UNICESUMAR

RENATO DE ALMEIDA MENDES

TRABALHO PRÁTICO MONTAGEM DE UM AMBIENTE VIRTUAL WEB VULNERÁVEL

CURITIBA

2023

UNICESUMAR

RENATO DE ALMEIDA MENDES

TRABALHO PRÁTICO MONTAGEM DE UM AMBIENTE VIRTUAL WEB VULNERÁVEL

Trabalho apresentado à disciplina de Desafio profissional apresentada a disciplina de Desafio profissional III por solicitação da professora Ana Paula Costacurta.

CURITIBA

2023

Sumário

CURITIBA

2023

INTRODUÇÃO

As aplicações hoje em dia estão cada vez mais vulneráveis, assim através do software VirtualBox, que executa uma máquina virtual, nela podemos acessar o site WebGoat que é uma aplicação desenvolvida pela Open Web Application Security Project (OWASP), ela ensina os desenvolvedores sobre as vulnerabilidades que se pode ter em uma aplicação web e como resolvê-las, ou seja, é um site que de treinamento na prática de teste de invasões em aplicações webs.

OBJETIVO

O WebGoat fornece um ambiente educacional para que os usuários possam aprender sobre vulnerabilidades e técnicas de segurança em aplicações web. Ele é projetado para ajudar desenvolvedores e profissionais de segurança a aprimorarem suas habilidades na identificação e exploração de falhas comuns em aplicações web. Ele faz com que os usuários identifiquem e explorem vulnerabilidades, e a como se prevenir sobres esses problemas.

METODOLOGIA

WebGoat oferece aos usuários a oportunidade de aprenderem na prática sobre vulnerabilidades e técnicas de segurança em aplicações web. Ele incentiva a experimentação, o erro e a compreensão dos conceitos subjacentes, permitindo que os usuários adquiram habilidades em testes de segurança e desenvolvimento seguro.

AMBIENTE VIRTUAL

INSTALAÇÃO E CONFIGURAÇÃO DO VIRTUALBOX

Acessei o site oficial da VirtualBox https://www.virtualbox.org/ a baixei a versão mais recente, e executei o arquivo, segui os passos padrões de instalação, após a

instalação comecei a configurar, para poder abrir a maquina virtual fiz o donwload da iso do Kali no site https://www.kali.org/docs/virtualization/import-premade-virtualbox/.

Com a iso do Kali a baixada, abri ela pelo VirtualBox, quando mandei iniciar deu um erro de SVM. Onde ele pedia para que acessasse a BIOS do meu computador e ativasse o SVM. Após isso mandei iniciar a máquina virtual e deu tudo certo.

INSTALAÇÃO E CONFIGURAÇÃO DO LINUX NA MÁQUINA VIRTUAL

Após acessar a máquina virtual abri o cmd e coloquei os seguintes códigos:

sudo apt-get install default-jre; wget https://github.com/WebGoat/WebGoat/releases/download/v2023.4/webgoat-2023.4.jar;

java -jar webgoat-2023.4.jar;

Com esses códigos o Linux está configurado, e com a instalação do WebGoat feita também.

CONFIGURAÇÃO DO WEBGOAT

Com a instalação do WebGoat feita no tópico passado, agora é só configurar. Acesse o site http://localhost:8080/WebGoat/ e nele você vai fazer o seu cadastro, com o cadastro feito, o site já está liberado para poder estudar e aprender sobre as vulnerabilidades.

VISÃO GERAL DO WEBGOAT

DESCRIÇÃO E FUNCIONALIDADES DO WEBGOAT

O WebGoat é um software de código aberto que fornece um ambiente educacional e interativo para aprender sobre vulnerabilidades e técnicas de segurança

em aplicações web. Ele foi criado para ajudar desenvolvedores, estudantes e profissionais de segurança a adquirirem conhecimentos práticos em testes de segurança e identificação de falhas em aplicações web.

COMO ACESSAR E NAVEGAR NO WEBGOAT

Você faz o acesso através de uma máquina virtual, pois como você vai fazer testes de vulnerabilidades em sites é importante você estar em uma máquina virtual permitindo que você faça uso de um computador sem estar vinculado a um lugar físico.

PRÁTICAS COMUNS DE SEGURANÇA EM APLICAÇÕES WEB

CONCEITOS BÁSICOS DE SEGURANÇA EM APLICAÇÕES WEB

A segurança em aplicações web é essencial para proteger dados e informações em um ambiente online. Alguns conceitos básicos incluem autenticação, autorização, criptografia, injeção de código, XSS, CSRF, gerenciamento de sessão. Esses conceitos visam garantir a integridade e a privacidade dos usuários, protegendo contra ameaças e vulnerabilidades.

IDENTIFICAÇÃO DE VULNERABILIDADES COMUNS EM APLICAÇÕES WEB

Vulnerabilidades comuns em aplicações web incluem injeção de código, crosssite scripting, cross-site request forgery, vazamento de informações sensíveis, redirecionamento e encaminhamento a sites não confiáveis.

BOAS PRÁTICAS PARA MITIGAÇÃO DE VULNERABILIDADES EM APLICAÇÕES WEB

Implementar autenticação e autorização de duas etapas, utilizar criptografias, limitar a exposição de informações sensíveis e ensinar para os usuários sobre segurança de sites e informações. Utilizando essas medidas de segurança, vai te proteger contra ameaças e vai garantir a sua integridade de dados e a usa privacidade.

