FACULDADE ADVENTISTA DA BAHIA
GESTÃO DA TECNOLOGIA DA INFORMAÇÃO

ANATÉRCIA DA RÉLIA ARRONE

LUIZ PAULO RODRIGUES

ESPECIFICAÇÃO DO TRABALHO – PENTESTER

CACHOEIRA-BA
2022

ANATÉRCIA DA RÉLIA ARRONE

LUIZ PAULO RODRIGUES

ESPECIFICAÇÃO DO TRABALHO – PENTESTER

Trabalho de grupal de implementação de pentester como requisito da disciplina de segurança da informação e projeto de desenvolvimento profissional ministrada pelo prof. Erick de Souza Lago e Jean do Ouro.

CACHOEIRA-BA

2022

SUMÁRIO

1. INTRODUÇÃO 4

3. MÉTODO 5

4. DETALHAMENTO DOS DADOS DO SITE, SUBDOMÍNIOS E SOFTWARES INSTALADOS 5

5. Quadro SWOT da segurança do site (FORÇAS, FRAQUEZAS, OPORTUNIDADES E AMEACAS) 6

6. RELATÓRIO E FERRAMENTAS USADAS 7

8. POLÍTICA DE SENHAS 16

Diretrizes do Uso de Senhas 16

9. POLÍTICA DE SGURANÇA CIBÉRICA 19

10. RECOMENDAÇÕES PARA O TRATAMENTO DA INFORMAÇÃO 20

11. CONTRATO DE SERVIÇO DE 23

12. PRESTAÇÃO DE SERVIÇOS DE EXECUÇÃO DE TESTES DE PENETRAÇÃO (PENTEST) E ANÁLISE DE VULNERABILIDADES DE 28

13. CONCLUSÃO 30

14. LINKS DAS REFERÊNCIAS USADAS 31

1. INTRODUÇÃO

O teste de penetração é uma série de atividades realizadas para identificar e explorar vulnerabilidades de segurança. Ajuda a confirmar a eficácia ou ineficácia das medidas de segurança implementadas (BACUDIO, et al., 2011). Com o cenário de ameaças cibernéticas ficando cada vez mais sombrio, os testes de penetração se tornaram uma necessidade extrema para vários setores. O risco do usuário final entra em jogo quando uma empresa fornece ao usuário final médio acesso a processos baseados em sistema. Isso pode ser mitigado por meio do gerenciamento de risco de computação do usuário final.

O teste de penetração é necessário, além de avaliar a segurança, para avaliar também a eficiência dos sistemas defensivos e estratégias de segurança. Em um pentest, um hacker ético encontra vulnerabilidades de segurança em seu aplicativo, rede ou sistema e ajuda você a corrigi-los antes que os invasores descubram esses problemas e os explorem. Isso torna o Petesting uma etapa fundamental não negociável para um site ou proprietário de empresa (VARGHESE, 2022).

O teste de penetração não é uma operação única. É um processo sofisticado e dinâmico vitalício para as organizações e deve ser realizado de forma abrangente por profissionais. Normalmente o contratante “Ethical Hackers” realiza os pentests. O teste realizado por alguém que não conhece o sistema garante que todas as vulnerabilidades do sistema sejam expostas.

2. OBJETIVO DA PESQUISA, ESCOPO E DESCRIÇÃO DA EMPRESA

O presente trabalho objetiva a realização de pentests em uma rede de redox- APIs e plataforma para sistemas de saúde para identificar suas vulnerabilidades. Através a aplicação de pentests. O site foi encontrado através da plataforma digital Bugcrowd. Este, possui 76 vulnetrabilidades recompensadas, com validação em três dias e a sua aceitação ou rejeição pode ser dada 75% em três dias. Sua média de pagamento gira em média de 598 $ nos últimos três meses. As vulnerabilidades encontradas não devem ser divulgadas ao público.

O Redox existe para melhorar a saúde, unindo pacientes e provedores por meio de tecnologia facilmente acessível. A tecnologia pode melhorar drasticamente a saúde. Ele ajuda as organizações de saúde a se tornarem mais eficientes. Dá aos pacientes mais controle de sua experiência de saúde. E quando bem feita, a tecnologia remove as distrações para que os provedores possam se concentrar no que é importante: seus pacientes. O Redox mantém os

pacientes na vanguarda, ajudando fornecedores e fornecedores a se integrarem com segurança, facilidade e custo reduzido.

A integração de assistência médica entre aplicativos de software críticos e inovadores prejudica as experiências de assistência médica nos Estados Unidos todos os dias. As estimativas são de que há mais de $ 750 bilhões desperdiçados em saúde a cada ano. Redox pretende se tornar uma das marcas mais confiáveis na área da saúde. A plataforma Redox fornece uma solução altamente escalável que elimina barreiras técnicas. Desde a obtenção de dados HL7 por VPNs até uma infinidade de APIs de fornecedores de EHR (registro eletrônico de saúde) e até mesmo XML por SFTP, precisamos fazer tudo com segurança.

Edifício da empresa redox.

Em relação ao escopo, fazem parte os sites fornecidos e permitidos sendo alvo primário: 10x.redoxengine.com: ReactJS, Bootstrap, jQuery, jQuery, +1 _ sendo subdividos dentro dele os demais outros links de sites parte do escopo; Alvos de escopo sencundário: https://docs.redoxengine.com/ para teste de site. Sendo considerado fora do escopo: https://dashboard.redoxengine.com/. O teste só é autorizado nos alvos listados como Dentro do escopo. Qualquer domínio/propriedade do Redox não listado na seção de destinos está fora do escopo. Isso inclui qualquer/todos os subdomínios não listados acima.

3. MÉTODO

Os testes foram realizados entre os dias 27-28 de Novembro de 2022.

