Web Attack Runtime Detection (WAR)

Mr. Pratik Kadam, Prof. Neelkamal More

Abstract— **The internet has provided several services yet it is vulnerable to several attacks. These services include web banking, Social networking and online shopping. With this advancement, the attacks over the web applications have also increased. According to Cenzic vulnerability report 2014[1] 96% of all tested applications have one or more security vulnerabilities from last year's count of 99%.According to Imperva Web Application Attack Report[2] the frequency of web attacks are different on Retail Sector and others. The main cause for this is the lack of security awareness, security being neglected at design phase and lack of secure coding. Mostly all developers write their code application oriented they overlook other constraints due to workload and deadlines. These small security bugs can lead to great intellectual or financial loss for any industry. In this paper we have proposed a WAR (Web Attack Runtime) Detection mechanism which will monitor all major web attacks at runtime. The main focus will be on the major attacks harming Retail Sector. The proposed model is implemented in PHP web application and its future potential is we can add more new attacks with less complexity.**

Index Terms— **Web attack, owasp,security.**

I. INTRODUCTION

The Internet technology is growing rapidly day by day due to which almost all organisations are establishing their business on Web. Web Applications provide important and easy medium of interface for using web services over Internet. It is observed that security is overlooked by many organisations which lead to major loss of organisation. The reason behind lack of security is lack of awareness about security in small scale organisations, developers major concern is working of product, no security expertise in organisations and stress to complete task within deadlines.

The Open Web Application Security Project (OWASP) is a 501(c) (3) worldwide not-for-profit charitable organization focused on improving the security of software. OWASP [3] mission is to make software security visible, so that individuals and organizations worldwide can make informed decisions about true software security risks. According to OWASP top most deadly web attacks are:

- A1- Injection
- A2- Broken Authentication and Session Management
- A3- Cross-Site Scripting
- A4- Insecure Direct Object Reference
- A5- Security Misconfigurations
- A6- Sensitive Data Exposure
- A7- Missing Function Level Access Control
- A8- Cross-Site Request Forgery
- A9- Using Components with known Vulnerabilities
- A10- Unvalidated Redirects and Forwards

Information Leakage (23%), Authentication and Authorization (15%), Session Management (13%), SQL Injection (7%), Cross Site Request Forgery (CSRF) (6%), and other (11%) round out the list of the total vulnerabilities found..

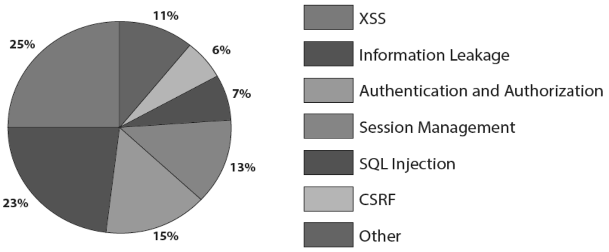


Fig. No.1 Cenzic vulnerability report attack percentage

It has been observed that different attacks have different impact on different sectors. According to Imperva Web Application Attack Report, when compared to other industries, retail applications suffered twice as many SQL injection attacks, but fewer Remote File Inclusion (RFI) attacks.

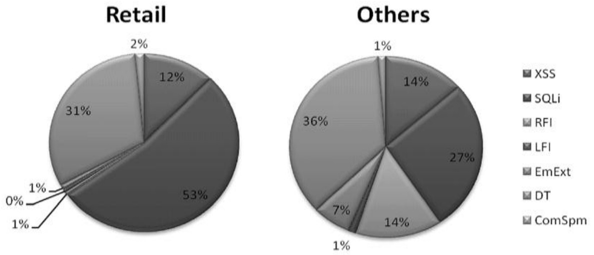


Fig. No.2 Attack type Retail Web Applications Vs Other Web Applications

So our major concern is Retail Web Applications as security awareness in retail sector is very less and also loss suffered by retail sector is huge compared to others. There are various tools and techniques like Firewall, IDS, IPS and proxy servers but major problem is they concentrate more on network security. Application security is not given as importance as network security, though attacks on application are so easy. Due to this reason application level attacks are increasing drastically.

II. RELATED WORK

This section describes some of the techniques and proposals develop to detect and prevent web application attacks.

In [4] Simple Web Application Response Tool (SWART) a mechanism is proposed for detecting and preventing web application attack. Its main focus is on Input Validation attacks. The attack patterns and filtering is used to monitor

Mr. Pratik Kadam, Currently Pursuing Master in IT with specialization in Information Security.

Prof. Neelkamal More, Currently working in KJSCE Mumbai. Completed ME in Computers .

attacks. It also founds attack severity to understand the impact of attack. The limitations of SWART are it is only implemented in ASP.NET and also it is not completely implemented yet

In [5] a Web Application Intrusion Detection Framework (WAIDS) is proposed. Profile matching approach to request data for web is used by WAIDS. Keyword extraction and common points measurement process is used for detecting malicious activity. The limitation to this approach is it requires very good knowledge about security to use it and also it is very complex to implement WAIDS.

