



BURP SUITE FOR PENTESTER ENGAGEMENT TOOLS


TABLE OF CONTENTS

1	Abstract	3
2	Engagement Tools in Burp Suite	5
2.1	Find References	5
2.2	Discover Content	6
2.3	Site Map	7
2.4	Schedule Task	8
2.5	Generate CSRF PoC	11
4	About Us	15

Abstract

Information gathering is the biggest thing. There is just an endless TO-DO list.

So, today in this publication we are going to discuss the Importance of **Engagement tools** which is a Pro-only feature of Burp Suite. It is mainly used in information gathering and hence the analysis of any web application testing.



Engagement Tools in Burp Suite

Engagement Tools in Burp Suite

Its four important utilities are the following:

- Find References
- Discover Content
- Schedule Task
- Generate CSRF POC

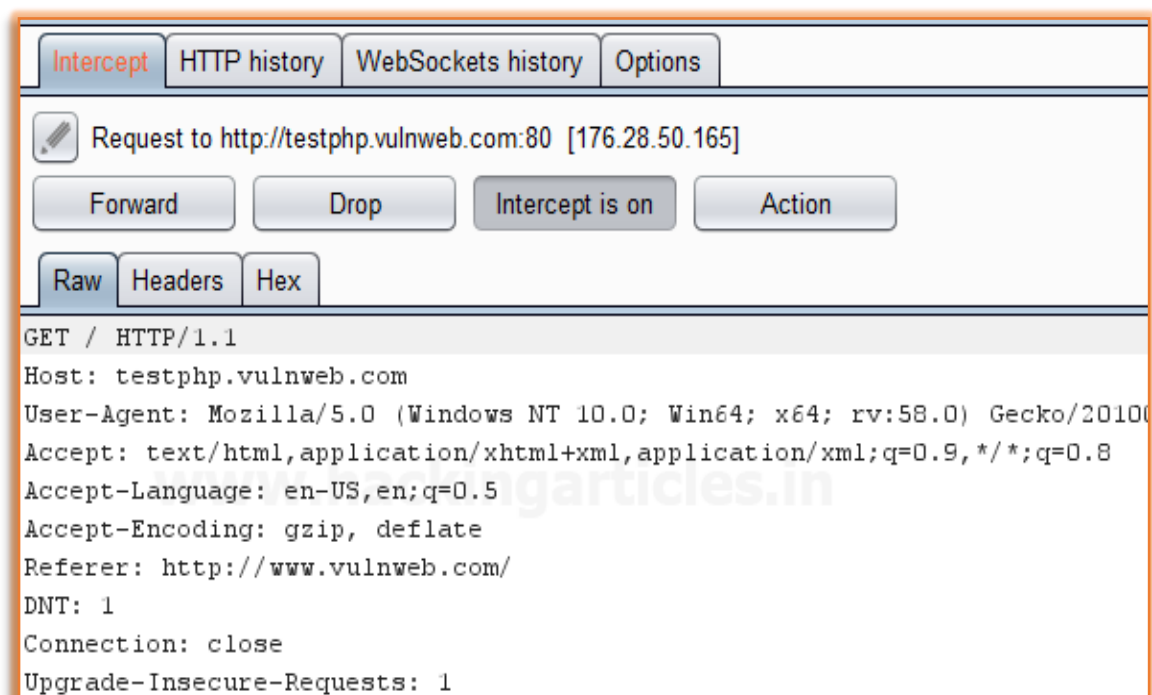
Find References

This function can be used to search all Burp suite tools for HTTP responses that link to a particular item. To make use of this function, select an HTTP request anywhere in Burp suite, or any part of the site map, and choose "Find references" in "Engagement tools" in the context menu which can be seen clicking Action Tab within Burp suite.

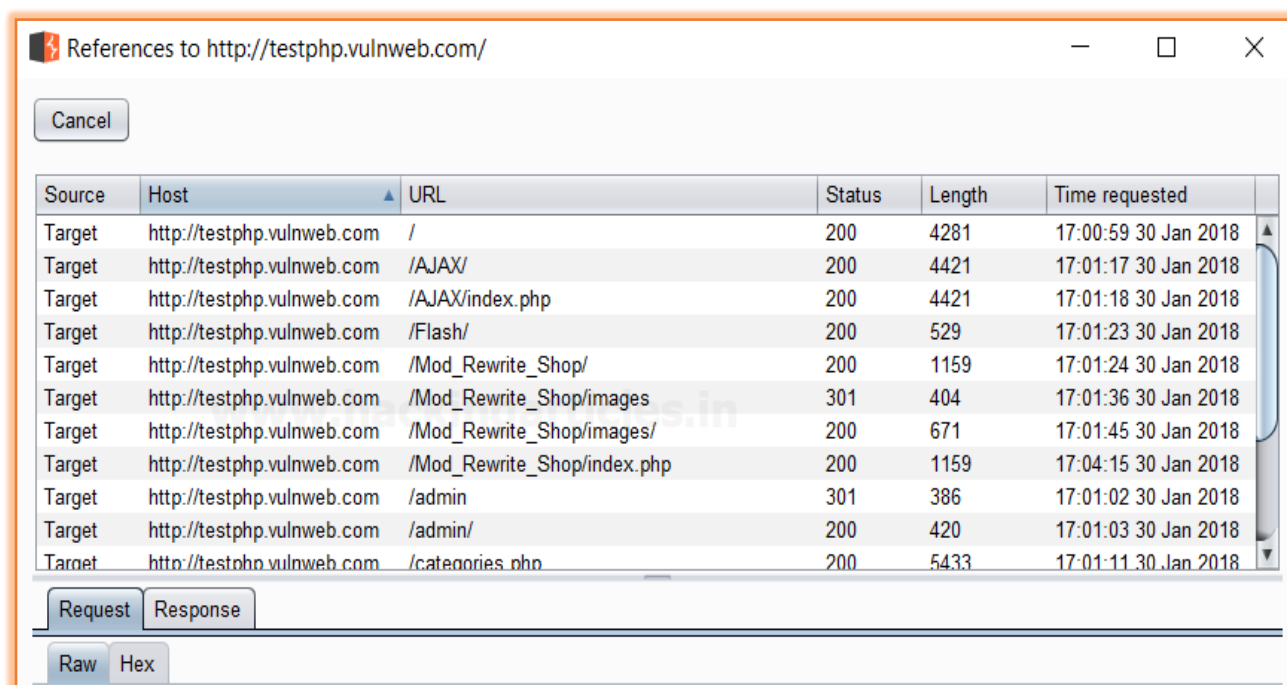
The result window of the search shows responses (from all Burp tools) that are linked to the selected item. Whenever we view an individual search result, the response will be automatically highlighted to show where the linking reference is occurring.

