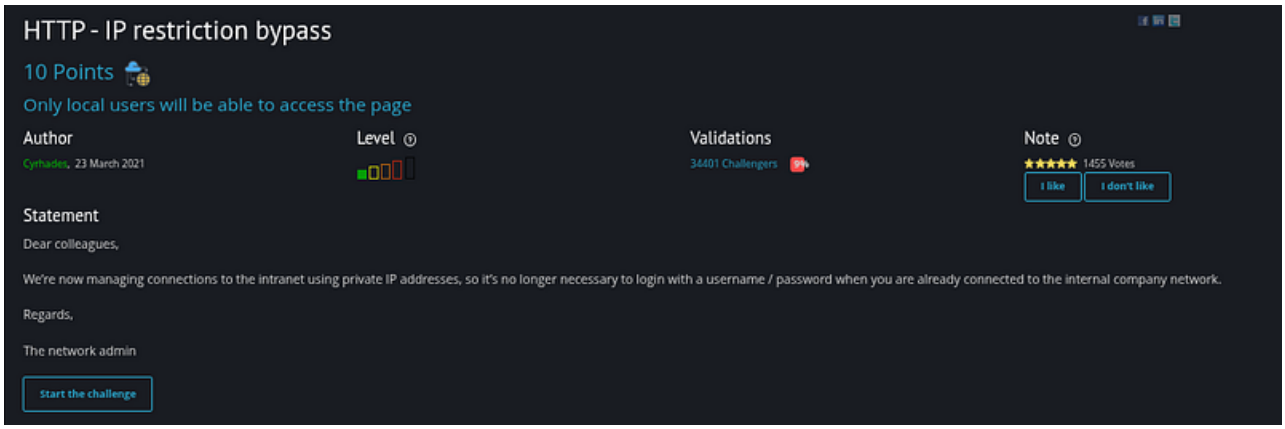
# Root-Me Write-up: HTTP IP Restriction-Bypass




## Challenge Statement

**Dear colleagues,**

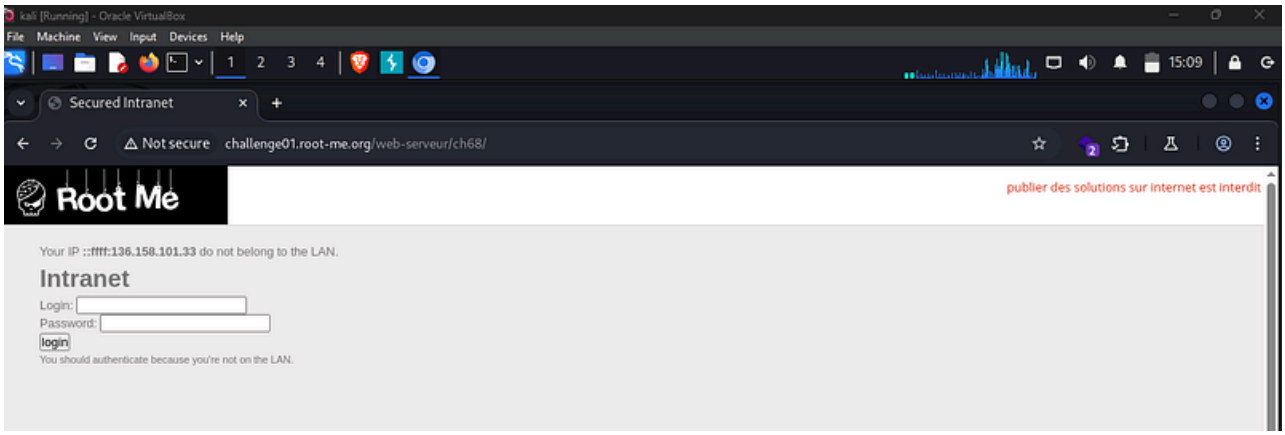
We’re now managing connections to the intranet using private IP addresses, so it’s no longer necessary to log in with a username and password when you are already connected to the internal company network.

**Regards,**
The Network Administrator

---

## Objective

The application restricts access to **internal or private IP addresses only**. The goal is to bypass this IP-based access control and obtain the validation password.




---

# Initial Analysis

The server relies on IP-based restrictions to determine whether a request originates from an internal network. In many web environments, upstream proxies or load balancers pass client IP information to the backend server through HTTP headers.

Common headers that may influence IP validation include:

- X-Forwarded-For
- X-Original-URL
- X-Rewrite-URL

If the backend server trusts these headers without proper validation, an attacker may spoof their IP address.

---

# Exploitation Technique

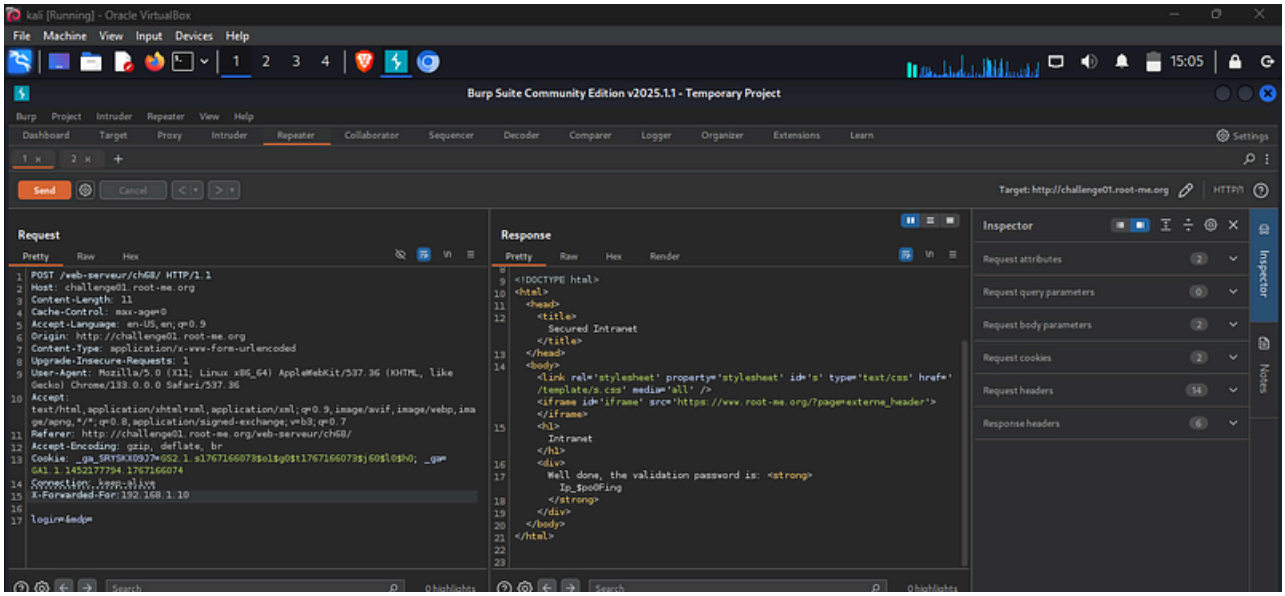
The application was found to trust the X-Forwarded-For header when determining the client's IP address.

By manually adding this header to the request and supplying a **private/internal IP address**, the server incorrectly treated the request as originating from the internal network.

# Injected Header

X-Forwarded-For: <private_ip>

This request was sent using **Burp Suite**.




---

# Result

After forwarding the modified request, the server responded with the validation message:

> ***Well done, the validation password is:*** *Ip_$pooFing*

---

# Flag

Ip_$pooFing

By Alexander Sapo on January 6, 2026.

Canonical link

Exported from Medium on February 7, 2026.