4. DETALHAMENTO DOS DADOS DO SITE, SUBDOMÍNIOS E SOFTWARES INSTALADOS

Primários

10x.redoxengine.com	ReactJS Bootstrap jQuery +1
https://testapi.redoxengine.com	Teste de API
testapp.redoxengine.com	Teste de API ExpressJS HTTP +1
testftp.redoxengine.com	Teste de API HTTP
https://webhooks10x.redoxengine.com	Teste de API HTTP
https://testcarequality.redoxengine.com	Teste de API HTTP
https://testclientcert.redoxengine.com	Teste de API HTTP
https://test-pointclickcare.redoxengine.com	Teste de API HTTP
https://testblob.redoxengine.com/upload	Teste de API HTTP
https://testflatfileparser.redoxengine.com	Teste de API HTTP

Secundários

https://docs.redoxengine.com/	Teste de site
https://fhir.redoxengine.com/	Teste de site
https://explore.redoxengine.com/	Teste de site
https://www.redoxengine.com/	wordpress Teste de site
https://help.redoxengine.com	Teste de site

Fora do escopo

https://dashboard.redoxengine.com/	Teste de site
candi.redoxengine.com	Teste de API HTTP
api.redoxengine.com	Teste de API HTTP
Contact forms on https://www.redoxengine.com	Teste de site
https://sso.redoxengine.com	Teste de site
https://jobs.lever.co/redoxengine/	Teste de site
https://redox.slack.com	
https://api.segment.io	
https://docs.redoxengine.com/feedback	

5. Quadro SWOT da segurança do site (FORÇAS, FRAQUEZAS, OPORTUNIDADES E AMEACAS)

Forças:	Oportunidades:

• Sistemas seguros; • Promessa de remuneração ao invasor que encontrar alguma fragilidade.	• O sistema de recompensa permite conseguir hackers se tornarem parceiros e não inimigos. • Oportunidade de parceria com hackers.
Fraquezas: • Fragilidade na senha do e-mail que permitiu ser hackeada por 3 vezes. • Fragilidade do sistema de identificação de acessos não permitidos.	Ameaças: • Ser invadido uma vez, pode fazer do e-mail uma porta de invasão para outros sistemas da empresa.

6. RELATÓRIO E FERRAMENTAS USADAS

Primeiro Ataque

Social Engineering Toolkit- Também conhecido como SET, o Social Engineering Toolkit é desenvolvido para auxiliar em testes de penetração contra elementos humanos.

Select from the menu:

1) Spear-Phishing Attack Vectors

2) Website Attack Vectors

3) Infectious Media Generator

4) Create a Payload and Listener

5) Mass Mailer Attack

6) Arduino-Based Attack Vector

7) Wireless Access Point Attack Vector

8) QRCode Generator Attack Vector

9) Powershell Attack Vectors

10) Third Party Modules

99) Return back to the main menu.

set> 2

The Web Attack module is a unique way of utilizing multiple web-based attacks in order to compromise the intended victim.

The Java Applet Attack method will spoof a Java Certificate and deliver a metasploit based payload. Uses a customized java applet created by Thomas Werth to deliver the payload.

The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a Metasploit payload.

The Credential Harvester method will utilize web cloning of a web- site that has a username and password field and harvest all the information posted to the website.

The TabNabbing method will wait for a user to move to a different tab, then refresh the page to something different.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements to make the highlighted URL link to appear legitimate however when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settings in the set_config if its too slow/fast.

The Multi-Attack method will add a combination of attacks through the web attack menu. For example you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based powershell exploitation through the browser.

1) Java Applet Attack Method

2) Metasploit Browser Exploit Method

3) Credential Harvester Attack Method

4) Tabnabbing Attack Method

5) Web Jacking Attack Method

6) Multi-Attack Web Method

7) HTA Attack Method

99) Return to Main Menu set:webattack>5

The first method will allow SET to import a list of pre-defined web applications that it can utilize within the attack.

The second method will completely clone a website of your choosing and allow you to utilize the attack vectors within the completely same web application you were attempting to clone.

The third method allows you to import your own website, note that you should only have an index.html when using the import website functionality.

1) Web Templates

2) Site Cloner

3) Custom Import

99) Return to Webattack Menu set:webattack>2

--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ---

The way that this works is by cloning a site and looking for form fields to rewrite. If the POST fields are not usual methods for posting forms this could fail. If it does, you can always save the HTML, rewrite the forms to be standard forms and use the "IMPORT" feature. Additionally, really important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL IP address below, not your NAT address. Additionally, if you don't know

basic networking concepts, and you have a private IP address, you will

need to do port forwarding to your NAT IP address from your external IP

address. A browser doesns't know how to communicate with a private IP

address, so if you don't specify an external IP address if you are using

this from an external perpective, it will not work. This isn't a SET issue

this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]:The first method will allow SET to import a list of pre-defined web

applications that it can utilize within the attack.

The second method will completely clone a website of your choosing

and allow you to utilize the attack vectors within the completely

same web application you were attempting to clone.

The third method allows you to import your own website, note that you

should only have an index.html when using the import website

functionality.

1) Web Templates

2) Site Cloner

3) Custom Import

99) Return to Webattack Menu

set:webattack>1

[-] Credential harvester will allow you to utilize the clone capabilities within SET

[-] to harvest credentials or parameters from a website as well as place them into a report

---

--- * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ---

The way that this works is by cloning a site and looking for form fields to rewrite. If the POST fields are not usual methods for posting forms this could fail. If it does, you can always save the HTML, rewrite the forms to be standard forms and use the "IMPORT" feature. Additionally, really important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL IP address below, not your NAT address. Additionally, if you don't know basic networking concepts, and you have a private IP address, you will need to do port forwarding to your NAT IP address from your external IP address. A browser doesns't know how to communicate with a private IP address, so if you don't specify an external IP address if you are using this from an external perpective, it will not work. This isn't a SET issue this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.2.15]:https://forms.hubspot.com/collected-forms/submit/form

---

** Important Information **

For templates, when a POST is initiated to harvest

credentials, you will need a site for it to redirect.