This function treats the original URL as a Prefix whenever we search for links, so if you select a host, you will find all references related to the host and if you select a folder, you will find all references to items inside that folder.

First, we have intercepted the request of the **Vulnweb.com** which is a **demo lab** available over the internet which can be used for testing attacks. Then click on enter after writing the URL of the Vulnerable Web in your browser, then the burp suite will capture the request of the web page in the intercept tab.



Then **click on Action Tab**, after that select the **Engagement tools** then click on **Find References**. This will open a result window which will show all the references related to the **URL** whose request has been captured which is the **Vulnerable Web** as shown in the image.



Source	Host	URL	Status	Length	Time requested
Target	http://testphp.vulnweb.com	/	200	4281	17:00:59 30 Jan 2018
Target	http://testphp.vulnweb.com	/AJAX/	200	4421	17:01:17 30 Jan 2018
Target	http://testphp.vulnweb.com	/AJAX/index.php	200	4421	17:01:18 30 Jan 2018
Target	http://testphp.vulnweb.com	/Flash/	200	529	17:01:23 30 Jan 2018
Target	http://testphp.vulnweb.com	/Mod_Rewrite_Shop/	200	1159	17:01:24 30 Jan 2018
Target	http://testphp.vulnweb.com	/Mod_Rewrite_Shop/images	301	404	17:01:36 30 Jan 2018
Target	http://testphp.vulnweb.com	/Mod_Rewrite_Shop/images/	200	671	17:01:45 30 Jan 2018
Target	http://testphp.vulnweb.com	/Mod_Rewrite_Shop/index.php	200	1159	17:04:15 30 Jan 2018
Target	http://testphp.vulnweb.com	/admin	301	386	17:01:02 30 Jan 2018
Target	http://testphp.vulnweb.com	/admin/	200	420	17:01:03 30 Jan 2018
Target	http://testphp.vulnweb.com	/categories.php	200	5433	17:01:11 30 Jan 2018

Discover Content

This function is used to discover contents and functionality which are not linked with visible content that you can browse or spider.

There are various techniques that the burp suite uses to discover content, which includes name guessing, web spidering, and extrapolation from naming conventions observed within the use of an application.

Control

This tab shows you the current status of the session. The **toggle button** represents whether the session is running or not, and it also allows you to pause and restart the session.

The following information is displayed about the progress of the discovery session:

- Number of requests made
- Number of bytes transferred in server responses
- Number of network errors
- Number of discovery tasks queued
- Number of spider requests queued
- Number of responses queued for analysis

Target

This option allows you to define or state the start directory of the content discovery session, and whether the files or directories should be targeted. The options that are available are as follows:

