Desafio Final CTF
Formação em
CyberSegurança

Aluno: Waldecy Façanha

Instrutor: José Menezes

1. Importante:

Esse relatório é o resultado do treinamento de 6 meses de CyberSegurança, do Vai na Web preparando os alunos, através de aulas online, gravadas, usando a teoria e práticas em laboratórios controlados e mentorias para quem tem dificuldades focados em Hacker ético abrangendo uma base para quem quiser seguir em Cybesegurança mostrando todas as tecnologias, prints e ferramentas utilizadas na criação do relatório e resultados nas práticas em laboratórios práticos com autorização do responsável pela aplicação web.

Índice

2. Escopo

3.Objetivo

O Objetivo é criar um relatório de todas que foi aprendido durante seis meses de treinamento de CybeSegurança aulas online, materialno Classroom e Github e laboratórios para práticas com os Alunos e uma mentoria para os alunos que ficaram com dúvidas nas disciplinas nesse último relatório falar qual foi o alvo e as ferramentas para obter informações, credenciais, flags escodidas no código e outras partes do site alvo, trabalho de conclusão de curso usar tudo que foi aprendido para criação de relatório. O site tem autorização pelo instrutor para fazer pentester.

4. Flags Encontradas no Site da Empresa:

FLAG{r0b0ts_txt_l34k4g3}

FLAG{d4t4b4s3_cr3d3nt14ls_3xp0s3d}

FLAG{sql_1nj3ct10n_m4st3r}

FLAG{h1dd3n_d4t4_1n_d4t4b4s3}

FLAG{b4s1c_s0urc3_c0d3_1nsp3ct10n}

FLAG{v13w_d1sc0v3ry_4dv4nc3d}

FLAG{g1t_cr3d3nt14ls_l34k}

FLAG{s3cr3t_p4n3l_d1sc0v3ry}

FLAG{xss_r3fl3ct3d_vuln3r4b1l1ty}

4. Introdução e descrição da Empresa

TechCorp Solutions

A TecnoCorp Solution é uma Empresa na área de tecnologia que presta serviços: Cloud Computing, Segurança da Informação e Consultoria de TI A Empresa Alvo para pentester foi encontrado várias vulnerabildades, Flags, domínios e subdomínios Ip: http://98.89.50.16.

5. Detalhamento dos dados do site e subdomínios

É uma Empresa que presta serviços em Ti: Cloud Computing, Segurança da Informação e Consultoria de TI. Nessa Empresa Alvo tem várias vulnerabilidades, Banco de Dados credenciais vazadas, informações de clientes, Flags e configurações de Sistema.

