	Unauthorized user, Outdated Application	Access control, Update patches & application
Behavior-based	Gain information, Sql	It works to gathering precise	All SQL queries can insure that

	injection	information about the type of database	each query is properly desolate before execution.
Hybrid-based	Remote code execution, File inclusion	manipulates input to cause execution of unintended commands	Strictly controlled and limited to a predefined set of values.

According to Table 3. As per classified against zero-day attack there are different vulnerabilities that we mentioned in comparison table with problems and solution. The most common root cause of a vulnerabilities are due to poor patching, 63% of vulnerabilities discovered in 2015 could have been avoided due to robust patching, component security policy and procedure was implemented Over 7.1% of patch related vulnerabilities were Critical or High.

9. CONCLUSION AND FUTURE WORK

We can conclude that Zero-day attacks are tough to find out because they can exploit unknown vulnerabilities due to no anti-virus, no patches and intrusion-detection signatures. In this paper we have mentioned different techniques that how we can try to avoid such vulnerability. Updates are needed because they can disclosed the patch of unknown necessary vulnerabilities, which is not be detected at the time of deployment. New vulnerabilities are consistently being identified as new technologies and handling updates that are used to improve the overall quality process, which is really means that security fixes, need to be perceptive of past vulnerabilities because while catching those steps it will ensure maximum security in the future. In the future we also need strong framework for pen tester that can be used to avoid Zero-day vulnerability and Remote Code Execution that can help us to minimize the increasing such types of vulnerability.

10. ACKNOWLEDGMENT

With enormous pleasure, I would like to present this paper on the part of my dissertation work related to “Identifying Zero- day Vulnerabilities in Web Applications” My sincere thanks and gratitude to Mr. Bhadreshsinh Gohil Asst. Professor of Gujarat Technological University for their continual kind words of encouragement and motivation.

11. REFERENCES

[1] Vibhandik,R. and Arijit Kumar Bose. 2015. Vulnerability Assessment of Web Applications – A Testing Approach. Forth International Conference on e-Technologies and Networks for Development(Bangalore, India, 21-23 Sept. 2015),IEEE , 1-6. DOI= 10.1109/ICeND.2015.7328531.

[2] Vieira Marco., Antunes Nuno., and Madeira Henrique. 2009. Using web security scanners to detect vulnerabilities in web services.International Conference on Dependable Systems & Networks(Lisbon, Portugal, June 29-July 2, 2009). DSN '09.IEEE, 566-571. DOI= 10.1109/DSN.2009.5270294.

[3] Makino, Yuma., and Klyuev, Vitaly. 2015. Evaluation of Web Vulnerability Scanners. 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (Warsaw, Poland, September24 - 26, 2015).IEEE, 399-402. DOI= 10.1109/IDAACS.2015.7340766.

[4] R.Selvam., and A.Senthilkumar. 2014. Webservice Based Vulnerability Testing Framework. International Conference on Green Computing Communication and Electrical Engineering(Coimbatore, India, March6-8, 2014).IEEE,1-6 DOI= 10.1109/ICGCCEE.2014.6921391.

[5] World's Biggest Data Breaches, February 2016. http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/.

[6] Leyla Bilge., and Tudor Dumitras. 2012. Before We Knew It: An Empirical Study of Zero-Day Attacks In The Real World.https://users.ece.cmu.edu/~tdumitra/public_documents/bilge12_zero_day.pdf

[7] Current Statistics of different Vulnerabilities Report, January 2016. http://www.cvedetails.com

[8] David Hammarberg. The Best Defenses Against Zero-day Exploits for Various-sized Organizations. September 2014. https://www.sans.org/readingroom/whitepapers/bestprac/defenses-zero-day-exploits-various-sized-organizations-35562

[9] Vulnerability Statistics Report. March 2015. https://www.edgescan.com/assets/docs/reports/2015-edgescan-Stats-Report-%282015%29-v5.pdf

[10] WhiteHat’s Website Security Statistics Report. May 2015. https://info.whitehatsec.com/rs/whitehatsecurity/images/2015-Stats-Report.pdf

[11] Nuno Antunes., Marco Vieira. 2014. Assessing and Comparing Vulnerability Detection Tools for Web Services: Benchmarking Approach and Examples. IEEE Transactions On Services Computing(Coimbra, Portugal, March 11,2014). IEEE, 269 - 283. DOI= 10.1109/TSC.2014.2310221.

[12] Leyla Bilge., and Tudor Dumitras. 2012. An Empirical Study of Zero-Day Attacks in the Real World. ACM conference on Computer and communications security. CCS '12. ACM, New York, NY, 833-844. DOI= 10.1145/2382196.2382284.

[13] Miles A. McQueen., Trevor A. McQueen., Wayne F. Boyer., and May R. Chaffin. 2009. Empirical Estimates and Observations of 0Day Vulnerabilities. Hawaii International Conference on System Sciences (Big Island, HI, January 5-8 2009).HICSS '09.IEEE, 1 - 12. DOI= 10.1109/HICSS.2009.186

[14] ZERO-DAY DANGER: A Survey of Zero-Day Attacks and What They Say About the Traditional Security Model. June 2015. https://www2.fireeye.com/WP-Zero-Day-Danger-LP.html

[15] Trend Micro Discovers New Adobe Flash Zero-Day Exploit. February 2015. http://trendmicro.com/trendlabs-security-intelligence/trend-micro-discovers-new-adobe-flash-zero-day-exploit-used-in-malvertisements

[16] Millions of WordPress sites open to attack. April 2015. http://www.scmagazineuk.com/millions-of-wordpress-sites-open-to-attack/article/411725/

[17] History and the way of Avoiding Zero-Day Attacks. May 2015. http://www.zonealarm.com/blog/2015/05/what-the-heck-are-zero-day-attacks-and-3-ways-to-avoid-them/