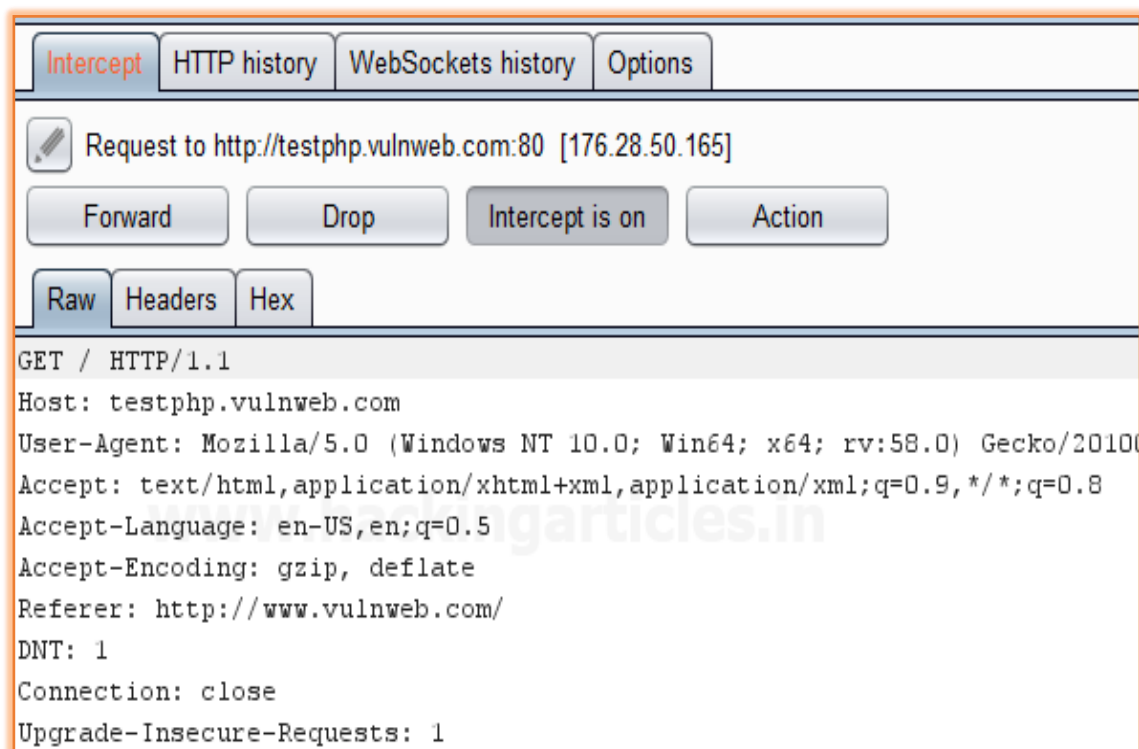
Start directory – This is the location where Burp suite is used to look for content. The items within this path and sub-directories are requested during the session.

Discover – This option can be used to determine whether the session will look for files or directories or both.

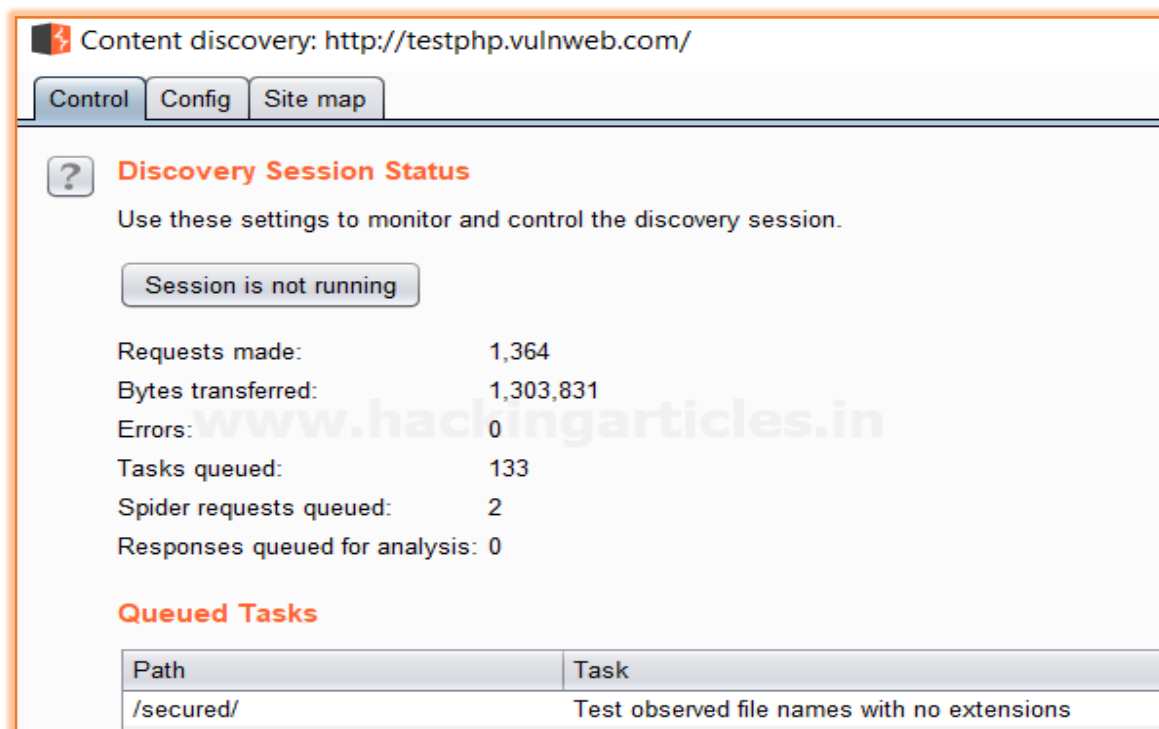
Site Map

The discovery session uses their own site map, showing all of the content which has been discovered within the defined scope. If you have configured your Burp suite to do so, newly discovered items can be added to Burp suite's main site map.

First, we have intercepted the request of the **vulnweb.com** which is a **demo lab** available over the internet which can be used for testing attacks. Then click on enter after writing the URL of the Vulnerable Web in your browser, then the burp suite will capture the request of the web page in the intercept tab.



Then **click** on **Action Tab** within the Burp suite, after that select the **Engagement tools** then click on **Content Discovery**. This will open a result window which will show the discovery session status and queued tasks which are related to the **URL** whose request has been captured which is the **Vulnerable Web** as shown in the image.



