Detection and Avoidance of Web Vulnerability using XSS

Nischitha G. K, Sahana S, Santhosh Kumar B. J.

Abstract— ***In today's life style web applications have become so much essential part. We make use of web applications in most of our day-to-day activities. Hence it has become a big challenge to protect these web applications from hacking. Databases are central to modern websites as they provide storage medium for critical information. It may be of any companies' sensitive information. Henceforth these websites are targeted by malicious users to gain authority. This paper provides necessary security to the websites, blogs from being attacked and miss leaded. It detects the attack and soon after well avoid by script posting. The application also demonstrate login through SQL injection[16][17] without having the proper required credentials.***

Keywords:-XSS-Cross site scripting, Detection, Prevention, Web vulnerability.

I. INTRODUCTION

As we use web applications practically in each phase of our lives which many include education, banking, health care, entertainment, news etc, Web applications[16]are of such a kind which has become so easy for any common individual to access with high internet speed communication connection though it was thought impossible few years ago. So to protect some credentials against hacking we have taken up this project. Basically an attacker will never try to target a user directly. Instead an attacker tries to exploit the website or an application by knowing its vulnerability. So, the first step of an attacker chooses is to checkup for the applications vulnerability which provides him a clear path to inject malicious scripts to the users browser. Companies mainly have their own websites[17] to make communication between clients and company a easy things and also lower business processing lost, speed up outcomes. So, to providing the data stands at the center here.Hence web applications should include high security level to the users with reliable mechanism[18].

(1) Literature Survey

In this paper XuePing-Chen have introduced the concept of SQL injection attack and principle, and realization process of attack. The author has given explanation about how the SQL injection can happen in different areas. SQL injection attack method, principle and attack implementation process is discussed and summarized. The total process of implementation about SQL injection attacks. Dr. G. Rama KoteswaraRao, K.V.J.S. Sree Ram, M. Akhil Kumar, R. Supritha, S. Ashfaq Reza, have tried to restrict the XSS attack with the help of code filtering algorithm. Basically this kind of attack happen when the attacker tries to inject the malicious code to the database directly. So that when there comes the use of database the injected malicious code will get executed instead of the work to be done. Henceforth this algorithm works fine because it allows no script to store in the database and thus no script can be made executed. In this Paper Ashish Kumar, Sumitra Binu these authors have discussed various techniques for identification and prevention using the concept of tokenization for SQL injection attack . The tokenization concept is of detecting and preventing SQL injected code. As it helps the attacker to steal the sensitive data stored. The concept of tokenization gives a function which would verify the user's query in search of pre-defined tokens and which directly prevents the access to web pages in few cases where the user query includes any of the defined tokens. In the paper Daljit Kaur , Dr. Parminder Kaur, discussed about attacks like injection vulnerabilities such as SQL injection, Cross Site Script, Cross Sitescript Request Forgery(CSRF) and classification of types of XSS. They have focused on countermeasures of XSS vulnerability and classified countermeasures with respect to SDLC and known countermeasures and mitigation techniques they have made use of vulnerability scanner to test their effectiveness in each classified SDLC phases. For scanning they concentrated on Denial of Service with XSS In the paper Kunal Gupta 1,RajniRanjan Singh , Manish Dixit have concentrated on detect XSS attack using Intrusion Detection System. For testing effective usefulness they have a work proof concept of prototype by which using SNORT IDS have been implemented . They explained classification of IDS based on architecture and detection method. They have used Cisco tool SNORT IDS so they can create rule according to the need. They introduced Snort rule and created an alert entry and setup experiment with results. Ankit Shrivastava, Santosh Choudhary, Ashish Kumar have concentrated on attack like injection attack, detection and prevention of different categories of XSS. They have briefly explained how different there 3 are categorized where in Dom and reflected based XSS need users to first visit their page henceforth attackers hacks information. But in persistent attack.

Revised Manuscript Received on 30 July 2019.
***** Correspondence Author

Nischitha G K*: Department of Computer Science, Amrita School of Arts and Sciences, Amrita Vishwa Vidyapeetham, Mysuru, India
Sahana S: Department of Computer Science, Amrita School of Arts and Sciences, Amrita Vishwa Vidyapeetham, Mysuru, India
Santhosh Kumar B J: Department of Computer Science, Amrita School of Arts and Sciences, Amrita Vishwa Vidyapeetham, Mysuru, India

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC-BY-NC-ND license http://creativecommons.org/licenses/by-nc-nd/4.0/

The code is injected to database and it is stored there ex-They have made use of black box and white box technology. To detect-Burp suite tool. Client side-signature mechanism. Assigned a unique taken for client-server request. Escape methods-prevent script.