You can configure this option under:

/etc/setoolkit/set.config

Edit this file, and change HARVESTER_REDIRECT and
HARVESTER_URL to the sites you want to redirect to
after it is posted. If you do not set these, then
it will not redirect properly. This only goes for
templates.

---

1. Java Required
2. Google
3. Twitter

set:webattack> Select a template:2

[*] Cloning the website: http://www.google.com
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
^[[A^[[A^[[B^[[B^C

Press <return> to continue[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:

[*] Cloning the website: http:// applications that it can utilize within the attack.

[*] This could take a little bit...

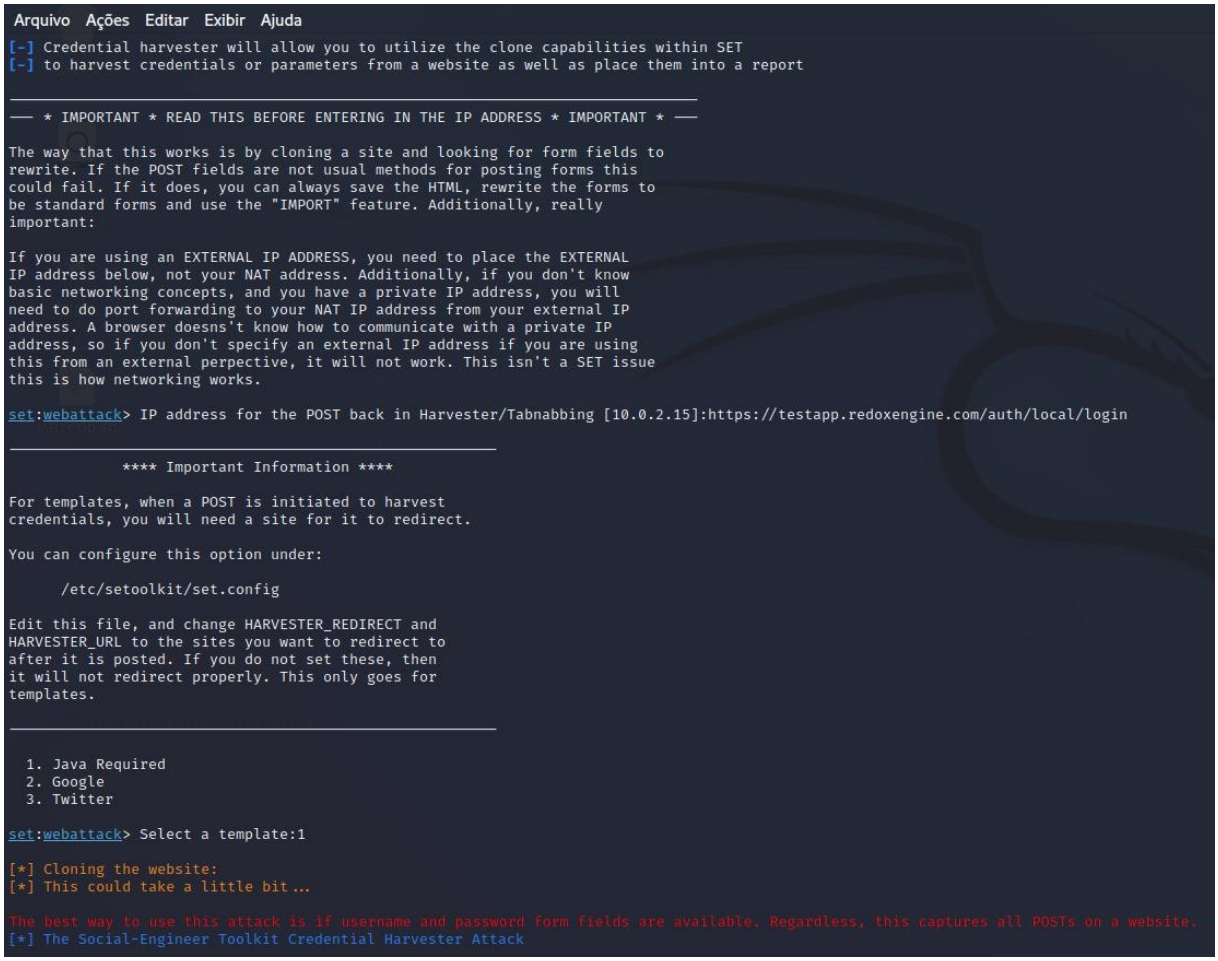
The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.

[*] Web Jacking Attack Vector is Enabled...Victim needs to click the link.

