



e-ISSN: 2319-8753 | p-ISSN: 2347-6710

# IJIRSET

International Journal of Innovative Research in  
**SCIENCE | ENGINEERING | TECHNOLOGY**



# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 11, Issue 7, July 2022

**ISSN** INTERNATIONAL  
STANDARD  
SERIAL  
NUMBER  
INDIA

Impact Factor: 8.118



9940 572 462



6381 907 438



ijirset@gmail.com



www.ijirset.com



# A Novel Approach for Security Testing Using Burp suite Tool

**Mr.Puneeth S P, Sujan Shetty**

Assistant Professor, Department of Information Science and Engineering, Bapuji Institute of Engineering and Technology, Davangere. India

B.E Student, Department of Information Science and Engineering, Bapuji Institute of Engineering and Technology, Davangere. India

**ABSTRACT:** Security Testing is a type of Software Testing that looks for weaknesses, threats, and risks in a piece of software to stop hackers from doing damage. The main goal of security testing is to find the problems in the system. To find out how likely it is that the system could be broken. To help find all of the system's possible security risks. To help developers fix security problems with their code. Security testing is a way to find problems in the security features of an information system that keep data safe and keep the system running as it should. Burp Suite is a platform and graphical tool that can be used to check the security of web applications. Its different tools work well together to help with the whole testing process, from mapping and analysing an application's attack surface to finding and using security holes.

**KEYWORDS:** Security Testing, Vulnerabilities, Burp Suite.

## I. INTRODUCTION

Security Testing is a subset of Software Testing that identifies vulnerabilities, hazards, and dangers in software to prevent hackers from causing harm. The objective of Security Tests is to identify any defects and vulnerabilities in the software system that might allow workers or outsiders to steal information, money, or a good reputation. The primary objective of security testing is to identify a system's risks and determine how susceptible it is, so that the threats can be addressed and the system does not cease to function or can't be used against itself. It also aids developers in identifying system vulnerabilities and demonstrates how to eliminate them.

The Burp Suite is one of the most used tools for testing security. You can stop HTTP requests from leaving a web browser by using Burp Suite. Burp Suite is a proxy server, which means that it sits between the user's browser and the web server. This lets you see and change all the back and forth web traffic that happens when a specific web application is used. With the burp suite, you can test what's happening behind the GUI. We can test more technical things now. Burp Suite is a vulnerability scanner that can act as a proxy, an intruder, a scanner, a decoder, and so on.

**Proxy:** Proxy is used to block our requests from going through, and its proxy functions are.

**Intruder:** Intruder has a number of attacks that can be done on a remote website, such as a dictionary attack or a brute force attack.

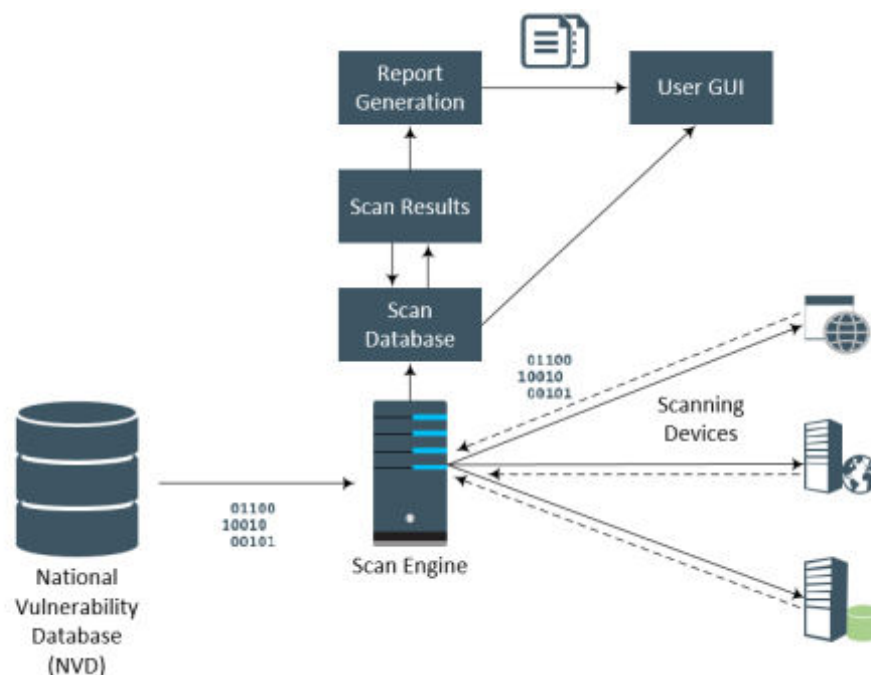
**Scanner:** Using a scanner, you may verify the security of a website.

