Fundamentos de Segurança Informática

CTF para a semana #4 (com início a 8/11)

Encontram-se na plataforma CTF (ctf-fsi.fe.up.pt) os desafios para esta semana, cujo enunciado aqui se replica.

Matéria relacionada: Common Vulnerabilities and Exposures (CVE)

Objetivo: Fazer login como administrador num servidor wordpress utilizando uma CVE com exploit conhecido.

Contexto

No endereço http://ctf-fsi.fe.up.pt:5001 encontra-se um servidor de Wordpress.

O Wordpress é um software que facilita a criação e gestão de conteúdo em websites. Uma das suas características mais apreciadas, é a modularidade, que permite a utilização de plugins para expandir as suas funcionalidades, por exemplo, com um simples plugin podemos criar uma loja online. Os plugins podem ser desenvolvidos por qualquer pessoa, o que acarreta riscos de segurança. O desafio proposto para esta semana tem como objetivo familiarizar-te com a utilização de CVEs no mundo real, a importância dos CVEs para partilha de conhecimento em segurança informática, e como é que estes podem ser utilizados para atacar sistemas.

Tarefas

- Reconhecimento - Recolhe toda a informação que podes obter ao navegar pela aplicação web. Exemplos de informação pertinente são os seguintes:
  - Versão do wordpress;
  - Plugins instalados e versões dos mesmos;
  - Possíveis utilizadores e nomes de utilizadores.

Toda a informação pode-nos ajudar a encontrar e explorar vulnerabilidades. Este processo, num ambiente real, é parcialmente automatizado. No entanto, para este caso não necessitas de recorrer a qualquer ferramenta automática.

- Pesquisa por vulnerabilidades - Depois de teres feito o reconhecimento, deves utilizar a informação recolhida para confirmar se o software tem alguma vulnerabilidade conhecida. Deves utilizar motores de busca e base de dados de CVE's para procurar por vulnerabilidades que afetem as versões que identificaste.
- Escolha da vulnerabilidade - No mundo real, terias de perceber qual é que seria a melhor vulnerabilidade para utilizar dependendo do objetivo que tens. Neste caso, o teu objetivo é identificar uma CVE que te permita fazer login como outro utilizador. Quando a identificares, deves submeter a CVE na plataforma CTF no desafio "Semana 4 - Desafio 1", de forma a confirmar que escolheste a vulnerabilidade correta. A CVE deve ser submetida no seguinte formato: "flag{CVE-XXXX-XXXXX}".
- Encontrar um exploit - Na internet, em plataformas como o Exploit Database, existem programas automáticos que te permitem explorar CVEs (exploits). Agora que já sabes que o servidor está vulnerável, deves encontrar uma exploit para essa CVE e entender como é que a podes correr contra o servidor. Nesta fase, pode ser importante outras informações que recolheste na fase de Reconhecimento, como por exemplo, os utilizadores que existem na plataforma.
- Explorar a vulnerabilidade - Agora que já tens uma exploit e analisaste o seu funcionamento, chegou a hora de a usares contra o servidor. Depois de conseguires acesso ao servidor como admin, deves ir ao http://ctf-fsi.fe.up.pt:5001/wp-admin/edit.php, onde encontrarás um post privado com a flag que deves submeter no desafio "Semana 4 - Desafio 2".

Notas: A metodologia que foi apresentada nas diferentes tarefas é uma adaptação da que é utilizada em testes de penetração (pentests). No ambiente real o analista depois de ter efetuado a Tarefa 5 iria voltar à Tarefa 1, agora fazendo o reconhecimento da nova superfície de ataque.

Enunciado CTF

Num concurso CTF normal, os concorrentes não receberiam a informação passo a passo acima. Um enunciado possível para este problema seria um teaser com algumas pistas, como o seguinte.

A empresa para qual trabalhas está a pensar contratar a um terceiro o hosting de um site wordpress. A tua equipa é responsável por avaliar se a empresa a quem tencionam contratar cumpre ou não os requisitos de segurança. Foi disponibilizado pelo potencial prestador de serviços uma instância de wordpress para que procedam à avaliação de segurança - http://ctf-fsi.fe.up.pt:5001.
O objetivo é perceber se a instância tem alguma vulnerabilidade e se a tiver, estão autorizados a explorá-la de forma a demonstrarem o seu impacto.

Última alteração: sexta, 5 de novembro de 2021 às 18:52

◄ Tarefas para a semana #4 (com início em 8/11)

Ir para...

Tarefas para a semana #5 (com início em 15/11) ►