CSS- running approaches in web applications year-2017.Abdalla Wasef Marashdin and ZarulFitr Zaaba. Through this paper we came across strip tags for prevention of attack which they said a bit difficult task and even they told about HTML entities. or UTF8 decode. Which till now none has used. They have also mentioned some of the mechanisms of HTML purifiers PHP commands. OSWASP-ESAPI security mechanism. They have just discussed the possibilities and no implementation part is include.

In this paper, Divya.M , Monisha.S, Reena .R , Kapilavani.R.K. have analysed the query attacks and web intrusions in the web database and find the prevention measures. The faults in the web are identified and validated using various techniques and algorithms. Hackers cannot by-pass login authentication since there exist double encryption.

II. METHODOLOGY

Case 1: SQL injection

Usually the attacker can get to know the admin's username of the admin page login. Hence when we inject the code in password section without having the correct password we login to Admin page where the attacker gains all admin access.

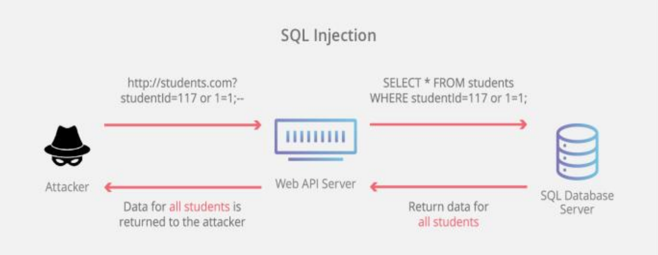
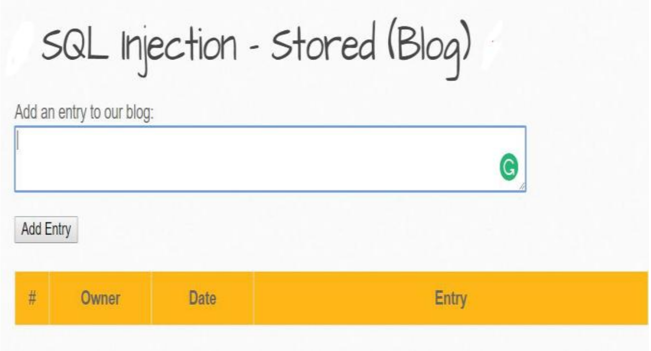


Fig 1: SQL injection

Case 2: How blog attack happens and avoidance that takes place in description section To damage a blog attacker can even pass scripts in description section and we try to avoid it by using strip tags which will not allow any scripts to be posted which may cause damage to the blog through attack.



SQL Injection - Stored (Blog)

Add an entry to our blog:

Add Entry

#	Owner	Date	Entry

Fig 2:Blog attack

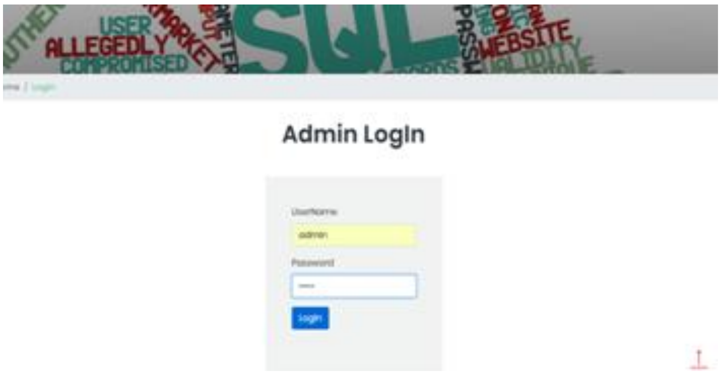
Case 3: blog attack and avoidance in comment section

Blog can be attacked even in the comment section which even a user with minimal knowledge can do so we are avoiding it by making use of ‘strip tags'.

Experimental results

Case 1:

Successfully injected the Sql code in password section and logged in to admin page.
Code- abcOR’1=1’



Admin Login

UserName

admin

Password

Login

Fig 3: Admin page

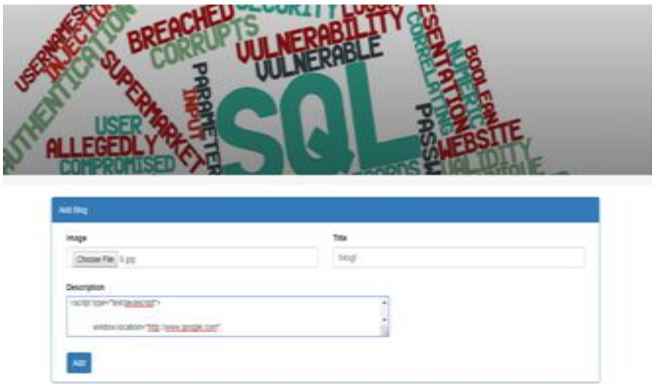
Case 2:

We show how the attack happens in description section by adding scripts . Attacker tries to redirect the page into some other page which may cause bad impression to the user. Hence we avoid it by making use of strip tag which skips the scripts added in the description section.