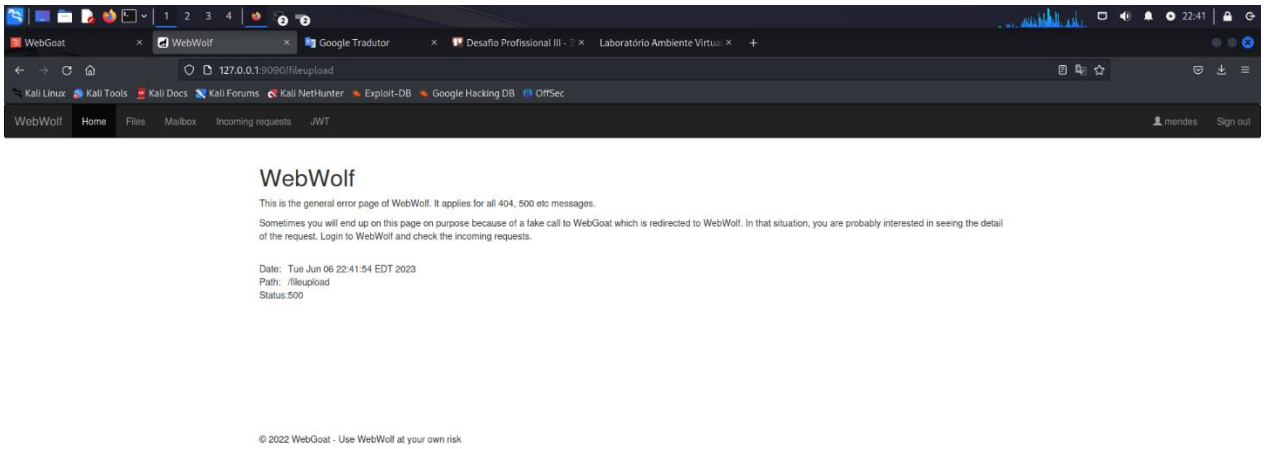
SQL INJECTION

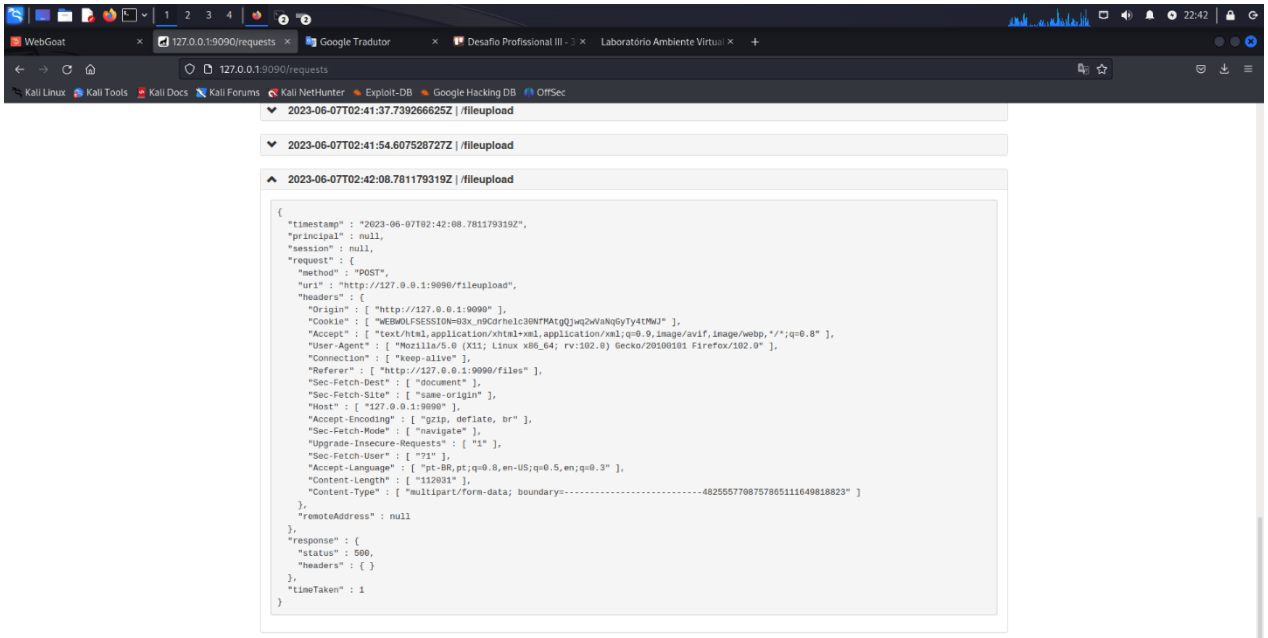
Injeção de SQL é um tipo de ameaça de segurança que se aproveita de falhas em sistemas que trabalham com bases de dados realizando ataques com comandos SQL.