Static Analysis Framework (SAFELI) is proposed for identifying vulnerabilities in SQLi. SAFELI [6] works at byte code of application using symbolic execution in ASP.NET. Library is maintained where preset attack patterns are stored for pattern matching of attacks. The limitation of SAFELI is it works on for web applications developed in ASP.NET .

In [7] Analysis and Monitoring for Neutralization SQL-Injection Attacks (AMNESIA) proposes a new technique for detecting and preventing SQL Injection attacks. AMNESIA works by combining static analysis and runtime monitoring. It statically builds SQL-Query model and checks at runtime. Queries that violate the model represent potential SQL attacks. The limitations to this approach it we have to have good knowledge to build sql-query model and we have to update this tool with every minor change in application.

So as such there are many proposed approaches to detect and prevent web applications. The major limitations that I found in all approaches are that there is no mechanism to catch attacker. Also all approaches focuses on mainly one attack but now need it to propose approach that will help in monitoring all major attacks.

III. Proposed Work

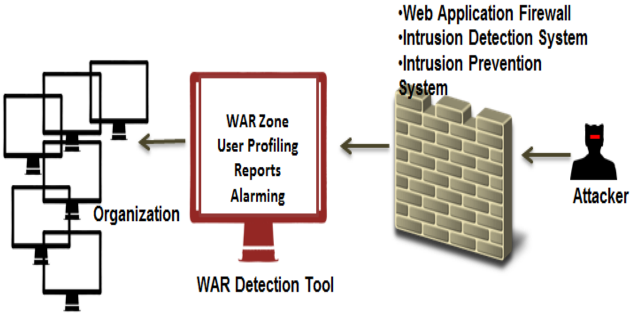
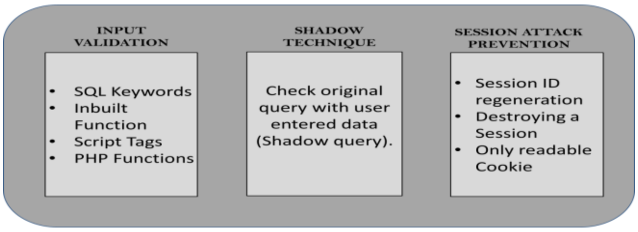

•Web Application Firewall
•Intrusion Detection System
•Intrusion Prevention System
WAR Zone
User Profiling
Reports
Alarming
Organization
WAR Detection Tool
Attacker

Fig No.3 Working Of WAR detection

Our proposed WAR Detection is a tool for monitoring all major web application attacks. WAR Detection is used for detecting and preventing major web attacks like SQL Injection and Cross-Site Scripting. WAR Detection consists of four modules. We are assuming it to be php web application with all necessary connectivity's.

WAR ZONE: WAR zone has 3 components which are as follows:

- Input Validation
- Shadow Technique
- Session Attack Preventio



INPUT VALIDATION

- SQL Keywords
- Inbuilt Function
- Script Tags
- PHP Functions

SHADOW TECHNIQUE

Check original query with user entered data (Shadow query).

SESSION ATTACK PREVENTION

- Session ID regeneration
- Destroying a Session
- Only readable Cookie

Fig No.4 Components of WAR Zone

1. *Input Validation*: In this all data entered by user is filtered. The fields that are validated are :

- PHP Keywords
- PHP Inbuilt Functions
- Scripting Tags

2. *Shadow Technique*: This is very unique technique in which the actual query (Original Query) is compared with the shadow query. If there is slight difference between two query it means there is some possibility of attack.

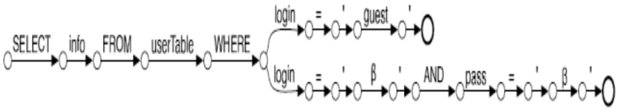
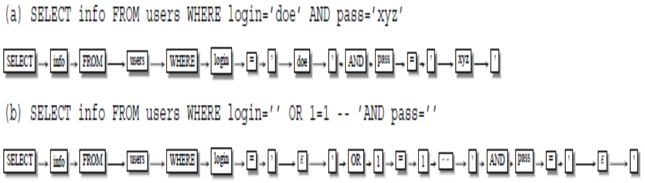


Fig No. 5 SQL Query Model for Servlet



```
(a) SELECT info FROM users WHERE login='doe' AND pass='xyz'
(b) SELECT info FROM users WHERE login='' OR 1=1 -- 'AND pass=''
```

Fig No. 6 Parsed Runtime Queries

3. *Session Attack Detection*: There are two types of session attacks.

First is **Session Fixation** attack, where attacker already has access to a valid session and tries to force the victim to use this particular session.

Second is **Session Hijacking** attack, where attacker tries to get the ID of a victim's session to use his/her session. In both attacks the session ID is the sensitive data. So session ID needs to be protected for both a read access (Session Hijacking) and a write access (Session Fixation). Simple approach is used to deal with Session attacks with every login or access of website a new session is generated and old session is destroyed. If multiple logins of common account is found the account is blocked till user verification. Also care should be taken that cookies are given read only access so that no one can manipulate the cookie for their benefits or illegal activity.