[*] The Social-Engineer Toolkit Credential Harvester Attack

[*] Credential Harvester is running on port 80

2.2 Segundo ataque

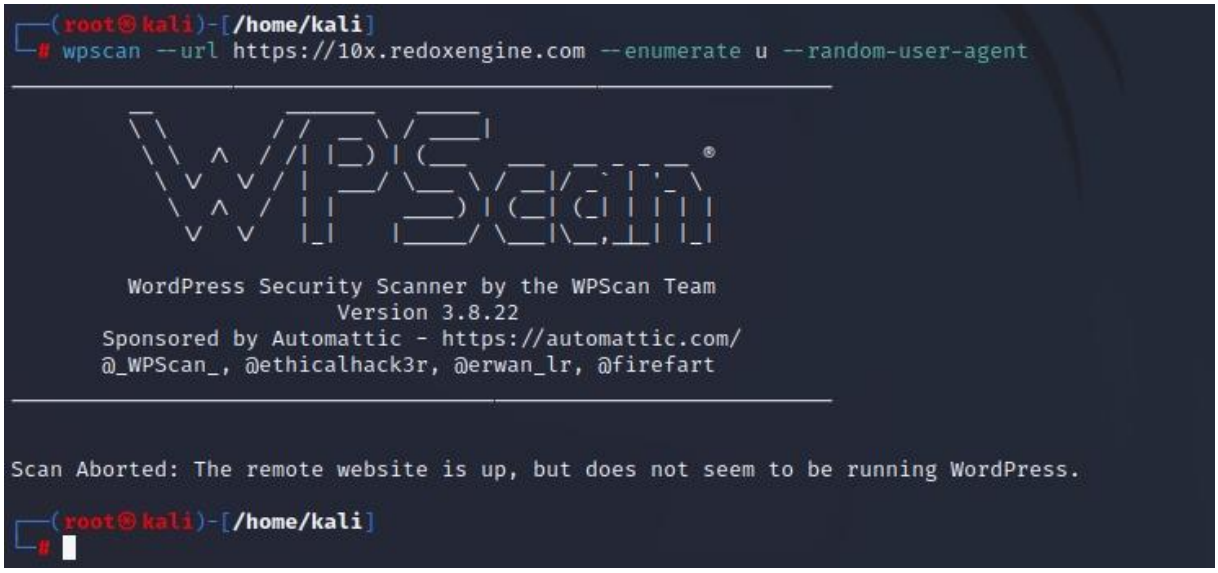


Terceiro relatório

Levantamento de informações em servidores DNSenum para identificação de fraquezas.

Quarto ataque

O WPScan é uma ferramenta voltada para a análise de vulnerabilidades presentes em um site desenvolvido no WordPress. Além de detectar os pontos que apresentam fragilidade, o programa ainda informa qual exploit deve ser utilizado para explorar e corrigir o problema.



7. VERIFICAÇÃO DE VULNERABILIDADES SOFRIDAS NO E-MAIL DA EMPRESA

Observa-se que o e-mail da empresa já sofreu 3 invasões. Uma das estratégias para proteção é a escolha forte de senha do e-mail. Conforme as recomendações de segurança para senhas descritas neste trabalho.

8. POLÍTICA DE SENHAS

Diretrizes do Uso de Senhas

1. Senhas de Uso Normal

a) O usuário é o único responsável pelo uso de suas credenciais deacesso. Considerando que a senha é a principal ferramenta de autenticação, ela deve ser individual, intransferível e mantida em segredo, sendo o usuário responsabilizado por qualquer transação efetuada durante o seu uso. Então, nunca revele sua senha a ninguém, nem mesmo o seu gestor e jamais deixe que alguém utilize os sistemas da FGV autenticado com o seu login e senha.

b) As senhas não devem ser trafegadas em mensagens de e-mail, em chamados, em aplicativos de mensagens instantâneas, não devem ser anotadas e ou armazenadas em dispositivos moveis (salvo em aplicativo específico para tal funcionalidade que conte com criptografia forte);

c) Os sistemas, serviços e dispositivos da FGV devem ser configurados para que os padrões mínimos de senha forte sejam exigidos na criação, conforme as recomendações abaixo:

Conter pelo menos 3 das 4 diretrizes abaixo:

Conter pelo menos uma letra maiúscula;

Conter pelo menos uma letra minúscula;

Conter números (0 a 9);

Conter símbolos, incluindo: ! @ # $ % ^ & * - _ + = [ ] { } | \ : ‘, . ? / ` ~ “ < > ( ) ;

Tamanho de no mínimo 8 caracteres;

Não é permitido utilizar as 5 últimas senhas cadastradas;

Mandatório alterar a senha a cada 180 dias;

A conta do usuário é bloqueada após 10 tentativas de acesso com senha errada;

A conta permanecerá bloqueada por 30 minutos. Após os 30 minutos, a conta é automaticamente desbloqueada para até 10 tentativas de acesso;

d) As solicitações de acesso devem ser realizadas através do Service Desk e autorizadas pelo gestor imediato;

e) As solicitações de recuperação de senhas, por esquecimento ou outro motivo, devem ser realizadas através do Service Desk e seguirão um procedimento de validação de informações do usuário para disponibilizar as senhas iniciais;

f) As senhas iniciais devem ser fornecidas diretamente aos usuários e configuradas de forma que, no primeiro acesso, a solicitação de troca ocorra automaticamente.

2. Senhas de Uso Privilegiado

a) Todas as contas privilegiadas (ex: administrator, asgv, root, etc.) devem ter as senhas trocadas, renomeadas e desabilitadas;

b) Os acessos privilegiados, por questões de segurança, devem ser realizados por uma quantidade mínima de usuários, que terão perfis de administradores e autorização de acesso para essas funcionalidades;

c) Caso as contas privilegiadas não possam ter as senhas trocadas ou renomeadas, serão desabilitadas e consideradas “contas de serviço” não sendo utilizadas para qualquer tipo de acesso;

d) As senhas não devem ser introduzidas em linhas de comando (códigos fontes) e ou em scripts abertas, mas, caso seja necessário, devem ser criptografadas e consideradas “contas de serviço”.

e) Todas senhas em trânsito, ou seja, que sejam trafegadas pela rede obrigatoriamente deverão estar encriptadas.

3. Boas práticas para Criação de Senhas

a) Evitar a utilização de:

Nomes, sobrenomes, nomes de contas de usuários e dados de membros da família, números de documentos, números de telefone, placa de carros e datas comemorativas;

Sequência do teclado (ex.: asdfg123);

Palavras do dicionário, nomes de times de futebol, de música, de produtos, de personagens de filmes, etc.

b) Utilizar:

Números aleatórios;

Vários e diferentes tipos de caracteres;

Caracteres especiais;

Substituir uma letra por número com semelhança visual;

A primeira, a segunda ou a última letra de cada palavra. Exemplo: com a frase "O Cravo brigou com a Rosa debaixo de uma sacada" você pode gerar a senha "?OCbcaRddus" (o sinal de interrogação foi colocado no início para acrescentar um símbolo à senha).