**Decoder:** URL decoding is one example of a function in the decoder's toolkit that may be used to decode data.

## II. LITERATURE SURVEY

### Vulnerability Scanning

System, application, or service vulnerabilities allow an attacker to overcome security safeguards and modify systems in ways the creator never intended [1]. Scanning for vulnerabilities on another machine is known as vulnerability scanning. It's also useful for identifying weak spots in a network [2]. Vulnerability scanning is a technique used by security specialists to identify and address any weaknesses in a system. It's also possible that hackers may utilise it to harm a system in this way. Vulnerability scanners are programmes that evaluate a network's architecture for weaknesses and provide instructions on how to resolve them. At its heart, a vulnerability scanner is shown in Figure 1.[1]



**Fig.1: Vulnerability Scanner System Diagram [1]**

Scanners refer to the National Vulnerability Database (NVD) [1] for definitions. For known vulnerabilities, the CVE (Common Vulnerabilities and Exposures) is a collection of standard names. CVE data is available in NVD. It is possible to assess the NVD's risk level using the Common Vulnerability Scoring System (CVSS). It takes into consideration factors such as the kind of attack, its complexity, what permissions are required, how the user interacts with the attack and how it impacts confidentiality, integrity, and usability. [1]. [2].

Burp Suite: PortSwigger provides you with Burp Suite, one of the greatest security tool sets available. By providing superior analysis, we want to provide our customers a competitive advantage. By pretending to be a user of a web application, you may test its security. From mapping and analysing an application's attack surface to detecting and exploiting security problems, its numerous tools work in concert to map and analyse an application's attack surface and to identify and exploit security weaknesses. With Burp, you can combine expert manual approaches with



incremental automation to speed up your job, make it more valuable and interesting, and improve productivity. As a result of the Burp Scanner tool, web applications are automatically checked for security flaws.

