Analysis of The Bug Bounty Platform Using Machine Learning for the Small Business

Shivprasad Jadhav [1], Sanika Zagade[2], Ayush Iche[3]

[1] Department of Computer Science, MIT Alandi, Pune Pune, India shivprasadjadhav226@gmail.com
[2] Department of Computer Science, MIT Alandi, Pune Pune, India sanikazagade457@gmail.com
[3] Department of Computer Science, MIT Alandi, Pune Pune, India ayushiche@gmail.com

ABSTRACT-

Our bug bounty platform is a new way to secure small businesses and big businesses. It is designed to be easy to use, affordable, comprehensive, and secure. The platform makes it easy for small businesses to start a bug bounty program. This is important because small businesses are just as vulnerable to cyberattacks as large enterprises, but they often don't have the resources to invest in expensive security solutions. The platform also indexes a wide range of websites, including government websites, educational websites, and other websites that are in the public interest. This makes it more difficult for hackers to find and exploit vulnerabilities in websites that are not currently indexed by bug bounty platforms. Finally, the platform offers a wider range of bounty amounts and rewards. This is intended to attract a wider range of security researchers, from beginners to experienced professionals. I believe that Our platform has the potential to make a significant contribution to improving the security of the internet. It is designed to make bug bounty programs more accessible to small businesses, to increase the number of websites that are indexed by bug bounty platforms, and to offer a wider range of bounty amounts and rewards. This will benefit both bug bounty hunters and program managers.

Keywords- Bug Bounty Platform, Cyber Security.

Introduction :

Our platform is designed to make bug bounty programs more accessible to small businesses and big businesses alike. We are also working to index as many websites as possible on our platform, including government websites, educational websites, and other websites that are in the public interest. We believe that bug bounty programs are a valuable tool for improving the security of the internet. By making it easy for companies to start a bug bounty program, and by indexing a wide range of websites, we hope to make the internet a safer place for everyone.

Analysis

How Hackers target small businesses websites-

Small businesses are often less secure than larger companies: They may have fewer resources to invest in Cyber Security, and their employees may be less aware of the latest threats.
Small businesses often have valuable data that hackers can steal: This could include customer information, financial data, or trade secrets.

Proposed System

We create a bug bounty platform more accessible to small businesses and big businesses alike. We are also working to index as many websites as possible on our platform, including government websites, educational websites, and other websites that are in the public interest.

The unique features of our platform-

Focus on small businesses: Most bug bounty platforms are primarily focused on large enterprises. However, small businesses are just as vulnerable to cyberattacks, and they often don't have the resources to invest in expensive security solutions. Our platform would make it easy and affordable for small businesses to start a bug bounty program.
Government involvement: I am working with the government to index as many websites as possible on Our platform. This would make it more difficult for hackers to find and exploit vulnerabilities in government websites, educational websites, and other websites that are in the public interest.

Variety of bounty amounts and rewards: I would offer a variety of bounty amounts and rewards to attract a wide range of security researchers, from beginners to experienced professionals. I would also offer special rewards for critical vulnerabilities, and for vulnerabilities that are reported in a timely manner.

The strengths of our platform-

Easy to use: I would design Our platform to be easy to use for both companies and security researchers. The signup process would be simple and straightforward, and the platform would provide clear guidance on how to scope bug bounty programs and report vulnerabilities.

Affordable: I would offer a free tier for small businesses, and I would keep Our pricing competitive for larger businesses.

Comprehensive: Our platform would index a wide range of websites, including government websites, educational websites, and other websites that are in the public interest.

Secure: I would implement strong security measures to protect the confidentiality of vulnerability reports and to prevent unauthorized access to the platform.

The target audience for platform-

Small businesses: Small businesses are often more vulnerable to Cyberattacks than large enterprises, but they often don't have the resources to invest in expensive security solutions. Our platform would make it easy and affordable for small businesses to start a bug bounty program.

Big businesses: Big businesses are also vulnerable to cyberattacks, and they often have the budget to invest in expensive security solutions. However, bug bounty programs can be a cost-effective way for big businesses to supplement their existing security measures.

Government agencies: Government agencies are often targeted by hackers, and they need to take steps to protect their websites and systems. Our platform would make it easier for government agencies to start a bug bounty program.

Educational Institutions: Educational institutions are also targeted by hackers, and they need to take steps to protect their websites and systems. Our platform would make it easier for educational institutions to start a bug bounty program.

Use of machine learning in platform-

To recommend remediation steps: Once a vulnerability has been reported, we can use machine learning to recommend remediation steps to the affected company. This can help to reduce the time and effort that it takes to fix vulnerabilities.

REFERENCES :

1. google.com
2. gimini.google.com
3. wikipedia.org