Schedule Task

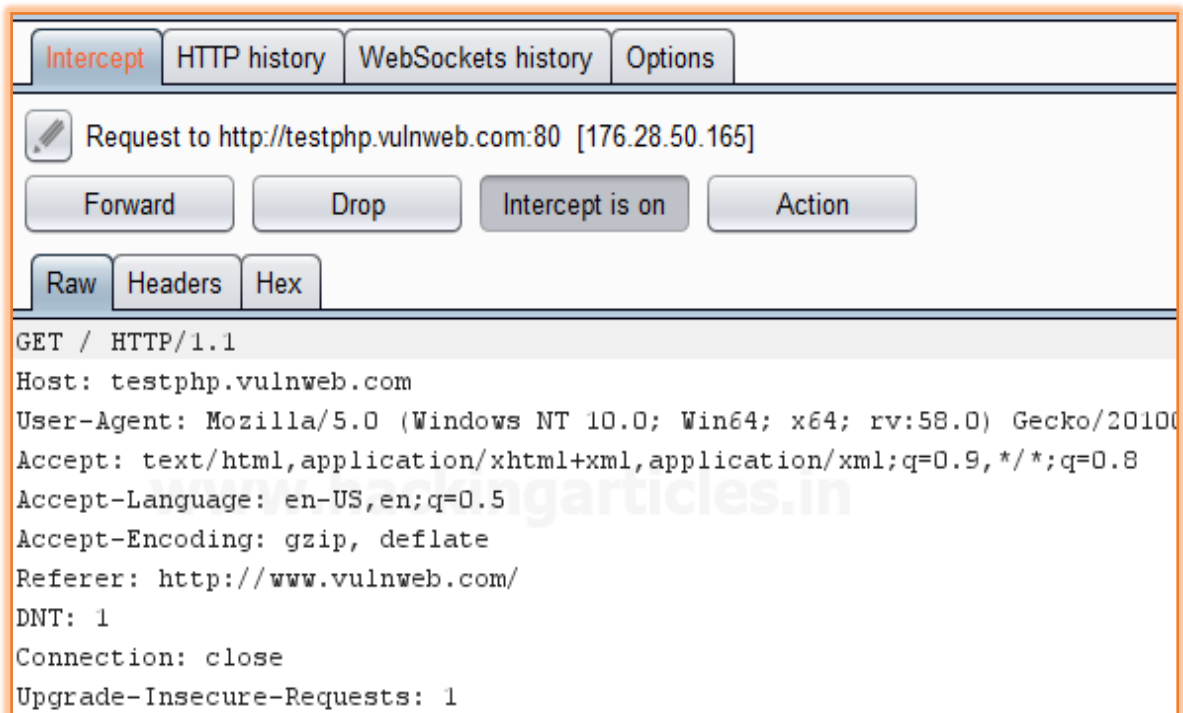
This function can be used to automatically start and stop certain tasks at defined times and intervals. We can use the task scheduler to start and stop certain automated tasks while you are not working, and to save your work periodically or at a specific time.

To make use of this function, select an HTTP request anywhere in Burp suite, or any part of the target site map, and choose "Schedule task" within "Engagement tools" in the context menu which can be seen by clicking right within Burp suite.

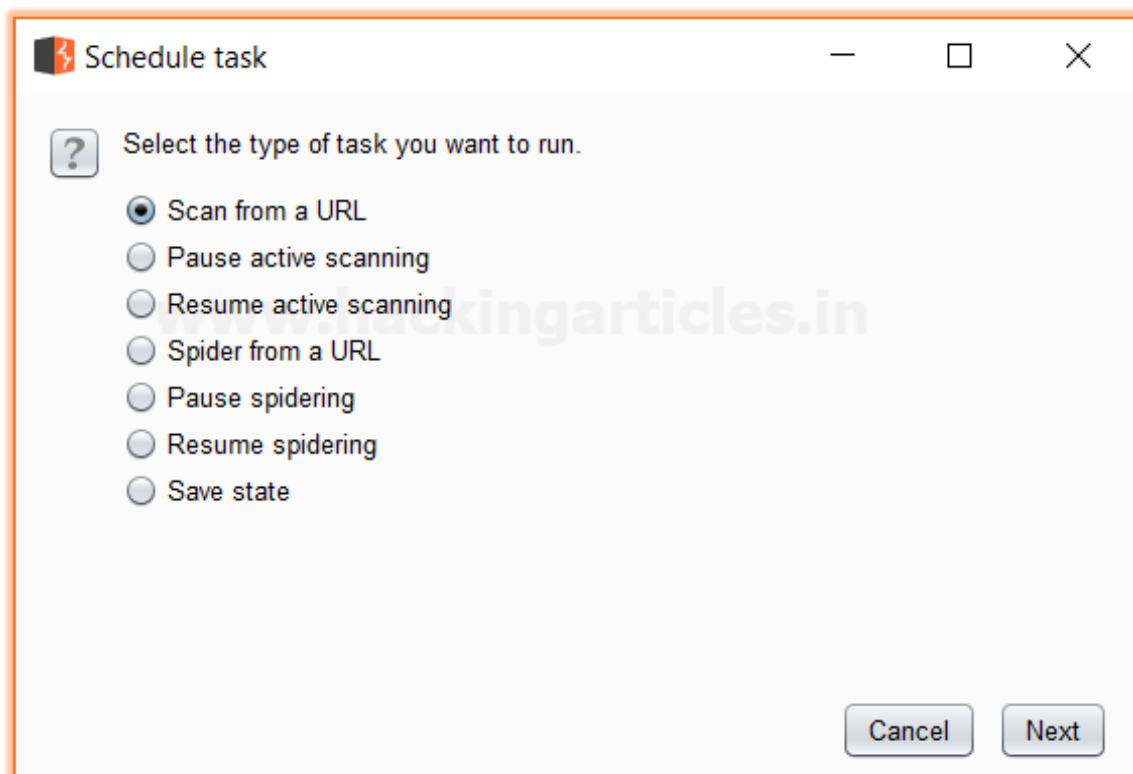
The types of task that are available within this function are as follows:

