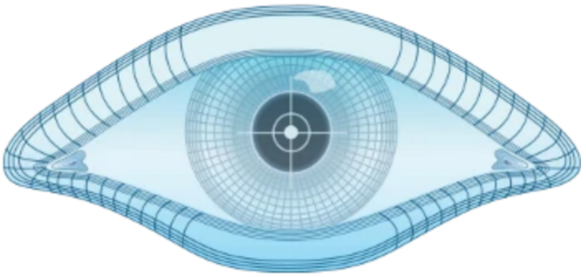


DJC PenTest

Relatório PenTest

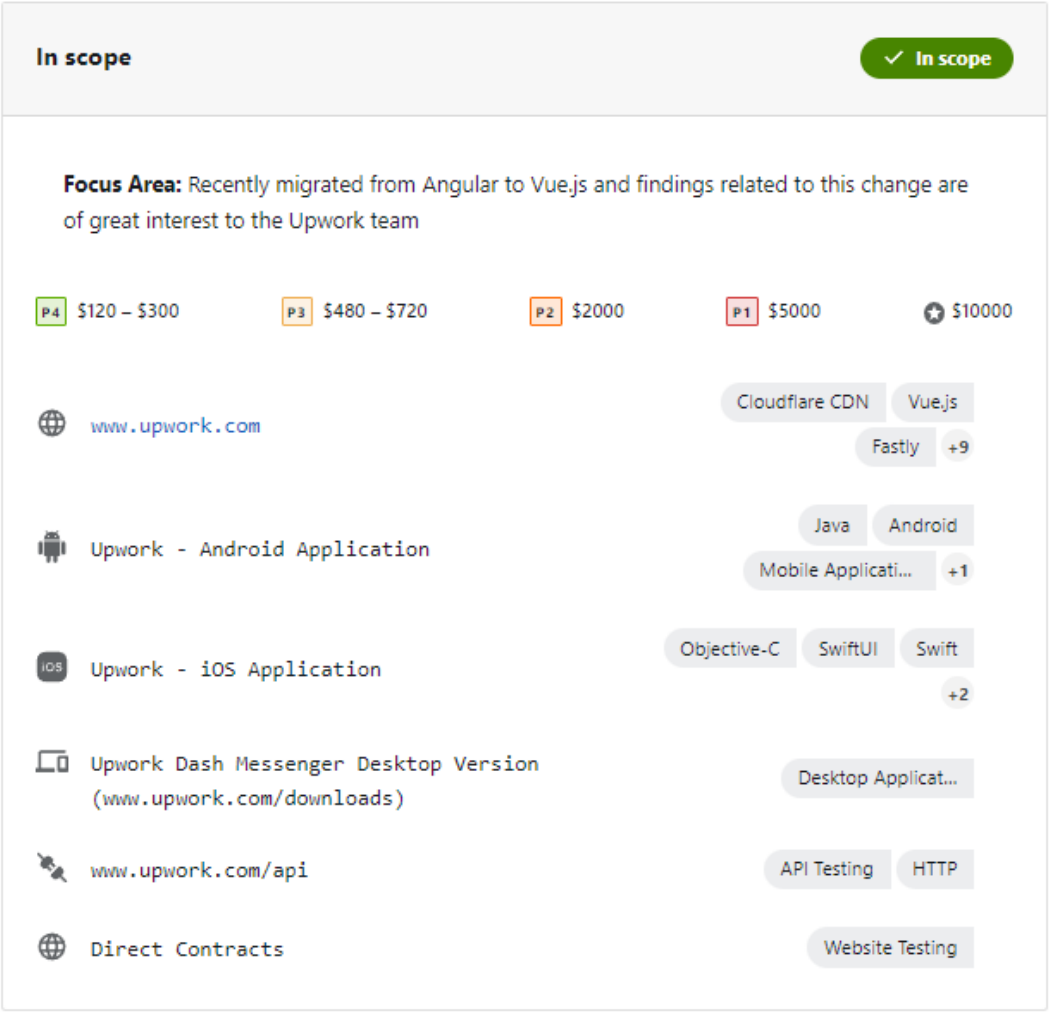
Por: Carlos Alberto, Danilo Caldas e Jônathan Real
PDP- 4

Importante

Este documento contém informação confidencial e privilegiada,sendo seu sigilo protegido por lei. Se você não for o destinatário ou a pessoa autorizada a receber este documento, não pode usar, copiar ou divulgar as informações nele contidas ou tomar qualquer ação baseada nessas informações. Se você recebeu este documento por engano, por favor, avise imediatamente ao remetente e em seguida apague-o. O presente relatório não deve ser enviado por e-mail, fax ou qualquer outro meio eletrônico a menos que este seja previamente aprovado pelas políticas de segurança da contratante.

Índice

1. Escopo



2. Objetivo da pesquisa

A DJC PENTEST foi contratada para conduzir um PENETRATION TEST contra sistema da UPWORK. A avaliação foi conduzida de maneira a simular um ataque malicioso com objetivo de determinar o impacto que falhas de segurança podem ter no que diz respeito à integridade, disponibilidade e confidencialidade do negócio.

3. Contato

Razão Social: UPWORK GLOBAL INC.
Responsável Técnico: Hayden Brown
Contato: press@upwork.com
Telefone: 866.262.4478
URL: https://www.upwork.com/

4. Declaração de Limite da responsabilidade e confidencialidade do Pentester

Todos resultados obtidos, serão utilizados apenas para avaliação acadêmica, sem nenhum objetivo de causar dano a empresa, nem a exposição das possíveis vulnerabilidades para outras pessoas.