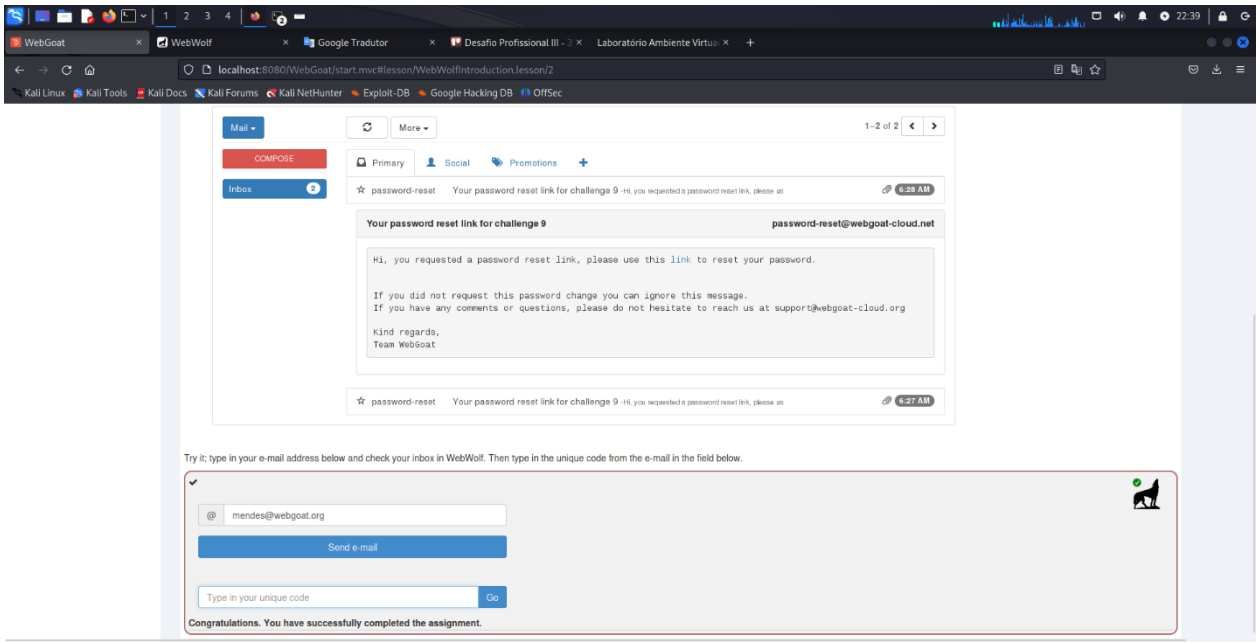
CONCLUSÃO

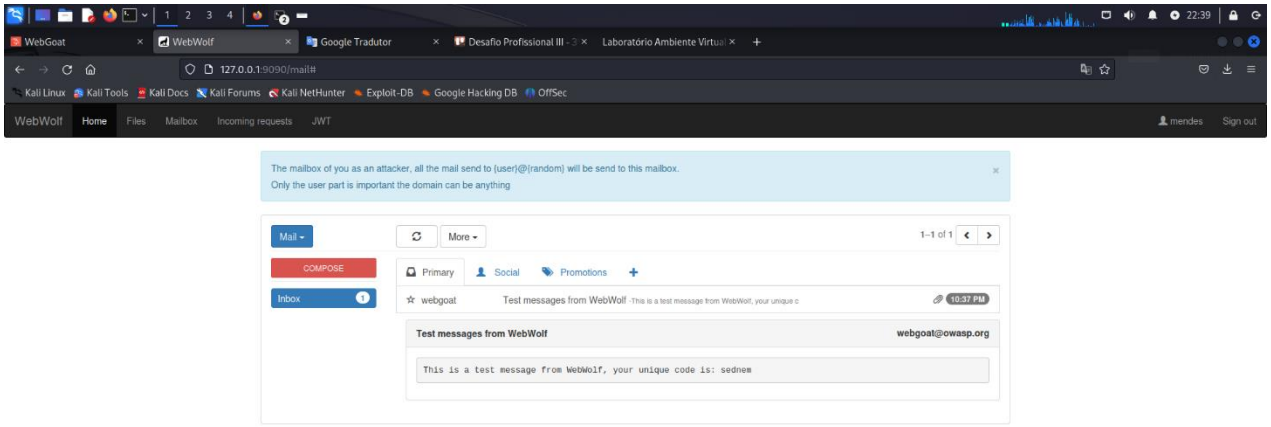
SÍNTESE DOS RESULTADOS E CONCLUSÕES DO TRABALHO PRÁTICO

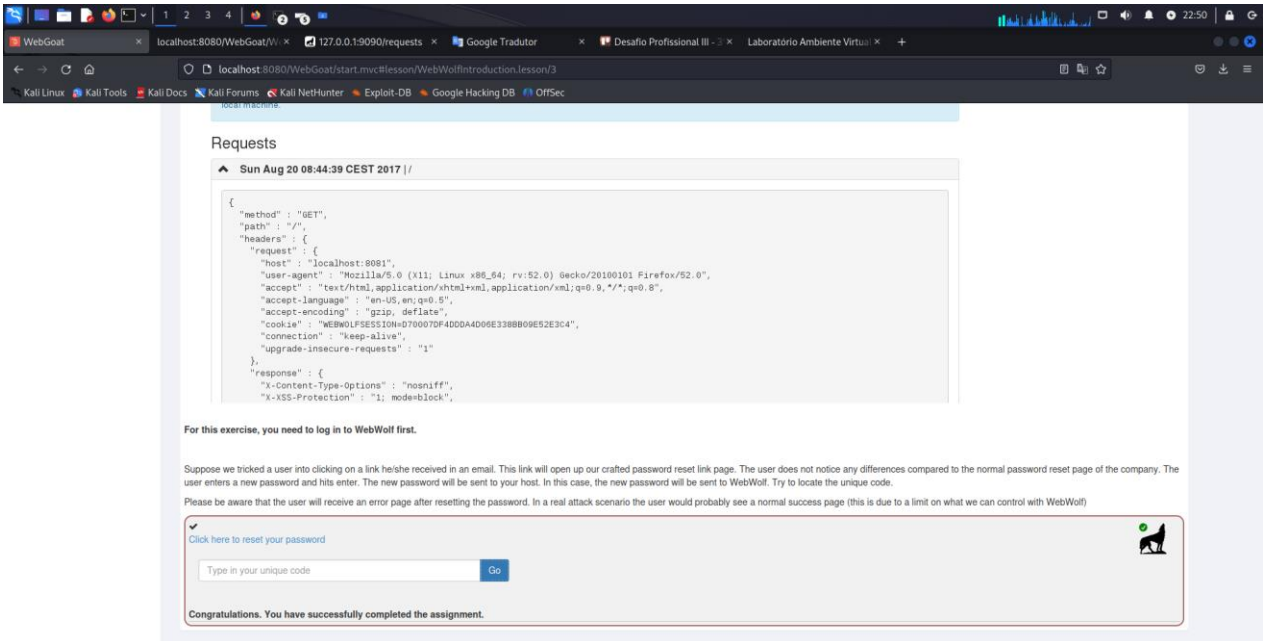
Depois de ter executado toda a instalação do software para acessar a máquina virtual e ter feita a configuração dela, realizei tarefas de falhas na criptografia, onde eu compreendi melhor como são feitos as criptografias e os métodos utilizados para fazer. Percebi que tem todo um sistema lógico para cada tipo de criptografia, dificultado o acesso do invasor.

