

**Bolt**



**Bolt**  
A hero is unleashed

# writeup

--ran my custom recon script and found open ports 22, 80, and 8000 and an index.html page  
--went to **http://<IP-address>** and looked through the source code and found the following credentials:  
**bolt:boltadmin123**

--found version **Bolt 3.7.1** after login in at **http://<IP-address>/bolt**, and investigating the dashboard

--searched exploit-db and found the exploit number 48296  
--searched metasploit for Bolt vulnerabilities and found the right one **exploit/unix/webapp/bolt\_authenticated\_rce**  
--changed all the options to following:  
**LHOST: <MY-IP-address>**  
**LPORT: 4444**  
**RHOST: <Remote-Machine-IP-address>**  
**USERNAME: bolt**  
**PASSWORD: boltadmin123**

--inside of **msfconsole** I ran **run** command and got a root shell  
--found **flag.txt** in **/home** directory and ran **cat flag.txt** to get the flag:  
**THM{wh0\_d035nt\_l0ve5\_b0l7\_r1gh7??}**

# auto-recon-scan

## ----- NMAP-ALL-Ports -----

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 2048 f3:85:ec:54:f2:01:b1:94:40:de:42:e8:21:97:20:80 (RSA)

| 256 77:c7:c1:ae:31:41:21:e4:93:0e:9a:dd:0b:29:e1:ff (ECDSA)

| 256 07:05:43:46:9d:b2:3e:f0:4d:69:67:e4:91:d3:d3:7f (ED25519)

80/tcp open http Apache httpd 2.4.29 ((Ubuntu))

| http-methods:

| Supported Methods: GET POST OPTIONS HEAD

| http-server-header: Apache/2.4.29 (Ubuntu)

| http-title: Apache2 Ubuntu Default Page: It works

8000/tcp open http (PHP 7.2.32-1)

| fingerprint-strings:

| FourOhFourRequest:

| HTTP/1.0 404 Not Found

| Date: Thu, 13 Aug 2020 13:51:26 GMT

| Connection: close

| X-Powered-By: PHP/7.2.32-1+ubuntu18.04.1+deb.sury.org+1

| Cache-Control: private, must-revalidate

| Date: Thu, 13 Aug 2020 13:51:26 GMT

| Content-Type: text/html; charset=UTF-8

| pragma: no-cache

| expires: -1

| X-Debug-Token: 8f3d84

| <!doctype html>

| <html lang="en">

| <head>

| <meta charset="utf-8">

| <meta name="viewport" content="width=device-width, initial-scale=1.0">

| <title>Bolt | A hero is unleashed</title>

| <link href="https://fonts.googleapis.com/css?family=Bitter|Roboto:400,400i,700" rel="stylesheet">

| <link rel="stylesheet" href="/theme/base-2018/css/bulma.css?8ca0842ebb">

| <link rel="stylesheet" href="/theme/base-2018/css/theme.css?6cb66bfe9f">

| <meta name="generator" content="Bolt">

| </head>

| <body>

| href="#main-content" class="vis

| GetRequest:

| HTTP/1.0 200 OK

| Date: Thu, 13 Aug 2020 13:51:25 GMT

| Connection: close

| X-Powered-By: PHP/7.2.32-1+ubuntu18.04.1+deb.sury.org+1

| Cache-Control: public, s-maxage=600

| Date: Thu, 13 Aug 2020 13:51:25 GMT

| Content-Type: text/html; charset=UTF-8

| X-Debug-Token: 0d6934

| <!doctype html>

| <html lang="en-GB">

| <head>

| <meta charset="utf-8">

| <meta name="viewport" content="width=device-width, initial-scale=1.0">

| <title>Bolt | A hero is unleashed</title>

| <link href="https://fonts.googleapis.com/css?family=Bitter|Roboto:400,400i,700" rel="stylesheet">