4. Perda da Credencial

a) No caso de perda da credencial o usuário deverá avisar imediatamente ao Service Desk que entrará em contato com os responsáveis pela gestão de acessos e esses irão:

Invalidar a credencial antiga; e

Em até um dia útil enviar uma nova credencial.

5. Desligamento / Remoção do acesso

a) No caso de interrupção de vínculo do usuário com a FGV, deverá ser solicitado ao Service Desk a remoção de todos os acessos com pelo menos dois dias uteis de antecedência;

b) A área de Recursos Humanos (RH) poderá solicitar, de forma proativa, a revogação dos acessos;

c) A conta deve ser inativada de forma imediata pela área técnica e consequentemente bloqueados os acessos em todos os recursostecnológicos e áreas físicas da FGV.

6. Desvio e Exceção

a) Todo e qualquer desvio e/ou exceção deve ser comunicado à área de Segurança da Informação que fará a devida avaliação;

b) Qualquer uso indevido da credencial, seja intencional ou não, será comunicado ao responsável pelo usuário e/ou ao Departamento de Recursos Humanos para que sejam tomadas as medidas administrativas e/ou legais cabíveis.

9. POLÍTICA DE SGURANÇA CIBÉRICA

- Toda informação deve ter regras claramente definidas pelo seu proprietário para proteção contra perda, alteração e acesso, seja ela armazenada em meio eletrônico (computador central, servidores de rede, microcomputadores, pen drive), em papel (correspondências, atas, relatórios, manuscritos, etc.) ou outros meios.
- Toda informação deve ter usuários explicitamente definidos (instituições, áreas, pessoas) e os tipos de direitos que cada um terá para acessá-la.
- Toda informação deverá ter procedimentos para protegê-la do acesso de pessoas não autorizadas.
- Toda informação que garanta a continuidade das atividades dos integrantes do sistema RODAX, deverá ter cópia de segurança em local físico distinto, devidamente protegido para essa finalidade ou outro meio eficiente para permitir sua pronta recuperação em caso de perda ou danos.
- As informações contidas em material que se tornar disponível paradescarte (papel, pendrives, cd, etc.) deverão ser destruídas ou mantidas em locais fechados, protegidas do acesso de pessoas não autorizadas.
- Todo colaborador do RODAX é responsável pela segurança da informação a que tem acesso.
- Toda informação encontrada extraviada deverá ser, imediatamente, devolvida a sua origem.
- Os equipamentos que contiverem informações dos integrantes do sistema RODAX, somente poderão ser deslocados para venda, manutenção, etc., quando certificado de que as informações neles contidos estejam formatadas.

10. RECOMENDAÇÕES PARA O TRATAMENTO DA INFORMAÇÃO

- Os colaboradores não devem efetuar tentativas de obter acesso às informações que não lhe são permitidos, devendo solicitá-las ao respectivo proprietário da informação, pasta ou arquivo.
- A elaboração das normas e procedimentos de acesso deverá levar em consideração os riscos do acesso e alteração não autorizados, divulgação indevida e indisponibilidade dos dados, que tem por consequência às fraudes, problemas legais, perdas de negócios, danos à imagem e dificuldade na recuperação da informação.
- Todas as informações devem ser classificadas.
- Toda a informação deverá ser considerada sigilosa e de alto risco até que se tenha estabelecido sua classificação.
- A proteção proporcionada à informação, tanto em termos de acesso quanto de conservação, deve estar de acordo com sua classificação.
- Quando em um mesmo meio físico existirem informações classificadas de formas diferentes, deve-se adotar, para fins de segurança, a classificação mais restrita.
- Sempre que forem efetuadas alterações significativas em um sistema, ou nas características de uma informação, deverá ser comunicado aos usuários com antecedência e efetuada uma revisão de classificação.

Restrições de acesso

- Controlado: O acesso às informações sigilosas, confidenciais e internas, deverá ser determinado pelo Conselho de Administração, que estabelecerá as áreas, pessoas e o nível desse acesso;
- Não Controlado: As informações públicas não estarão sujeitas ao controle de acesso. Somente para consulta: Nível de acesso do usuário permite somente a leitura das informações.
- Consulta e alteração: Nível de acesso do usuário permite efetuar mudanças nas informações disponibilizadas, como inclusão de pareceres, informações complementares, valores, etc.

  De Alto Risco: Informações cuja indisponibilidade e/ou inexatidão poderão causar prejuízos à continuidade dos negócios.

- De Médio Risco: Informações que impõem ao negócio problemas de disponibilidade e dificuldade na recuperação. O proprietário da informação e os usuários aceitam a disponibilidade limitada e a existência de um determinado tempo para recuperação.
- De Baixo Risco: Informações cuja exatidão e acessibilidade apresentam pouco ou nenhum risco ao negócio. Os usuários aceitam eventuais indisponibilidades e longos períodos para recuperação das informações.

Análise de vulnerabilidade

- Periodicamente devem ser realizados testes de vulnerabilidades técnicas dos equipamentos críticos da infraestrutura.
- Após os levantamentos, as comparações e identificações dos riscos devem ser executadas, possibilitando o tratamento dos riscos de acordo com seus níveis.
- Nos casos em que não for possível a eliminação total da vulnerabilidade, deve ser apresentada aceitação do risco ou a determinação de falso positivo.
- Verificações ou auditorias regulares devem verificar a conformidade com as exigências técnicas dos sistemas e das redes.
- As auditorias realizadas por terceiros devem identificar claramente as interações com os sistemas em operação.
- As auditorias técnicas dos sistemas e das redes devem respeitar as práticas estabelecidas e devem ser realizadas de acordo com as recomendações da organização. Estas auditorias devem ser realizadas por fornecedores reconhecidos e competente.
- Prevenção e detecção de intrusão
- Todos os recursos do sistema de informação expostos à Internet devem ser acompanhados e protegidos por um IDS / IPS.
- Sempre que o IDS / IPS detecta ou responde a uma tentativa externa mal-intencionada suficientemente grave para ameaçar os recursos do sistema de informações protegidas, uma análise estruturada e procedimento de resposta deve ser acionado.

