International Research Journal of Education and Technology

Peer Reviewed Journal
ISSN 2581-7795

Website Vulnerability Tester with BrowserHistory Tracker

Kavitha V[1], Arshad I[2], Harikrishnan S[3], Ranjith B, Sudhakar C[5]

[1]Associate Professor, [2,3,4,5]UG Students - Final Year, Department of Information Technology, Nandha College of Technology, Perundurai – 638052, Tamilnadu, India

Abstract

Server hacking is an attempt to exploit a computer system or a private network inside a computer. Google hacking is a computer hacking technique that uses Google Search and other Google applications to find security holes in the configuration and computer code that websites use. Web servers are often the vector through which finders mount successful online attacks. Understanding the nature of exploitable risks at this level is essential to properly protecting applications from malicious actors. This application looks at a broad range of risks in web server implementations and more importantly, how you can defend against these being compromised by finders. The Main objective of this project is finding IP address of a website and also other website available in the server and the host IP or Domain example is to be entered after typing that it fetches and give the Start and End port of that host. This application gives the clear details of protocol major version and minor version and it gives the Server software and also server UTF encoding. This project provides a modern way of tracking the Compute, Browser's and Network IP. This application is additionally used to check the IP address of the user even when the internet is down. This application is used for all type of people with basic computer knowledge.

Introduction

This is the web application vulnerability assessment/penetration testing phase. Two major methods are used in the phase. One is the manual web application software vulnerability assessment and the other is the automated software vulnerability assessment method. In spite of having secure web application development framework for software development and application vulnerability assessment phases for identification of web vulnerabilities, open security researches and responsible disclosure ventures have proved that web applications are susceptible for vulnerabilities that cannot be fully vetted merely by using secure frameworks .Once a web application is on the internet, it attracts the interest of a group of cyber Security researchers who constantly analyse the web application with a security eye. Their keep interest on having secure web applications result in the identification of security vulnerabilities on production environment which are then reported through appropriate channels for mitigation. Hackers constantly hunt for web app vulnerabilities. On discovering vulnerability on a web application, they do not report it as required. Most of the large scale web application companies and businesses lay down clear rules and policies on how web application vulnerability should be handled and reported if found in their web portal. Failing to adhere to responsible vulnerability disclosure policies often violates the Terms and Conditions with regard to the usage of the web application portal.

Existing and Proposing System

The existing system of this project is finding IP Address of a website. This application looks at a broad range of risks in web server implementations and more importantly, how you can defend against these being compromised by finders. There is no process of finding other website available with the same IP Address in the server and the host IP or Domain example is to be entered after typing that it fetch and give the Start and End port of that host. The existing application does not give the clear details of protocol major version and minor version and it does not give the Server software and also server UTF encoding. In the existing systems, The IP addresses of the host arefound by the command prompt using IP Config.The machine information is also capture by using the windows log. The History of the browser can be viewed in the existing system and the exact Manual Count cannot be encountered. When the Internet is down we unable to extract the IP address of the user host and also the machine information.

The proposed system of this project finding IP Address of a website and additionally finding other website available with the same IP Address in the server. The host IP or Domain example is to be entered after typing that it fetch and give the Start and End port of that host. This application gives the clear details of protocol major version and minor version and it gives the Server software and also server UTF encoding. A tracker is any skilled computer expert who uses their technical knowledge to overcome a problem. In proposed system, The IP address Such as IPV6/IPV4 can be extracted even when the internet is down. The timing, title of the web search, count visited by the user in the browser are encountered in this application. When the user using in one IP Address and shifted to another IP Address, The history of previous IP can be easily tracked in this application. The main objective of this Application is the User Entire Action can be tracked.

System Study

The feasibility of the project is analyzed in this phase and business proposal is put forth with a very general plan for the project and some cost estimates. During system analysis the feasibility study of the proposed system is to be carried out. This is to ensure that the proposed system is not a burden to the company. For feasibility analysis, some understanding of the major requirements for the system is essential.