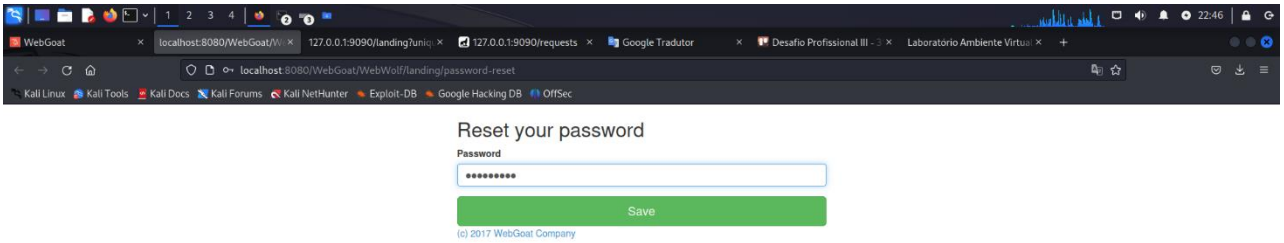


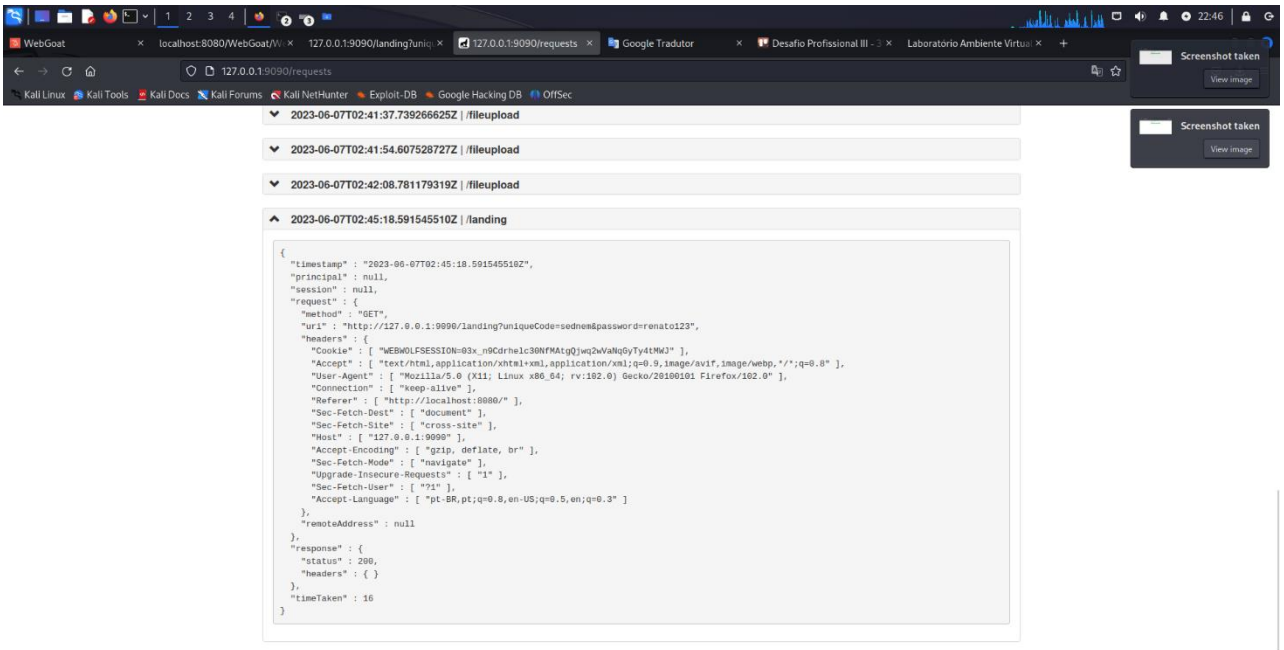

WebGoat
127.0.0.1:9090/requests
Google Tradutor
Desafio Profissional III - 3
Laboratório Ambiente Virtual
127.0.0.1:9090/requests
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
2023-06-07T02:41:37.739266625Z | /fileupload
2023-06-07T02:41:54.607528727Z | /fileupload
2023-06-07T02:42:08.781179319Z | /fileupload
{
"timestamp" : "2023-06-07T02:42:08.781179319Z",
"principal" : null,
"session" : null,
"request" : {
"method" : "POST",
"uri" : "http://127.0.0.1:9090/fileupload",
"headers" : {
"Origin" : ["http://127.0.0.1:9090"],
"Cookie" : ["WEBWOLFSESSION=03x_n9Cdrhe1c36NfMAtgQjwq2wVaNqGyTy4tMWJ"],
"Accept" : ["text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8"],
"User-Agent" : ["Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"],
"Connection" : ["keep-alive"],
"Referer" : ["http://127.0.0.1:9090/files"],
"Sec-Fetch-Dest" : ["document"],
"Sec-Fetch-Site" : ["same-origin"],
"Host" : ["127.0.0.1:9090"],
"Accept-Encoding" : ["gzip, deflate, br"],
"Sec-Fetch-Mode" : ["navigate"],
"Upgrade-Insecure-Requests" : ["1"],
"Sec-Fetch-User" : ["?1"],
"Accept-Language" : ["pt-BR,pt;q=0.8,en-US;q=0.5,en;q=0.3"],
"Content-Length" : ["112031"],
"Content-Type" : ["multipart/form-data; boundary=--------------------------482555770875786511164981882 3"]
},
"remoteAddress" : null
},
"response" : {
"status" : 500,
"headers" : { }
},
"timeTaken" : 1
}