| <link rel="stylesheet" href="/theme/base-2018/css/bulma.css?8ca0842ebb">

| <link rel="stylesheet" href="/theme/base-2018/css/theme.css?6cb66bfe9f">

| <meta name="generator" content="Bolt">

| <link rel="canonical" href="http://0.0.0.0:8000/">

| </head>

| <body class="front">

| http-generator: Bolt

| http-methods:

| Supported Methods: GET HEAD POST OPTIONS

| http-open-proxy: Proxy might be redirecting requests

| http-title: Bolt | A hero is unleashed

## ----- GoBuster-Common-Dirs -----

**/.hta (Status: 403)**  
**/.htaccess (Status: 403)**  
**/.htpasswd (Status: 403)**  
**/index.html (Status: 200)**  
**/server-status (Status: 403)**

## ----- WhatWEB -----

**WhatWeb report for http://10.10.65.138**

**Status : 200 OK**  
**Title : Apache2 Ubuntu Default Page: It works**  
**IP : 10.10.65.138**  
**Country : RESERVED, ZZ**

**Summary : HTTPServer [ Ubuntu Linux ][ Apache/2.4.29 (Ubuntu) ], Apache [ 2.4.29 ]**

**Detected Plugins:**

**[ Apache ]**

The Apache HTTP Server Project is an effort to develop and maintain an open-source HTTP server for modern operating systems including UNIX and Windows NT. The goal of this project is to provide a secure, efficient and extensible server that provides HTTP services in sync with the current HTTP standards.

**Version : 2.4.29 (from HTTP Server Header)**  
**Google Dorks: (3)**  
**Website : <http://httpd.apache.org/>**

**[ HTTPServer ]**

HTTP server header string. This plugin also attempts to identify the operating system from the server header.

**OS : Ubuntu Linux**  
**String : Apache/2.4.29 (Ubuntu) (from server string)**

**HTTP Headers:**

**HTTP/1.1 200 OK**  
**Date: Thu, 13 Aug 2020 13:57:18 GMT**  
**Server: Apache/2.4.29 (Ubuntu)**  
**Last-Modified: Sat, 18 Jul 2020 19:09:40 GMT**  
**ETag: "2aa6-5aabc03f3631a-gzip"**  
**Accept-Ranges: bytes**  
**Vary: Accept-Encoding**  
**Content-Encoding: gzip**  
**Content-Length: 3138**  
**Connection: close**  
**Content-Type: text/html**

## ***[Task 1] Deploy the machine***

This room is designed for users to get familiar with the Bolt CMS and how it can be exploited using Authenticated Remote Code Execution.

You should wait for at least 3-4 minutes for the machine to start properly.

If you have any queries or feedback you can reach me through the TryHackMe Discord server or through Twitter.

**#1**

Start the machine

**No answer needed**

## ***[Task 2] Hack your way into the machine!***

**A hero is unleashed**

Once you have successfully deployed the VM , enumerate it before finding the flag in the machine.

**#1**

What port number has a web server with a CMS running?

**8000**

**#2**

What is the username we can find in the CMS?

**bolt**

**#3**

What is the password we can find for the username?

**boltadmin123**

**#4**

What version of the CMS is installed on the server? (Ex: Name 1.1.1)

**Bolt 3.7.1**

**#5**

There's an exploit for a previous version of this CMS, which allows authenticated RCE. Find it on Exploit DB. What's its EDB-ID?

**48296**

**#6**

Metasploit recently added an exploit module for this vulnerability.

What's the full path for this exploit? (Ex: exploit/....)

Note: If you can't find the exploit module its most likely because your metasploit isn't updated. Run `apt update` then `apt install metasploit-framework`

**exploit/unix/webapp/bolt\_authenticated\_rce**

**#7**

Set the LHOST, LPORT, RHOST, USERNAME, PASSWORD in msfconsole before running the exploit

**No answer needed**

**#8**

Look for flag.txt inside the machine.

**THM{wh0\_d035nt\_l0ve5\_b0l7\_r1gh7??}**