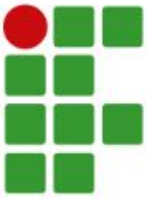

INSTITUTO FEDERAL
São Paulo | Campus Votuporanga

TÉCNICO INTEGRADO EM INFORMÁTICA

BOAS PRÁTICAS DE PROGRAMAÇÃO NO DESENVOLVIMENTO WEB

MARIANA DE ALMEIDA RODRIGUES

UBIRATAN ZAKAIB DO NASCIMENTO

VOTUPORANGA
2020

1. INTRODUÇÃO

O projeto tem a finalidade de mostrar formas de deixar o desenvolvimento, neste caso destinado à *web*, mais seguro, mitigando ao máximo, as possíveis falhas ou ataques. Para o norteamento dos principais problemas de segurança, foi usado o OWASP (Projeto Aberto de Segurança em Aplicações Web), que visa demonstrar as maiores falhas do ano e listá-las em tópicos, entre outras coisas como documentos, artigos, ferramentas do ramo, segundo o OWASP (2020).

Segundo o autor Carvalho et al.(2013), a indiferença em relação ao tema, talvez seja pela falta de conhecimento sobre essas vulnerabilidades. Para mostrá-las e corrigi-las, partiremos de uma ferramenta que contém diversos erros, até desenvolver uma aplicação sem falhas.

2. OBJETIVOS

2.1. OBJETIVO GERAL

Ressaltar a importância de uma programação pensada corretamente, que vai gerar mais segurança tanto para quem programa, para quem compra o produto e principalmente para quem usa. Provar também que a segurança é um assunto de extrema importância, que não deve ser feita a partir de lógicas ou retalhos de códigos que não seguem algum padrão, ou norma específica, para que seja discutida como a principal parte de um projeto em execução.

2.2. OBJETIVO ESPECÍFICO

- Desenvolver uma aplicação *web*;
- Estudar a linguagem de programação PHP orientada a objeto;
- Explorar as diversas formas de proteger o sistema contra-ataques;
- Mostrar os resultados dos ataques em uma aplicação não segura;
- Mostrar as falhas de segurança que pode acontecer se a entrada e saída de dados não forem tratadas devidamente.

3. JUSTIFICATIVA

A cada dia, mais pessoas estão conectadas no mundo virtual, oferecendo seus dados, muitas vezes de forma não intencional. O inconveniente é que existem diversos criminosos tentando acessá-los a todo momento. Quando esses dados são expostos por alguém ilicitamente, vazamento de fotos íntimas, contas de banco, informações pessoais e empresariais, podem se tornar um transtorno maior do que se imagina, como, por exemplo, a fraude em uma eleição devido a dados pessoais. Segundo o autor Machado et al.(2019), as pesquisas mostram um aumento considerável tanto dos dados vazados, quanto a frequência com o que isso ocorre.

Com isso, o mercado de trabalho vem procurando mais profissionais especializados em segurança, já que a maioria das empresas trabalha diretamente

com dados pessoais, como os bancos, e falhas como vazamento de informações são inadmissíveis. Portanto, este trabalho ressaltará o valor de se investir nessa área, pois existem diversas vulnerabilidades já conhecidas.

4. METODOLOGIA

Antes do desenvolvimento prático, deve-se realizar uma pesquisa exploratória e explicativa, isto é, levantar informações sobre o problema e poder, assim, formular hipóteses mais precisas. Além disso, deve-se fazer pesquisas experimentais e bibliográficas para se familiarizar mais com o tema proposto.

Assim como é importante realizar um estudo de caso e teste prático, de modo a concretizar as análises feitas. Elas terão baseamento bibliográfico, além de artigos e trabalhos acadêmicos de outros profissionais. Uma das técnicas que será usada é a pesquisa de campo, será elaborado um pequeno questionário destinado aos profissionais que desenvolvem para tentar comprovar a ideia principal do trabalho.

É válido citar que o espaço em que esse estudo irá ocorrer é no meio virtual, pois o foco do trabalho são aplicações *web*. Então sites com vulnerabilidades serão testados com afinco.

5. ANÁLISE DE REQUISITOS TÉCNICOS DO PROJETO

Para a realização do trabalho, será utilizado as linguagens de programação PHP e JavaScript, o Apache como servidor *web*, PostgreSQL para o gerenciamento do banco de dados e o Bootstrap para tornar o *design* mais fácil de ser feito.

Fora os requisitos citados, será necessário também infraestrutura de rede para o desenvolvimento e pesquisa do trabalho e um computador que contenha todas as exigências para o progresso esperado.

6. PLANO DE TRABALHO

	Feb.	Mar.	Abr.	Mai.	Jun.	Ago.	Set.	Out.	Nov.	Des.
A1	X	X								
A2			X	X	X	X	X			
A3			X	X	X	X	X			
A4				X	X	X	X			
A5					X	X				
A6				X	X	X	X			
A7							X			
A8								X		
A9								X	X	
A10									X	
A11									X	X

Descrição das atividades da tabela:

Atividade Descrição

A1. Elaboração do Projeto de TCC.

A2. Levantamento bibliográfico**.**

A3. Leitura e fichamento do material bibliográfico**.**

A4. Desenvolvimento**.**

A5. Exame de qualificação - Impresso ou digital de variando por membro da banca.

A6. Redação do TCC**.**

A7. Revisão da redação.

A8. Entrega para a banca - 3 copias impressas e encadernadas em espiral.

A9. Defesa pública do TCC.

A10. Correções sugeridas pela banca.

A11. Entrega da versão definitiva em arquivo com ficha catalográfica, gravado em um DVD com caixa branca e capa impressa.

7. REFERÊNCIAS

OWASP. **Quem é a fundação OWASP?** Disponível em: https://owasp.org/. Acesso em: 20 mar. 2020.

CARVALHO, Fernanda Ramos et al.. Vulnerabilidades em aplicações web. **Revista Eletrônica Científica de Ciência da Computação**, [s.i.], v. 8, n. 1, p.1-1, jul. 2013. Disponível em: http://revistas.unifenas.br/index.php/RE3C/article/view/60. Acesso em: 20 mar. 2020.

MACHADO, Rodrigo; KREUTZ, Diego; PAZ, Giulliano; RODRIGUES, Gustavo. Vazamentos de Dados: Histórico, Impacto Socioeconômico e as Novas Leis de Proteção de Dados. In: ESCOLA REGIONAL DE REDES DE COMPUTADORES (ERRC), 17. , 2019 Anais da XVII Escola Regional de Redes de Computadores. Porto Alegre: Sociedade Brasileira de Computação, jan. 2020 . p. 154-159.