A] Attack

Attack code:

$description = $_POST['description'];



Add Blog

Image

Choose File 1.jpg

Title

blog

Description

```
<script type="text/javascript">
        window.location="http://www.google.com"
```

Add

Fig 4:description section attack

Redirected as per the script post.

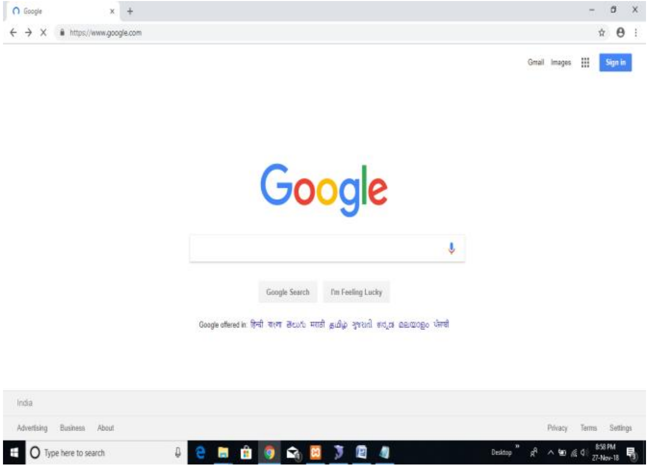
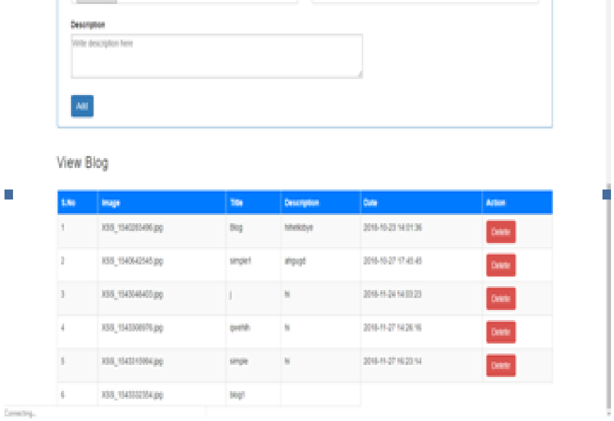

Google
https://www.google.com
Gmail Images Sign in
Google Search I'm Feeling Lucky
Google offered in: हिन्दी বাংলা తెలుగు मराठी தமிழ் ગુજરાતી ಕನ್ನಡ മലയാളം ਪੰਜਾਬੀ
India
Advertising Business About
Privacy Terms Settings
Type here to search

Fig 4.1: attack occured

B] preventing the attack in description section.
Preventing code
$description = strip_tags($_POST['description']);



View Blog

S.No	Image	Title	Description	Date	Action
1	XSS_1540283496.jpg	Blog	hthelkbye	2018-10-23 14:01:36	Delete
2	XSS_1540642545.jpg	simple1	ahgugd	2018-10-27 17:45:45	Delete
3	XSS_1543046403.jpg	j	hi	2018-11-24 14:03:23	Delete
4	XSS_1543308976.jpg	qwehh	hi	2018-11-27 14:26:16	Delete
5	XSS_1543315994.jpg	simple	hi	2018-11-27 16:23:14	Delete
6	XSS_1543332354.jpg	blog1			

Connecting...

Fig 4.2: description section attack prevention

Case 3:

We show how the attack happens in comment section by adding scripts .When the attacker adds the script in comment section when the user tries to access that blog it will re-direct to some other page(may be vulgar pages). Hence we avoid it by making use of strip tag which skips the scripts added in the comment section and safeguards the blog by not being attacked.

A]Attack
Attack code:
$Subject = $_POST['Subject'];

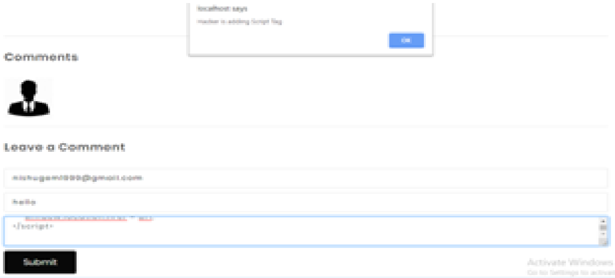


Fig 5: comment section attack

Redirected as per the script post.

