PROFEPT
PROGRAMA DE PÓS-GRADUAÇÃO EM EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA

INSTITUTO FEDERAL
Alagoas

Sequência Didática

O ensino de segurança da informação por meio de aplicação virtual disponibilizada em contêiner utilizando abordagem Problem-Based Learning

Maceió, AL - 2023

FICHA TÉCNICA DO PRODUTO EDUCACIONAL

Título: Sequência didática para o ensino de segurança da informação por meio de aplicação virtual disponibilizada em contêiner utilizando abordagem Problem-Based Learning

Autor: Byron Loureiro Lanverly de Melo Junior

Orientador: Prof. Dr. Eduardo Cardoso de Moraes

Público Alvo: Alunos do Curso Superior de Sistemas de Informação.

Vínculo do Produto Educacional: Dissertação de Mestrado Profissional – O ensino de segurança da informação por meio de aplicação virtual disponibilizada em contêiner utilizando abordagem Problem-Based Learning

Programa de Ensino: Pós-Graduação em Educação Profissional e Tecnológica.

Instituição Associada: Instituto Federal de Alagoas – Campus Benedito Bentes.

Linha de Pesquisa: Práticas Educativas em Educação Profissional e Tecnológica.

Lócus de Implementação do Produto Educacional: Instituto Federal de Alagoas – Campus Maceió.

Palavras-chave: Segurança da informação; Contêiner; Problem-Based Learning

INSTITUTO FEDERAL
Alagoas

Dados Internacionais de Catalogação na Publicação
Instituto Federal de Alagoas
Campus Avançado Benedito Bentes
Biblioteca

M528s

Melo Junior, Byron Loureiro Lanverly de.
Sequência didática: o ensino de segurança da informação por meio de aplicação virtual disponibilizada em contêiner utilizando abordagem problem-learning / Byron Loureiro Lanverly de Melo Junior. – 2024.
30 f. : il.

Produto Educacional da Dissertação - O ensino de segurança da informação por meio de aplicação virtual disponibilizada em contêiner utilizando abordagem de aprendizagem baseada em problemas - (Mestrado em Educação Profissional e Tecnológica) Instituto Federal de Alagoas, Campus Avançado Benedito Bentes, Maceió, 2024.

1. Ensino. 2. Metodologia Ativas 3. Educação Profissional e Tecnológica.
4. Sequencia Didática I. Título.

CDD: 370

Fernanda Isis Correia da Silva
Bibliotecária - CRB-4/1796

Sumário

Apresentação

Sobre os autores

Byron Loureiro Lanverly de Melo Junior

AUTOR

Graduado em Sistemas e especialista em redes de computadores. Atualmente é professor auxiliar da Universidade Estadual de Ciências da Saúde de Alagoas. Tem experiência na área de Ciência da Computação, com ênfase em Segurança de Redes e Informação e Engenharia de Software, atuando principalmente nos seguintes temas: software livre, integração de bases, compromisso social e excelência académica, devops e relevante histórico de entregas relacionadas à Transformação Digital.
Para conhecer mais sobre a trajetória acadêmica e profissional, o currículo Lattes é a fonte mais completa.
Clique aqui para conhecer mais.

Eduardo Cardoso de Moraes

ORIENTADOR

Doutor em Engenharia Industrial com ênfase em automação e mecatrônica, com doutorado sanduíche na Alemanha. Mestre em Ciências da Computação, MBA em Gestão e Planejamento Estratégico, especialização em Informática em Saúde e graduação em Ciências da Computação. Bacharel em Direito com ênfase em Direito Digital. Técnico em Automação Industrial e Técnico em Informática.
Professor efetivo do Instituto Federal de Alagoas (IFAL).Professor permanente do Mestrado em Educação Tecnológica - ProfEPT.
Para conhecer mais sobre a trajetória acadêmica e profissional, o currículo Lattes é a fonte mais completa.
Clique aqui para conhecer mais.

1. Introdução

O mundo digital está cada vez mais presente em nossas vidas, o que torna a segurança da informação um tema cada vez mais relevante. É importante que as pessoas sejam capazes de proteger suas informações pessoais e profissionais, bem como as informações das organizações nas quais trabalham. Esta sequência didática, é um produto educacional que versa sobre a aplicação de identificação de uma vulnerabilidade web que corresponde a um dos itens que se apresenta de forma recorrente na lista que reúne as 10 falhas mais comuns, perigosas ou críticas ligadas ao desenvolvimento de projetos web, um projeto chamado OWASP (Projeto Aberto de Segurança em Aplicações Web, que é uma comunidade online que cria e disponibiliza de forma gratuita artigos, metodologias, documentação, ferramentas e tecnologias no campo da segurança de aplicações web) e pode ser acessado através deste site OWASP Foundation da (OWASP FOUNDATION, THE OPEN SOURCE FOUNDATION FOR APPLICATION SECURITY | OWASP FOUNDATION, [s. d.])