### III. TECHNOLOGY

#### Burp Suite Tool

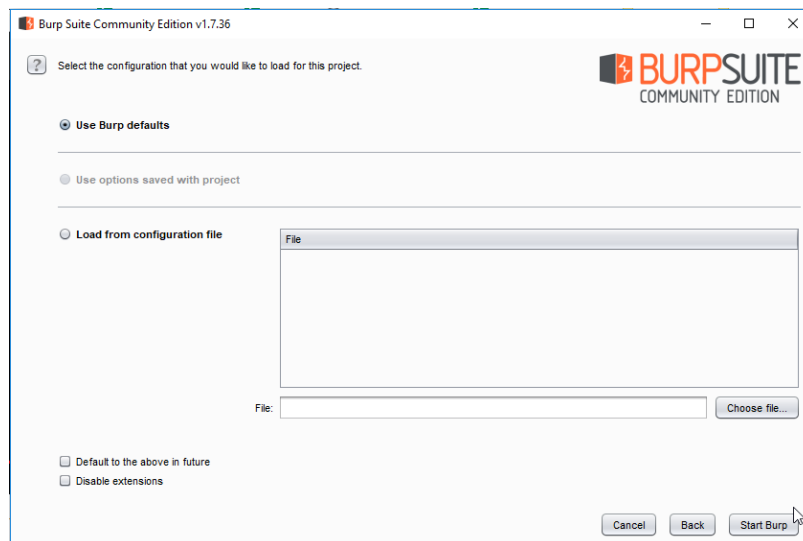
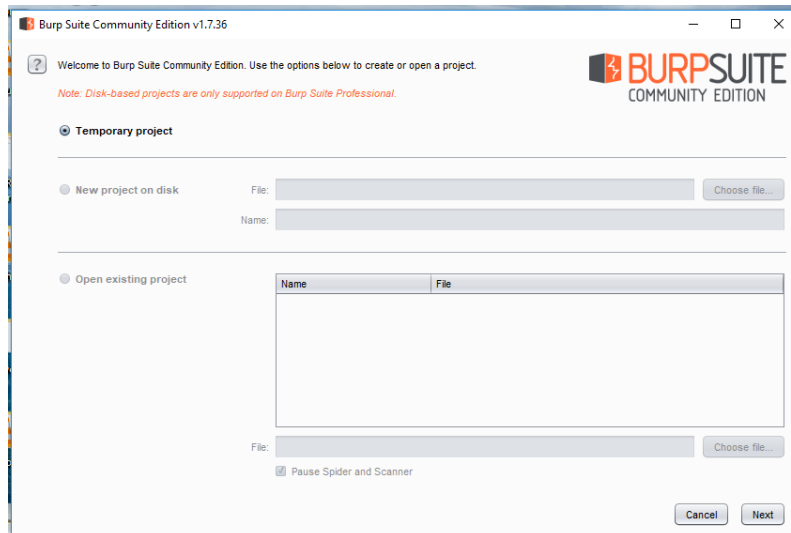
Burp Suite, sometimes known as Burp, may be used to test Web applications for security vulnerabilities. It was written in Java by PortSwigger Security and was developed by them. This proxy allows you to send and receive all requests and responses, enabling you to study and query them in a number of ways. Burp is an outstanding option for penetration testing. "Community edition" is free and provides the most essential manual tool. All requests and answers between the browser and the target application may be intercepted with the simplest manual technique. Web apps communicate with one another using the HTTP protocol. The Hypertext Transfer Protocol (HTTP) specifies the communication protocol between a web browser and a web server. Both HTTP and HTTPS web apps may be tested with Burp Suite.

#### Features of Burp suite

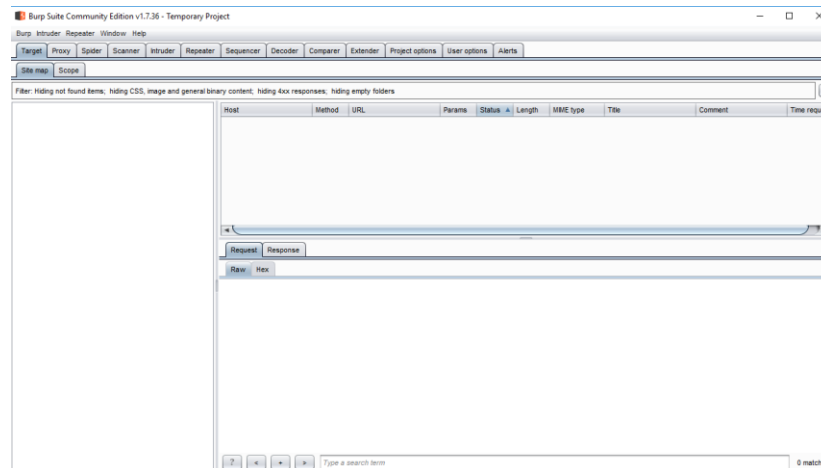
- In addition, manual penetration testing is included.
- Everything your browser sees will be intercepted.
- Automated assaults that are very customised and advanced. It's easier to use brute force and fuzzing in a shorter amount of time.
- Vulnerability scanning is done automatically. Take use of cutting-edge AST technology.
- Productivity aids. Analysis of messages in great detail.
- Extensions. Make your own unique add-ons.
- Allows for many requests to be sent at once.

