

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

The screenshot shows a challenge card for 'HTTP - IP restriction bypass'. It has a dark background with white text. At the top left is the title 'HTTP - IP restriction bypass' and '10 Points' with a globe icon. Below that is the statement 'Only local users will be able to access the page'. To the right are sections for 'Author' (Cyrhades, 23 March 2021), 'Level' (Easy, represented by a green bar), 'Validations' (34401 Challengers), 'Note' (1455 Votes with a star rating), and 'I like'/'I don't like' buttons. The main body contains a 'Statement' from 'The network admin' and a 'Regards' section. A blue 'Start the challenge' button is at the bottom.

Challenge Statement

Dear colleagues,

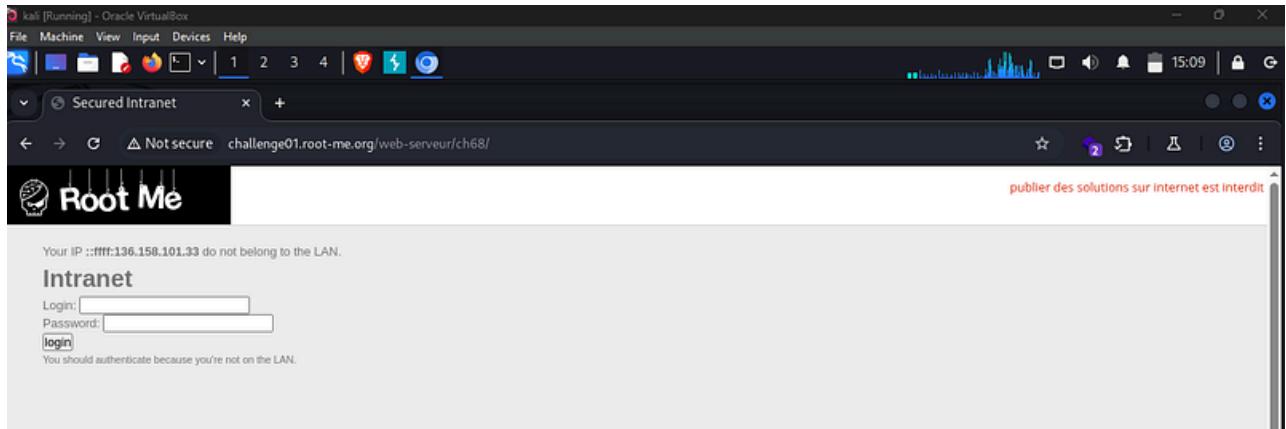
We're now managing connections to the intranet using private IP addresses, so it's no longer necessary to log in with a username and password when you are already connected to the internal company network.

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

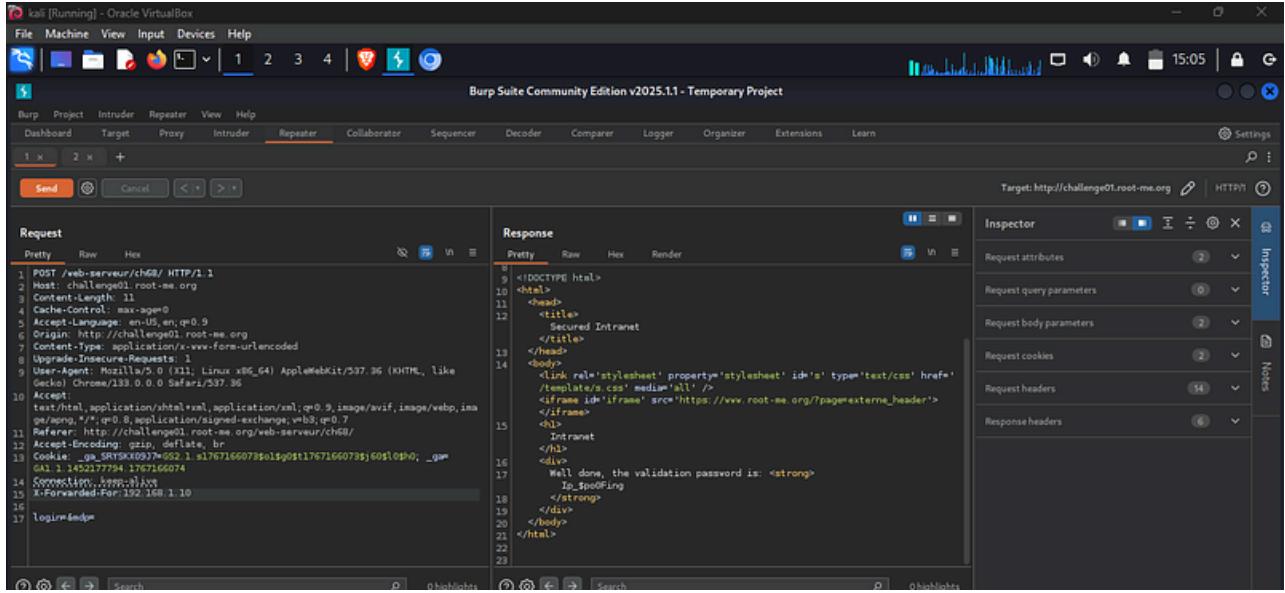
The application was found to trust the X-Forwarded-For header when determining the client's IP address.

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_Spoofing

By [Alexander Sapo](#) on [January 6, 2026](#).

Canonical link

Exported from [Medium](#) on February 7, 2026.