Esta sequência didática (SD) é uma ferramenta eficaz para o ensino de segurança da informação. A abordagem PBL promove a aprendizagem ativa e a resolução de problemas, enquanto a aplicação virtual facilita a distribuição e a aplicação do conteúdo.

Para melhor compreensão deste documento, sugere-se leitura total do documento e uso das referências internas aos tópicos, não deixando de visitar os links externos.

Caro leitor, fique atento ao aparecimento deste imagem durante a leitura deste material, Esta mão indica uma URL, que significa: Uniform Resource Locator, que é definida como "Localizador Uniforme de Recursos" e traz material complementar a Sequência Didática

2. Objetivos

O objetivo desta sequência didática é capacitar os alunos a compreender os conceitos básicos de segurança da informação e a aplicar esses conceitos na prática, culminando em uma avaliação por competência do aluno. A avaliação por competência, conceito proposto, pela primeira vez, associado à dimensão da gestão de pessoas, em 1973, por David McClelland, é uma metodologia de avaliação de desempenho que se baseia na identificação e avaliação das competências necessárias para o exercício de um determinado cargo ou função. As competências por sua vez são definidas como um conjunto de conhecimentos, habilidades e atitudes que permitem ao indivíduo desempenhar suas atividades de forma eficaz e eficiente. A avaliação por competência visa identificar o nível de desenvolvimento das competências pessoais, a fim de promover seu desenvolvimento e crescimento profissional. Como principais benefícios da avaliação por competência, podemos elencar: a melhoria no desempenho dos colaboradores, a Promoção do desenvolvimento profissional pessoal; a redução da rotatividade de pessoas em uma empresa e o aumento da motivação e satisfação dos colaboradores.

Para apoiar a prática em um ambiente replicável, adotamos como base o uso de tecnologia de container Docker. O Docker é uma plataforma de código aberto que permite a criação, implantação e gerenciamento de aplicativos em contêineres. Um contêiner é uma unidade de software empacotada que contém tudo o que é necessário para executar um aplicativo, incluindo o código, os arquivos de configuração e as bibliotecas. Os contêineres são isolados uns dos outros, o que significa que eles não podem acessar diretamente os recursos do sistema operacional host. Isso os torna mais leves e eficientes do que as máquinas virtuais, que virtualizam todo o sistema operacional.

Caro leitor, neste link você terá acesso ao passo a passo simples de instalação do Docker no sistema operacional proposto, o Debian.

Os contêineres são uma tecnologia importante para a computação, pois permitem que os aplicativos sejam implantados de forma rápida e fácil em diferentes ambientes. Eles também são usados em ambientes de desenvolvimento e teste para facilitar a criação e a execução de ambientes de desenvolvimento consistentes.

A avaliação, por si, deverá se dar após o ensino procedimental, capturando as percepções do aluno através de respostas em linhas conceituais e atitudinais.

3. Metodologia

A abordagem adotada para esta SD é a Problem-Based Learning (PBL) ou Aprendizagem Baseada em Problemas, que é utilizada para promover a aprendizagem ativa e a resolução de problemas. Os alunos são apresentados a um problema real do mundo da segurança da informação e são desafiados a resolvê-lo.

> O método da Aprendizagem Baseada em Problemas tem como propósito tornar o aluno capaz de construir o aprendizado conceitual, procedimental e atitudinal por meio de problemas propostos que o expõe a situações motivadoras e o prepara para o mundo do trabalho. A (BOROCHOVICIUS; TORTELLA, 2014).

3.1. Aprendizagem Baseada em Problemas

A Aprendizagem Baseada em Problemas (PBL) é uma metodologia ativa de ensino-aprendizagem na qual os alunos são desafiados a resolver um problema complexo, real ou simulado, que os leva a investigar e aprender os conceitos e habilidades necessários para resolvê-lo.