#### Installation of Burpsuite

- Download burp suit from <https://portswigger.net/>.
- Install Burp Suite After running the installer,
- select "new temporary project", followed by "use burp defaults".



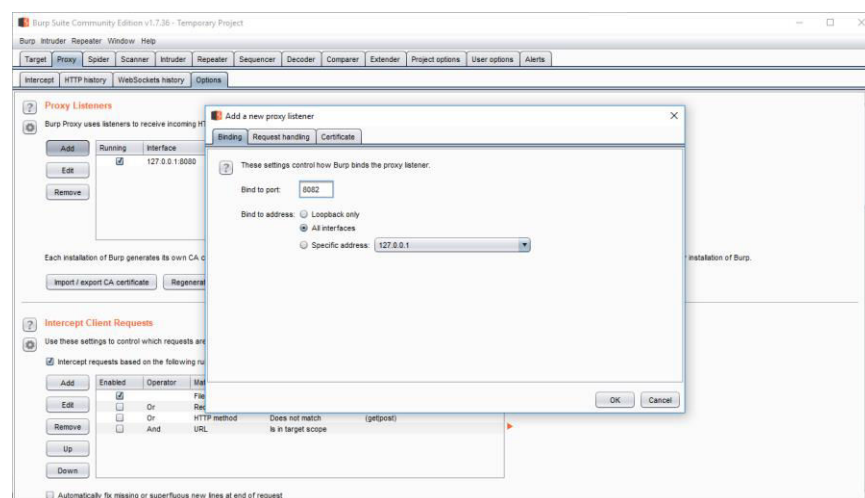
4). Click on Start Burp



5). Look under the "Proxy Listeners" section under the "Proxy" tab, then under the "Options" subtab.

6). You should see an entry in the table with the checkbox ticked in the Running column, and "127.0.0.1:8080" showing in the Interface column.

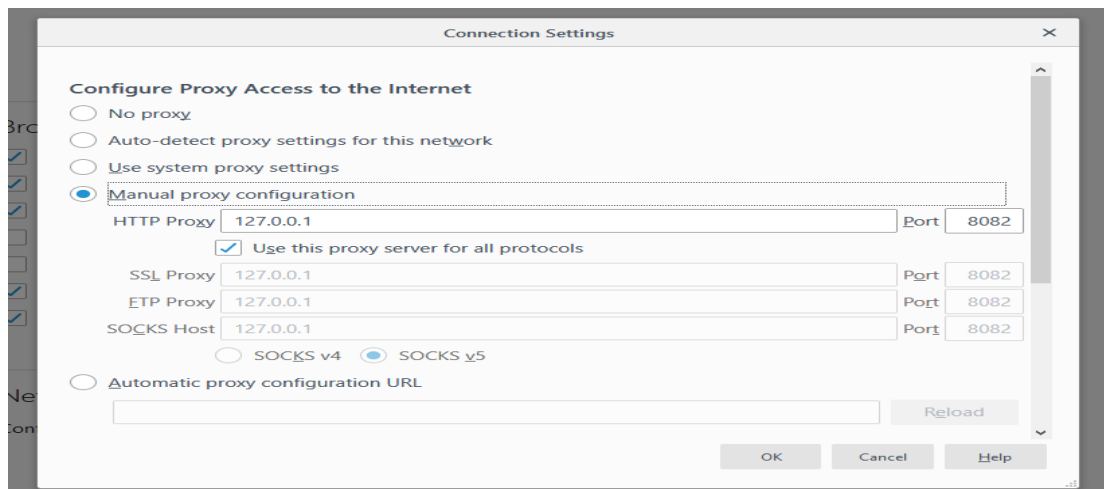
7). In order to alter the port number of the listener, you will need to pick the table item, click "Edit," and change the port number.