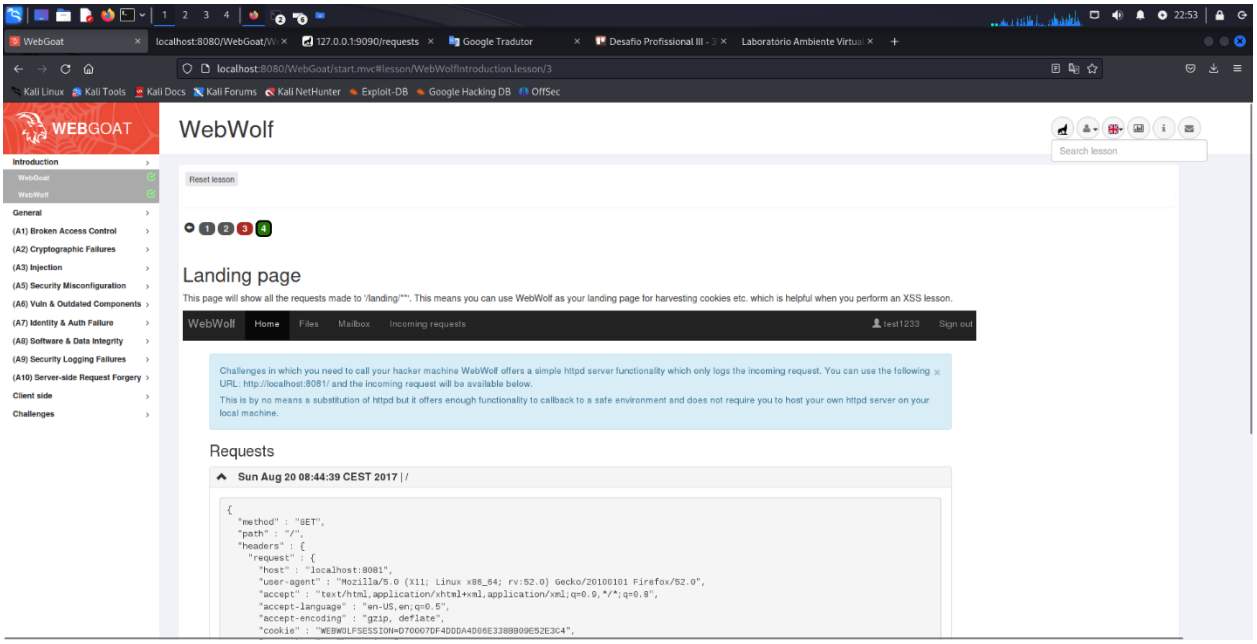

WebGoat
WebWolf
Google Tradutor
Desafio Profissional III - 3
Laboratório Ambiente Virtual
localhost:8080/WebGoat/start.mvc#lesson/WebWolfIntroduction.lesson/2
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Mail
More
1–2 of 2
COMPOSE
Primary
Social
Promotions
Inbox
password-reset
Your password reset link for challenge 9 -Hi, you requested a password reset link, please us
6:28 AM
Your password reset link for challenge 9
password-reset@webgoat-cloud.net
Hi, you requested a password reset link, please use this link to reset your password.
If you did not request this password change you can ignore this message.
If you have any comments or questions, please do not hesitate to reach us at support@webgoat-cloud.org
Kind regards,
Team WebGoat
password-reset
Your password reset link for challenge 9 -Hi, you requested a password reset link, please us
6:27 AM
Try it; type in your e-mail address below and check your inbox in WebWolf. Then type in the unique code from the e-mail in the field below.
@
mendes@webgoat.org
Send e-mail
Type in your unique code
Go
Congratulations. You have successfully completed the assignment.


WebGoat
WebWolf
Google Tradutor
Desafio Profissional III
Laboratório Ambiente Virtual
127.0.0.1:9090/mail#
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
WebWolf
Home
Files
Mailbox
Incoming requests
JWT
mendes
Sign out
The mailbox of you as an attacker, all the mail send to {user}@{random} will be send to this mailbox.
Only the user part is important the domain can be anything
Mail
More
1–1 of 1
COMPOSE
Primary
Social
Promotions
Inbox
webgoat
Test messages from WebWolf
10:37 PM
Test messages from WebWolf
webgoat@owasp.org
This is a test message from WebWolf, your unique code is: sednem


WebGoat
localhost:8080/WebGoat/requests
127.0.0.1:9090/requests
Google Tradutor
Desafio Profissional III
Laboratório Ambiente Virtual
localhost:8080/WebGoat/start.mvc#lesson/WebWolfIntroduction.lesson/3
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Requests
Sun Aug 20 08:44:39 CEST 2017 / /
{
"method" : "GET",
"path" : "/",
"headers" : {
"request" : {
"host" : "localhost:8081",
"user-agent" : "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0",
"accept" : "text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8",
"accept-language" : "en-US,en;q=0.5",
"accept-encoding" : "gzip, deflate",
"cookie" : "WEBWOLFSESSION=D70007DF4DDDA4D06E338BB09E52E3C4",
"connection" : "keep-alive",
"upgrade-insecure-requests" : "1"
},
"response" : {
"X-Content-Type-Options" : "nosniff",
"X-XSS-Protection" : "1; mode=block",
For this exercise, you need to log in to WebWolf first.
Suppose we tricked a user into clicking on a link he/she received in an email. This link will open up our crafted password reset link page. The user does not notice any differences compared to the normal password reset page of the company. The user enters a new password and hits enter. The new password will be sent to your host. In this case, the new password will be sent to WebWolf. Try to locate the unique code.
Please be aware that the user will receive an error page after resetting the password. In a real attack scenario the user would probably see a normal success page (this is due to a limit on what we can control with WebWolf)
Click here to reset your password
Type in your unique code
Go
Congratulations. You have successfully completed the assignment.