A adaptação da sequência didática a PBL foi cuidadosamente planejada para garantir o sucesso da aprendizagem. Para tanto seguimos os seguintes passos:

Definição do problema: O primeiro passo é definir o problema que os alunos serão desafiados a resolver. O problema deve ser complexo e desafiador, mas possível de ser resolvido com o conhecimento e as habilidades dos alunos.

- Distribuição da atividade: Os exercícios são aplicados de forma individual, pois deveremos avaliar para cada aluno, os níveis de conhecimento e habilidades.
- Investigação: Os alunos devem investigar o problema, coletando informações e dados relevantes. A investigação pode ser realizada por meio de pesquisas bibliográficas, entrevistas, experimentos, etc.
- Análise e solução do problema: Os alunos devem analisar as informações e dados coletados para identificar possíveis soluções para o problema.

- Apresentação da solução: Os alunos devem apresentar sua solução para o problema para o professor e os colegas.
- Reflexão: Os alunos devem refletir sobre o processo de aprendizagem, identificando os conhecimentos e habilidades adquiridos.

O objetivo é aproveitar uma série de vantagens oferecidas para a aprendizagem, incluindo:

- Aprendizagem significativa: O PBL estimula os alunos a aprenderem conceitos e habilidades de forma significativa, ou seja, de modo que eles compreendam o significado e a utilidade do que estão aprendendo.
- Engajamento dos alunos: O PBL é um método de ensino ativo que envolve os alunos de forma significativa, estimulando seu interesse e motivação.
- Desenvolvimento de habilidades: O PBL promove o desenvolvimento de habilidades importantes para a vida, como trabalho em equipe, resolução de problemas e pensamento crítico.

Considerando a eficácia desta metodologia no ensino-aprendizagem, desejamos promover a aprendizagem significativa, o engajamento dos alunos e o desenvolvimento de habilidades importantes para a vida.

3.2. Perfil do aluno

Alinhado ao Projeto Pedagógico do Curso (PPC) do curso Sistemas de Informação do Instituto Federal de Alagoas (IFAL), essa sequência didática deverá tornar o aluno capaz de gerenciar a segurança da informação dos sistemas e da infraestrutura tecnológica das organizações. O mesmo deve ter conhecimentos básicos no uso do sistema operacional Linux;

Eixo formativo

Formação profissional geral. Utilizar modelos, métodos, técnicas e ferramentas computacionais, arquiteturas de redes e sistemas operacionais

Objeto de conhecimento

Fundamentos de Segurança Cibernética

Habilidade

Entender como os dados são armazenados, processados e transmitidos usando dispositivos computacionais, considerando aspectos da segurança cibernética.

(EF07CO07) Identificar problemas de segurança cibernética e experimentar formas de proteção.

Explicação da habilidade

A utilização de sistemas e redes de computadores precisa respeitar algumas propriedades fundamentais da segurança da informação, como confidencialidade, integridade e disponibilidade. No entanto, essas propriedades podem ser ameaçadas por eventos maliciosos ou não-maliciosos. A fim de diminuir a ocorrência desses eventos, mecanismos de proteção podem ser empregados.

Competências

Analisar criticamente artefatos computacionais, sendo capaz de identificar as vulnerabilidades dos ambientes e das soluções computacionais buscando garantir a integridade, privacidade, sigilo e segurança das informações.

Analisar situações do mundo contemporâneo, selecionando técnicas computacionais apropriadas para a solução de problemas.

4. Conteúdo

A sequência didática aborda os seguintes tópicos:

1. Fundamentos de contêiner com Docker
2. Vulnerabilidade web SQLInjection (https://owasp.org/www-community/attacks/SQL_Injection)

SQL injection é uma técnica de ataque de injeção de código que permite a um invasor inserir código SQL malicioso em uma aplicação web. Isso pode ser feito inserindo caracteres especiais, como aspas duplas ou chaves, em campos de entrada que são usados para construir uma consulta SQL. Quando o código SQL malicioso é inserido, ele é executado pelo servidor da web, o que pode permitir que o invasor acesse dados confidenciais, execute comandos arbitrários ou cause uma interrupção no serviço. SQL injection é uma das vulnerabilidades de segurança mais comuns em aplicações web. É importante que os desenvolvedores tomem medidas para proteger suas aplicações contra esse tipo de ataque.

E o material de apoio da sequência didática, que está presente no tópico 8. Material de apoio deste material, inclui:

- Plano de aula (Guia do professor)
- Vídeos instrucionais
- Material didático para alunos
- Aplicação virtual

A aplicação virtual é disponibilizada em contêiner Docker, o que facilita sua distribuição e implantação. A aplicação é baseada em uma plataforma de DIY (Do It Yourself, Faça-você-mesmo) promovendo a autonomia, o que torna o aprendizado mais envolvente e motivador.