- Scan from a URL
- Pause active scanning
- Resume active scanning
- Spider from a URL
- Pause spidering
- Resume spidering
- Save state

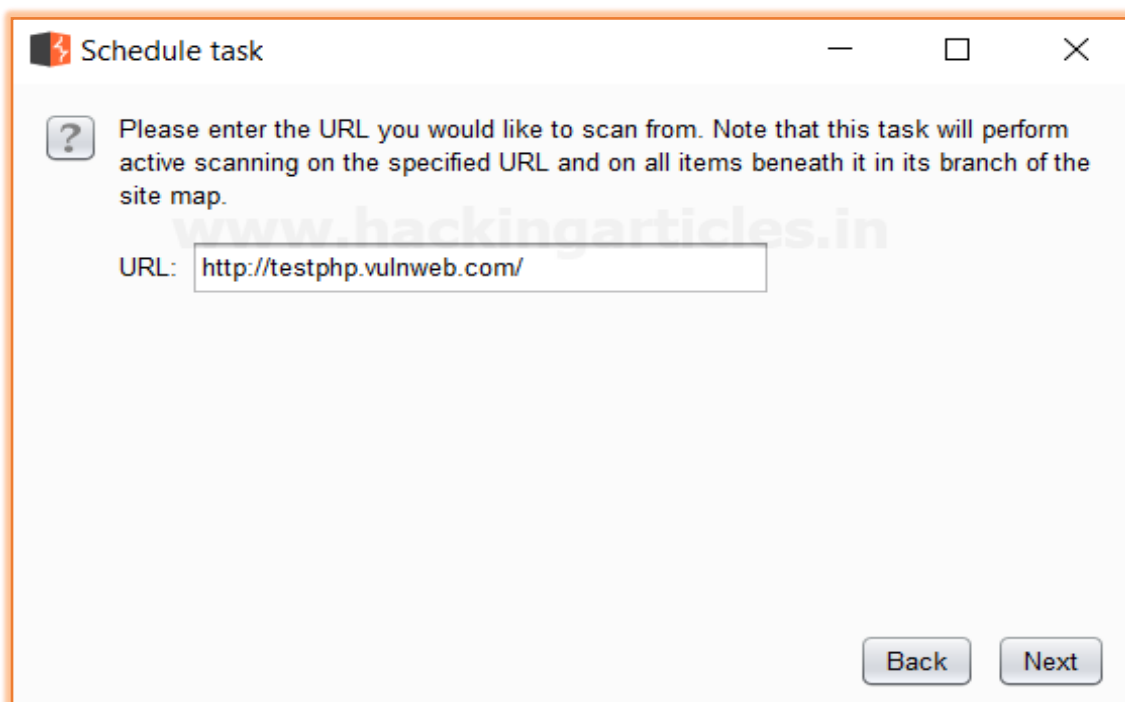
First, we have intercepted the request of the **vulnweb.com** which is a **demo lab** available over the internet which can be used for testing attacks. Then click on enter after writing the URL of the Vulnerable Web in your browser, then the burp suite will capture the request of the web page in the intercept tab.



Then **click** on Action Tab within the Burp suite, after that select the **Engagement tools** then click on **Schedule Task**. This will open a window of schedule task options where we have selected **Scan from a URL** option as shown in the image.



Then Click **Next** a window will open where we have to give the **URL** we want to scan its branches from the site map.



Then Click **Next** we see that the scanner tab of the burp suite is open which **scans** all the branches beneath the site map of the given **URL** which is seen in the **scan queue tab** as shown in the image which is related to the **URL** whose request has been captured which is the **Vulnerable Web** as shown in the image.

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options Use					
Issue activity Scan queue Live scanning Issue definitions Options					
#	Host	URL	Status	Issues	Req
1	https://www.google.com	/doodles/finder/	cancelled	2	50
2	http://testphp.vulnweb.com	/	25% complete	2	60
3	http://testphp.vulnweb.com	/admin	0% complete	2	34
4	http://testphp.vulnweb.com	/admin/	20% complete	3	70
5	http://testphp.vulnweb.com	/admin/create.sql	20% complete		71
6	http://testphp.vulnweb.com	/cgi-bin	20% complete		66
7	http://testphp.vulnweb.com	/images/	20% complete	3	64
8	http://testphp.vulnweb.com	/images/logo.gif	20% complete		66
9	http://testphp.vulnweb.com	/images/remark.gif	20% complete		71
10	http://testphp.vulnweb.com	/style.css	20% complete		58
11	http://testphp.vulnweb.com	/images	0% complete		35
12	http://testphp.vulnweb.com	/index.php	waiting		
13	http://testphp.vulnweb.com	/categories.php	waiting		
14	http://testphp.vulnweb.com	/AJAX/	waiting		
15	http://testphp.vulnweb.com	/AJAX/index.php	waiting		

Generate CSRF PoC

This function can be used to generate a proof-of-concept (PoC) cross-site request forgery (CSRF) attack for any given request.