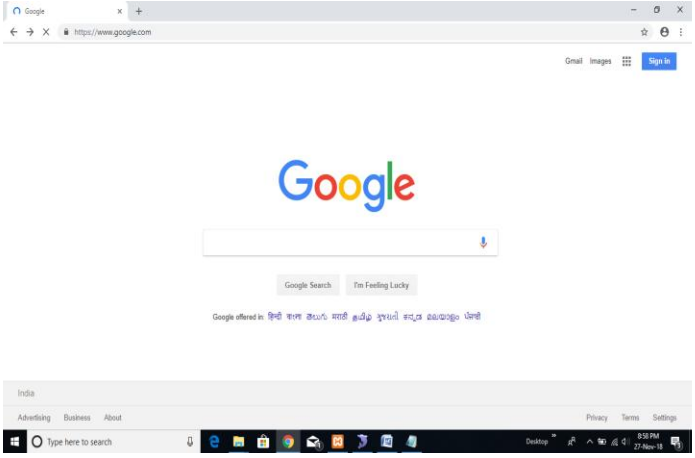

Google
https://www.google.com
Gmail Images Sign in
Google Search I'm Feeling Lucky
Google offered in: हिन्दी বাংলা తెలుగు मराठी தமிழ் ગુજરાતી ಕನ್ನಡ മലയാളം ਪੰਜਾਬੀ
India
Advertising Business About
Privacy Terms Settings
Type here to search

Fig 5.1: attack occured

B] preventing the attack in comment section.
Preventing code
$Message = strip_tags($_POST['Message']);

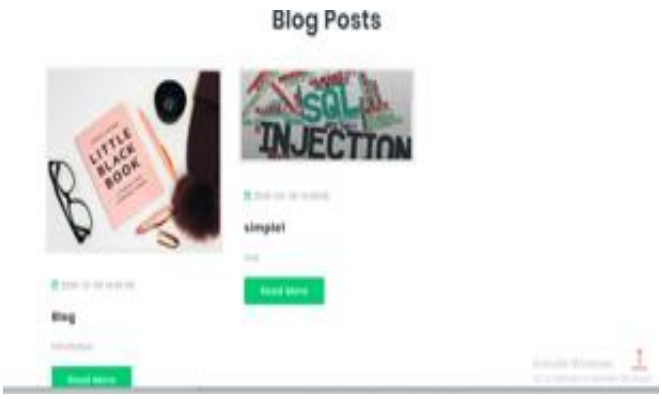


Fig 5.2: comment section attack prevention

III. FIGURES DESCRIPTION

Fig 1:SQL injection.

The above fig1 shows that the admin login page where normally admin enters his username and password that is, admin and admin respectively then it will be redirected to admin home page.Here by knowing username and when the Sql injection code is used in password section the system redirects to the admin home page

The SQL injection code that has been used is **abcOR1=1**

Fig4:description section attack

The above fig2 is understood as the attacker tries to add scripts in description section in order to cause damage to the blog which depicts attack

$description = $_POST['description'];

Fig 4.2: description section attack prevention

The fig2.1 shows that the attack which is tried by the attacker through inputting some scripts here in this figure a pop-up box is shown to the user parallel attack is avoided

$description = strip_tags($_POST['description']);

Fig 5:comment section attack

In this fig3 we can understand by using that attacker tries to attack a particular blog by adding malicious scripts in comment section

$Message = $_POST['Message'];

Fig 5.2:comment section attack prevntion

In the fig3.1 it represents a pop-up box in accordance with the attack that is taking place and parallely the attack will be avoided.

$Message = strip_tags($_POST['Message']);

IV. Conclusion

In the proposed work , prevention of cross site scripting and SQL injection prevention on web applications is proposed. Various vulnerabilities have been successfully detected using an algorithm. It is found Cross Site Scripting is to be the most common kind of security problem faced by web applications. It is possible that the cookies can be stealed and users account will be gained access and transfer of private data can also happen. Many studies were being conducted in order to check with the problems related to XSS vulnerability but we found those results were not efficient enough.