Ip: http://98.89.50.16

Subdomínios: http://98.95.207.28/config

Contact.php

Dashboard.php

Robots.txt

Login.php

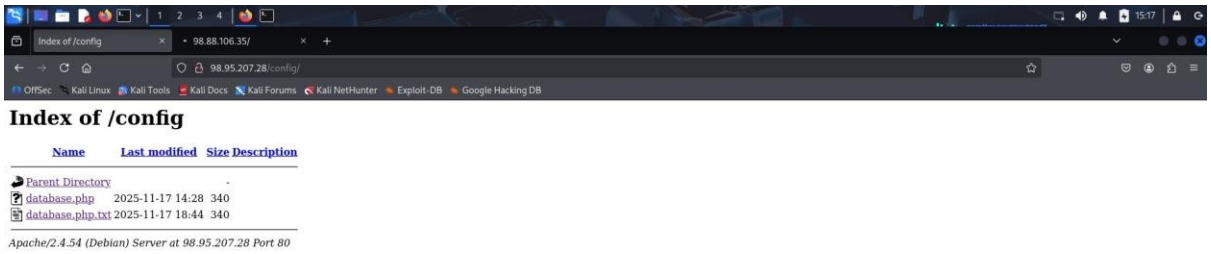
Panel.php

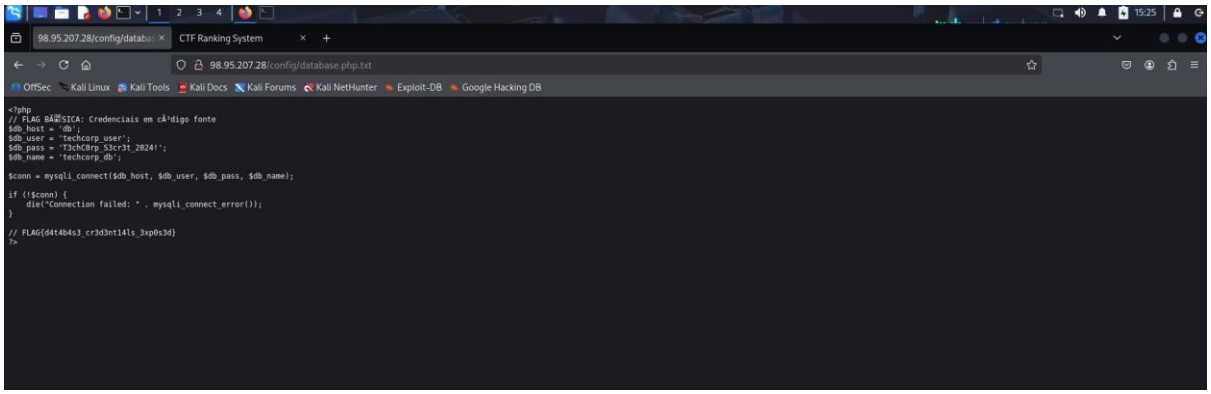
Logout.php

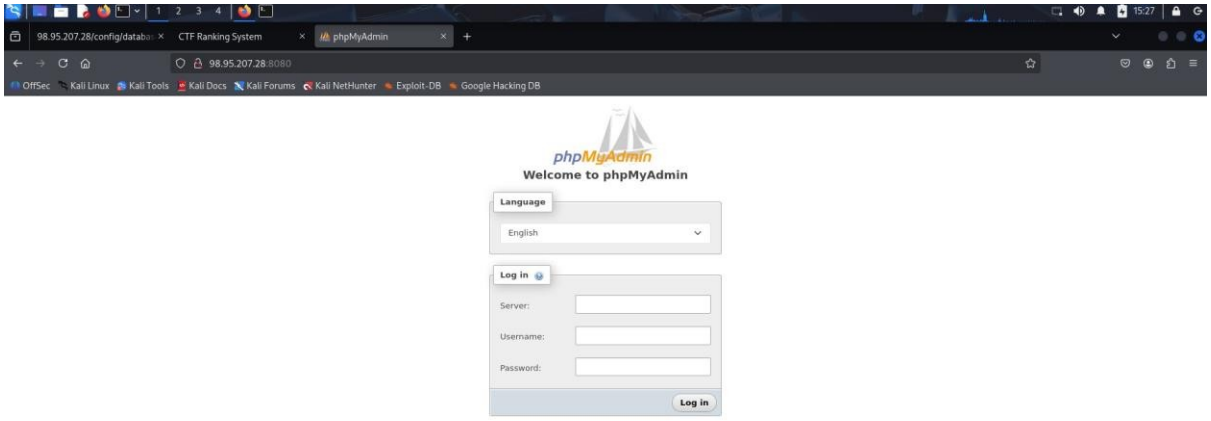
6. Detalhamento dos software instalados:

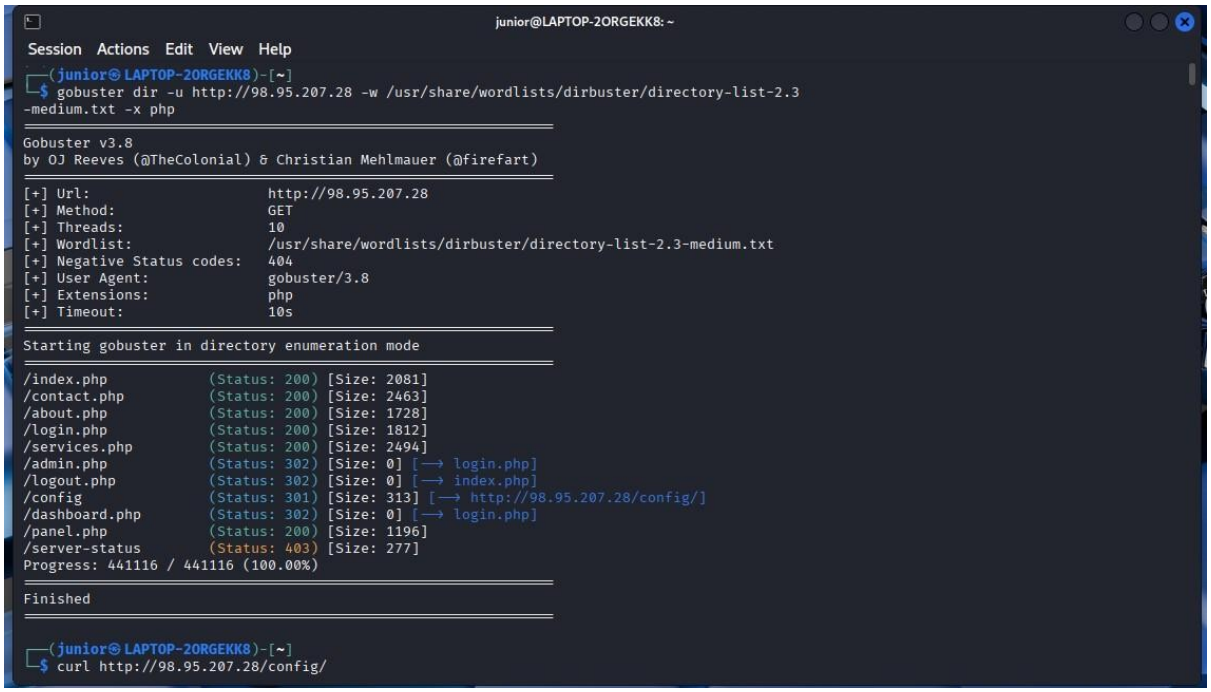
WSL, Kali Linux, Ubuntu. Ferramentas: Nmap, Dirb, Gobuster.

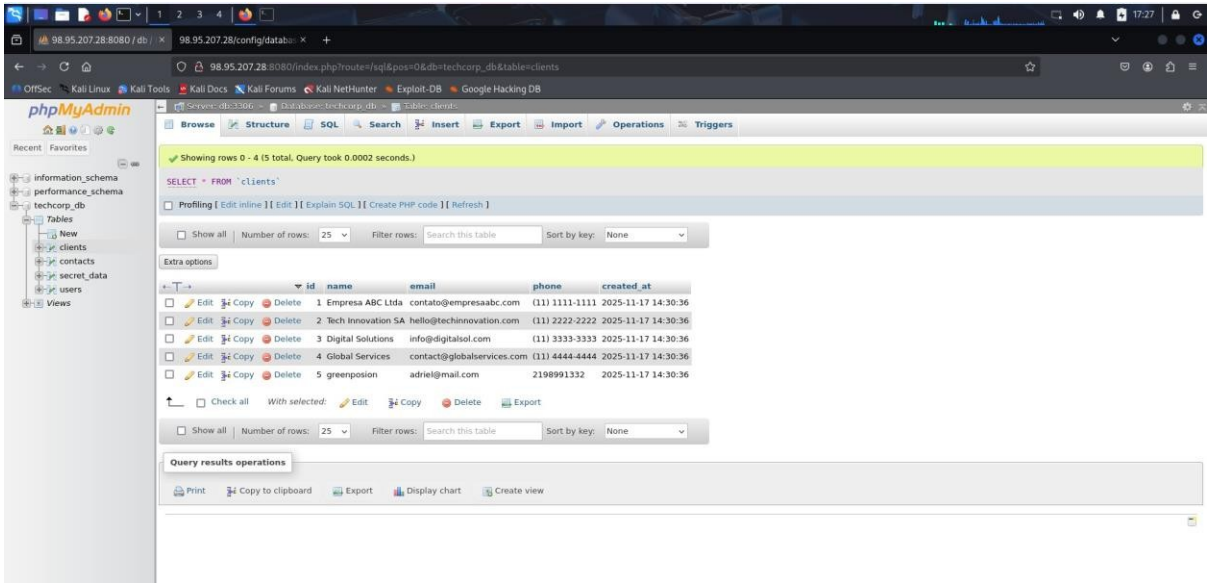
7. Prints do Sistema Alvo TechCorp Solutions

