ISSN XXXX XXXX © 2018 IJESC

Research Article Volume 8 Issue No.4

Prevention of Phishing Attack on Online Voting System

Manoj Sabnis[1], Manisha Bahrani[2], Bhavna Bajaj[3], Payal Popat[4]
Assistant Professor[1], BE Student[2, 3, 4]
Department of Information Technology
Vivekanand Education Society's Institute of Technology, Mumbai, India

Abstract:
Online Voting system aims at providing a facility to cast vote for critical and confidential internal corporate decisions. It has the flexibility to allow casting of vote from any remote place. The election is held in full confidentiality by applying appropriate security measures to allow the voter to vote for any participating candidate. Once the user creates an account by uploading necessary details, the user needs to wait for the verification process which is done by the administrator. Administrator verifies the users account by sending a confirmation email with a generated password. The user can log into the account and view the candidates profile and can decide whom to vote. And the time of voting, the user gets only one minute to vote after which the account is disabled. In this Open Redirection method is used so that the user is not redirected to any other phished website. Internet voting focuses on security, privacy, and secrecy issues, as well as challenges for stakeholder involvement and observation of the process. A new approach is proposed for voting system to prevent phishing attacks.

Keywords: Verification, Online Voting, Phishing Attack, Open Redirection, Cyber Security, Website Forgery.

1. INTRODUCTION

Online voting refers to both the electronic means of casting a vote and the electronic means of tabulating votes. Using just a small sample of reported phishing content, a fairly good picture of which hosting providers may be more vulnerable to compromise or more forgiving of malicious behavior can be captured.In this voting system each voter will be provided with a specific voter-id and a password through which access for the voting can be granted. If once the access is granted for a voter-id then the access is denied for logging in till the voting system is refreshed for the next election. Similarly the administrator will be provided with a special id through which he can view the status of the election. Based on the id segregation between the voter and administrator is carried out initially. If the user id is invalid then an error message will be displayed. If the id entered is of type administrator then an information i.e., the election status will be displayed which changes dynamically. Otherwise the voter information will be displayed which changes dynamically depending on the changes made which will proceed him to the next level in which he can cast his vote and it is updated automatically. The advantages of the online voting system is that the speed of information retrieval and updating is made easy and other advantage are

- High level security to avoid illegal polling.
- Online implementation makes it easy for voters to participate in election.
- As for considering election commission board it becomes easier to conduct election.
- Election expenses can be reduced.
- Non-Residential citizens can also participate in the election.

2. METHODOLOGY

Open Redirection Method

Open Redirect vulnerabilities don't get enough attention from developers because they don't directly damage website and do not allow an attacker to directly steal data that belong to the company. However, that doesn't mean that Open Redirect attacks are not a threat. One of the main uses for this vulnerability is to make phishing attacks more credible and effective.

When an Open Redirect is used in a phishing attack, the victim receives an email that looks legitimate with a link that points to a correct and expected domain. What the victim may not notice, is that in a middle of a long URL there are parameters that manipulate and change where the link will take them. To make identification of the Open Redirect even more difficult, redirection could take place after victim provides login on a legitimate website first. Attackers have found that an effective way to trick a victim is to redirect him to a fake website after they enter their credentials on a legitimate page. The fake website would look identical to a legitimate website, and it would ask the victim to re-enter their password. After the victim re-enters their password it would be recorded by the attacker and victim would be redirected back to a valid website. If done correctly, victim would think that he mistyped password once and would not notice that his username and password were stolen.

Phishing is used in most successful targeted hacks and also regularly in opportunistic attacks. Considering how prominent phishing is in our daily lives, Open Redirect vulnerabilities should not be dismissed.

It would have been unfair to single out any specific website or company as being vulnerable to Open Redirect because so many companies have it. Instead, it's more useful to demonstrate how common those websites are and how easy it is to find them.

Doing a web search is one of the best tools to find Open Redirect on your own website and across a wider Internet.

Google Search allows for a great flexibility in writing search queries, including queries that specifically search through URLs of pages.

Using this simple search technique you can find dozens of Open Redirect vulnerabilities within minutes. List of vulnerable websites includes banking websites, websites of international corporations, trusted companies, beloved projects and numerous websites of smaller organizations. As an additional bonus, each time Google's web crawler comes across new website that has Open Redirect, we will get updated results through our queries.

