
A 10:2021: Server-Side
Request Forgery (SSRF)

A10:2021: SSRF

Server-Side Request Forgery (SSRF) flaws occur whenever a web application fetches a remote resource without validating the user-supplied URL

A10:2021: SSRF

Web applications can trigger requests between HTTP servers to fetch remote resources such as software updates or to import meta data.

2 responses to “How to Start a WordPress Blog – The Complete Guide”

1.  *Lynn Creger* says:
   March 8, 2021 at 2:50 am Edit

   Well explanation about starts a WordPress blog. You have covered all the necessary points in this article. That’s why it is easy to understand for any new users who will start blogging. Thanks for sharing this valuable article.

   Reply
2.  John Barry says:
   October 29, 2022 at 3:57 am Edit

   Great article. You can read more about this here – *https://mashable.com/archive/russian-ads*

   Reply

Leave a Reply

A10:2021: SSRF

- Used to gain access to sensitive internal data
- Can be used to launch DDoS attacks

A10:2021: SSRF

SSRF exploits could also be used to launch DDoS attacks against a third party website by using the vulnerable server.

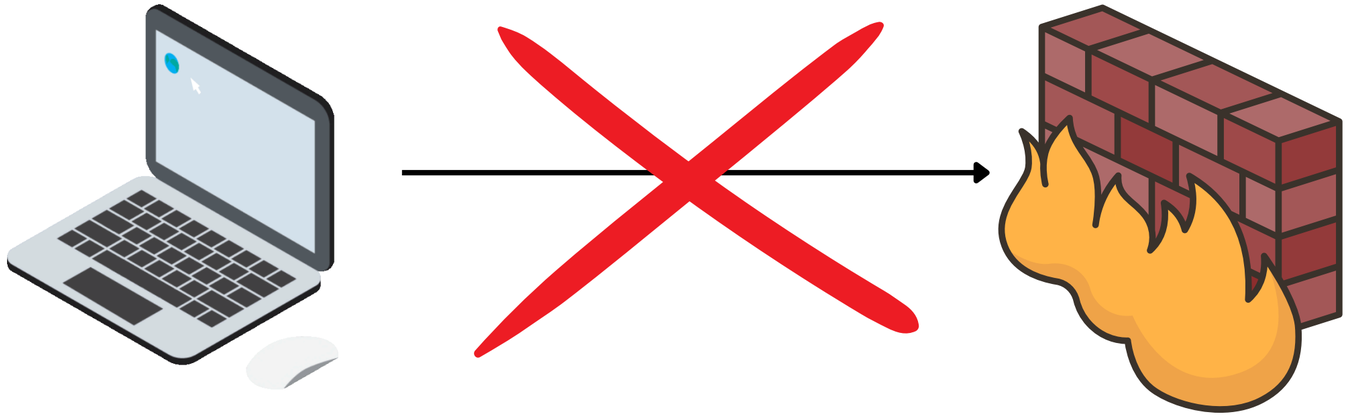
A10:2021: SSRF

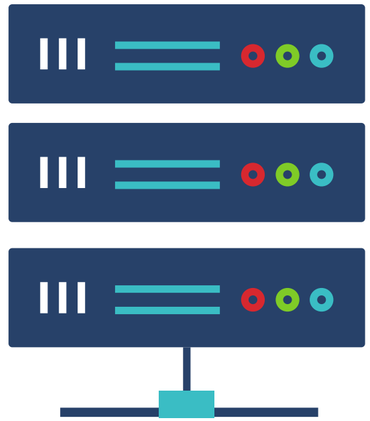
By spamming the vulnerable server with requests to fetch meta data from a third party website, the attacker can overwhelm the third party website while hiding behind the vulnerable web server.

A10:2021: SSRF

In a typical SSRF attack, the attacker might cause the server to make a connection to internal-only services within the company infrastructure. In other cases, they may be able to force the server to connect to arbitrary external systems, potentially leaking sensitive data such as authorization credentials.

