# SSRF-Server Side Request Forgery

Briskinfosec Follow
Aug 19 · 4 min read


Server-Side Request Forgery (SSRF) refers to an attack, wherein an attacker can send a crafted request from a vulnerable web application. SSRF is mainly used to target internal systems behind

WAF (web application firewall), that are unreachable to an attacker from the external network. Additionally, it's also possible for an attacker to mark SSRF, for accessing services from the same server that is listening on the loopback interface address called (127.0.0.1).

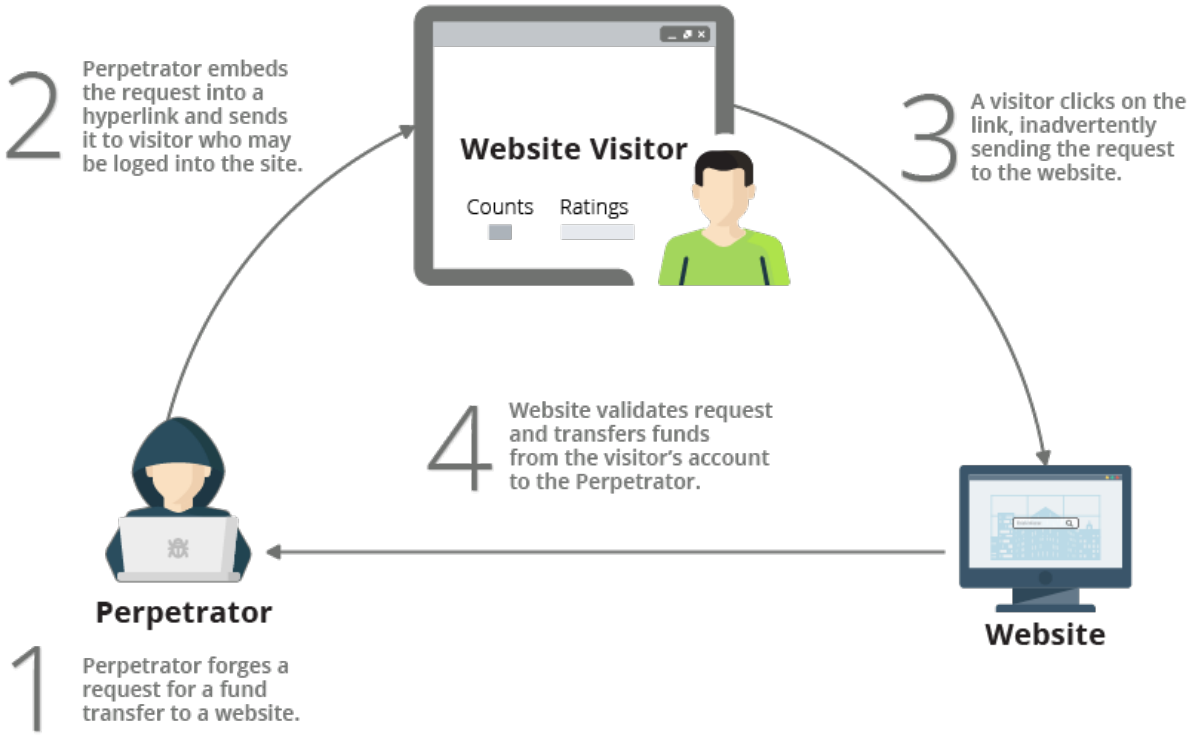
## CONTENTS:


- What is SSRF?
- A lucid example for SSRF
- SSRF Impacts
- Prevention from SSRF
- Conclusion
- How Briskinfosec helps you?
- Curious to read our case studies?
- Last but not the least


## A lucid example for SSRF:

Typically, Server Side Request Forgery (SSRF) occurs when a web application is making a request, where an attacker has full or partial control of the claim that is sent. A typical example is, when an attacker can control all, or a part of the URL to which the web application makes a request to some third-party services. Here, I had

captured the parameter of file= URL, and I've tried to perform this server-side forgery attack.




In the above figure, the perpetrator forges a request for a fund transfer website, and he embeds it into the visitor site. When the visitor logs the website for the transaction and clicks the perpetrator created link, it eventually redirects to the perpetrator's site, and the amount is transferred to his account.