5. Público-alvo

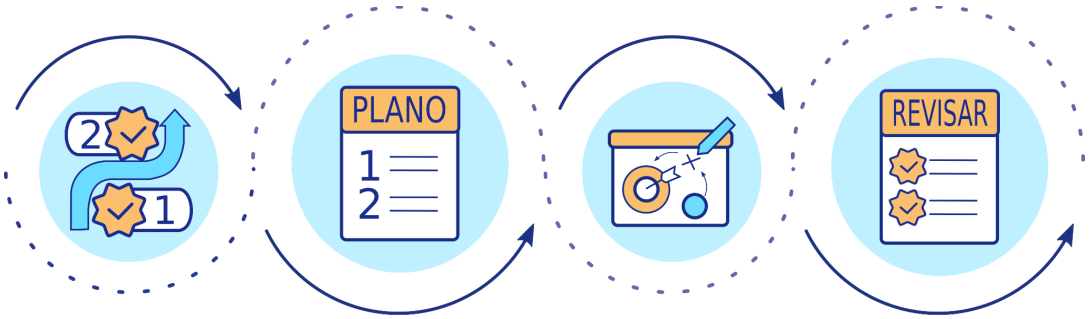
A sequência didática é voltada para alunos do ensino médio e superior. Que possuam perfil compatível com o elencado no item 3.2. Perfil do aluno

6. Avaliação

6.1. Protocolo sugerido de avaliação

Este protocolo segue alguns indicadores para padronizar uma avaliação por competência com relação aos conceitos e significados envolvidos no problema ora apresentado. Para tanto, é proposto um total de 3 (três) indicadores para as 05 (cinco) perguntas da parte conceitual e de 8 (oito) indicadores para a pergunta relacionada a avaliação atitudinal, elaborados de acordo com as perguntas mediadoras contidas na lista de problemas e apresentados nas tabelas abaixo.

Os indicadores são introduzidos a partir das 4 (quatro) etapas que são executadas pelos estudantes na resolução de um problema.



As etapas utilizadas para resolução de um problema conforme este protocolo, conforme imagem acima, são: 1. Compreender o problema. 2 Construir um plano de ação. 3 Executar o plano. 4 Rever a resolução.

E, após a avaliação, será obtido o indicador mais próximo, conforme as tabelas abaixo que apresentam indicadores para as respectivas avaliações.

Tabela de **avaliação conceitual**:

N°	INDICADOR
3	A resposta apresenta o conteúdo correto de forma completa e abrangente.
2	A resposta apresenta o conteúdo correto, mas é incompleta ou pouco abrangente.
1	A resposta não apresenta o conteúdo correto ou é muito superficial.
0	Sem resposta (conteúdo incorreto, nulo ou em branco)

Para este caso, recomenda-se para a nota final, que se aplique a seguinte fórmula:

*Nota final = (Somatório das notas das perguntas / Número total de perguntas) * 3.33*

Explicação da fórmula de nota final de P1:

1. Soma das notas das perguntas: Some as notas que você obteve em cada uma das cinco perguntas.
2. Número total de perguntas: Neste caso, o número total de perguntas é 5.
3. Divisão: Divida a soma das notas pelo número total de perguntas. Isso fornecerá a média das suas notas.
4. Multiplicação por 3.33: Multiplique a média por 3.33 para converter a escala de 0 a 3 para a escala de 0 a 10. O número 3.33 é o resultado de dividir 10 (nota máxima) por 3 (nota máxima por pergunta). Chegando ao resultado.

Tabela de **avaliação atitudinal**:

N°	INDICADOR
8	Identificam a ideia da operação que resolve o problema e acertam os procedimentos
7	Identificam a ideia da operação que resolve o problema, mas não utilizam os procedimentos corretamente.
6	Identificam a operação que resolve o problema, mas apenas indicam a operação, e não a desenvolvem.
5	Não identificam a operação e acertam os procedimentos/algoritmos utilizados.
4	Não identificam a operação e erram os procedimentos
3	Não identificam a operação que resolve o problema, apenas indicam uma operação, e não a desenvolvem.
2	Indicam apenas o resultado e acertam.
1	Não resolvem.
0	Sem resposta (conteúdo nulo ou em branco)

Em síntese, quanto maior o número do indicador atingido, maior foi a competência adquirida/apresentada pelo aluno, pois ele demonstrou maior conhecimento, habilidade e atitude para a resolutividade do problema apresentado.