WebGoat
localhost:8080/WebGoat/WebWolf/landing/password-reset
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Reset your password
Password
Save
(c) 2017 WebGoat Company

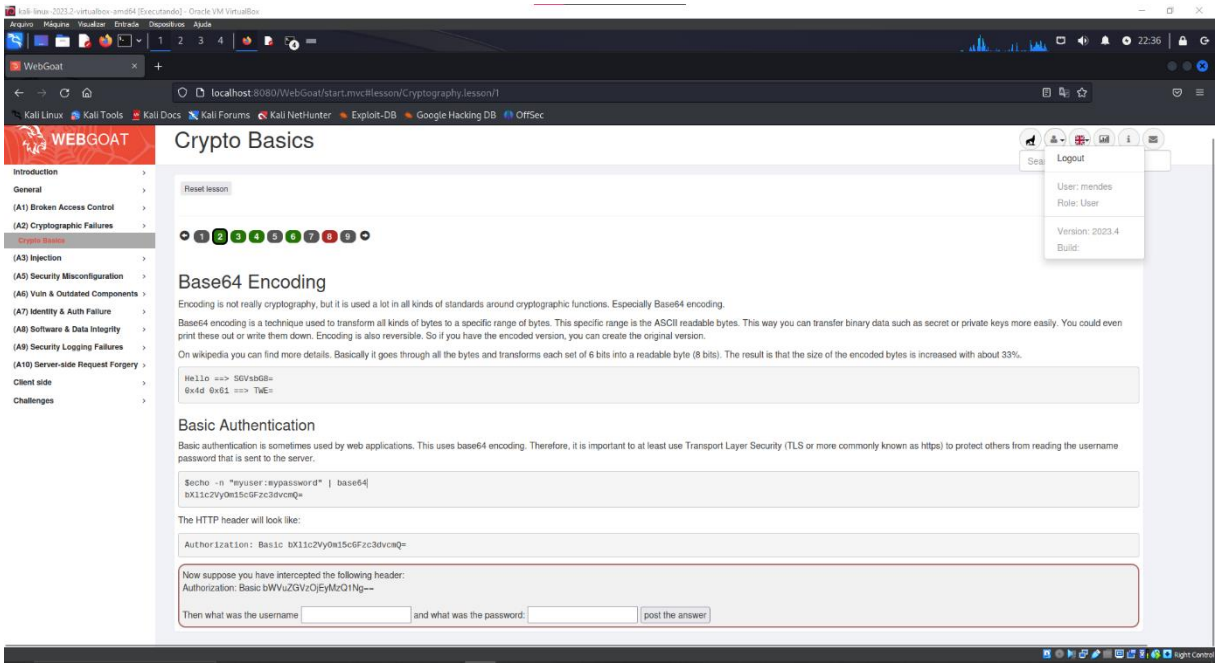

WebGoat
127.0.0.1:9090/requests
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Screenshot taken
View image
2023-06-07T02:41:37.739266625Z | /fileupload
2023-06-07T02:41:54.607528727Z | /fileupload
2023-06-07T02:42:08.781179319Z | /fileupload
2023-06-07T02:45:18.591545510Z | /landing
{
"timestamp" : "2023-06-07T02:45:18.591545510Z",
"principal" : null,
"session" : null,
"request" : {
"method" : "GET",
"uri" : "http://127.0.0.1:9090/landing?uniqueCode=sednem&password=renato123",
"headers" : {
"Cookie" : ["WEBWOLFSESSION=03x_n9Cdrhelc30NfMAtgQjwq2wVaNqGyTy4tMWJ"],
"Accept" : ["text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8"],
"User-Agent" : ["Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0"],
"Connection" : ["keep-alive"],
"Referer" : ["http://localhost:8080/"],
"Sec-Fetch-Dest" : ["document"],
"Sec-Fetch-Site" : ["cross-site"],
"Host" : ["127.0.0.1:9090"],
"Accept-Encoding" : ["gzip, deflate, br"],
"Sec-Fetch-Mode" : ["navigate"],
"Upgrade-Insecure-Requests" : ["1"],
"Sec-Fetch-User" : ["?1"],
"Accept-Language" : ["pt-BR,pt;q=0.8,en-US;q=0.5,en;q=0.3"]
},
"remoteAddress" : null
},
"response" : {
"status" : 200,
"headers" : { }
},
"timeTaken" : 16
}