Economical Feasibility Study

This study is carried out to check the economic impact that of the system will have on the organization. The amountfund that the company can pour into the research and development of the system is limited. The expenditures must be justified. Thus the developed system as well within the budget and this was achieved because most of the technologies used are freely available. Only the customized products had to be purchased.

Technical Feasibility Study

This study is carried out to check the technical feasibility, that is, the technical requirements of the system. Any system developed must not have a high demand on the available technical resources. This will lead to high demands on the available technical resources. This will lead to high demands being placed on the client. The developed system must have a modest requirement, as only minimal or null changes are required for implementing this system.

SocialFeasibility Study

The aspect of study is to check the level of acceptance of the system by the user. This includes the process of training the user to use the system efficiently. The user must not feel threatened by the system, instead must accept it as a necessity. The level of acceptance by the users solely depends on the methods that are employed to educate the user about the system and to make him familiar with it. His level of confidence must be raised so that he is also able to make some constructive criticism, which is welcomed, as he is the final user of the system.

Architecture Diagram

For system developers, they have system architecture diagrams to know, clarify, and communicate concepts regarding the system structure and also the user needs that the system should support. It's a basic framework may be used at the system designing section serving to partners perceive the architecture, discuss changes, and communicate intentions clearly.

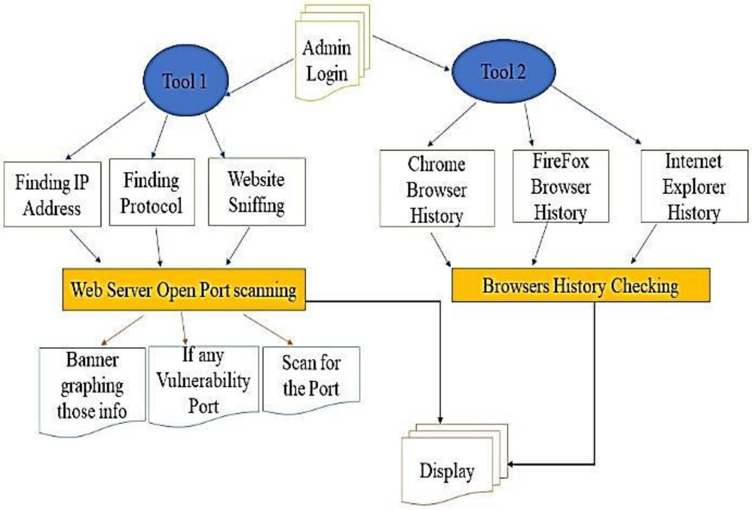

Figure 1Architecture diagram

Backtracking Algorithm

Backtracking is algorithm for searching all solutions to computational problems, satisfaction problem, that creates candidates to the solutions.Backtracking is considered an important technique to solve constraint satisfaction issues and puzzles.

General Method

- Useful technique for optimizing search under some constraints.
- Express the desired solution as an n-tuple (x1, . , xn) where each xi ∈ Si , Si being a finite set
- The solution is based on finding one or more vectors that maximize, minimize, or satisfy a criterion function P(x1, . . . , xn)
- Sorting of a[n] - Find an n-tuple where the element xi is the index of ith smallest element in a Criterion function is given by a[xi] ≤ a[xi+1] for 1 ≤ i < n Set Si is a finite set of integers in the range [1,n]

List of Modules

- Login Module
- Finding IP Address Module
- Server Port Scanning Module
- Protocol Module
- Website Sniffing Module
- Browsers history checking Module
- Track User Action Module

Login Module:In this login module, it displays an admin interface for user authentication. This login page for a project is used to provide a proper genuine authentication to the application with this we can restrict the unauthorized and illegal users in to the application. It acts as a very great security feature to the application. If the Admin use proper user id and password it enters in to application or else it returns back in to the authentication login page indicating the user is invalid.