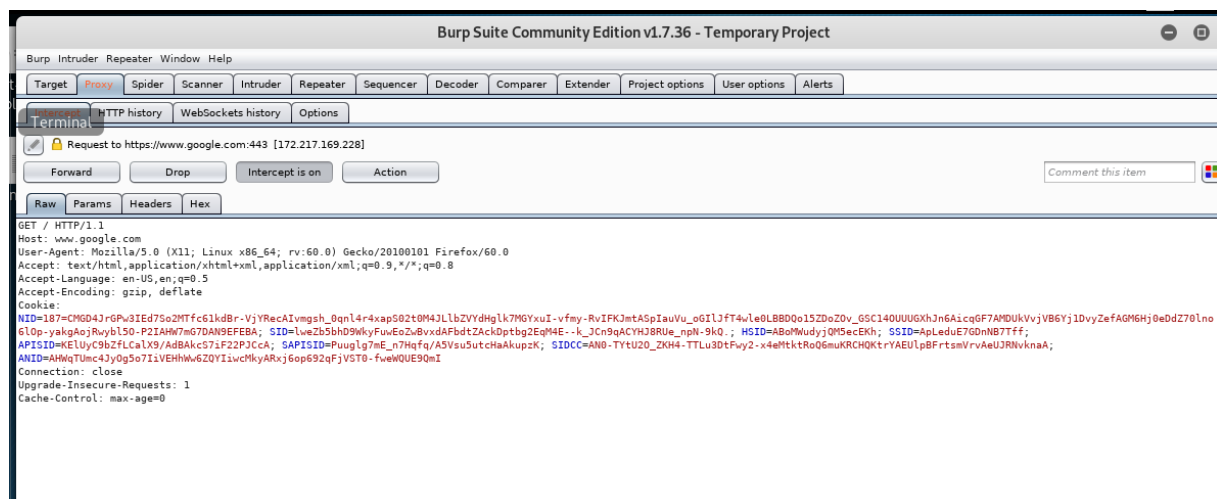
## Burpsuite And Browser Configuration

Open Firefox and choose Customize from the Tools drop-down menu. Select "Options" from the Customize menu, then "Settings" from the Network Section menu.



In order to set up your host computer, click on this option. Select Manual proxy settings from the drop-down menu and input the same HTTP Proxy and Port number you used in Burp Suite. To save your changes, just click "OK" at the bottom of the page.

Using Firefox, type "google.com" into the address bar and then switch to the burp suite. You may be able to identify a few "fire fox profile tracing" images. Click the "drop" button to get rid of them.



As a last resort, you may analyse the HTTP headers, parameters, and hex values in the burpsuite tabs if necessary (similar to the firefox inspector, but prior to the request being filled by the server)

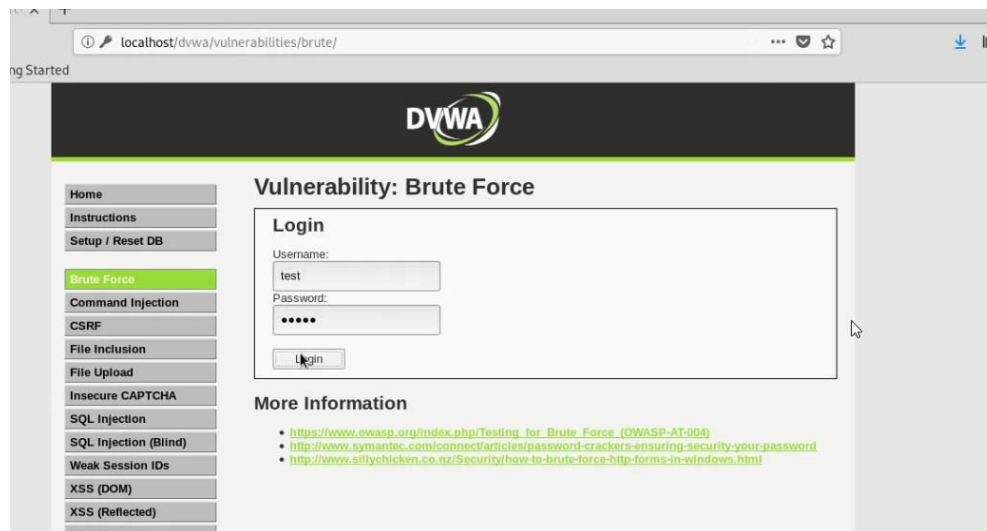
- at this point, nothing has been sent to the remote server!
- click 'forward'
- the request is sent to the server
- You now have to switch to the 'http history tab'