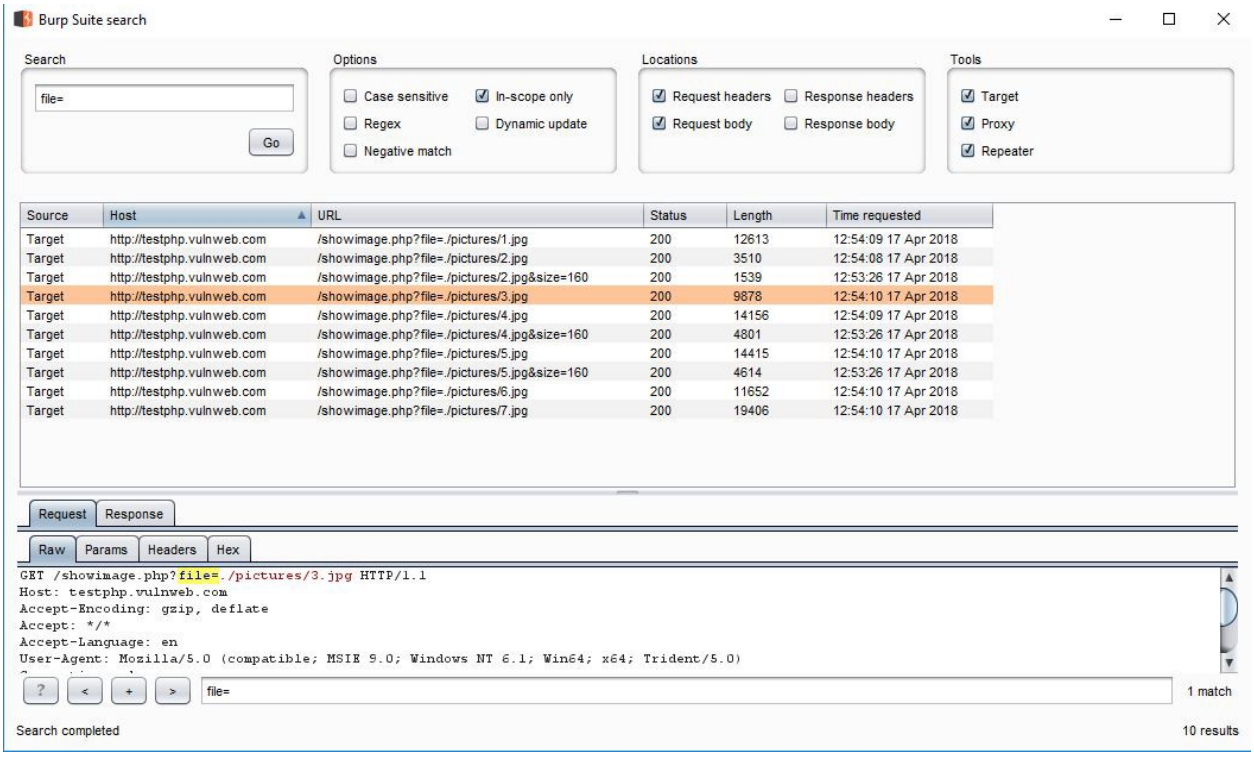
# SSRF IMPACTS:

By this attack, an attacker can gather information about ports, IP addresses, Remote Code Execution (RCE), and can also discover the IP addresses of servers running behind a reverse proxy, etc.

For example, I had tried SSRF attack on a testing site for your reference.