Finding IP Address Module: Hacker means someone who finds weaknesses in a computer or computer network. In this Module, It find the IP Address of the website and also the other website with same IP Address in the server. The main objective in this module is finding the other website in the server.Fields requiredin this module are listed below:

- **Website Name :** Name of a website finding
- **IP Address :**IP Address of that website
- **Other Website Available :** Other Website available with the same IP

Server Port Scanning Module: In this Module, the host IP or Domain example is to be entered after typing that it fetch and give the Start and End port of that host. Additionally it gives the Maximum thread to run the host and time out seconds. Banner grabbing is a system used to increase information about a computer system on a network and the services running on its ports. A port scanner is an application designed to analyse a server or host for open ports. This is often used by administrators to verify security policies of their networks and by attackers to identify network services running on a host and exploit vulnerabilities. Fields required in this module are listed below:

- **Host IP or Domain Name:** Enter host IP or Domain
- **Start Port:** Starting port number
- **End Port:** Ending Port number
- **Time Out:** Enter time out

Protocol Module: In Protocol Module, the existing system only gives the version of the protocol. But this application gives the clear details of protocol major version and minor version. The main objective of this application is it gives the status of the protocol. A protocol is a controlled sequence of messages. A protocol is a set of policy and guiding principle for communicate data.Fields required in this module are listed below:

- **Protocol Major Version:** Major version of protocol
- **Protocol Minor Version:** Minor version of protocol
- **Protocol Version:** Version of Protocol
- **Protocol Status:** Status of Protocol

Website Sniffing Module: A website is a group of linked web pages, with multimedia content. In this Module, the existing system gives the technology name while sniffing in website. The Main objective of this module is it fetch and gives the Server software and also server UTF encoding.Fields required in this module are listed below:

- **Target Server Type:** Server type
- **Website Type:** Website type
- **Target Server Encoding Type:** Encoding type
- **Web Server Status:** Status of Webserver

Browsers History Checking Module

Chrome Browser History Checking Module: In this module, we used environment getfolderpath method this method gets the path to the system special folder that is identified by the specified enumeration.The backend connection is using SQLITE for getting better result.Dataset, datatable, dataadapter is used in this module for hacking the browser.

- **DataSet-** It is connectionless oriented. Whenever binding data from database. It connects indirectly to the database and then disconnected. Its easily read and write data from database.

- **Data Table-**Represents a single table in the database. It has rows and columns. There is no much difference between dataset and Data Table, Dataset is simply the collection of Data Tables.
- **Data Adapter-** Data Adapter is a disconnected oriented architecture. Data Adapter is like a mediator between Data Set (or) Data Table and database. This Data Adapter is used to read the data from database and bind to dataset.

FireFox Hacking Module: In FireFox Hacking module designer variable is required. The module has disposing object for hacking the computer. Dispose is an object method invoked to execute code required for memory clean-up and release and reset unmanaged resources, such as file handles and database connections. The disposing object is true if managed resources should be disposed otherwise, it remains false. Additionally it includes data grid view cell style property for providing different cell styles. The Firefox hacking module use auto scale dimensions property that gets the current run-time dimensions of the screen and also it include auto scale mode enumeration which specifies the different types of automatic scaling modes supported by windows forms.

Internet Explorer Hacking: Internet Explorer hacking designer variable is required. The module has disposing object for hacking the computer.

Dispose: An object method invoked to execute code required for memory release and reset unused resources.Disposing object is true if managed resources are disposed otherwise, it remains false.Additionally it includes data grid view cell style property for providing different cell styles.

AutoScaleDimension: The AutoScaleDimensions property signifies the DPI or font setting of the screen.The CurrentAutoScaleDimensions property is different from the AutoScaleDimensions.

Track User Action Module

Computer checking Module: In computer hacking module designer variable is required. The module has disposing object for hacking the computer.Dispose is an object method invoked to execute code required for memory clean-up and release and reset unmanaged resources, such as file handles and database connections.The disposing object is true if managed resources should be disposed otherwise, it remains false.

Hack Computer track user action: In hack computer track user action module designer variable is required. Also it required method for designer support. Additionally include data grid view cell style property for providing different cell styles

- **Designer variable:**Designer variable numbers whole values that can be spontaneously different by the designer to define a designed object.

