Guide to SSRF 🌐

The Basics

- Server Side Request Forgery (OWASP)
- SSRF: Web App Security Basics
- SSRF-Server Side Request Forgery
- What is Server-Side Request Forgery (SSRF)?
- SSRF: What is Server Side Request Forgery?
- Understanding the Web Vulnerability Server-Side Request Forgery (1/2)
- Exploiting the SSRF vulnerability (2/2)
- 3 Types of SSRF Attacks and How to Prevent Them
- SSRF

Server Side Request Forgery Prevention 🚫

- Server-Side Request Forgery Prevention Cheat Sheet

A powerful tool: SSRFmap, SSRF bug with automation 🛠️

- SSRFmap
- tomnomnom/gf
- tomnomnom/qsreplace
- ffuf
- gau

- waybackurls
- quickpress
- automate SSRF wordpress and XMLRPC finder
- Finding SSRF by Full Automation
- Bug Bounty tip Automating SSRF
- ssrf-sheriffhggi

SSRF Techniques 🛡️

- SSRF Techniques

Writeups ✍️

- An unknown Linux secret that turned SSRF to OS Command injection
- Story Behind Sweet SSRF
- GITLAB — Just another SSRF issue.
- Blind SSRF Chains
- A New Era of SSRF Trending Programming Languages! - BlackHat 2017
- Blind SSRF Chains
- $10000 Facebook SSRF (Bug Bounty)
- 31k$ SSRF in Google Cloud Monitoring led to metadata exposure
- SSRF (Server Side Request Forgery) worth $4,913 | My Highest Bounty Ever !

- Blind SSRF - The Hide & Seek Game
- How i found 3 SSRF in one day on different bug bounty targets
- Exploiting: SSRF For Admin Access
- Unauthenticated Full-Read SSRF in Grafana CVE-2020-13379
- My First Bug: Blind SSRF Through Profile Picture Upload
- A tale of my first ever full SSRF bug
- How I Chained 4 vulnerabilities on GitHub Enterprise, From SSRF Execution Chain to RCE!
- Story of a 2.5k Bounty — SSRF on Zimbra Led to Dump All Credentials in Clear Text
- From . in regex to SSRF — part 1
- From . in regex to SSRF — part 2
- (SSRF) ON LYFT
- How I made $31500 by submitting a bug to Facebook
- The road from sandboxed SSTI to SSRF and XXE
- Exploiting SSRF in RethinkDB
- Blind SSRF - Sentry Misconfiguration
- Exploiting an SSRF: Trials and Tribulations
- Blind SSRF exploitation
- 31k$ SSRF in Google Cloud Monitoring

- Tale of 3 vulnerabilities to account takeover!
- An unknown Linux secret that turned SSRF to OS Command injection
- SSRF inside Google production network
- Pivoting from blind SSRF to RCE with HashiCorp Consul
- Hunting Headers for SSRF
- WRITE UP – GOOGLE VRP N/A: SSRF BYPASS WITH QUADZERO IN GOOGLE CLOUD MONITORING
- Escalating SSRF to RCE
- GITLAB — Server Side Request Forgery in “Project Import” page.
- SSRF’s up! Real World Server-Side Request Forgery (SSRF)
- SSRF - Server Side Request Forgery (Types and ways to exploit it) Part-1
- Weaponizing BURP to work as an evil SSRF Confluence Server.
- Google VRP SSRF in Google Cloud Platform StackDriver
- Vimeo upload function SSRF
- SSRF via FFmpeg HLS processing
- My First SSRF Using DNS Rebinding
- BugBounty | A Simple SSRF
- ssrf reading local files
- An Accidental SSRF Honeypot in Google Calendar

- Gain adfly SMTP access with SSRF via Gopher Protocol
- SVG XLink SSRF fingerprinting libraries version
- Server Side Request Forgery(SSRF){port issue hidden approch }
- The journey of Web Cache + Firewall Bypass to SSRF to AWS credentials compromise!
- Ssrf to Read Local Files and Abusing the AWS metadata
- From SSRF To RCE in PDFReacter
- SSRF vulnerability via FFmpeg HLS processing
- Escalating SSRF to RCE
- Vimeo SSRF with code execution potential.
- Unauthenticated Blind SSRF in Oracle EBS
- $1.000 SSRF in Slack
- Exploiting SSRF in AWS Elastic Beanstalk

HackerOne Reports 💻

- SSRF in imgur video GIF conversion
- Full Read SSRF on Gitlab's Internal Grafana
- SSRF protection bypass
- SSRF on project import via the remote_attachment_url on a Note

- Blind SSRF on debug.nordvpn.com due to misconfigured sentry instance
- Blind SSRF on errors.hackerone.net due to Sentry misconfiguration
- SSRF PDF documentconverterws
- Blind SSRF on https://labs.data.gov/dashboard/Campaign/json_status/ Endpoint
- SSRF In Get Video Contents
- SSRF in webhooks leads to AWS private keys disclosure
- SSRF - RSS feed, blacklist bypass (IP Formatting)
- SSRF
- SSRF in CI after first run
- SSRF in Exchange leads to ROOT access in all instances
- SSRF in api.slack.com, using slash commands and bypassing the protections.

PayloadsAllTheThings / Server Side Request Forgery / 🚀

- PayloadsAllTheThings / Server Side Request Forgery