To access this function, select a URL or HTTP request anywhere in the Burp suite, and choose "Generate CSRF PoC" within "Engagement tools" in the context menu which can be seen by clicking right within Burp suite.

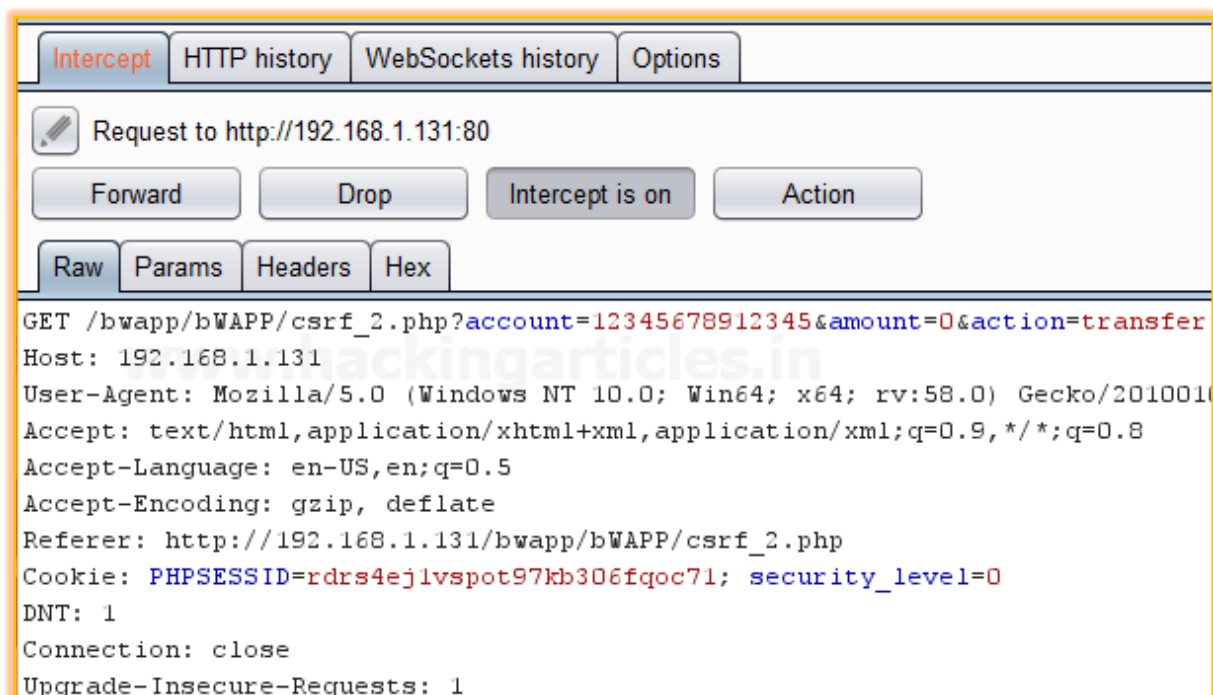
Let's start!!

First, we have intercepted the request of the **CSRF (transfer amount)** option in the **Bwapp LAB**, where we have given an **Account Number**.