LIMITAÇÕES DO TRABALHO E SUGESTÕES PARA TRABALHOS FUTUROS

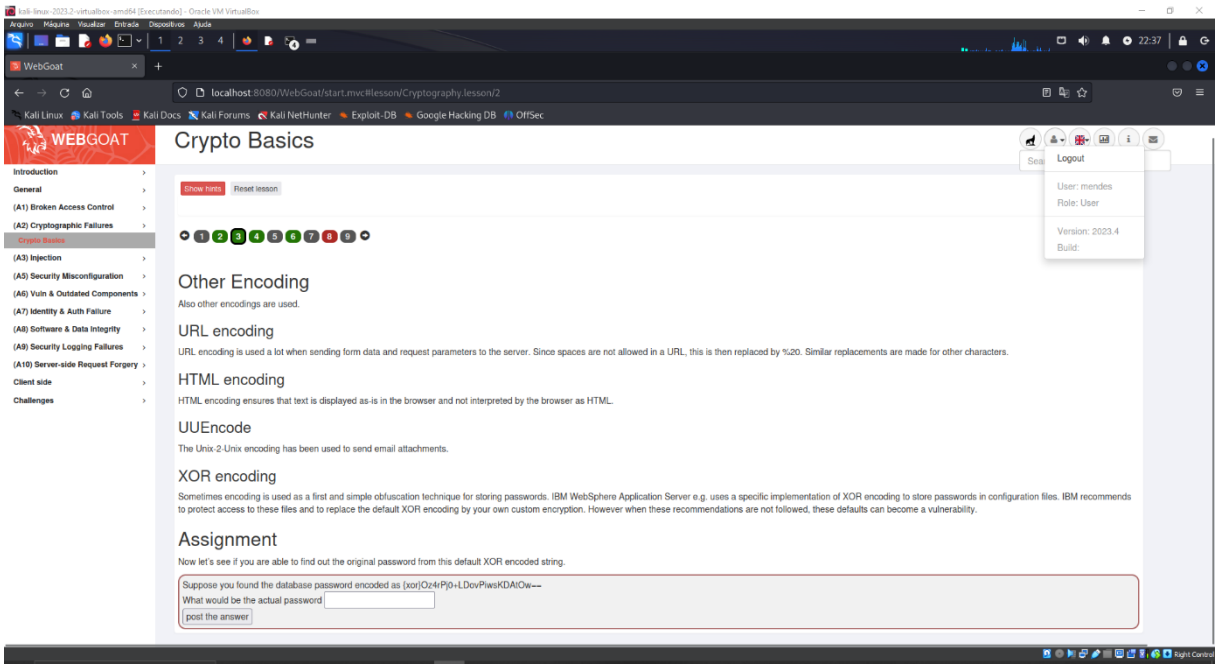
Após eu ter terminado a introdução, os próximos exercícios que eu pretendo fazer é o A2 que é falha de criptografia, onde eu irei aprender as seguintes formas de técnicas: Codificação, Hash, Criptografia, Assinando, Keystores, Padrõesde segurança e Criptografia pós-quântica. sugestão para futuros trabalhos deixar explicar mais algumas etapas, e utilizar links que estejam funcionado.

TAREFA (A2) CRYPTO BASICS



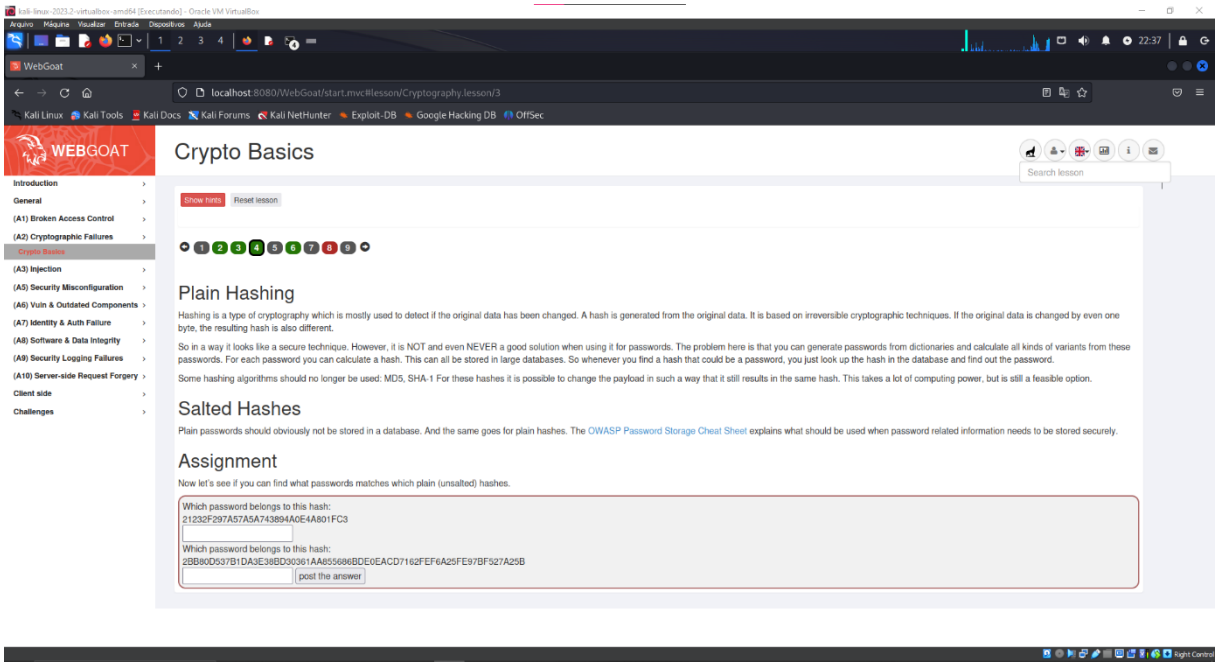
Nessa tarefa eu tinha que decodificar o login e senha, eles estavam codificados na base64.

<https://www.base64decode.org/>.