B. *User Profiling*

This is most striking feature WAR Detection. With the help of php user agent and curl, we can store all possible data of the user accessing our website. The possible data that we can collect for any user are IP, Hostname, Country, Country Code, Continent, State, Latitude, Longitude, ISP, OS and Browser. This data is helpful in tracing down attackers' machine and blacklisting them. WAR Zone provides the type of attack and its severity which is added to user profile.

C. *Reporting*

This module creates reports of all attacks monitored by WAR Zone. It helps company to understand what kind of attacks can be tried more by attackers on company website. Reports can be generated about users trying to attack website. Reports will simplify in understanding most used attack, area from where attacks are done most and other collected data from user profiling.

D. *Alarming*

This is small module which sends alarm to monitoring engineer about attack. If frequency of attacks increases or if any new attack is detected alarms are sent to all security team to alert them about it.

IV. CONCLUSION

The threats of web attacks are increasing drastically day by day. As it is said that in future Cyber war is going to be more dangerous than world wars. Also the rate of web applications attacks are increasing rapidly day by day. The proposed WAR Detection proves to be very helpful in detection of major attacks like SQL-Injection, Cross-Site Scripting and Session Attacks. WAR Detection is very simple to use and can easily cope up with new attacks. WAR Detection can be more helpful once it covers all OWASP Top-10 web application attacks.

V. FUTURE WORK

In future we will try to add all OWASP Top-10 web application attacks in WAR Detection so that it will be complete web security tool. Currently the application is PHP based but we will try to integrate WAR Detection with other website development languages.

ACKNOWLEDGMENT

We would like to thank the constant support of our subordinates and friends. We would thank all the contributors.

REFERENCES

[1] Cenzic vulnerability report 2014 http://info.cenzic.com/rs/cenzic/images/Cenzic-Application-Vulnerability-Trends-Report-2014.pdf

[2] Imperva Web Application Report 2012 http://www.imperva.com

[3]https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

[4] 1Kanika Sharma, 2Naresh Kumar 1, 2 Department of Computer Science & Engineering, 1, 2 University Institute of Engineering & Technology, Kurukshetra University 1,2Kurukshetra, Haryana 1Kanikasharma1312@gmail.com

[5] YongJoon Park , JaeChul Park , "Web Application Intrusion Detection System For Input Validation Attack" , IEEE Third International Conference On Convergence And Hybrid Information Technology ,2008, PP 498-504

[6] Xiang Fu ,Xin Lu , "A Static Analysis Framework For Detecting SQL Injection Vulnerabilities" IEEE 31ST Annual International Computer Software And Application Conference , 2007 .PP-87-96.

[7] Xiang Fu ,Xin Lu , "A Static Analysis Framework For Detecting SQL Injection Vulnerabilities" IEEE 31ST Annual International Computer Software And Application Conference , 2007 .PP-87-96.

[8] William G.J. Halfond and Alessandro Orso College of Computing *Georgia Institute of Technology {whalfond|orso}@cc.gatech.edu* "AMNESIA: Analysis and Monitoring for SQL Injection Attacks".

Authors:

Mr. Pratik Kadam, Currently Pursuing Master in IT with specialization in Information Security

Achievements:

-"Certified Information Security Expert (CISE)" By Innobuz Solutions

- Gate 2013 Qualified with AIR(All India Ranking) 6406 and 1st in College

- CMAT Qualified AIR 9403 and 1st in College

Prof. Neelkamal More, Currently working in KJSCE Mumbai. Completed ME in Computers

Achievements:

-IBM Rational Application Developer certified programmer

- Recipient of Gold Medal of University of Dr. Babasaheb Ambedkar Technological University, 1998

Publications:

Book: Database Management System, Techmax Publication, Pune, India

Paper:

-Nilkamal More,"Recommendation of book using Improved Apriori algorithm "International Journal for Innovative Research in Science & Technology,Volume 1 issue 4,Sept 2014.

- Nilkamal More and Suchitra Patil,"Recommending an insurance policy using Association rule Mining "International Journal for Innovative Research in Science & Technology,Volume 1 issue 4,Sept 2014.

Conference Papers:

-Nilkamal Surve, "Iris Recognition using Haar transform and Weighted Euclidean Distance," International Conference on emerging trends and technologies in computer and information technology at Chandigarh, Jan, 2011.

Nilkamal Surve and Arun Kulkarni , "Iris Recognition using discrete sine transform and neural network," International Conference and Workshop on Emerging technologies, TCET, Mumbai, Mar. 18-19, 2010. 3) Nilkamal Surve and Arun Kulkarni , "Iris Recognition using discrete cosine transform and neural network," National Conference on emerging trends and technologies in computer and information technology at KJSCE, Mumbai, Feb, 2009.