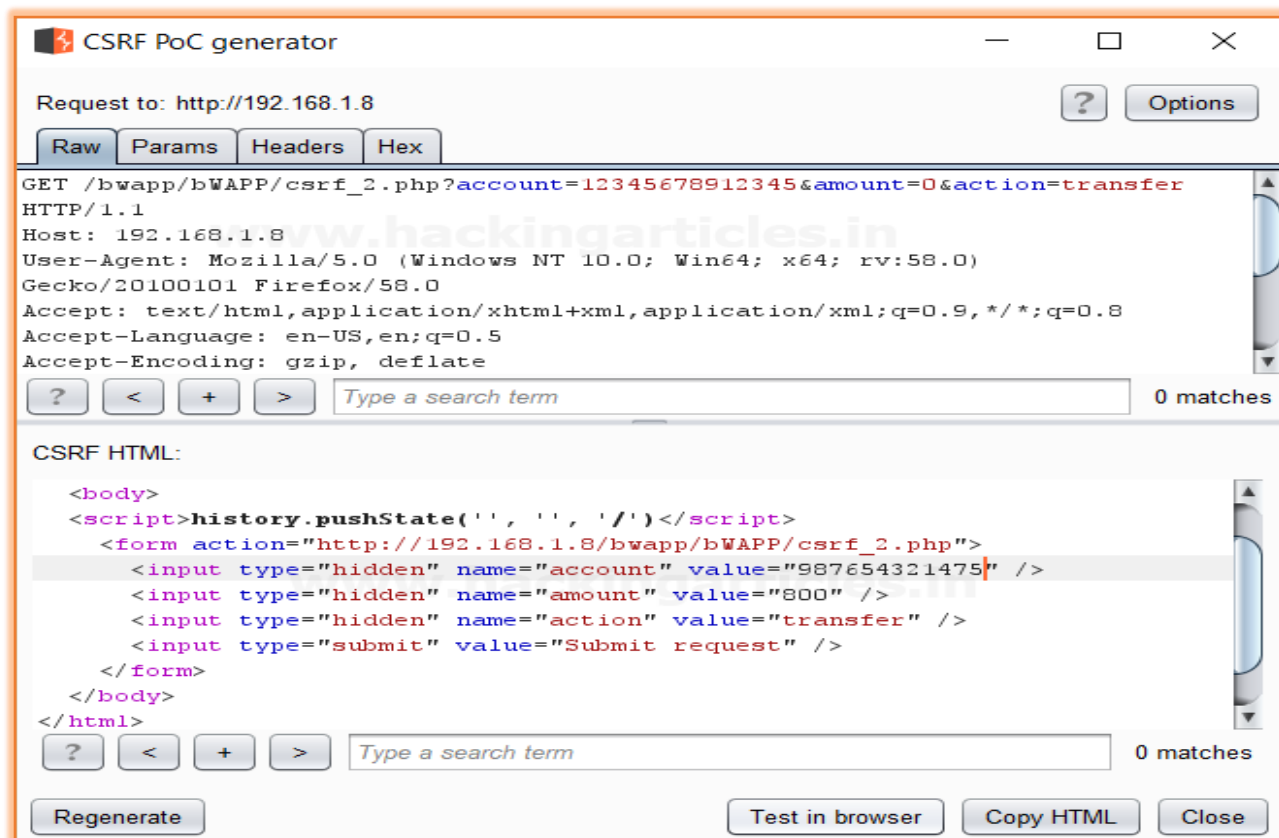


The screenshot shows a web application interface with a dark header containing navigation links: "Bugs", "Change Password", "Create User", "Set Security Level", and "R...". The main content area has a title "**CSRF (Transfer Amount)**" flanked by red slashes. Below the title, it displays "Amount on your account: 1000 EUR". There are two input fields: "Account to transfer:" with the value "12345678912345" and "Amount to transfer:" with the value "0". A "Transfer" button is located at the bottom of the form.

Then **click** on transfer, the burp suite will capture the request of the page in the **intercept tab**.



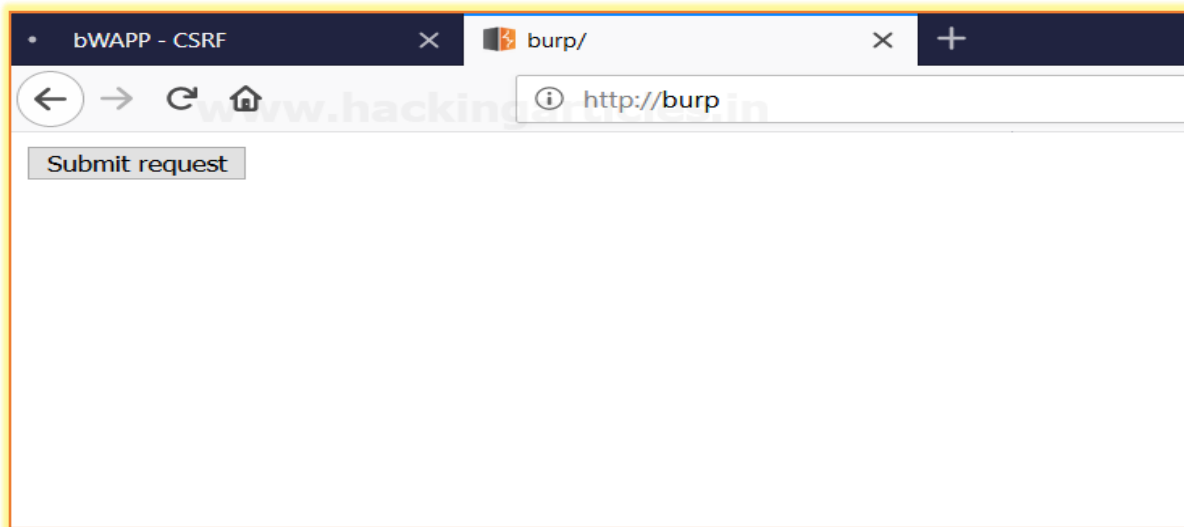
Then click on Action Tab within the Burp suite, after that select the **Engagement tools** then click on **Generate CSRF PoC**. This will open a window of the CSRF PoC where we made a change in **Account value** and **Amount value** in CSRF HTML code as shown in the image.



