hardsecure

CASE STUDY

PENTEST

QUAL O IMPACTO NO SEU NEGÓCIO?

R. Acácio de Paiva nº16, 1ºdir,
1700-006 Lisboa, Portugal

www.hardsecure.com
geral@hardsecure.com

ÍNDICE

OBJETIVO

O presente documento tem como objetivo a exposição em traços gerais de uma vulnerabilidade, de um pentest realizado a um cliente da Hardsecure, abordando, quando necessário, aspetos mais técnicos dos testes efetuados, mas focando a sua composição numa apresentação clara e concisa, que permita a alguém não versado nos detalhes técnicos entender o impacto do que se encontrou, qual a contribuição que a realização de um pentest pode ter para o negócio, seja pelo que revela acerca da real proteção dos dados visados nas aplicações de clientes, seja pela mitigação das vulnerabilidades e consequente redução de superfície de ataque, e do potencial dano que a exploração das mesmas poderia causar a uma instituição (financeiro, reputacional, entre outros).

ENQUADRAMENTO

Foi pedido à Hardsecure a execução de um pentest a uma aplicação web que funciona como portal para os colaboradores e associados do cliente em causa.

Após autenticação na mesma, utilizadores internos à entidade possuem contas com papéis (doravante denominados como roles) adequados à função que desempenham na mesma (eg. Departamento Financeiro, Departamento de IT, Administração, entre outros), existindo também contas para parceiros da entidade, com acessos muito reduzidos e permissões limitadas face às ações que podem executar.

A autenticação na aplicação é feita por uma entidade terceira, que após a inserção das credenciais corretas por parte de um utilizador, o encaminha para a sua homepage na plataforma, adequada ao role que o utilizador possui na mesma.

Uma vez dentro da plataforma, consoante o role do utilizador, é possível configurar alocações de fundos financeiros, alterar prioridades de negócio previamente definidas para os vários setores da entidade, ou criar novas, modificar prazos de projetos, fazer a administração da própria plataforma (criar, atualizar, ler ou apagar entidades da plataforma, sejam essas entidades utilizadores, permissões dos mesmos, documentos, entre outros), ou, para contas com privilégios mais reduzidos, simplesmente visualizar informação, que utilizadores com permissões de criação, edição e remoção de conteúdo na plataforma colocam à disposição.

INTENÇÃO DO CLIENTE NA REALIZAÇÃO DO PENTEST

Numa fase prévia ao pentest, percebeu-se junto do cliente o que seria prioritário para si, ou seja, atendendo às funcionalidades disponibilizadas pela plataforma e às preocupações de negócio, que tipo de vulnerabilidades considerariam mais prementes e às quais seria útil despender blocos de tempo maiores durante os testes, dada a janela temporal acordada para os mesmos.

O intuito nesta fase era simples: perceber, dadas as limitações de tempo para o engagement, o que preocupava o cliente, e o que considerava prioritário numa pipeline de testes de intrusão.

Dado tratar-se de uma plataforma com uma panóplia de roles e informação que tinha de estar bastante bem segmentada entre todos os departamentos com representação na mesma, o cliente deu a entender durante este processo que era fulcral garantir que o acesso aos dados de um departamento estava contido a esse departamento, e a restrição de acesso a dados fora do âmbito de um determinado role era assegurada, ainda para mais atendendo a que alguns dos dados visíveis e editáveis na plataforma visavam informação com alguma relevância para o negócio.

Por cima de toda esta segmentação lateral, no sentido de utilizadores com mais ou menos permissões, mas sem uma hierarquia direta entre eles, a secção de administração da plataforma teria de estar bastante bem resguardada também, à parte de qualquer uma das outras, dado que um comprometimento da mesma colocava em causa o comprometimento da totalidade das secções.

Ficou portanto claro que, dado o papel que a plataforma representava para o cliente e os vários tipos de utilizadores que com ela interagiam numa base diária, um dos focos do pentest estaria em perceber se havia algum tipo de Broken Access Control, ou seja, se utilizadores não autorizados conseguiam de algum modo aceder ou alterar informação fora do que, à partida, seria o seu âmbito de ação, dado o role atribuído. A título de exemplo, se alguém como utilizador comum, sem grandes privilégios, conseguiria aceder ao painel de administração (tendo-se chegado no decorrer do pentest à conclusão de que sim, conseguiria).

REQUISITOS

No sentido de testar esta vulnerabilidade em particular, foi pedido ao cliente a disponibilização de contas de utilizador que na sua ótica, justificassem testes mais exaustivos.

FINDINGS

Durante a execução dos testes foi possível perceber que uma conta de parceiro, que à partida deveria ter apenas permissões de leitura do que lhe era disponibilizado por roles com maior autoridade na plataforma, conseguia aceder aos painéis de gestão financeira da empresa. Ainda que algumas ações da área Financeira não pudessem ser diretamente executadas com esta conta menor, através da análise de código presente em várias páginas foi possível não apenas identificar funções que executavam determinadas ações do departamento, e chamá-las com os parâmetros adequados consoante a intenção, como também identificar funcionalidades escondidas apenas por estilos (CSS), nas páginas. Através da inspeção e alteração de código no próprio browser, client-side, foi então possível revelar uma série de painéis escondidos, mas ainda assim presentes na plataforma, visíveis a alguém com a disposição para olhar para o código da mesma e perceber a totalidade do que esta continha.

