

**HTTP TRAFFIC ANALYSIS AND DOMAIN  
INVESTIGATION USING WIRESHARK,  
VIRUSTOTAL, AND WHOER.NET**

**BY**

**SOMKENE RICHARD**

**21st SEPTEMBER, 2024**

## **EXECUTIVE SUMMARY**

An analysis of network traffic on <http://altoromutual.com> identified a critical security risk. This analysis, utilizing Wireshark for packet capture, revealed that login credentials are being transmitted in plain text.

This lack of encryption, due to the use of an unencrypted HTTP protocol, exposes user data to potential interception by a threat actor.

## **INTRODUCTION**

Encryption plays a crucial role in keeping data safe from unauthorized access and interception. Many websites now use HTTPS to secure and encrypt information entered by users. However, attackers can still create fake versions of these sites using the less secure HTTP protocol. When users unknowingly interact with these fraudulent sites, their login details and other sensitive information can be exposed and exploited by cybercriminals.

## **TOOLS**

1. Wireshark
2. Whoer.net
3. Abuseipdb
4. Pen and paper

# ANALYSIS

The image shows a Wireshark packet capture of an HTTP login request. The packet list pane at the top shows a series of packets, with packet 1720 selected. The packet details pane shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. The Hypertext Transfer Protocol section shows the request line and the body, which is an HTML Form URL Encoded application/x-www-form-urlencoded. The body contains the following data:

```
uid=admin
passw=admin
btnsubmit=Login
```

The packet bytes pane at the bottom shows the raw data of the packet, which is a hexadecimal representation of the packet bytes.

From the image above, the login details could be seen as a plaintext under "uid" and "passw" due to the HTTP protocol

https://www.virustotal.com/gui/ip-address/65.61.137.117/detection

65.61.137.117

2 / 94  
Community Score

2/94 security vendors flagged this IP address as malicious

65.61.137.117 (65.61.136.0/22)  
AS 33070 (RMH-14)

US  
Last Analysis Date  
10 days ago

Reanalyze Similar Graph API

DETECTION DETAILS RELATIONS COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis Do you want to automate checks?

Criminal IP	Malicious	SOCradar	Malware
Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	AlLabs (MONITORAPP)	Clean
AlienVault	Clean	alphaMountain.ai	Clean

on virustotal, the IP address of the domain was flagged malicious by 2 security vendors

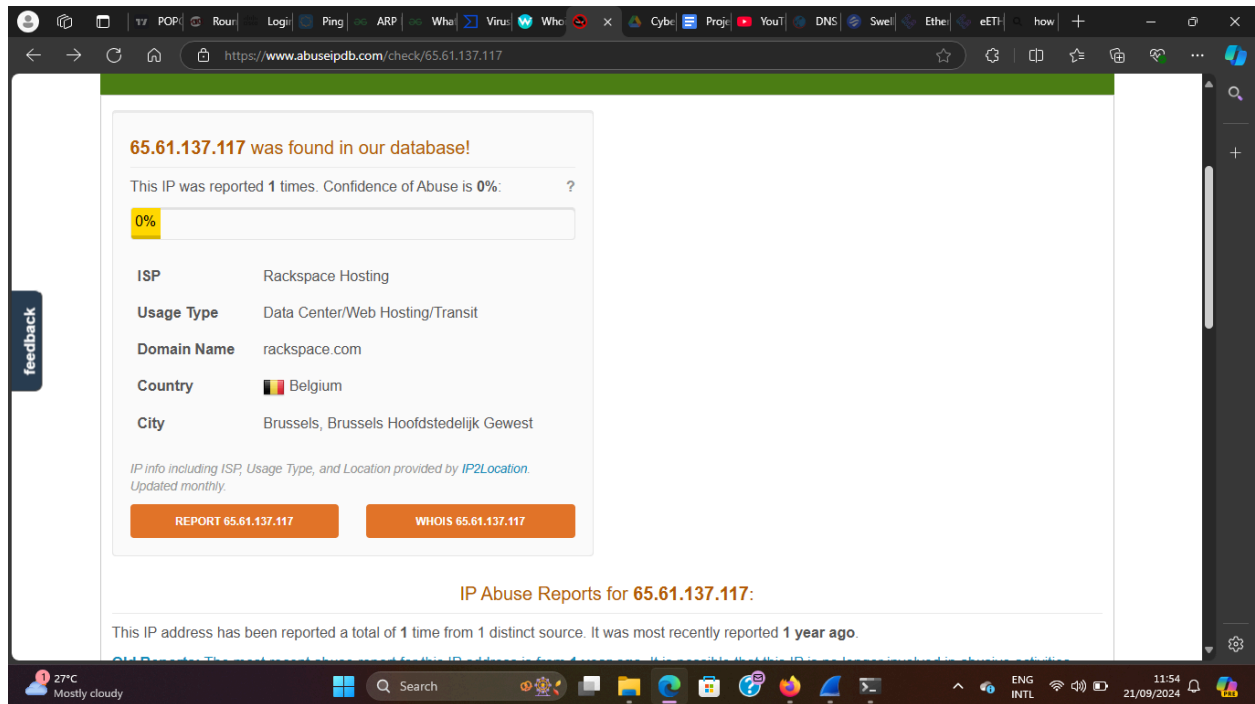
https://whoer.net/checkwhois

WHOER My IP VPN Download Antidetect Browser AMLcheck Services Help Buy VPN now

IP address: 65.61.137.117

Location:	United States (US), N/A	Hostname:	N/A → N/A
Region:	N/A	IP range:	65.61.128.0 - 65.61.191.255
City:	N/A	ISP:	Rackspace Hosting
ZIP:	N/A	Organization:	Rackspace Hosting
Blacklist:	Yes ()	Zone:	America/Chicago
TOR:	No	Local:	Sat Sep 21 2024 05:47:17 GMT-0500 (CDT)

On Whoer.net, the location of the domain could be seen including the ISP and organization



Further scanning on abuseipdb shows that the IP address of the domain has been reported once about a year ago.

## RECOMMENDATIONS

Based on my analysis, I'd recommend the following:

1. Temporarily disabling the login functionality on the website until a secure HTTPS connection is implemented. This would prevent further exposure of user credentials.
2. To address the malicious flagging and reports of the IP address, the domain owner(s) should investigate and resolve the underlying security issues that are causing these flags.
3. Implement a security awareness training program to educate users on how to identify and avoid insecure websites (HTTP) and encourage safe online practices.

## CONCLUSION

The domain was found to be insecure, as it exposes users' login credentials, making them vulnerable to interception by threat actors. This issue can be addressed by using secure domains that implement HTTPS encryption, which significantly reduces the risk of data exposure compared to HTTP connections.