Proteção contra códigos maliciosos

- Deverão ser implementados controles tecnológicos para a proteção dos equipamentos de processamento de informação que executem algum tipo de software (tanto de usuário final como servidores) para a prevenção, detecção, correção e erradicação de códigos executáveis maliciosos.

- Deve ser verificada a atualização das ferramentas de proteção baseadas em assinaturas, para que estejam nas últimas atualizações disponíveis.

Controles criptográficos

- Deverão ser utilizados controles criptográficos para proteger as informações segundo os requerimentos da sua classificação.
- Somente algoritmos de criptografia aprovados pela área de gestão de risco podem ser utilizados nas soluções e sistemas adotados pelo RODOX.
- O gerenciamento das chaves de criptografia deve prever mecanismos para o armazenamento seguro, geração segura da chave e destruição da chave.
- Deverá existir um mecanismo de recuperação da informação caso seja perdida uma chave de criptografia.
- As chaves de criptografia devem ser trocadas periodicamente, dependendo da sua frequência de utilização.
- Caso seja comprometida uma chave criptográfica, deve ser revogada imediatamente. Se for uma chave para criptografia de arquivos, deve ser trocada.
- Mecanismos de autenticação e auditoria devem ser estabelecidos para garantir a segurança do acesso às chaves.

Penalidade

- O Colaborador que presenciar o descumprimento de alguma das regras acima tem o dever de denunciar tal infração. Ademais, o descumprimento das regras e diretrizes impostas neste documento poderá ser considerado falta grave, passível de aplicação de sanções disciplinares.

Serviço de nuvem

- A possibilidade de utilização de uma solução de hospedagem externa, e, mais especificamente, uma solução 'cloud computing', depende do nível de ensibilidade dos dados e os processos em questão. Esta escolha deve ser feita com base em uma análise de risco.
- Toda e qualquer contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem deverá ser previamente comunicada ao Banco Central do Brasil.
- Os serviços para processamentos de dados e ou armazenamento em nuvem, sejam eles software como serviço (SaaS) ou armazenamento de base de dados devem possuir

acesso seguro através de interfaces HTTPS bem como a autenticação segura e em ambientes segregados.

- Os acessos devem ser controlados por meio de logins e senhas individuais, previamente fornecidos, de acordo com a atividade de cada colaborador/terceiro ou administrador, possuindo também tais acessos e ações registrados em trilhas de auditorias.

Aquisição e desenvolvimento seguro de sistemas

- Sistemas da informação desenvolvidos ou adquiridos devem contar com atributos e funcionalidades de segurança que protejam adequadamente as informações.
- Os requerimentos devem ser identificados e documentados na fase de concepção do sistema, para assegurar que as demandas de segurança sejam atendidas.
- Deve haver controles que previnam erros de operação, perda, ou vazamento de informações. Todo sistema deve ser documentado, tornando sua implantação e operação independente de conhecimentos informais.
- Devem ser estabelecidos controles criptográficos para proteger a confidencialidade, autenticidade ou integridade das informações. Faz-se necessária a documentação do uso de chaves, quando necessário.
- Sistemas devem ser protegidos contra alteração indevida, evitando a exposição de dados sensíveis. Devem ser estabelecidos controles para monitorar e corrigir as vulnerabilidades e falhas desses

11. CONTRATO DE SERVIÇO DE ACORDO DE CONFIDENCIALIDADE DA INFORMAÇÃO E RESPONSABILIDADE

A empres Redox de Bulhayau, com sede na Av. camaris bargat, nº 251, bist merp, inscrito no CNPJ/MF sob o nº 04.911.713/0001-08, doravante denominado CONTRATANTE, neste ato representado por seu Diretor Presidente, Welguwer Baslayu, CPF nº 25348596147, residente e domiciliado nesta Capital, no uso das atribuições que lhe são conferidas e Lunat, Ltd, inscrita no CNPJ/MF nº 12.565.545./0001-24, com endereço na <Rua cabast>, doravante denominada CONTRATADA, residente e domiciliado na namaacha, firmam o presente ACORDO DE CONFIDENCIALIDADE DE INFORMAÇÃO E RESPONSABILIDADE, decorrente da realização do Contrato nº <número do contrato>, que entra em vigor neste dia ___45_ de _____Novembro_____ de 2022__ e é regido mediante as cláusulas e condições seguintes:

1. DA INFORMAÇÃO CONFIDENCIAL

Para fins do presente Acordo, são consideradas INFORMAÇÕES SIGILOSAS, os documentos e informações transmitidos pela CONTRATANTE e recebidos pela CONTRATADA através de seus diretores, sócios, administradores, empregados, prestadores de serviço, prepostos ou quaisquer representantes.

Tais documentos e informações não se limitam, mas poderão constar de dados digitais, desenhos, relatórios, estudos, materiais, produtos, tecnologia, programas de computador, especificações, manuais, planos de negócio, informações financeiras, e outras informações submetidas oralmente, por escrito ou qualquer outro tipo de mídia. Adicionalmente, a expressão INFORMAÇÕES SIGILOSAS inclui toda informação que CONTRATADA possa obter através da simples visita às instalações da CONTRATANTE.