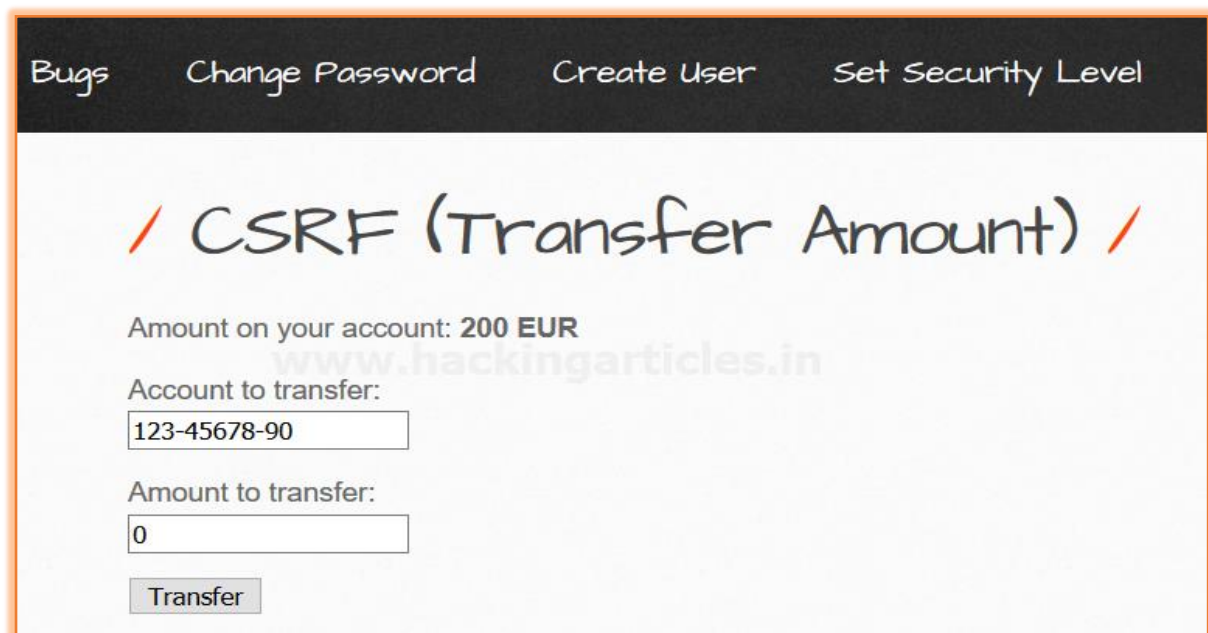
After making changes in the values click on **Test in Browser option** or **Copy HTML** this will open the window of Show response in the browser then click on **COPY**, and then paste it in the Browser and Press Enter as shown in the image.



We see a Submit request Button is seen in the browser after that click on it.



It appears to us that the amount is reduced as we have transferred the amount from the account by making changes in the CSRF HTML code as shown in the image.



Reference

<https://www.hackingarticles.in/engagement-tools-tutorial-burp-suite/>



About Us

About Us

“Simple training makes Deep Learning”

“IGNITE” is a worldwide name in IT field. As we provide high-quality cybersecurity training and consulting services that fulfil students, government and corporate requirements.

We are working towards the vision to “Develop India as a Cyber Secured Country”. With an outreach to over eighty thousand students and over a thousand major colleges, Ignite Technologies stood out to be a trusted brand in the Education and the Information Security structure.

We provide training and education in the field of Ethical Hacking & Information Security to the students of schools and colleges along with the corporate world. The training can be provided at the client’s location or even at Ignite’s Training Center.

We have trained over 10,000 + individuals across the globe, ranging from students to security experts from different fields. Our trainers are acknowledged as Security Researcher by the Top Companies like - Facebook, Google, Microsoft, Adobe, Nokia, Paypal, Blackberry, AT&T and many more. Even the trained students are placed into a number of top MNC's all around the globe. Over with this, we are having International experience of training more than 400+ individuals.

The two brands, Ignite Technologies & Hacking Articles have been collaboratively working from past 10+ Years with about more than 100+ security researchers, who themselves have been recognized by several research paper publishing organizations, The Big 4 companies, Bug Bounty research programs and many more.

Along with all these things, all the major certification organizations recommend Ignite's training for its resources and guidance.

Ignite's research had been a part of number of global Institutes and colleges, and even a multitude of research papers shares Ignite's researchers in their reference.

What We Offer



Ethical Hacking

The Ethical Hacking course has been structured in such a way that a technical or a non-technical applicant can easily absorb its features and indulge his/her career in the field of IT security.



Bug Bounty 2.0

A bug bounty program is a pact offered by many websites and web developers by which folks can receive appreciation and reimbursement for reporting bugs, especially those affecting to exploits and vulnerabilities.

Over with this training, an individual is thus able to determine and report bugs to the authorized before the general public is aware of them, preventing incidents of widespread abuse.



Network Penetration Testing 2.0

The Network Penetration Testing training will build up the basic as well advance skills of an individual with the concept of Network Security & Organizational Infrastructure. Thereby this course will make the individual stand out of the crowd within just 45 days.



Red Teaming

This training will make you think like an "Adversary" with its systematic structure & real Environment Practice that contains more than 75 practicals on Windows Server 2016 & Windows 10. This course is especially designed for the professionals to enhance their Cyber Security Skills



CTF 2.0

The CTF 2.0 is the latest edition that provides more advance module connecting to real infrastructure organization as well as supporting other students preparing for global certification. This curriculum is very easily designed to allow a fresher or specialist to become familiar with the entire content of the course.



Infrastructure Penetration Testing

This course is designed for Professional and provides an hands-on experience in Vulnerability Assessment Penetration Testing & Secure configuration Testing for Applications Servers, Network Devices, Container and etc.



Digital Forensic

Digital forensics provides a taster in the understanding of how to conduct investigations in order for business and legal audiences to correctly gather and analyze digital evidence.