Posteriormente verificou-se a possibilidade de exfiltração de logs de acesso, relatórios e alteração de conteúdos afetos à área Financeira por esta conta com privilégios menores, de parceiro.

Eventualmente, ainda com a mesma conta, foi possível aceder ao painel administração da plataforma, onde, entre outras ações, podia ser executada a elevação desta conta particular de parceiro a conta de administrador, ou, a título de exemplo, uma total desconfiguração da plataforma, desde colocar todos os administradores da mesma com menos privilégios do que qualquer conta de parceiro, à remoção por inteiro de permissões (não apenas a sua alocação ou não a determinados roles, mas mesmo tornar a regra inexistente), alteração de filtros da plataforma, que colocariam informação mais reservada à disposição de utilizadores que à partida não deveriam ter permissão para lhe aceder, entre outros.

Estas últimas ações enumeradas, facilmente chamariam a atenção dos responsáveis pela plataforma, e dado não serem minimamente silenciosas, rapidamente se perceberia a existência de algo de errado, ou de alguém a interagir de modo destrutivo com a plataforma.

Ainda assim, todas estas ações eram uma possibilidade e exploradas de modo mais furtivo e comedido, durante um longo intervalo de tempo, certamente causariam um dano mais do que efémero à entidade, sem fazer soar de imediato tantos e tão ruidosos alarmes.

A Hardsecure constatou a possibilidade deste cenário, não tendo concretizado qualquer tentativa de desregular a plataforma, cingindo-se à recolha de evidências que provassem a possibilidade das ações em causa. Em momento algum foi perturbado o normal funcionamento da plataforma.

Através da análise do código disponibilizado pelo browser (nomes de funções presentes em ficheiros, parâmetros, etc...) foi ainda possível perceber a nomenclatura utilizada predominantemente pelos developers da plataforma, para acesso a páginas/caminhos/ficheiros particulares à mesma, dada a natureza do negócio, e a partir daí enumerar outras áreas cuja existência, inicialmente, estava velada a qualquer uma das contas passadas, mas que ainda assim se encontravam presentes na plataforma.

O impacto de um finding deste género - uma conta sem grandes privilégios chegar à administração de uma pataforma – é grave, atendendo aos dados com que a plataforma lida e às ações que permite. Acresce que durante o pentest, um considerável número de contas de utilizador foi encontrado em data breaches, com o domínio da entidade, tendo, após acesso ao painel de administrador, verificado a presença destas mesmas contas na plataforma, ao listar todos os utilizadores da mesma.

Dependendo do restante cuidado do cliente no que respeita à segurança da plataforma, perifericamente a este pentest isolado, alguém mal-intencionado poderia ter tido acesso a estes dados, a painéis de administração, fundos, entre outros, durante um tempo potencialmente ilimitado.

A mitigação desta vulnerabilidade em particular, segmentando corretamente os acessos de utilizadores às áreas pertinentes ao seu role, permite a criação de barreiras concretas entre os diferentes tipos de ações passíveis de serem executadas na plataforma, limitando-as a quem legitimamente tem permissão para as executar.

Imaginando que alguém, só por possuir conta num site/plataforma, conseguiria chegar aos painéis de administração do mesmo, eventualmente configurá-lo como entender, visualizar informação de outros utilizadores sem grandes restrições, entre outros poderes que o papel de um administrador acarreta, fica claro então, sem grande margem para dúvida, o valor que acrescenta a um negócio, ganhar visibilidade deste facto e garantir algo que à partida é tomado como certo por maioria dos utilizadores com conta em qualquer site: A segmentação das ações da sua conta face a outras.

CONCLUSÃO

Outras vulnerabilidades foram encontradas durante a realização deste teste, mas tratando o documento da análise muito particular a apenas uma vulnerabilidade de um engagement, o intuito passa por tentar demonstrar o quão longe apenas uma vulnerabilidade pode ir.

O propósito face a esta vulnerabilidade em concreto passou por dar visibilidade ao cliente de lacunas em elementos basilares de uma plataforma que incorpora os conceitos de contas de utilizador e roles associados às mesmas, elementos esses que, precisamente por serem basilares, são praticamente tidos como garantidos, por qualquer utilizador de uma plataforma do mesmo género. Nomeadamente referimo-nos à segmentação entre a sua conta, o que ela pode fazer, ao que pode aceder e modificar, e as restantes contas da plataforma. Revelar-se-ia como claro o abalo à confiança e credibilidade de uma entidade, acaso uma eventual exploração desta vulnerabilidade com propósitos que não os de teste, daí frisar a importância de um pentest, e a visibilidade que dá.