2. DOS LIMITES DA CONFIDENCIALIDADE DAS INFORMAÇÕES

Para fins do presente Acordo, não serão consideradas INFORMAÇÕES SIGILOSAS as que:

2.1 São ou tornaram-se públicas sem ter havido a violação deste Acordo pela CONTRATADA;

2.2 Eram conhecidas pela CONTRATADA, comprovadas por registros escritos em posse da mesma, antes do recebimento delas pela CONTRATANTE;

2.3 Foram desenvolvidas pela CONTRATADA sem o uso de quaisquer INFORMAÇÕES SIGILOSAS;

2.4 Venham a ser reveladas pela CONTRATADA quando obrigada por qualquer entidade governamental jurisdicionalmente competente;

2.4.1 Tão logo inquirida a revelar as informações, a CONTRATADA deverá informar imediatamente, por escrito, à CONTRATANTE, para que este requera medida cautelar ou outro recurso legal apropriado;

2.4.2 A CONTRATADA deverá revelar tão somente as informações que forem legalmente exigidas;

3. DAS OBRIGAÇÕES DA CONTRATADA

Consiste nas obrigações da CONTRATADA:

3.1 Garantir que as Informações Confidenciais serão utilizadas apenas para os propósitos do contrato nº <número do contrato>, e que serão divulgadas apenas para seus diretores, sócios, administradores, empregados, prestadores de serviço, prepostos ou quaisquer representantes, respeitando o princípio do privilégio mínimo com devida classificação de informação conforme ABNT NBR ISO IEC 27002:2005;

3.2 Não divulgar, publicar, ou de qualquer forma revelar qualquer INFORMAÇÃO SIGILOSA recebida através da CONTRATANTE para qualquer pessoa física ou jurídica, de direito público ou privado, sem prévia autorização escrita da CONTRATANTE;

3.3 Garantir que qualquer INFORMAÇÃO SIGILOSA fornecida por meio tangível não deve ser duplicada pela CONTRATADA exceto para os propósitos descritos neste acordo;

3.4 A pedido da CONTRATANTE, retornar a ele todas as INFORMAÇÕES SIGILOSAS recebidas de forma escrita ou tangível, incluindo cópias, reproduções ou outra mídia contendo tais informações, dentro de um período máximo de 10 (dez) dias após o pedido;

3.4.1 Como opção para CONTRATADA, em comum acordo com a CONTRATANTE, quaisquer documentos ou outras mídias possuídas pela CONTRATADA contendo INFORMAÇÕES SIGILOSAS podem ser destruídas por ela;

3.4.1.1 A destruição de documentos em papel deverá seguir recomendação da norma DIN 32757-1: 4, ou seja, destruição do papel em partículas de, no mínimo, 2 x 15mm;

3.4.1.2 A destruição de documentos em formato digital deverá seguir a norma DoD 5220.22-M (ECE) ou o método descrito por Peter Gutmman no artigo “Secure Deletion of Data From Magnetic and Solid-State Memory” ou através da utilização de desmagnetizadores (degausser);

3.4.1.3 A destruição das INFORMAÇÕES SIGILOSAS que não estiverem nos formatos descritos nos itens

3.4.1.1 e 3.4.1.2 deverá ser previamente acordada entre a CONTRATANTE e a CONTRATADA;

3.4.1.4 A CONTRATADA deverá fornecer à CONTRATANTE certificado com respeito à destruição, confirmando quais as informações que foram destruídas e os métodos utilizados, dentro de um prazo máximo de 10 (dez) dias;

3.5 A CONTRATADA deverá dar ciência deste acordo a todos seus sócios, empregados, prestadores de serviço, prepostos ou quaisquer representantes que participarão da execução dos serviços objetos do contrato vierem a ter acesso a quaisquer dados e informações confidenciais cumpram as obrigações constantes deste Acordo e que será responsável solidariamente por eventuais descumprimentos das cláusulas aqui descritas;

4. DA PROPRIEDADE DAS INFORMAÇÕES SIGILOSAS

4.1 A CONTRATADA concorda que todas as INFORMAÇÕES SIGILOSAS permanecem como propriedade da CONTRATANTE e que este pode utilizá-las para qualquer propósito sem nenhuma obrigação com ela;

4.2 A CONTRATADA concorda ter ciência de que este acordo ou qualquer INFORMAÇÕES SIGILOSAS entregues pela CONTRATANTE a ela, não poderá ser interpretado como concessão a qualquer direito ou licença relativa à propriedade intelectual (marcas, patentes, copyrights e segredos profissionais) à CONTRATADA;

4.3 A CONTRATADA concorda que todos os resultados dos trabalhos prestados por ela à CONTRATANTE, inclusive os decorrentes de especificações técnicas, desenhos, criações ou aspectos particulares dos serviços prestados, são reconhecidos, irrestritamente, neste ato, como de exclusiva propriedade do CONTRATANTE, não podendo a CONTRATADA reivindicar qualquer direito inerente à propriedade intelectual;

4.4. Utilizar os bens de informação disponibilizados por força de contrato celebrado com o SHARTEC exclusivamente para fins da adequada prestação dos serviços contratados, estritamente em observância aos interesses do SHARTEC.

4.5. Respeitar a propriedade do SHARTEC ou de terceiros, sobre os bens de informação disponibilizados, zelando pela integridade dos mesmos, não os corrompendo ou os divulgando a pessoas não autorizadas;

4.6. Manter, a qualquer tempo e sob as penas de lei, total e absoluto sigilo sobre os bens de informação do SHARTEC, utilizando-os exclusivamente para os fins de interesse deste, estritamente no desempenho das atividades inerentes a prestação dos serviços contratados, não os revelando ou divulgando a terceiros, em hipótese alguma, sem o prévio e expresso consentimento do SHARTEC;

4.7. Instalar e utilizar nos ambientes computacionais disponibilizados pelo SHARTEC somente softwares desenvolvidos ou adquiridos pelo SHARTEC; 4.8. Permitir ao SHARTEC

a fiscalização, a qualquer tempo, de todos os dados manejados através dos meios fornecidos pelo SHARTEC em razão da prestação de serviços contratados, pelo que autorizo o SHARTEC a monitorar todos os dados manejados nos meios de propriedade do contratante, não configurando o referido monitoramento qualquer quebra de sigilo ou invasão de privacidade.

