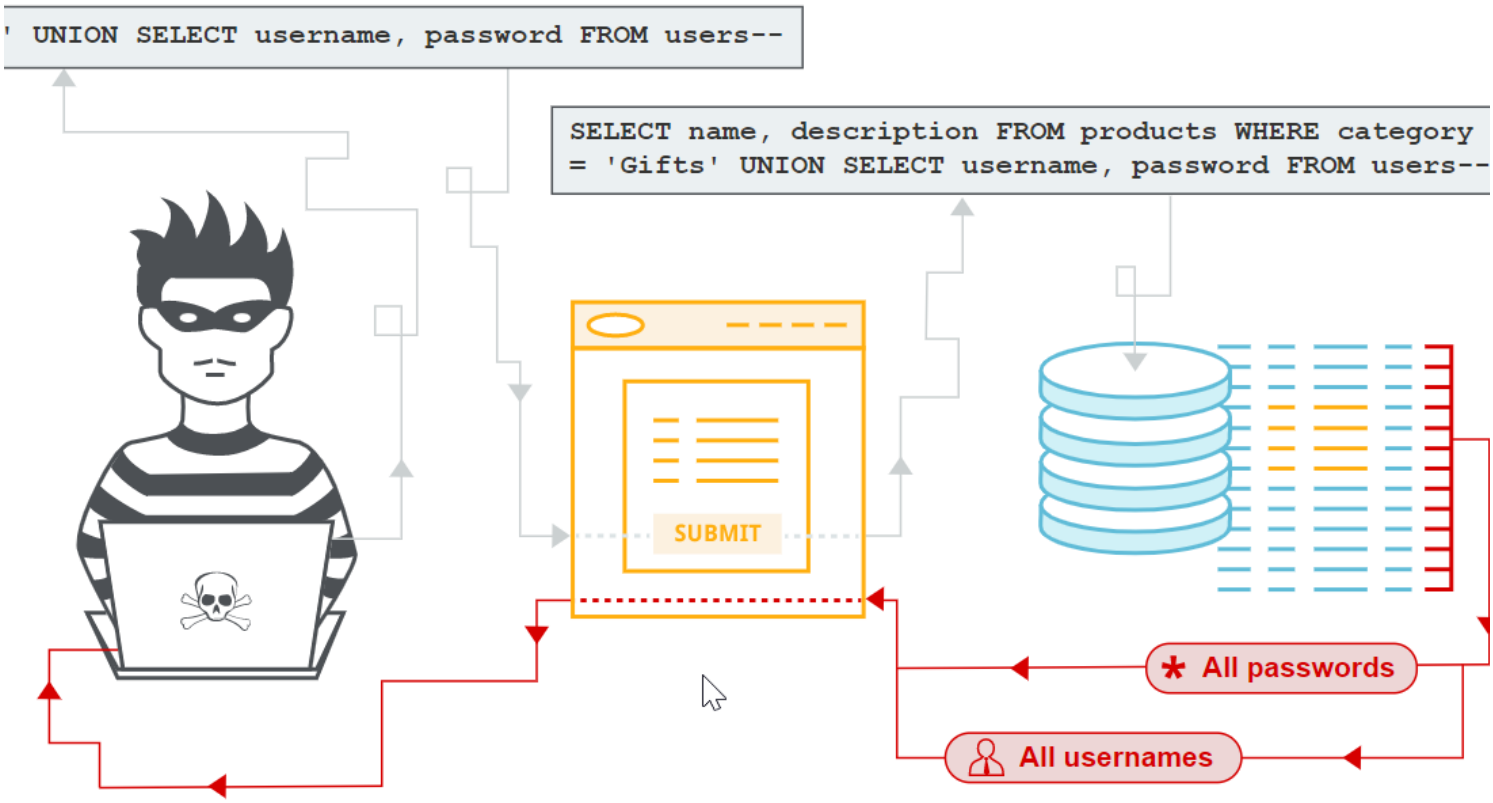

Crédito da capa: Portswigger

SQL Injection no IDCE MV

Iran Macedo
Pentester / Segurança ofensiva
Published May 6, 2022

+ Follow

Olá!

Neste artigo eu comprovo a falha de SQL Injection no software de gestão de saúde IDCE da empresa MV Informática para a base do CVE-2022-30496.

o tem rodando apenas em redes locais ou protegidos por VPN. Porém ainda é possível encontrar este software vulnerável sendo utilizado abertamente através da internet e sem nenhuma proteção extra.