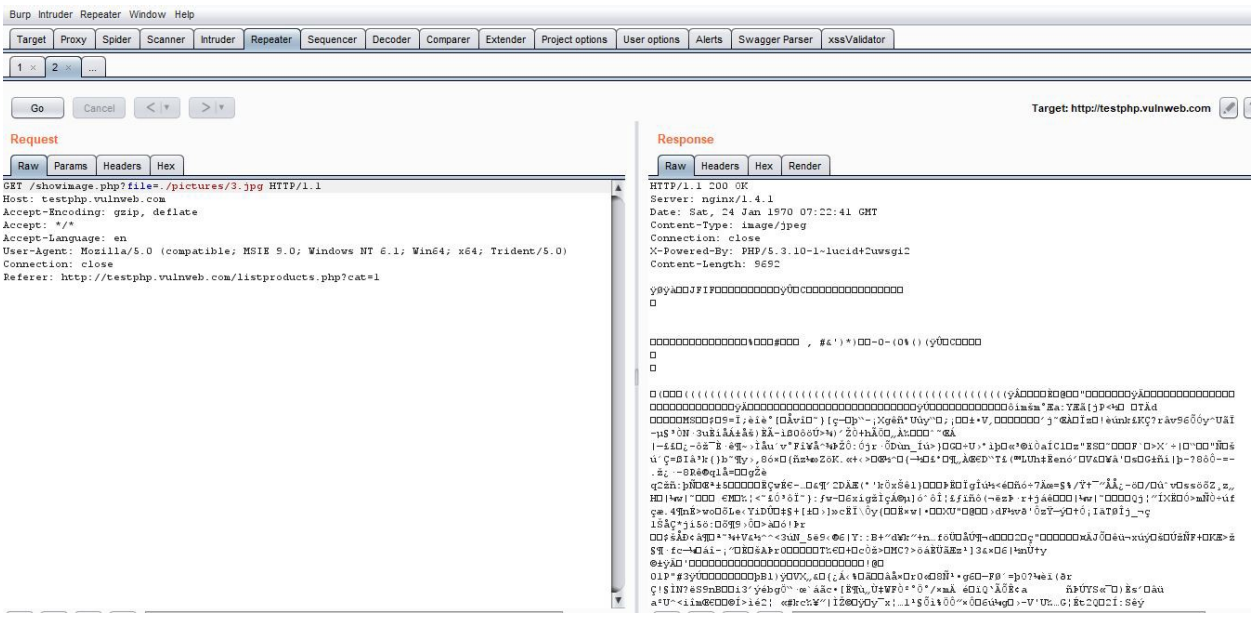
Vulnerable site: http://testphp.vulnweb.com/

# POC 1:



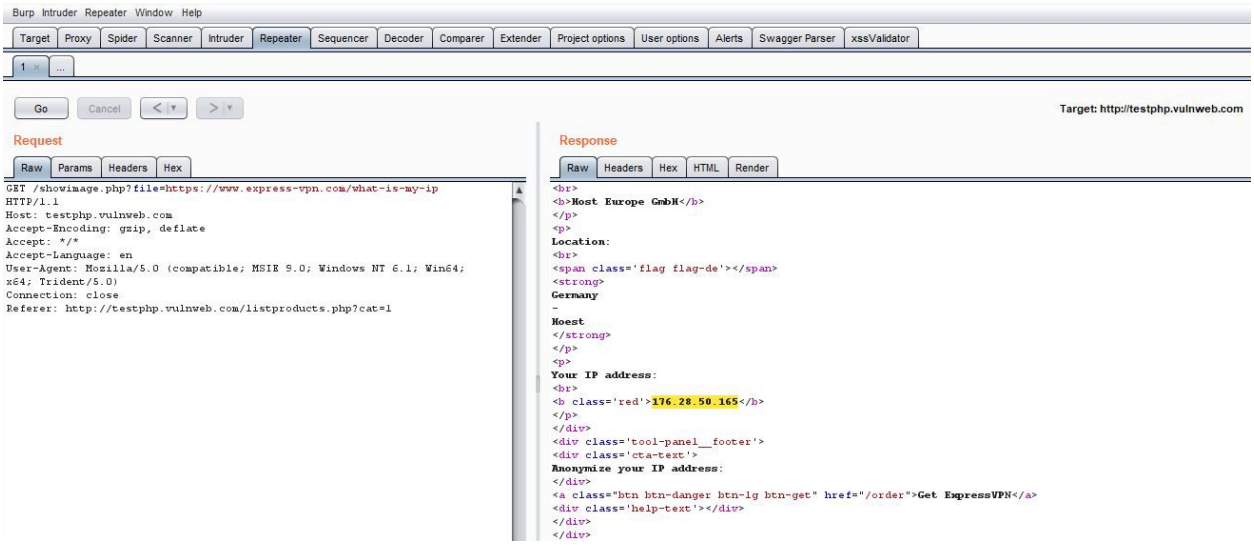
In Burp Suite, I checked for some different redirection parameter other than URL=, and in the search field, I've tried with various parameters. By using this parameter of , I've captured the request of the particular path and had sent it to the repeater.