## IV. VULNERABILITIES

### No Rate Limit On Login Page

A brute force assault is just attempting to breach a system over and over again. When it comes to usernames and passwords, they could test out several combinations until they discover one that works. However, more sophisticated brute force assaults do exist, and they do work on occasion.

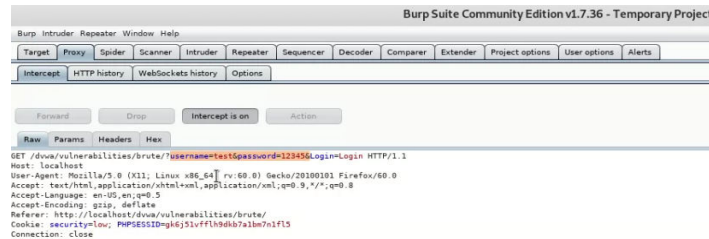
Enter any incorrect username and password



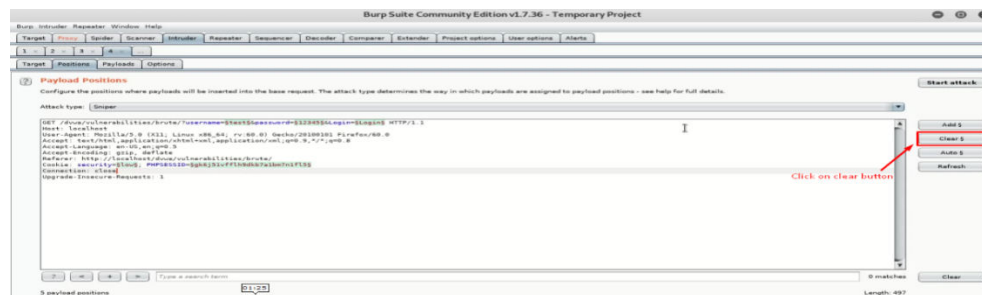


Log in by using the "Login" button.

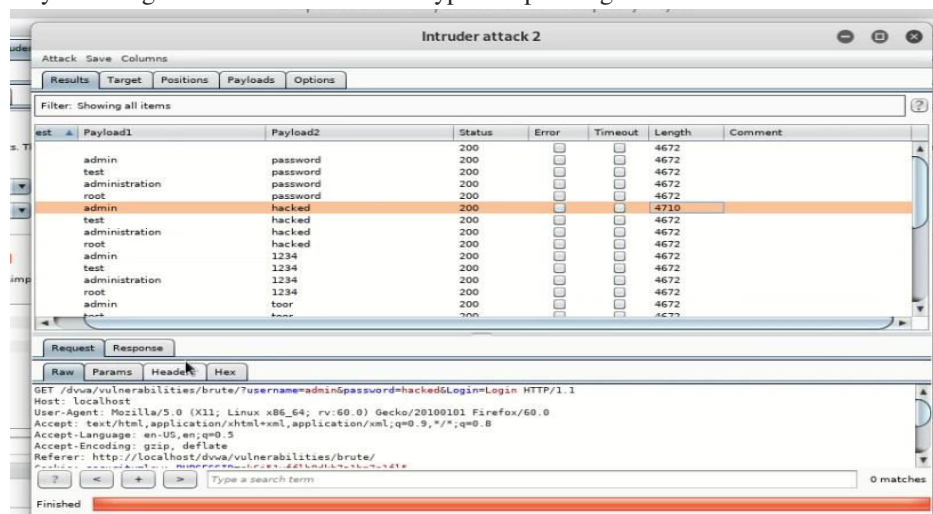
You may now see the call in Burp by switching to the application.