- **Managed resources:** Subject to classic memory leaks, one can still leak memory by not dereferencing unused resources.If managed resources should be disposed means true; otherwise false.
- **DataGridView:**It control displays cells using the styles detailed by the cell Inherited Style property.Which accepts styles from additional properties of type using datagridviewcellstyle?

Network IP Tracking: In network IP tracking designer variable is required. The module has disposing object for hacking the computer.Disposing object is true if managed resources are disposed otherwise, it remains false. Additionally it includes data grid view cell style property for providing different cell styles.

- **UseVisualStyle:**Visual styles are conditions for the appearance of controls.Visual styles define the color, size, and font of controls, and they allow organizing the visual interface to match with application interface.
- **PictureBox:**The same image in numerous picture box controls, create a duplicate of the image for each Picture Box**.**Retrieving the same image from multiple panels bases an concession to occur.
- **ISupportInitialize:**ISupportInitialize allow controls to optimize multiple property assignments.Call the Beginnit() method to signal the object that initialization is starting.

Scope for Future Developments

Every application has its own merits and demerits. The project has covered almost all the requirements. Further requirements and improvements can easily be done since the coding is mainly structured or modular in nature. Changing the existing modules or adding new modules can append improvements. Further enhancements can be made to the application, so that the web site functions very attractive and useful manner than the present one.

Conclusions

This Project provides Exact User Action performed in the webserver. The Main objective of this application is tracked the IP Address of the website and finding the other website available with same IP in the server Additionally it encountered the major and minor version of the protocol and tracked the previous IP Address that the user used even when the internet is down .The Ethical Hacking Project provides Exact User Action performed in the Browser's,Computer and Network IP. Additionally it encountered the timing, title of the web search and count that the user used in the browsing history.

References

1. Rafay Baloch"Ethical Hacking and Penetration Testing Guide".

2. Josh Pauli“The Basics of Web Hacking: Tools and Techniques to Attack the Web”.
3. Allen Harper, Shon Harris, Jonathan Ness,Chris Eagle, Gideon Lenkey, and Terron Williams,“Gray Hat Hacking”.
4. Steve Harris and Robmacdonald,“Web development with c#.Net”-Apres”.
5. Chris Goode, John Kauffman “Beginning asp.Net 1.0 with visual basic.Net”-Wrox programmer to programmer.
6. Douglas O Reilly, “Designing Microsoft Asp.Net applications”-TATA McGraw Hill.
7. Matthew Macdonald,“Microsoft c#et programmer’s cookbook”-TATA McGraw Hill.
8. CISCO ACN returns Cross Site Scripting Vulnerability, https://nvd.nist.gov/vuln/detail/CVE-2015-0774.
9. Jose Fonseca, Marco Vieira, and Henrique Madeira, "Evaluation of Web Security Mechanisms Using Vulnerability & Attack Injection",Dependable and Secure Computing, IEEE Transactions, 11(5).
10. Palma Salas, M.I.; Martins, E. "A Black-Box Approach to Detect Vulnerabilities in Web Services Using Penetration Testing", Latin America Transactions IEEE, 2015, 13 (3),pp.707 – 712.
11. LwinKhinShar; Briand, L.C.; HeeBengKuan Tan, "Web ApplicationVulnerability Prediction Using Hybrid Program Analysis and MachineLearning", Dependable and Secure Computing, IEEE Transactions, 2015, 12(6), pp.688 – 707.
12. Vlsaggio, C.A.; Blasio, L.C., "Session management vulnerabilities intoday's web" Security & Privacy IEEE Year: 2010, 8(5), pp. 48 – 56.
13. Wenliang Du "SEED: Hands-On Lab Exercises for Computer SecurityEducation", Security & Privacy, IEEE Year, 2011, 9(5), pp.70 – 73.
14. Farrell S, "Leaky or Guessable Session Identifiers", Internet Computing, IEEE, 2011, 15(1), pp.88 – 91.
15. LwinKhinShar and HeeBengKuan Tan "Defeating SQL Injection",IEEE Computer Society, 2013, 46(3), pp.69 – 77.