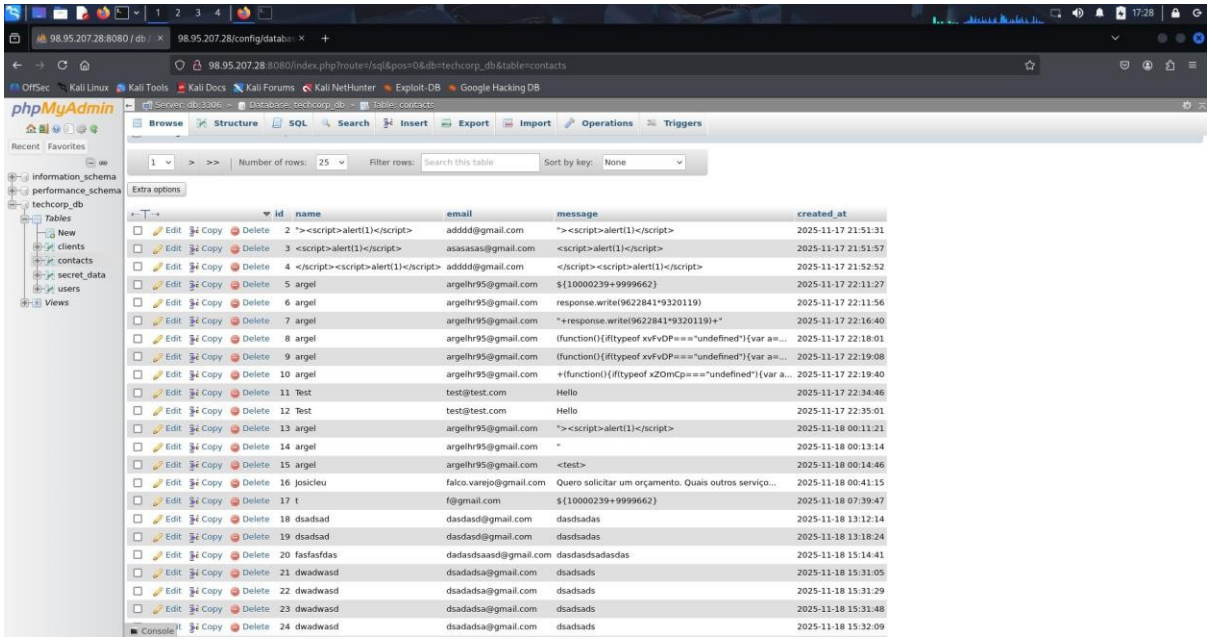


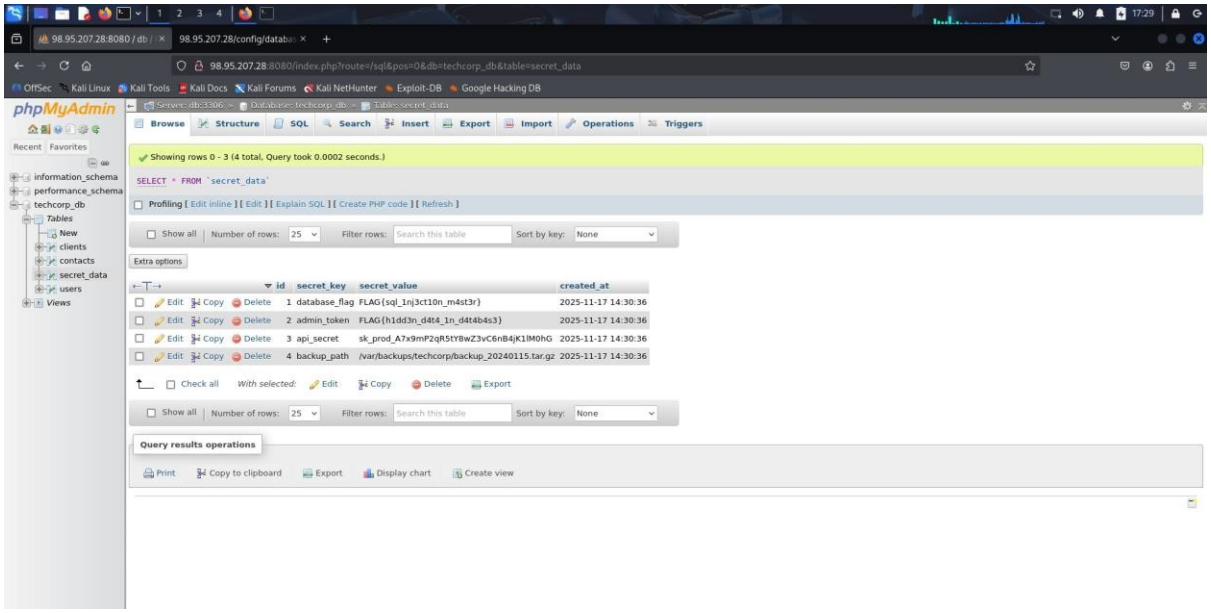



98.95.207.28/config/databa
CTF Ranking System
phpMyAdmin
98.95.207.28:8080
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
phpMyAdmin
Welcome to phpMyAdmin
Language
English
Log in
Server:
Username:
Password:
Log in

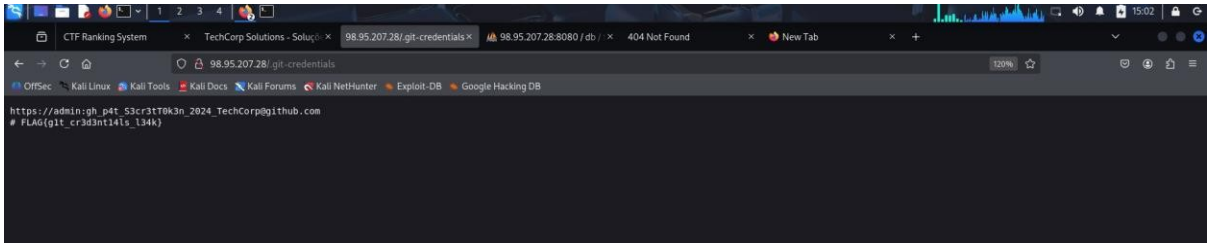

junior@LAPTOP-2ORGEKK8: ~
Session Actions Edit View Help
(junior㉿LAPTOP-2ORGEKK8)-[~]
$ gobuster dir -u http://98.95.207.28 -w /usr/share/wordlists/dirbuster/directory-list-2.3
-medium.txt -x php
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
[+] Url: http://98.95.207.28
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.8
[+] Extensions: php
[+] Timeout: 10s
Starting gobuster in directory enumeration mode
/index.php (Status: 200) [Size: 2081]
/contact.php (Status: 200) [Size: 2463]
/about.php (Status: 200) [Size: 1728]
/login.php (Status: 200) [Size: 1812]
/services.php (Status: 200) [Size: 2494]
/admin.php (Status: 302) [Size: 0] [--> login.php]
/logout.php (Status: 302) [Size: 0] [--> index.php]
/config (Status: 301) [Size: 313] [--> http://98.95.207.28/config/]
/dashboard.php (Status: 302) [Size: 0] [--> login.php]
/panel.php (Status: 200) [Size: 1196]
/server-status (Status: 403) [Size: 277]
Progress: 441116 / 441116 (100.00%)
Finished
(junior㉿LAPTOP-2ORGEKK8)-[~]
$ curl http://98.95.207.28/config/