4.9. Não utilizar o ambiente de internet disponibilizado pelo SHARTEC para uso pessoal, ilícito, ilegal, imoral ou para quaisquer outros fins senão os de estrita prestação dos serviços contratados.

5. DOS PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO DA CONTRATANTE

5.1 A CONTRATADA declara que recebeu cópia e está ciente da Política de Segurança da Informação da CONTRATANTE, definida pelo Conselho de Administração em Reunião Ordinária realizada em 13 de julho de 2016, e de todos os seus documentos acessórios já criados;

5.2 A CONTRATADA declara que seguirá todas as políticas, normas e procedimentos de segurança da informação definidos e/ou seguidos pela CONTRATANTE;

5.3. A CONTRATADA declara que seguirá todas as políticas, normas e procedimentos de continuidade definidos e/ou seguidos pela CONTRATANTE;

5.4. Seguir os Manuais de Normas e Procedimentos da área de Gestão de Riscos Operacionais, Manual de Boas Práticas de Segurança da Informação

6. DO PRAZO DE VALIDADE DO ACORDO As obrigações tratadas neste acordo subsistirão permanentemente, mesmo após a conclusão dos serviços ou até que a CONTRATANTE comunique expressa e inequivocadamente, por escrito, à CONTRATADA, que as informações já não são mais sigilosas.

7. DAS PENALIDADES Qualquer divulgação de dados, materiais, desenhos ou informações, obtidos em razão dos serviços por CONTRATADA, ou prepostos e seus funcionários, sem a respectiva autorização prévia, expressa e escrita da CONTRATANTE, implicará na obrigatoriedade de CONTRATADA ressarcir as perdas e danos experimentados pela CONTRATANTE, sem prejuízo das penalidades civis e criminais previstas em lei.

8. DO FORO Fica eleito o foro da Justiça Estadual, Seção Judiciária de Belém, na cidade do Belém, para dirimir dúvidas decorrentes do presente Acordo. E, por estarem assim justas e

contratadas, firmam o presente instrumento, em 3 (três) vias de igual teor e forma, para que se produzam os necessários efeitos legais.

EMPRESA CONTRATADA

LUTA, LTD.

Anatércia Arrone

Aos 22/09/2022

EMPRESA CONTRATANTE

Redox,ltd

Vilmer Cahdheb

22/09/2022

ORDEM DE SERVIÇO – Nº45

12. PRESTAÇÃO DE SERVIÇOS DE EXECUÇÃO DE TESTES DE PENETRAÇÃO (PENTEST) E ANÁLISE DE VULNERABILIDADES DE SEGURANÇA

CONTRATO Nº 5845 PREGÃO 99.999/99

A presente ordem de serviço é celebrada em conformidade com o procedimento para PRESTAÇÃO DE SERVIÇOS DE EXECUÇÃO DE TESTES DE PENETRAÇÃO (PENTEST) E ANÁLISE DE VULNERABILIDADES DE SEGURANÇA, previstos no Contrato Nº1 4 firmado entre a EMPRESA DE TECNOLOGIA DA INFORMAÇÃO LUNAT, ltd e a REDOX, em vigor desde 2 0 de 09 De2022, sendo incorporada ao mesmo por referência.

Quantidade de horas	Período		Valor Total
	Início	Fim	
8	07:00H	17:00	3000.00
TOTAL GERAL			

Para efeito do cumprimento desta ORDEM DE SERVIÇO a CONTRATANTE indica o seguinte responsável:

Nome: Maria nunes Cerleg		
Gerência:02	Unidade:A3	Matrícula:2554
Endereço:Av. Calet, rua bistoc		
Telefone:63 56554 245	Fax: 3345265	

Bulawof, 22/09/2022

REDOX LUNAT, LTD

CONTRATANTE CONTRATADA

13. CONCLUSÃO

Por meio do presente trabalho, foi possível realizar o pentest na empresa Redox, porém não foi possível identificar nenhuma vulnerabilidade por meio dos testes realizados. Não foi possível invadir pois o sistema de segurança deles está bem equiparado. Normalmente empresas que prometem bom pagamento em caso de descoberta de vulnerabilidade são difíceis de invadir porque já garantem sua segurança. Mas o e-mail demostrou que já foi hackeado por três vezes, possivelmente pela fragilidade da senha.

14. LINKS DAS REFERÊNCIAS USADAS

ASSUNÇÃO, Marcos Flávio Araújo. Análise de Vulnerabilidades e Testes de Invasão. 2017. 263 f. Monografia (Especialização) - Curso de Pós Graduação - Segurança da Informação, Centro Universitário Una, Belo Horizonte, 2017.

BACUDIO, et al. An Overview of Penetration Testing, 2011. Acesso em: 27 de Novembro de 2022. Disponível em: https://www.researchgate.net/publication/274174058_An_Overview_of_Penetration_Testing

BERTOGLIO, Daniel Dalalana; ZORZO, Avelino Francisco. Um Mapeamento Sistemático sobre Testes de Penetração. 2015. 42 f. Monografia (Doutorado) - Curso de Pós-Graduação em Ciência da Computação, Pontifícia Universidade Católica do Rio Grande do Sul Faculdade de Informática, Porto Alegre, 2015.

VARGHESE, J. Auditoria de segurança: O que é Pentest ou teste de penetração (em segurança cibernética), 2022. Acesso em: 27 de Novembro de 2022. Disponível em: **https://www.getastra.com/blog/security-audit/penetration-testing/**