Para este caso, recomenda-se para a nota final, que se aplique a seguinte fórmula:

*Nota final = (Nota da pergunta / 8) * 10*

Explicação da fórmula de nota final de P2:

- Divisão: Divida a nota que você obteve na pergunta por 8. Isso normaliza a nota para a escala de 0 a 1.

- Multiplicação por 10: Multiplique o resultado da divisão por 10 para converter para a escala de 0 a 10. Chegando ao resultado.

Os itens 6.2 e 6.3 a seguir, são exemplos de questionamento para aplicação de exercício avaliativo **CONCEITUAL** e **ATITUDINAL** desta **SD**.

6.2 Avaliação de conhecimento PARTE 01 (Conceitual)

Para avaliação CONCEITUAL, segue questões para que de forma subjetiva, tenha-se entendimento da compreensão do aluno sobre o tema proposto.

1. O que é um container Docker?
2. Quais são as ferramentas e recursos disponíveis para gerenciar containers Docker?
3. Quais são as vantagens de usar containers Docker?
4. Quais são as etapas para criar um container Docker?
5. Quais são as diferenças entre contêineres e máquinas virtuais?

6.3 Avaliação de conhecimento PARTE 02 (Atitudinal)

Para aplicar este item, sugerimos que seja feita a leitura da DESCRIÇÃO DO PROBLEMA com os alunos e sejam tiradas possíveis dúvidas e na sequência seja feita a liberação da PERGUNTA a este problema.

DESCRIÇÃO DO PROBLEMA

Leia atentamente a descrição e responda a pergunta que segue:

O site http://testphp.vulnweb.com/ é uma plataforma de comércio eletrônico que lida com informações confidenciais do usuário, como nomes, endereços e informações de pagamento. Recentemente, a equipe de segurança descobriu que o site é vulnerável a ataques de injeção SQL, o que significa que um invasor pode executar códigos maliciosos no banco de dados do site, extraindo informações confidenciais dos usuários ou até mesmo comprometendo todo o sistema.

Você lidera uma equipe encarregada de explorar a vulnerabilidade em questão usando os conhecimentos adquiridos em nossos encontros. E baseado nos conceitos aprendidos sobre containers Docker e SQL Injection, deverá desenvolver uma estratégia para explorar a vulnerabilidade do site. Depois disso, deve propor solução(ões) para corrigir a vulnerabilidade e prevenir ataques semelhantes no futuro.

Você deverá apresentar em um texto descrevendo os passos que você tomou para executar a essa atividade. O texto deverá conter uma solução eficaz para resolver o problema, e uma evidência do ataque (ex: o nome do banco de dados ou os dados de uma tabela.).

A avaliação será baseada na qualidade da estratégia de ataque, na precisão das descobertas e na solução proposta para evitar futuros ataques.

PERGUNTA

Com base nos dados contidos na descrição do problema acima, e fazendo uso dos conceitos de containers Docker e SQL Injection. Explore a vulnerabilidade que vimos em nossas aulas a partir de um site específico e proponha soluções para evitar ataques semelhantes no futuro?

7. Plano de aula

7.1 Como trilhar essa SD

Para apoiar a execução dessa SD, certifique-se de cumprir no mínimo o checklist abaixo:

- ☐ Preparar os recursos online;
- ☐ Personalizar slides ou disponibilizar vídeo instrucional;
- ☐ Planejar e executar a aula 01;
- ☐ Planejar e executar a aula 02;
- ☐ Planejar e executar as avaliações Conceitual e Atitudinal;
- ☐ Classificar a avaliação da competência individual do aluno usando o protocolo proposto no protocolo sugerido de Avaliação;

7.2 Plano de aula 01 - Docker básico

Nível: Básico

Duração: 3 horas

Objetivos:

- Os alunos serão capazes de definir o Docker e seus principais conceitos.
- Os alunos serão capazes de instalar e configurar o Docker em seu computador.
- Os alunos serão capazes de criar e executar um container Docker.

Recursos:

- Computador com acesso à internet
- Terminal
- Editor de texto
- Livro sobre Docker com link disponível no tópico 8.5.1 Livro sobre Docker

Atividades:

1. Introdução ao Docker
   - O professor apresenta o Docker e seus principais conceitos.

- O professor discute os benefícios do Docker.