REFERENCES

1. TejinderSingh ,"Detecting and Prevention Cross –Site Scripting Techniques ",IOSR Journal of Engineering Apr. 2012, Vol. 2(4) pp: 854-857.
2. Michelle E Ruse , SamikBasu "Detecting Cross-Site Scripting Vulnerability using Concolic Testing", 2013 10th International Conference on Information Technology: New Generations, 978-0-7695-4967-5/13 $26.00 © 2013 IEEE DOI 10.1109/ITNG.2013.97.
3. MohitDayal, Nanhay Singh, Ram Shringar Raw," A Comprehensive Inspection Of Cross Site Scripting Attack", International Conference on Computing, Communication and Automation (ICCCA2016). ISBN: 978-1-5090-1666-2/16/$31.00 ©2016 IEEE.
4. AnkitShrivastava, SantoshChoudhary, Ashish Kumar," XSS Vulnerability Assessment and Prevention in Web Application", 2016 2nd International Conference on Next Generation Computing Technologies (NGCT-2016) Dehradun, India 14-16 October 2016, 978-1-5090-3257-0/16/$31.00 ©2016 IEEE.
5. AbdallaWasefMarashdih, ZarulFitriZaaba," Detection and Removing Cross Site Scripting Vulnerability in PHP Web Application", 2017 International Conference on Promising Electronic Technologies, 978-1-5386-2269-8/17 $31.00 © 2017 IEEE DOI 10.1109/ICPET.2017.11
6. Neha Gupta, " A Study of Existing Cross Site Scripting Detection and Prevention Techniques in Web Applications", International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 3 Issue 9, September 2014 Page No. 8445-8450 .
7. AbdallaWasefMarashdidh and ZarulFitriZaaba," Cross Site Scripting: Removing Approaches in Web Application",Peer-review under responsibility of the scientific committee of the 4th Information Systems International Conference 2017 10.116/j.procs.2017.12.201.
8. Joaquin Garcia-Alfaro and Guillermo Navarro-Arribas," A Survey on Detection Techniques to Prevent Cross-Site Scripting Attacks on Current Web Applications", m the Spanish Ministry of Science and Education, under the projects CONSOLIDER CSD2007-00004 "ARES" and TSI2006-03481.
9. Bakare k Ayeni,Junaidu B Sahalu,Kolawole R Adeyanju,"Detecting cross Site Scripting in web application using Fuzzy Inference System", Journal of Computer Networks and Communications Vol-2018,Article ID 8159548,10PAGES.
10. XuePing-Chen," SQL injection attack and guard technical research", 1877-7058 © 2011 Published by Elsevier Ltd. doi: 10.1016/j.proeng.2011.08.775.
11. Dr. G. Rama KoteswaraRao, K.V.J.S. Sree Ram, M. Akhil Kumar, R. Supritha, S. Ashfaq Reza," CROSS SITE SCRIPTING ATTACKS AND PREVENTIVE MEASURES", International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056 Volume: 04 Issue: 03 | Mar -2017.
12. Ashish Kumar, SumitraBinu," Proposed Method for SQL Injection Detection and its Prevention", International Journal of Engineering & Technology, 7 (2.6) (2018) 213-216.
13. Divya.M , Monisha.S, Reena .R , Kapilavani.R.K.," SQL Query Injection a Hazard Using Web Application", International Journal of Engineering and Techniques - Volume 4 Issue 2, Mar – Apr 2018.
14. DaljitKaur , Dr. ParminderKaur," Cross-Site-Scripting Attacks and Their Prevention during Development", International Journal of Engineering Development and Research, 2017 IJEDR | Volume 5, Issue 3 | ISSN: 2321-9939.
15. Kunal Gupta 1,RajniRanjan Singh , Manish Dixit ," CROSS SITE SCRIPTING (XSS) ATTACK DETECTION USING INTRUSTION DETECTION SYSTEM", International Conference on Intelligent Computing and Control Systems ICICCS 2017.
16. P.P.Anaswara[1], B.J. Santhosh Kumar[2]" Vulnerability detection and prevention of sql injection"International Journal Of Engineering And Technogy(Uae), /IJET.V7I2.31.13388.
17. Kankanala Pujitha[1],B.J.Santhosh kumar[2], "Web Application Vulnerability Detection Using Hybrid String Matching Algorithm", International Journal Of Engineering And Technogy(UAE),Volume 7,No-3.6(2018)
18. Pushpa B.R, Enhancing Data Security by Adapting Network Security and Cryptographic Paradigms", International Journal of Computer Science and Information Technologies, Volume. 5 (2) , 2014, 1319-1321.

AUTHORS PROFILE

Nischitha G K , BCA, Amrita school of arts and sciences. Amrita Vishwa Vidyapeetham ,Mysuru.

Sahana S, BCA, Amrita school of arts and sciences. Amrita Vishwa Vidyapeetham ,Mysuru.

Santhosh Kumar B. J. MCA, Mtech, currently serves as Assistant Professor at the Department of Computer Science, School of Arts and Sciences, Mysuru.