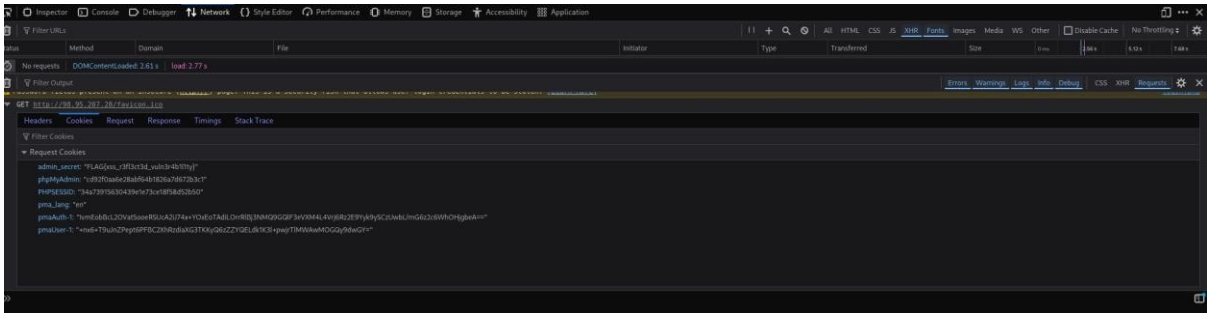

phpMyAdmin
Recent Favorites
information_schema
performance_schema
techcorp_db
Tables
New
clients
contacts
secret_data
users
Views
Browse Structure SQL Search Insert Export Import Operations Triggers
Showing rows 0 - 4 (5 total, Query took 0.0002 seconds.)
SELECT * FROM `clients`
Profiling [Edit inline] [Edit] [Explain SQL] [Create PHP code] [Refresh]
Show all | Number of rows: 25 Filter rows: Search this table Sort by key: None
Extra options
id name email phone created_at
1 Empresa ABC Ltda contato@empresaabc.com (11) 1111-1111 2025-11-17 14:30:36
2 Tech Innovation SA hello@techinnovation.com (11) 2222-2222 2025-11-17 14:30:36
3 Digital Solutions info@digitalsol.com (11) 3333-3333 2025-11-17 14:30:36
4 Global Services contact@globalservices.com (11) 4444-4444 2025-11-17 14:30:36
5 greenposion adriel@mail.com 2198991332 2025-11-17 14:30:36
Check all With selected: Edit Copy Delete Export
Query results operations
Print Copy to clipboard Export Display chart Create view


phpMyAdmin
Recent Favorites
information_schema
performance_schema
techcorp_db
Tables
New
clients
contacts
secret_data
users
Views
Browse Structure SQL Search Insert Export Import Operations Triggers
Number of rows: 25 Filter rows: Search this table Sort by key: None
Extra options
id name email message created_at
2 "><script>alert(1)</script> adddd@gmail.com "><script>alert(1)</script> 2025-11-17 21:51:31
3 <script>alert(1)</script> asasasas@gmail.com <script>alert(1)</script> 2025-11-17 21:51:57
4 </script><script>alert(1)</script> adddd@gmail.com </script><script>alert(1)</script> 2025-11-17 21:52:52
5 argel argelhr95@gmail.com ${10000239+9999662} 2025-11-17 22:11:27
6 argel argelhr95@gmail.com response.write(9622841*9320119) 2025-11-17 22:11:56
7 argel argelhr95@gmail.com "+response.write(9622841*9320119)+" 2025-11-17 22:16:40
8 argel argelhr95@gmail.com (function(){if(typeof xvFvDP==="undefined"){var a=... 2025-11-17 22:18:01
9 argel argelhr95@gmail.com (function(){if(typeof xvFvDP==="undefined"){var a=... 2025-11-17 22:19:08
10 argel argelhr95@gmail.com +(function(){if(typeof xZOmCp==="undefined"){var a... 2025-11-17 22:19:40
11 Test test@test.com Hello 2025-11-17 22:34:46
12 Test test@test.com Hello 2025-11-17 22:35:01
13 argel argelhr95@gmail.com "><script>alert(1)</script> 2025-11-18 00:11:21
14 argel argelhr95@gmail.com " 2025-11-18 00:13:14
15 argel argelhr95@gmail.com <test> 2025-11-18 00:14:46
16 Josicleu falco.varejo@gmail.com Quero solicitar um orçamento. Quais outros serviço... 2025-11-18 00:41:15
17 t f@gmail.com ${10000239+9999662} 2025-11-18 07:39:47
18 dsadsad dasdasd@gmail.com dasdsadas 2025-11-18 13:12:14
19 dsadsad dasdasd@gmail.com dasdsadas 2025-11-18 13:18:24
20 fasfasfdas dadasdsaasd@gmail.com dasdasdsadasdas 2025-11-18 15:14:41
21 dwadwasd dsadadsa@gmail.com dsadsads 2025-11-18 15:31:05
22 dwadwasd dsadadsa@gmail.com dsadsads 2025-11-18 15:31:29
23 dwadwasd dsadadsa@gmail.com dsadsads 2025-11-18 15:31:48
24 dwadwasd dsadadsa@gmail.com dsadsads 2025-11-18 15:32:09