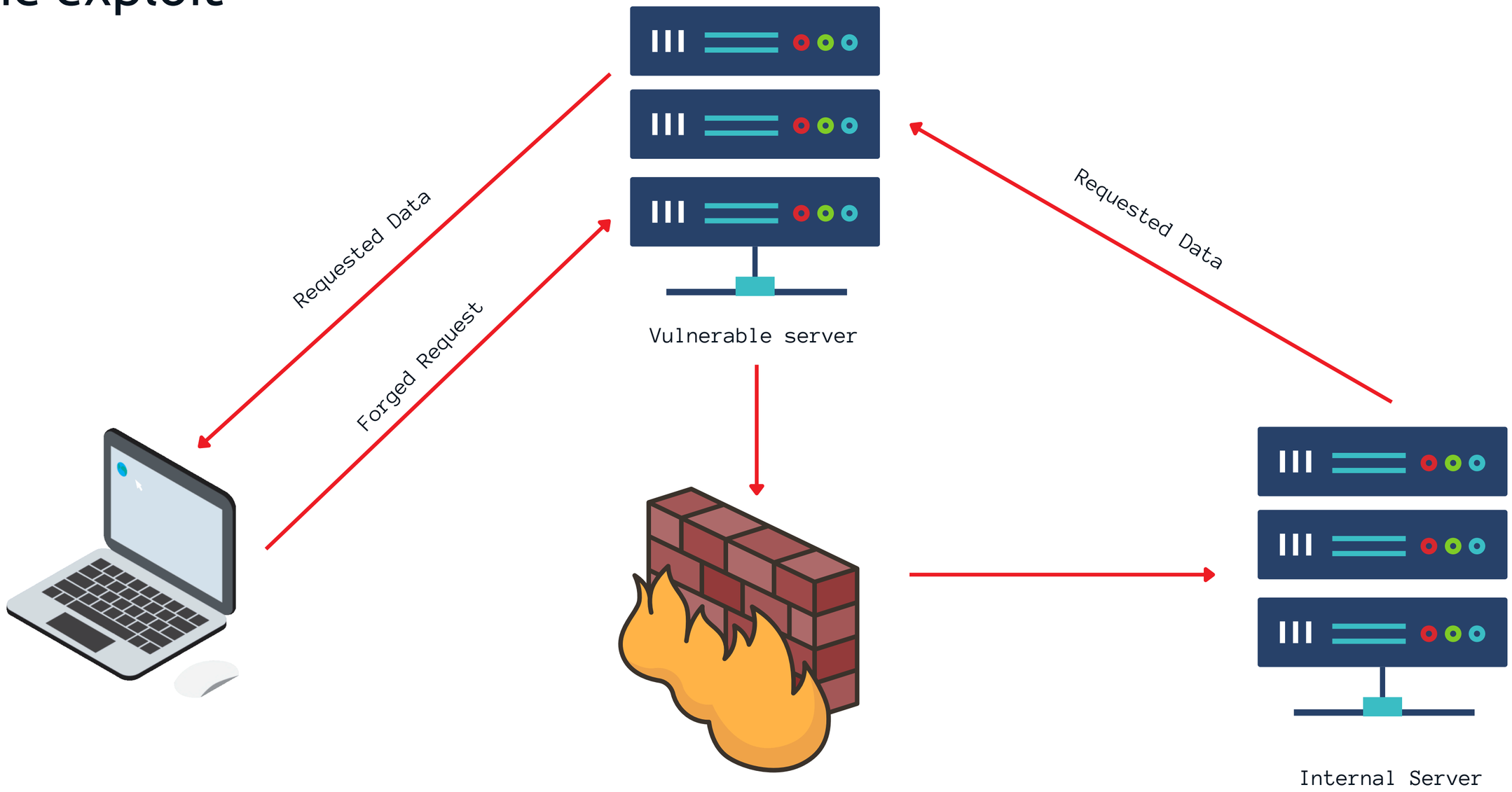
What happens if an attacker sends direct requests to access an internal server?





Internal Server

The exploit


Requested Data
Forged Request
Vulnerable server
Requested Data
Internal Server