



Fundamentos de Segurança de Aplicações Web

Cybersecurity 2x2

Preâmbulo: Neste módulo, você aprenderá sobre o famoso Oráculo de Padding.

Versão: 1.00

Sumário

I	Uma palavra sobre esta Imersão	2
II	Introdução	3
III	Instruções gerais	4
IV	Exercício 02	5
V	Parte bônus	7
VI	Submissão e avaliação entre pares	8

Capítulo I

Uma palavra sobre esta Imersão

Boas Vindas!

Você está prestes a embarcar nesta imersão em segurança cibernética. Nosso objetivo é introduzi-lo ao mundo da segurança cibernética e envolvê-lo em uma experiência de aprendizado entre pares, seguindo o modelo educacional da 42.

Em vez de fornecer um curso com uma única solução para cada problema, o que pode se tornar obsoleto em poucos anos, optamos por uma abordagem de aprendizado entre pares. Sua tarefa é explorar elementos que poderiam ser benéficos para seus desafios, identificar aqueles de interesse real por meio de testes e manipulação. Colabore com outras pessoas, troque perspectivas, gere novas ideias coletivamente e, por fim, realize seus próprios experimentos.

A avaliação entre pares desempenha um papel crucial na descoberta de abordagens alternativas e na descoberta de casos especiais que podem não ter passado pela sua cabeça, potencialmente impactando seu programa. Assim como diferentes clientes priorizam diferentes aspectos, cada revisor trará uma perspectiva única. Além disso, este processo pode levar a novas conexões e colaborações no futuro.

Ao final deste programa, sua jornada será diferente da dos outros participantes. Você terá abordado projetos distintos, escolhido desafios específicos em detrimento de outros, e isso é perfeitamente normal. É uma experiência que combina crescimento coletivo e pessoal, com todos se beneficiando de seus encontros únicos durante este período.

Boa sorte!

Capítulo II

Introdução

O que este módulo mostrará a você:

- Descoberta em segurança de TI do ponto de vista de um desenvolvedor.
- Descoberta das vulnerabilidades mais conhecidas.
- Descubra como detectar essa vulnerabilidade e os possíveis riscos de não proteger um aplicativo dela.

Capítulo III


Instruções gerais

A menos que explicitamente especificado, as seguintes regras se aplicarão a cada dia desta imersão.

- Este documento é a única fonte confiável. Não confie em nenhum boato.
- Este documento pode ser atualizado até uma hora antes do prazo de entrega.
- As tarefas em um documento devem ser feitas na ordem dada. Tarefas posteriores não serão avaliadas a menos que todas as anteriores estejam perfeitamente executadas.
- Cuidado com as permissões de acesso dos seus arquivos e pastas.
- Suas tarefas serão avaliadas por seus colegas.
- Você não deve deixar em sua pasta de trabalho qualquer arquivo além dos explicitamente solicitados pelo as tarefas.
- Você tem uma pergunta? Pergunte ao seu vizinho da esquerda. Caso contrário, tente a sorte com seu vizinho da direita.
- Todas as respostas técnicas de que você possa precisar estão disponíveis no **man** ou na Internet.
- Por Thor, por Odin! Use seu cérebro!!!

Capítulo IV

Exercício 02

	Exercício : 02
Ex02: Parte Obrigatória	
Pasta de entrega : <i>ex02/</i>	
Arquivos para entregar : <i>Readme.md, Payloads.md, Fix.md, e quaisquer outros arquivos necessários</i>	
Funções ou bibliotecas autorizadas : <i>Nenhum</i>	

Para concluir este projeto, você deve primeiro baixar o arquivo tar disponível na página do seu projeto. Em seguida, extraia o conteúdo deste arquivo onde preferir.

```
> ./start.sh
./start.sh
Cleaning Docker...
[.]
Waiting for the server to start...
[...]
You can connect on this website:
http://....
```



É importante acessar este diretório via seu terminal para prosseguir.

Assim que o comando for executado, você poderá acessar o aplicativo através do navegador de sua escolha usando o endereço fornecido no terminal.



Se você encontrar algum problema durante esta etapa, é importante entrar em contato com membros do staff ou voluntários.

Seu projeto agora está em andamento! Abaixo está a página que você deve ver:

LogIn

- Você deve agora encontrar uma maneira de explorar este site!
- Seu objetivo é fazer login facilmente, certo?

Aqui está a saída esperada:

```
<!doctype html>
<html>
<head><title>Login</title></head>
<body>Hello Nice to see you! 42Born{To_C0d3_1s_n1c3_pl4ce_r1ght?}<div><a href="logout.php">Log out</a></div>
</body>
</html>
SUCCESS
```



Para isso, você deve aprender o que é OWASP.



Não, você não deve explorar este aplicativo usando SQLI. :)

- Quando tiver certeza sobre o tipo de vulnerabilidade, você deve documentar o tipo de vulnerabilidade e fornecer uma explicação dela em um arquivo Readme.md.
- Documente as várias *payloads* que você conseguiu usar em um arquivo Payloads.md.
- Identifique pelo menos 2 cenários diferentes em que essas vulnerabilidades podem ser exploradas.
- A etapa final é relativamente simples: encontre uma maneira de proteger um aplicativo web desse tipo de vulnerabilidade. Depois de determinar as medidas de proteção, documente-as no arquivo Fix.md.
- Não hesite em incluir fontes se necessário.

Capítulo V

Parte bônus

Se você se encontrar com algum tempo disponível, pode considerar explorar esta tarefa bônus opcional. Embora não seja obrigatório, evite dedicar tempo excessivo a ela.

Você agora precisa criar um script na linguagem de programação de sua escolha que utilize várias payloads diferentes com o objetivo de mostrar a vulnerabilidade. O objetivo é que o aplicativo seja executado em um estado em que este script possa demonstrar automaticamente a presença da vulnerabilidade.



Certifique-se de reiniciar o aplicativo conforme necessário para verificar o funcionamento adequado do seu programa.

```
Scripts automatizados para explorar o site.
```



É importante garantir que o programa escolhido esteja funcionando corretamente e possa demonstrar de forma confiável a vulnerabilidade sempre que o aplicativo estiver funcionando.



A parte bônus só será avaliada se a parte obrigatória estiver PERFEITA. Perfeita significa que a parte obrigatória foi integralmente feita e funciona sem mau funcionamento. Se você não passou TODOS os requisitos obrigatórios, sua parte bônus não será avaliada.

Capítulo VI

Submissão e avaliação entre pares

- Crie uma pasta `imersao` na raiz da sua home e navegue até ela.
- Crie uma nova pasta `module02` e navegue até ela.
- Todos os exercícios devem estar na pasta correta de entrega. Exercício 00 na pasta `ex00`, Exercício 01 na pasta `ex01`, etc... você entende a lógica.



Observe que, durante sua defesa, qualquer coisa que não esteja presente na pasta do dia não será verificada.