Right click -> Send to Intruder



To remove everything, just click the "Clear" button. Now pick just the fields needed to brute force, namely the username and password, by clicking on the "Add" option. Only the username and password are being brute forced. Start the assault by selecting the Cluster Bomb attack type and pressing the start button.





Analyze the time taken by each request once the attack has been completed. Depending on what they are, username and password length will vary. Now, log in using your chosen username and password.

## V. CONCLUSION

Burp Suite is a Java-based platform for Web Penetration Testing. In order to check for security issues, it's designed for this purpose. It is possible to identify and verify assaults on applications using Burp Suite. Due to its importance in ensuring that private information does not leak out, security testing is the most crucial kind of testing for an app. In this kind of testing, the tester takes on the role of an attacker and messes about with the system in an attempt to uncover any security vulnerabilities. The importance of security testing in software engineering cannot be overstated. Software security testing is an essential and vital aspect of the development process. The only way to know whether your system is secure is to perform this test and then patch up any security flaws that are found. Regular application and system updates ensure the safety and security of the system. Even though security testing does not examine how well the product works or how it works, this form of software testing is nevertheless very vital for software engineers.

## REFERENCES

1. AL-Ghamdi and Abdullah Saad AL-Malaise, "A Survey on Software Security Testing Techniques," proceedings of ijst conference, 2016.
2. B. Arkin, S. Stender and G. McGraw, 2005, "Software penetration testing", IEEE Security & Privacy, vol. 3, no. 1, pp. 84-87.
3. Shah. Sugandh. & B.M. Mehtre, "A Modern Approach to CyberSecurity Analysis Using Vulnerability Assessment and Penetration Testing," Proceedings of 2013 NCRTCST, Hyderabad (A.P), India, 2014.
4. Buja, G., Bin AbdJalil, K., BtHjMohd Ali, F.; Rahman, T.F.A., "Detection model for SQL injection attack: An approach for preventing a web application from the SQL injection attack," proceedings of 2014 IEEE Symposium on Computer Applications and Industrial Electronics (ISCAIE).
5. OWASP Top 10 Application Security Risks, 2017, Information available from: [https://www.owasp.org/index.php/Top\\_10-2017\\_Top\\_10](https://www.owasp.org/index.php/Top_10-2017_Top_10) accessed at 11:30 hrs on 10-01-2019.
6. PortSwigger. (n.d.). Burp Suite, 2018, Information available from: accessed at 09:50 hrs on 17-01-2019.
7. Wireshark network protocol analyzer, 2018, Information available from: accessed at 14:40 hrs on 03-01-2019.
8. Sandhya S, SohiniPurkayastha, Emil Joshua, Akash Deep, "Assessment of Website Security by Penetration Testing Using Wireshark," proceedings of 2017 International Conference on Advanced Computing and Communication Systems (ICACCS -2017).



INNO  SPACE  
SJIF Scientific Journal Impact Factor  
Impact Factor: 8.118



ISSN INTERNATIONAL  
STANDARD  
SERIAL  
NUMBER  
INDIA



# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

 9940 572 462  6381 907 438  [ijirset@gmail.com](mailto:ijirset@gmail.com)



[www.ijirset.com](http://www.ijirset.com)

Scan to save the contact details