phpMyAdmin
Browse
Structure
SQL
Search
Insert
Export
Import
Operations
Triggers
Showing rows 0 - 3 (4 total, Query took 0.0002 seconds.)
SELECT * FROM `secret_data`
id secret_key secret_value created_at
1 database_flag FLAG{sql_1nj3ct10n_m4st3r} 2025-11-17 14:30:36
2 admin_token FLAG{h1dd3n_d4t4_1n_d4t4b4s3} 2025-11-17 14:30:36
3 api_secret sk_prod_A7x9mP2qR5tY8wZ3vC6nB4jK1lM0hG 2025-11-17 14:30:36
4 backup_path /var/backups/techcorp/backup_20240115.tar.gz 2025-11-17 14:30:36
Query results operations


junior@LAPTOP-2ORGEKK8: ~
Session Actions Edit View Help
Target: http://98.95.207.28/
[11:17:23] Starting:
[11:17:27] 200 - 87B - /.git-credentials
[11:17:28] 403 - 277B - /.ht_wsr.txt
[11:17:28] 403 - 277B - /.htaccess.bak1
[11:17:28] 403 - 277B - /.htaccess.orig
[11:17:28] 403 - 277B - /.htaccess.save
[11:17:28] 403 - 277B - /.htaccess.sample
[11:17:28] 403 - 277B - /.htaccess_extra
[11:17:28] 403 - 277B - /.htaccess_sc
[11:17:28] 403 - 277B - /.htaccess_orig
[11:17:28] 403 - 277B - /.htaccessBAK
[11:17:28] 403 - 277B - /.htaccessOLD
[11:17:28] 403 - 277B - /.htaccessOLD2
[11:17:29] 403 - 277B - /.htm
[11:17:29] 403 - 277B - /.html
[11:17:29] 403 - 277B - /.htpasswd_test
[11:17:29] 403 - 277B - /.htpasswds
[11:17:29] 403 - 277B - /.httr-oauth
[11:17:38] 200 - 690B - /about.php
[11:17:41] 302 - 0B - /admin.php -> login.php
[11:18:00] 301 - 313B - /config -> http://98.95.207.28/config/
[11:18:01] 200 - 485B - /config/
[11:18:02] 200 - 815B - /contact.php
[11:18:04] 302 - 0B - /dashboard.php -> login.php
[11:18:23] 200 - 657B - /login.php
[11:18:24] 302 - 0B - /logout.php -> index.php
[11:18:34] 200 - 616B - /panel.php
[11:18:46] 200 - 140B - /robots.txt
[11:18:48] 403 - 277B - /server-status/
[11:18:48] 403 - 277B - /server-status
Task Completed


https://admin:gh_p4t_S3cr3tT0k3n_2024_TechCorp@github.com
FLAG{g1t_cr3d3nt14ls_l34k}