The best way to avoid Open Redirect vulnerability is to avoid redirecting based on parameter controlled by users or supplied through GET method. If redirecting is unavoidable, it can be dealt with by validating a redirect target and sanitizing it using white list of approved URLs.

3. REQUIREMENTS ANALYSIS

Requirements analysis in systems engineering and software engineering, encompasses those tasks that go into determining the needs or conditions to meet for a new or altered users, taking account of the possibly conflicting requirements of the fake accounts.

Risk	Portability	Effects
Recognition of x 3 , x 4 (Users) etc.	High	Catastrophic
Attack recognition	Moderate	Catastrophic
Identifying correct details in timing of one minute	Moderate	Serious
Execution time	Low	Serious

Fig 1. Risk Analysis

4. HARDWARE REQUIREMENTS

1. System for website development: A computer system with web browser enabled in it for website development.

2. Processor: Above 2 GHz

3. Hard Disk: 50 GB

4. RAM: 4 GB

Image formats: bmp, jpg, gif.
Programming Language - Html,Css,Bootstrap and sql.

5. SOFTWARE REQUIREMENTS

1. Microsoft Visual Studio
2. SQL Management Studio

6. ANALYSIS

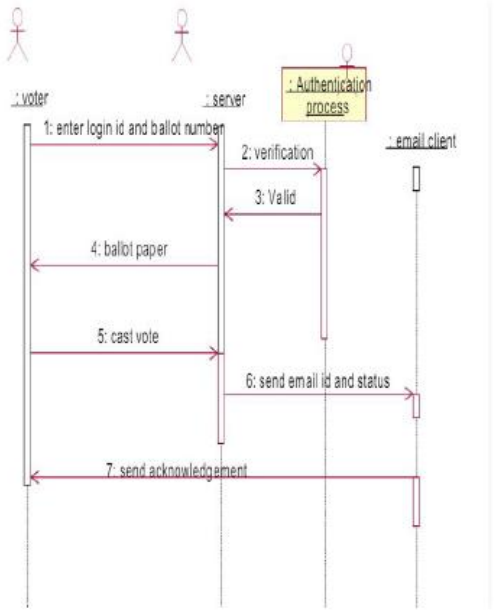

Fig 2. Sequence Diagram

7. RESULTS

Technical Feasibility: The application will require an internet connection, a device with Windows OS as the hardware for running the website successfully. Thus the website to be developed is technically feasible.

Operational Feasibility: New user will register and use the system. For this a small training program is required which will include briefing the working of the system. Demonstration will be performed so that the user actually gets to know the working of the system and what they need to do. Thus the required knowledge regarding the operations will be imparted to the users.

Financial Feasibility: It is concerned with the cost involved at the time of development and maintenance of the website. The overall feasibility analysis shows that the proposed system will be beneficial in terms of knowledge base provided as well as the cost than the older existing system.

Faster: The time span needed for the system is less than the manual voting system. Because the results are electronic. It saves a lot of time.

More accurate: The margin of error is greatly reduced with online surveys because participants enter their responses directly into the system. Traditional methods rely the attentiveness of staff to enter all details correctly, and naturally human error can creep in whenever a person has to perform a repetitive task.

Easy to use for participants: The majority of people that have access to the Internet prefer to answer surveys online instead of using the telephone. With an online survey, participants can pick a moment that suits them best and the time needed to complete the survey is much shorter.

8. CONCLUSION

Voting plays an important role for any democratic country. If this proposal is implemented, then the voting percent can be improved further since few percent of our citizens are working in worldwide and they cannot able to come to native country at the time of voting. For those people as well as for the people who are physically disabled and very old also can make use of the online voting system. Since Open Redirection technique is used, user can able to find out whether he is in phishing site or original site easily. Proposed online voting system is very effective and it will be useful for voters and organization in many ways and at the same time, it will reduce the cost and time.

9. REFERENCES

[1]International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE) ISSN: 0976-1353 Volume 22 Issue 1 – MAY 2016.

[2]Imperial Journal of Interdisciplinary Research (IJIR) Vol-2, Issue-12, 2016 ISSN: 2454-1362,http://www.onlinejournal.in

[3] International Journal of Advanced Research in Computer and Communication Engineering ISO3297:2007 Certified, Issue 5, May 2017 "Anti-Phishing I-Voting System using Visual Cryptography".