## POC 2:



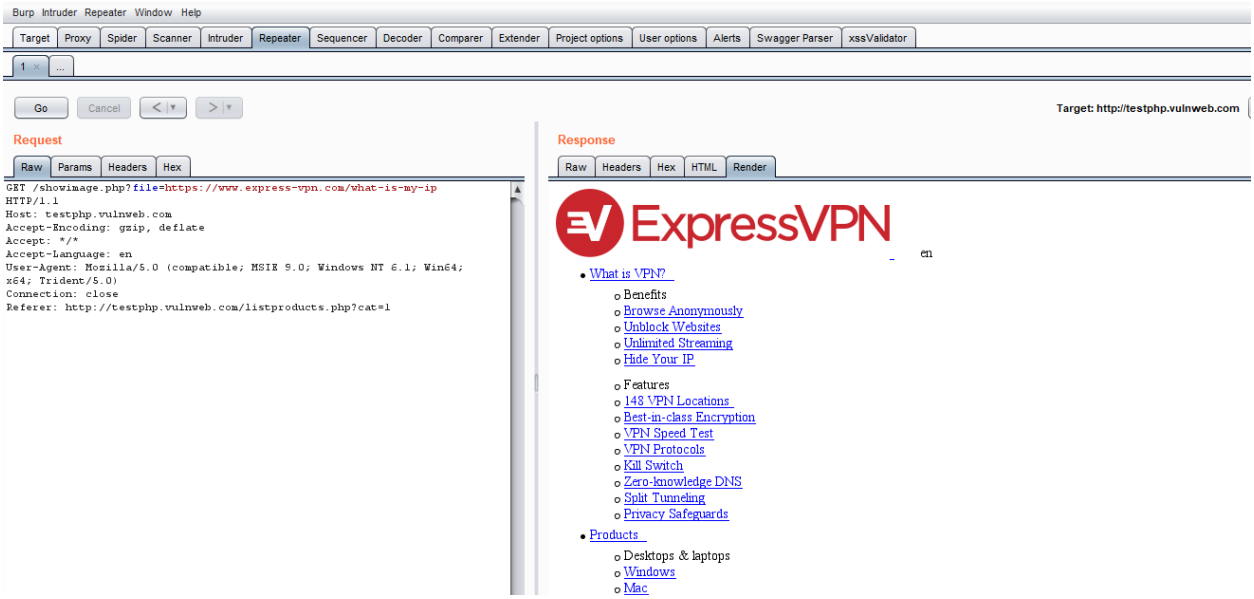

Request is captured from the search file in the repeater, and here in file feed, a .jpg file is available. Now, I had removed the file and entered a third party URL on file Redirected URL: https://www.expressvpn

# POC 3:




Once I click on Go to capture response, the response is changed to expessvpn.com and you can see the IP of the testphp.vulnweb.com. But in the render page, you can see the expressvpn.com site getting loaded as follows:

# POC 4:




# PREVENTION FROM SSRF:

- Generic error messages should be displayed to every client, as unhandled responses might end up in revealing sensitive information or data leakage about the server, when any other raw response or different parameter is used.
- URL schemes other than HTTP and HTTPS should be blacklisted. Instead, these two mentioned protocols should be whitelisted thereby blocking different schemes which are not in use like file:///, direct://, feed://, touch:// and FTP://, which might prove to be dangerous for SSRF.

# CONCLUSION:

Hence, the Server Side Request Forgery attack has been made from

the server side and the required web page has been redirected to some other web pages. To prevent such types of attacks, allow only the particular subdomains of the required web page and then whitelist the other web pages that are not in use.

## How Briskinfosec helps you?

To practically educate about these issues and to provide contemporary security quality, a competent cybersecurity firm is mandatory. Briskinfosec security professionals validate the input parameters of the incoming requests through effective security assessments. We scrutinize them and encumber those, if detected vulnerable. We also deliver you, noble notions of cyber awareness against both old and latest cyber threats, educating you to be cautious against such possible threats.

## Curious to read our Case studies?

Our case studies are one of the best totems of our security assessments quality. Our clients have always felt contented with our security assessments quality as we've always met their security requirements on time, with zero compromises. We have a vast collection of case studies, just take a look at them.

People check out for the recent and significant cyberattacks, to gain knowledge and sometimes, to check the affected companies. For

doing so, they've got to search spotlessly and at some point of time, they feel tiresome. But, Briskinfosec provides you an easy way to acknowledge the recent and significant cyberattacks, the impacts of them on respective organizations, the losses faced by them and all these are done in just one single report named as Threatsploit Adversary Report. Check them out and they'll surely be fulfilling.

*Originally published at https://www.briskinfosec.com.*