2. Instalação do Docker
    - O professor demonstra como instalar o Docker no computador dos alunos.
3. Criando um container Docker
    - O professor demonstra como criar um container Docker.
    - Os alunos praticam a criação de um container Docker.
4. Executando um container Docker
    - O professor demonstra como executar um container Docker.
    - Os alunos praticam a execução de um container Docker.
5. Conclusão
    - O professor discute o que os alunos aprenderam.

Avaliação:

- Os alunos serão avaliados com base em sua participação nas atividades.

O professor pode ainda obter uma visão mais detalhada deste plano no item 9.1 Plano de aula 01 detalhado: Introdução ao Docker localizado no item 9. Anexos deste documento.
Você pode ter acesso a um modelo de plano de aula neste link

7.3 Plano de aula 02 - SQLMAP

Nível: Básico

Duração: 2 horas

Objetivos:

- Os alunos serão capazes de instalar e configurar o Docker na máquina local e no https://labs.play-with-docker.com/.
- Os alunos serão capazes de criar e executar um container Docker com o sqlmap.
- Os alunos serão capazes de explorar uma vulnerabilidade SQL Injection em um site web.

Recursos:

- Computador com acesso à internet
- Terminal

- Editor de texto

Atividades

1. Introdução ao SQL Injection
   - O professor apresenta o SQL Injection e seus principais conceitos.
   - O professor discute os riscos do SQL Injection.
2. Identificando vulnerabilidades SQL Injection
   - O professor demonstra como identificar vulnerabilidades SQL Injection em um site web.
   - Os alunos praticam a identificação de vulnerabilidades SQL Injection em um site web.
3. Criando um container Docker com o sqlmap
   - O professor demonstra como criar um container Docker com o sqlmap.
   - Os alunos praticam a criação de um container Docker com o sqlmap.
4. Explorando uma vulnerabilidade SQL Injection
   - O professor demonstra como explorar uma vulnerabilidade SQL Injection em um site web usando o sqlmap.
   - Os alunos praticam a exploração de uma vulnerabilidade SQL Injection em um site web usando o sqlmap.
5. Conclusão
   - O professor discute o que os alunos aprenderam.
   - Encaminhar as atividades avaliativas de competência ATITUDINAL e CONCEITUAL conforme proposta do item 7.4 Plano de aula 03 - Execução das avaliações Conceitual e Atitudinal

Avaliação:

- Os alunos serão avaliados com base em sua participação nas atividades.
- E dá aplicação das avaliação constantes no item 7.4 Plano de aula 03 - Execução das avaliações Conceitual e Atitudinal

O professor pode ainda obter uma visão mais detalhada deste plano no item 9.2 Plano de aula 02 detalhado: SQLMAP localizado no item 9. Anexos deste documento.

7.4 Plano de aula 03 - Execução das avaliações Conceitual e Atitudinal

Nível: Básico

Duração: 2 horas

Objetivos:

- Planejar as avaliações conceitual e atitudinal da sequência didática.
- Executar as avaliações planejadas.

Recursos:

- Computador com acesso à internet
- Terminal
- Editor de texto

Avaliação conceitual

Objetivos:

- Avaliar o conhecimento dos alunos sobre os conceitos aprendidos.
- Identificar os alunos que precisam de apoio adicional.

Atividades:

- Criação de questões objetivas e dissertativas sobre os conceitos aprendidos.
- Aplicação das questões aos alunos.
- Correção das questões e análise dos resultados.

Avaliação atitudinal

Objetivos:

- Avaliar o interesse e a participação dos alunos nas atividades.
- Identificar os alunos que precisam de apoio adicional no desenvolvimento de habilidades de trabalho em equipe.

Atividades:

- Observação dos alunos durante as atividades.
- Entrevistas com os alunos.
- Análise dos resultados da observação e das entrevistas.

Materiais para aula

- Questões objetivas e dissertativas sobre os conceitos aprendidos.

- Formulário para avaliação conceitual do aluno.
- Formulário para avaliação atitudinal do aluno.

Dicas para explorar mais

- Utilizar diferentes tipos de questões para avaliar os alunos, como questões de múltipla escolha, questões de associação, questões de resposta curta, questões de resposta longa e questões abertas.
- Utilizar diferentes estratégias para observar os alunos, como observação direta, observação indireta e observação participante.
- Utilizar diferentes estratégias para entrevistar os alunos, como entrevistas individuais, entrevistas em grupo e entrevistas semiestruturadas.