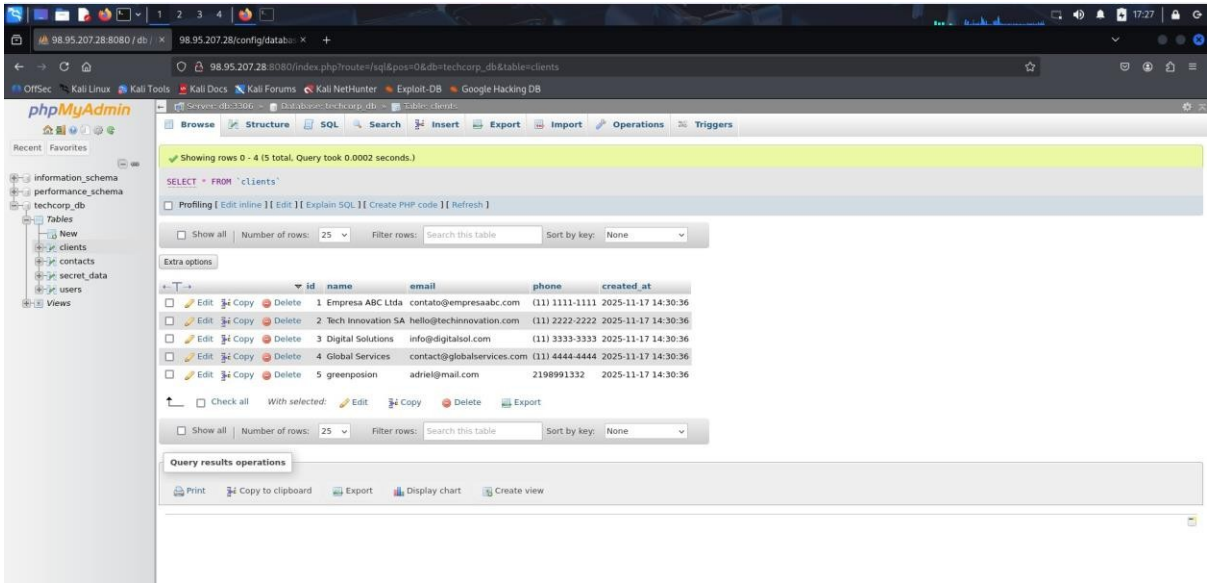


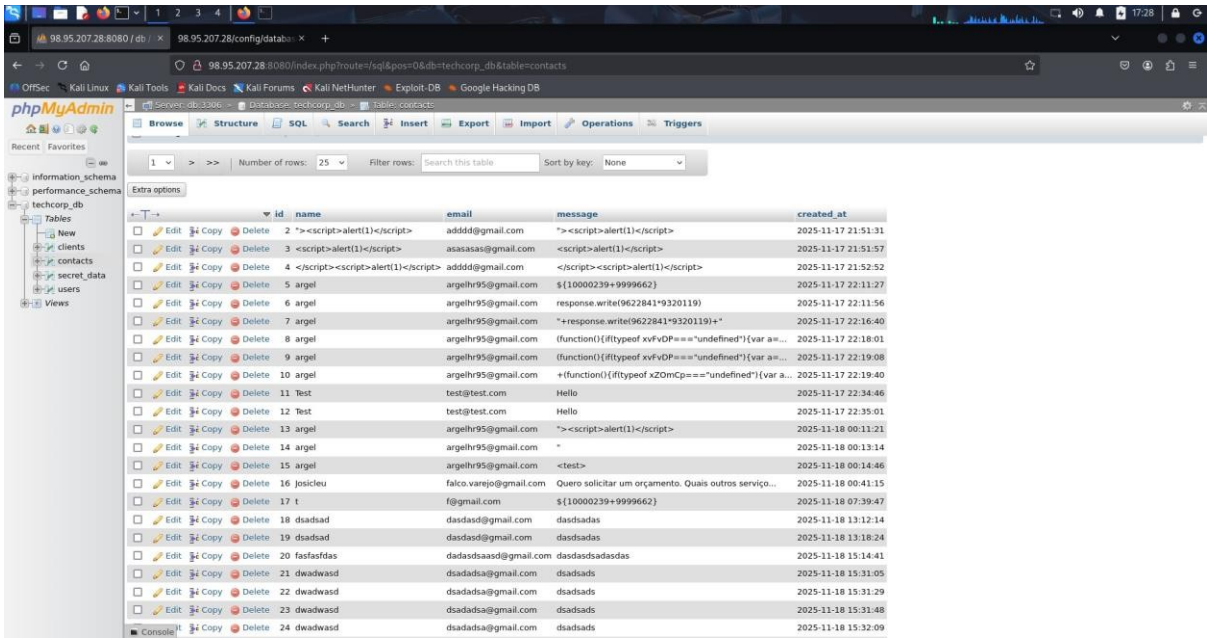
8. Resultados e vulnerabilidades relatadas

As vulnerabilidades estão mostradas nos prints acima, Credenciais de clientes, funcionários, Banco de Dados, Login e Flags escondidas nos códigos.

9. Lista de e-mails que já tiveram dados vazados

Lista de E-mails de funcionários e Clientes vazados





10. Conclusão:

Em todas as Empresas precisam de uma Equipe de Segurança Cibernética usando boas Práticas de Segurança de Sistemas Web e Aplicativos treinamento para todos os funcionários, usar ferramentas: SIEM, IDS, IPS, Firewall WAF equipes multidisciplinares para mater a segurança dos dados, funcionários e fornecedores.

11. Sugestões para o contratante:

Algumas sugestões para o contratante são: Contratar uma Consultoria de TI, equipe de CyberSegurança para implantar metodologias e ferramentas para manter a segurança dos Sistemas da Empresa: SIEM,IDS, WAF e Firewall ter um equipe de Blue Team dentro da Empresa e investir em Segurança da Informação.