Aproveito para informar que a ação de coletar informações de serviços não é caracterizado crime, uma vez que foi utilizado um ambiente controlado de teste e nenhuma informação privada foi revelada. Esta matéria tem como fins apresentar os métodos utilizados por hackers para encontrar informações de empresas e apresentar aos desenvolvedores as falhas de segurança que suas aplicações web (portais, sites de atendimento, etc) possuem. Corrigir ou não é uma decisão dos desenvolvedores e gestores/clientes destas aplicações.

Por Iran Macedo, especialista em proteção de dados e segurança ofensiva / Pentest.

A falha de SQLi

O software testado foi o IDCE - MV Medicina Diagnóstica. Este software é utilizado por hospitais e seus médicos para gerarem laudos de exames médicos de pacientes. Mas não somente isso, pois pode controlar fluxo de pagamentos, gerenciar usuários, suas informações e permissões, dados de parceiros, de fornecedores e de clientes (pacientes) e outros serviços gerenciais relativos aos hospitais e clínicas.

Realizando o teste mais básico de SQL Injection, não conseguimos nada. Por exemplo, ao adicionar uma aspas simples ' no campo usuário, temos a resposta "Usuário e/ou Senha inválidos!", o que parece ser um bom sinal, uma vez que a aplicação parece tratar a entrada enviada pelo usuário antes de envia-la ao banco de dados.

Time-Based Blind injection

Para iniciar meus testes, fiz o envio de um usuário e senha inválidos, interceptei pelo Burp, copiei os dados de requisição e salvei num arquivo TXT, que foi utilizado pelo SQLMap como base da requisição através do parâmetro "-r".

Num teste anterior em um outro produto do desenvolvedor MV, vimos que o banco de dados utilizado era um Oracle. Desta forma as chances do desenvolvedor utilizar na epoca o Oracle como a solução de banco de dados para todas as suas aplicações é grande. Partindo deste princípio, configurei o meu SQLMap para testar todas os possíveis ataques (level 5 e risk 3) somente para banco Oracle nesta aplicação. Isso reduz a quantidade e o tempo de execução dos testes.

Como resultado, o campo testado (Usuário) pareceu ser vulnerável a um ataque de SQL Injection em Oracle e Time-Based Blind.

Ao final dos testes o SQLMap trouxe a confirmação da falha de segurança da aplicação, evidenciando o banco de dados encontrado (Oracle), a versão e o sistema operacional do servidor do banco de dados (Windows 2008 R2) e outras informações. Isto já é suficiente para comprovar a falha de segurança na aplicação.

Para ser mais conclusivo, outros dados não sensíveis foram capturados, como por exemplo o usuário utilizado pelo banco de dados e a base atualmente acessada.

E, para evidenciar que seria possível acessar todas as informações dentro desta base, pegamos os nomes das colunas de uma dada tabela utilizada pela aplicação IDCE.

Estas evidências são suficientes para comprovar a falha de segurança da aplicação, que acaba expondo as informações dentro do seu banco de dados.

Por ser um falha baseada em tempo de resposta às cegas (Time-Based Blind), este tipo de ataque pode levar muito tempo para ser executado.

Correção da falha *(informação atualizada)*

Conversando por vídeo conferência com o desenvolvedor em maio de 2020 e em junho de 2022, fui informado de que a MV Informática corrigiu as falhas apresentadas nesta versão testada. Desta forma, é recomendado que a solução de medicina diagnóstica IDCE seja utilizada sempre de forma atualizada. Infelizmente algumas empresas ainda utilizam versões desatualizadas e vulneráveis.

Conclusão

Mantenha o seu software atualizado e sempre utilize as versões mais atuais e estáveis. Utilizar softwares piratas pode parecer como uma solução viável e barata para quem não quer gastar dinheiro pagando por programas licenciados. Mas lembre-se de que isto não é legal (no termo jurídico da palavra), além de não ter as atualizações necessárias para mantê-lo seguro. O "barato" pode acabar saindo muito, mas muito mais caro do que

banco de dados principal invadido.

Mantenha-se seguro e um grande abraço!

Documentação formal do CVE na Mitre: MeuGithub

CVE ID: CVE-2022-30496.

Segurança Ofensiva/Defensiva. O que são?

Iran Macedo · 4y

Firewall parte 3 – Invadindo o Linux Metasploitable

Iran Macedo · 5y

[InfoSec] Invadindo o Windows usando o Metasploit

Bruno Izidório · 4y

Escalação de privilégios/Faça a sua jogada

Iran Macedo · 4y

Explore topics

Workplace

Job Search

Careers

Interviewing

Salary and Compensation

Internships

Employee Benefits

See All

Iran Macedo