Reflexão

- As avaliações são essenciais para verificar o progresso dos alunos e identificar as áreas que precisam de apoio adicional. É importante que as avaliações sejam planejadas com antecedência e que sejam coerentes com os objetivos da sequência didática.

O professor pode ainda obter uma visão mais detalhada das questões propostas para avaliação deste plano no item 9.3 Plano de aula 03 detalhado: Modelo das avaliações localizado no item 9. Anexos deste documento.
Você pode ter acesso a um modelo de plano de aula neste link

8. Material de apoio

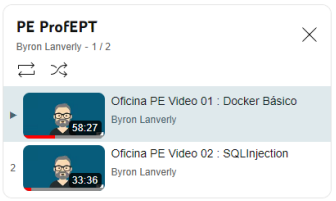
8.1. Guia do professor

Para guiar o professor durante o uso desta sequência didática, é recomendado utilizar o checklist da instrução do item 7.1 Como trilhar essa SD. Fazer a adoção de referência contida nos planos de aula contidos no capítulo 7. Plano de aula.

Fazer uso dos recursos existentes neste capítulo, para enriquecer a distribuição do conhecimento. E por fim, efetuar a análise das avaliações atitudinal e conceitual, usando como base o protocolo sugerido no item 6. Avaliação

8.2. Vídeos instrucionais

Os vídeos instrucionais complementares a essa sequência didática, fazem referência aos encontros 01 (Docker básico) e 02 (SQL Injection). A playlist encontra-se no YOUTUBE neste LINK.



8.3. Material didático para alunos

Os materiais linkados neste tópico 8.3, podem ser compartilhados diretamente com os alunos, mas lembre-se, eles são complementares às suas aulas ou aos vídeos do item 8.2

Slide 01 (Docker básico) LINK

Slide 02 (SQLInjection) LINK

8.4. Aplicação virtual

Foi criado um aplicativo da web vulnerável à injeção de SQL simples disponibilizado com Docker. Este é um aplicativo da web simples que é vulnerável a ataques de injeção de SQL. A aplicação web é baseada no **payroll_app** projeto Metasploitable3, e o código PHP é obtido (quase) diretamente desse projeto. A principal contribuição deste projeto é um ambiente Docker usando docker-compose e contendo contêineres Nginx, PHP e MySQL para executar o aplicativo web facilmente, e efetuar seus testes e estudos em um ambiente controlado.

Essa aplicação está disponível no repositório **profept-pe** do GITHUB acessível através deste LINK

8.5. Bônus

8.5.1 Livro sobre Docker

Com o objetivo de apoiar a execução das atividades relacionadas a container, segue link para um guia acessível para iniciantes que desejam aprender como utilizar containers em Docker com segurança. Trata-se de um ebook que apresenta um guia passo a passo para instalação, configuração e utilização de containers em Docker, além de dicas essenciais para garantir a segurança dos seus dados e aplicações. Desejamos boa leitura.

PDF: ACESSE AQUI

KINDLE: ACESSE AQUI

9. Anexos

9.1 Plano de aula 01 detalhado: Docker básico

9.1.1. Introdução ao Docker

Tempo: 10 minutos
Ação:

- O professor inicia a aula apresentando o Docker e seus principais conceitos.
- O professor discute os benefícios do Docker, como:
    - Isolamento de aplicativos
    - Portabilidade
    - Escalabilidade

9.1.2. Instalação do Docker

Tempo: 15 minutos
Ação:

- O professor demonstra como instalar o Docker no computador dos alunos.
- Os alunos seguem as instruções do professor para instalar o Docker em seu computador.
- Link com material de instalação ACESSE AQUI

9.1.3. Criando um container Docker

Tempo: 20 minutos
Ação:

- O professor demonstra como criar um container Docker.
- Os alunos praticam a criação de um container Docker.

Exercício:

- Os alunos são orientados a criar um container Docker com uma imagem de uma linguagem de programação, como Python ou Node.js.

9.1.4. Executando um container Docker

Tempo: 15 minutos

Ação:

- O professor demonstra como executar um container Docker.
- Os alunos praticam a execução de um container Docker.

Exercício:

- Os alunos são orientados a executar um container Docker com um aplicativo web, como um servidor web ou um banco de dados.

9.1.5. Conclusão

Tempo: 10 minutos

Ação:

- O professor discute o que os alunos aprenderam.
- O professor responde a quaisquer perguntas dos alunos.