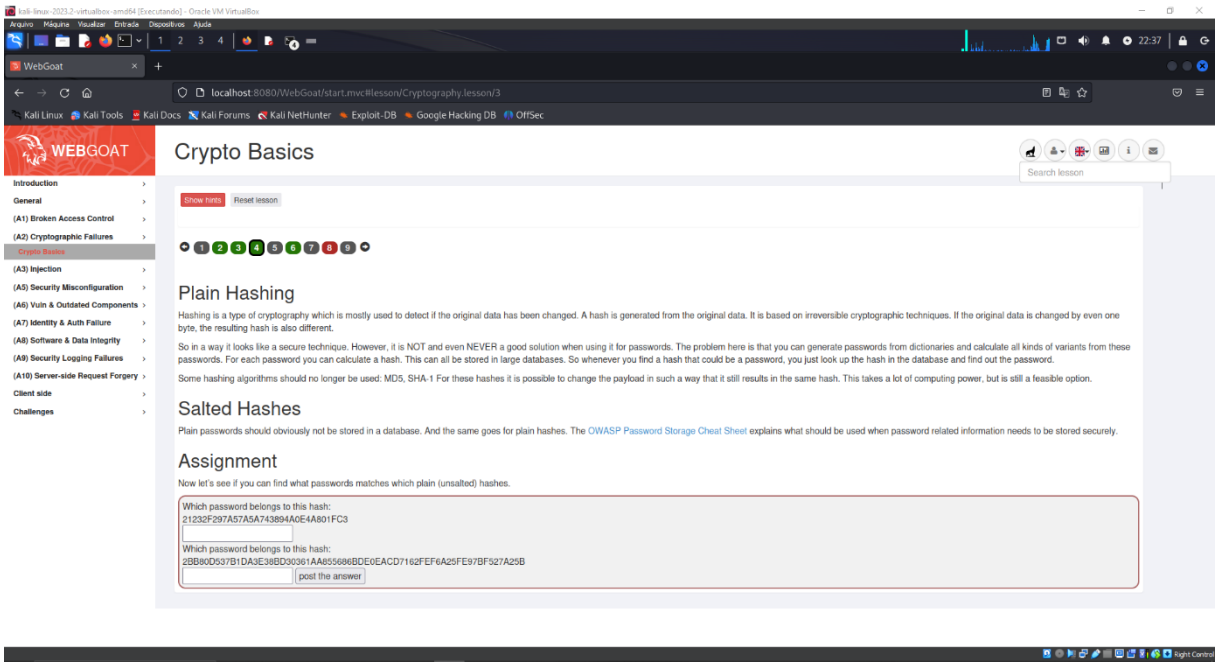
Nessa tarefa eu tinha que decodificar a senha, eles estavam codificado com XOR enconding.

<https://strelitzia.net/wasXORdecoder/wasXORdecoder.html>.

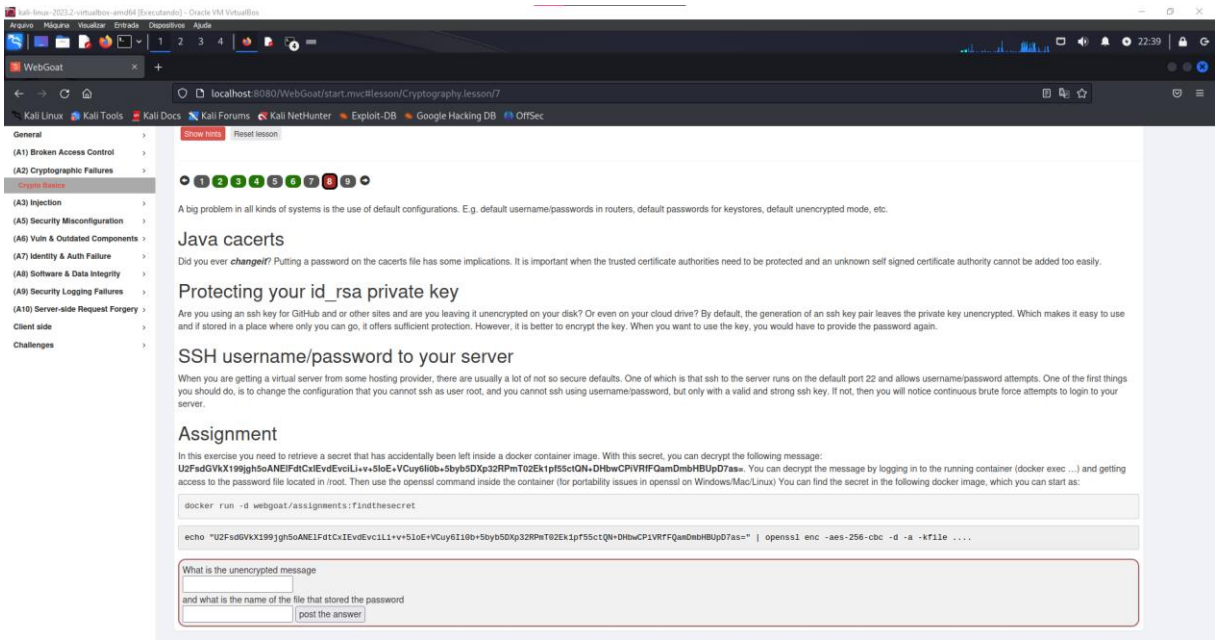


Na tarefa 4 tinha duas senhas codificas pelo tipo hash, e eu decodifiquei pelo esse site.

< https://hashes.com/en/decrypt/hash>.



Já na tarefa 6 eu acessei o openssl para poder pegar a chave pública e o modulo dessa chave.



A tarefa 8 foi a única questão que eu não conclui, pois não consegui baixar o Docker, mesmo acessando vários sites e assistindo vídeos de como executar o Docker, não fui capaz de fazer isso na minha máquina.

REFERÊNCIAS

MDN WEB DOCS. Learn Server-side - First Steps - Website Security. [S.l.], 2023. Disponível em: <https://developer.mozilla.org/pt-BR/docs/Learn/Server-side/First_steps/Website_security>. Acesso em: 6 jun. 2023.

CLOUDFLARE. What is Web Application Security? [S.l.], [s.d.]. Disponível em: <https://www.cloudflare.com/pt-br/learning/security/what-is-web-application-security/>. Acesso em: 6 jun. 2023.

BLOG 4LINUX. Conheça as 10 principais vulnerabilidades web de 2021. [S.l.], 2021. Disponível em: <https://blog.4linux.com.br/conheca-as-10-principais-vulnerabilidades-web-de-2021/>. Acesso em: 6 jun. 2023.

TRELLO. Aula 7 - Dia 10/05/2023 - Segurança em aplicações web. [S.l.], 2023. Disponível em: <https://trello.com/c/HorbZjhM/31-aula-7-dia-10-05-2023-seguran%C3%A7a-em-aplica%C3%A7%C3%B5es-web>. Acesso em: 6 jun. 2023.

CURITIBA

2023