Forum Response

In a traditional mainstream SSRF attack as in your example the hacker would trigger the remote server to make a connection to internal services within the perimeter of the infrastructure of the host. Or they would try to force the server to connect to external systems in order to leak sensitive data such as authorization tokens, usernames, passwords etc

One of the more interesting ways a SSRF can be leveraged it to use a SSRF weakness to attack the server itself that is hosting the application this involves forcing the application to make a request back to itself via the loopback network address (127.0.0.1 or localhost) as these addresses and hostnames would resolve back to the local device. An example of how this exploit cloud work is an application may query locally hosted REST API endpoints via a HTTP request. The attacker could try to visit the API endpoints directly. But these may be secured behind application firewalls and Access control Lists (ACLs) preventing accesses from external addresses.

If the request came from the local machine the access controls and firewall rules would be bypassed as the request would appear to come from a trusted internal host
References

Hacker-One Reports https://github.com/reddelexc/hackerone-reports/blob/master/tops_by_bug_type/TOPSSRF.md [Accessed 21.03.2022]
Calzavara Stefano (https://secgroup.dais.unive.it/wp-content/uploads/2020/03/more_server.pdf)
OWSAP https://cheatsheetseries.owasp.org/cheatsheets/Server_Side_Request_Forgery_Prevention_Cheat_Sheet.html [Accessed 21.03.2022]