Recursos adicionais:

- Docker documentation: https://docs.docker.com/
- Docker tutorial: https://docs.docker.com/get-started/
- Docker cheat sheet: https://docs.docker.com/engine/reference/commandline/cli

9.2 Plano de aula 02 detalhado: SQLMAP

9.2.1. Introdução a vulnerabilidade SQL Injection

Tempo: 20 minutos

Ação:

- O professor inicia a aula apresentando a vulnerabilidade SQL Injection e seus principais conceitos.
- O professor discute os benefícios do Docker, como:
    - Isolamento de aplicativos
    - Portabilidade
    - Escalabilidade

9.2.2. Identificando vulnerabilidades SQL Injection

Tempo: 20 minutos

Ação:

- O professor demonstra como identificar vulnerabilidades SQL Injection em um site web.
- O professor discute os seguintes sinais de vulnerabilidade SQL Injection:
    - Formulários que permitem a entrada de dados de usuário
    - Páginas web que retornam dados dinâmicos
    - Páginas web que não verificam a entrada do usuário

Exercício:

- Os alunos são orientados a identificar vulnerabilidades SQL Injection em um site web real ou simulado.

9.2.3. Criando um container Docker com o sqlmap

Tempo: 50 minutos

Ação:

- O professor demonstra como criar um container Docker com o sqlmap.
- Os alunos praticam a criação de um container Docker com o sqlmap.

Exercício:

- Os alunos são orientados a criar um container Docker com o sqlmap.

9.2.4. Explorando uma vulnerabilidade SQL Injection

Tempo: 50 minutos

Ação:

- O professor demonstra como explorar uma vulnerabilidade SQL Injection em um site web usando o sqlmap.
- Os alunos praticam a exploração de uma vulnerabilidade SQL Injection em um site web usando o sqlmap.

Exercício:

- Os alunos são orientados a explorar uma vulnerabilidade SQL Injection no site de teste da Acunetix http://testphp.vulnweb.com/login.php.

9.2.5. Conclusão

Tempo: 50 minutos

Ação:

- O professor discute o que os alunos aprenderam.
- O professor responde a quaisquer perguntas dos alunos.
- Na proposta de de metodologias ativas com a execução da PBL, encaminhe as atividades avaliativas de competência ATITUDINAL e CONCEITUAL por meio eletrônico como o Google Classroom ou outro de sua preferência.

Recursos adicionais:

- Docker documentation: https://docs.docker.com/
- Docker tutorial: https://docs.docker.com/get-started/
- Sqlmap documentation: https://github.com/sqlmapproject/sqlmap/wiki/Usage
- Rodar a imagem do SQLmap disponível no Hub DOcker com o nome **lanverly/sqlmap:1.0**
    - ***Ex:*** *$ docker run --rm -it -v $PWD/sqlmap:/root/.sqlmap/ lanverly/sqlmap:1.0 --url "* http://testphp.vulnweb.com/listproducts.php?cat=1*"*

9.3 Plano de aula 03 detalhado: Modelo das avaliações

As questões propostas, bem como o protocolo sugerido de avaliação, encontram-se no Capítulo 6. Avaliação e tratam das avaliações abaixo:

> *Você pode usar o meio mais adequado a sua realidade para aplicar as avaliações. Porém, sugerimos o uso da ferramenta Forms do Google para aplicar com facilidade.*

9.3.1. Avaliação conceitual

Para as questões propostas para a avaliação conceitual, as perguntas base, encontram-se no item 6.2 Avaliação de conhecimento PARTE 01 (Conceitual)

9.3.1. Avaliação atitudinal

Para as questões propostas para a avaliação conceitual, as perguntas base, encontram-se no item 6.3 Avaliação de conhecimento PARTE 02 (Atitudinal)

10. Referências

BOROCHOVICIUS, Eli; TORTELLA, Jussara Cristina Barboza. Aprendizagem Baseada em Problemas: um método de ensino-aprendizagem e suas práticas educativas. Ensaio: Avaliação e Políticas Públicas em Educação, [s. l.], vol. 22, no. 83, p. 263–294, 2014. Disponível em: http://dx.doi.org/10.1590/s0104-40362014000200002.

OWASP FOUNDATION, THE OPEN SOURCE FOUNDATION FOR APPLICATION SECURITY | OWASP FOUNDATION. [S. l.], [s. d.]. Disponível em: https://owasp.org/.