5. Data em que os testes foram feito

Os testes foram realizados entre os dias 25 de Novembro à 30 de Novembro de 2022

6. Introdução e descrição da Empresa

A Upwork é uma plataforma de serviços freelancer americana com sede em São Francisco, a empresa anteriormente se chamava Elance O-Desk, nome utilizado após uma fusão em 2013 entre duas empresas do mesmo setor, a Elance Inc. e a O-Desk Corp. Posteriormente a Elance O-Desk passou a se chamar Upwork.

7. Detalhamento dos Dados do Site e subdomínios

Nome: MarkMonitor, Inc
Servidor Whois: whois.markmonitor.com
url de referência: http://markmonitor.com
Estado: clientDeleteProhibited
(https://www.icann.org/epp#clientDeleteProhibited)clientTransferProhibited
(https://www.icann.org/epp#clientTaansferProhibited)clientupdateProhibited
(https://www.icann.org/epp#clientUpdateProhibited)serverDeleteProhibited
(https://www.icann.org/epp#serverTransferProhibited)

(serverUpdateProhibited (https://www.icann.org/epp#serverUpdateProhibited)

Dados Importantes

Expira em 2024-01-30
Registrado em 2002-01-30
Atualizado em 2021-12-29

Servidores de Nomes

fay.ns.cloudflare.com - 172.64.32.115
jim.ns.cloudflare.com - 173.245.59.125

Site Status
Estado: Ativo
Tipo de Servidor: cloudflare

8. Detalhamento dos Softwares Instalados

Gerador de site estático

Nuxt.js

Correio eletrónico

Google Workspace

Rastreadores de problemas

Obter feedback

Linguagens de programação

Node.js

Estruturas da Web


Nuxt.js

balanceadores de carga


Amazon ALB

servidores web


Nuxt.js

PaaS


Amazon Web Services

estruturas JavaScript


Vue.js


Nuxt.js

IaaS

Análise de limpa-neve

Gerenciadores de tags

Gerenciador de tags do Google

Segurança

Perímetro X

Cloudflare Bot Management

HSTS

forter

TruValidate

multidão de insetos

Autoridades certificadoras SSL/TLS

DigiCert

Personalização

agarrar

automação de marketing

MailChimpName

bibliotecas JavaScript

core-js

Lodash

E-mail

MailChimpName

Google Workspace

Conformidade com cookies

OneTrust

CDN

Cloudflare

Impressão digital do navegador

TruValidate

Análise

Google Analytics

Análise de limpa-neve

Linkedin Insight Tag

Pixel do TikTok

Pixel do Facebook

Acompanhamento de conversões do Google Ads

Microsoft Clareza

Programas afiliados

- Impacto

Publicidade

- Microsoft Advertising
- LiveRamp DPM
- Twitter Ads
- Podsights
- Reddit Ads

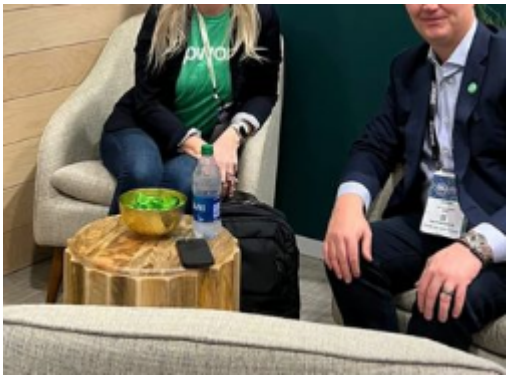
Diversos

- webpack
- HTTP/3
- LottieFiles
- Abrir gráfico
- DocuSign

9. Vulnerabilidades de engenharia social:

9.1. Nas Redes Sociais

Observamos, que nas rede socias da empresa, em marcações de posts, existem fotos que aparecem crachás de funcionários da empresa, algo que é perigoso, pois a depender da foto, pode se conseguir, pegar o QR code do crachá e ter acesso a dados importantes das pessoas, dados os quais podem ser usados posteriormente em engenharia social, ou até para ter acesso físico ao ambiente da empresa. Segue em anexo algumas fotos que foram encontradas.

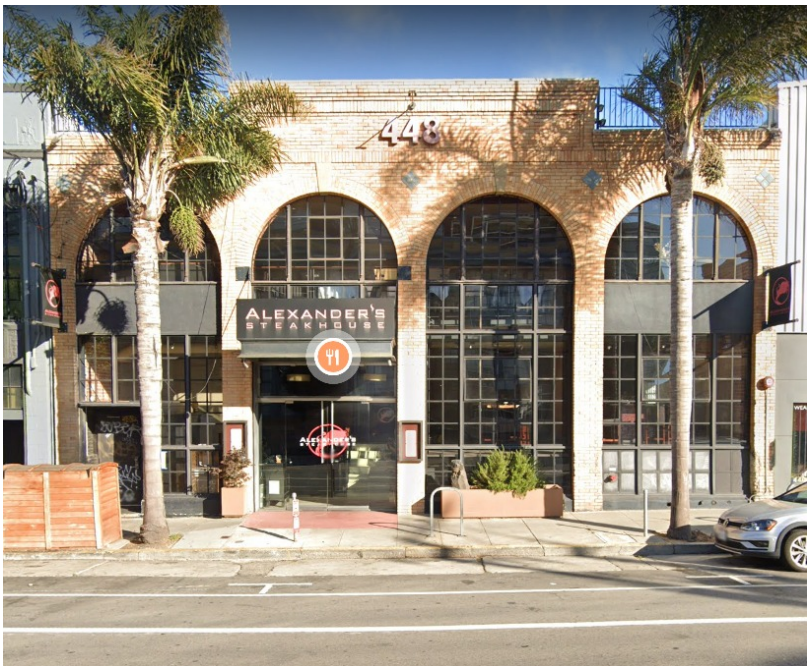


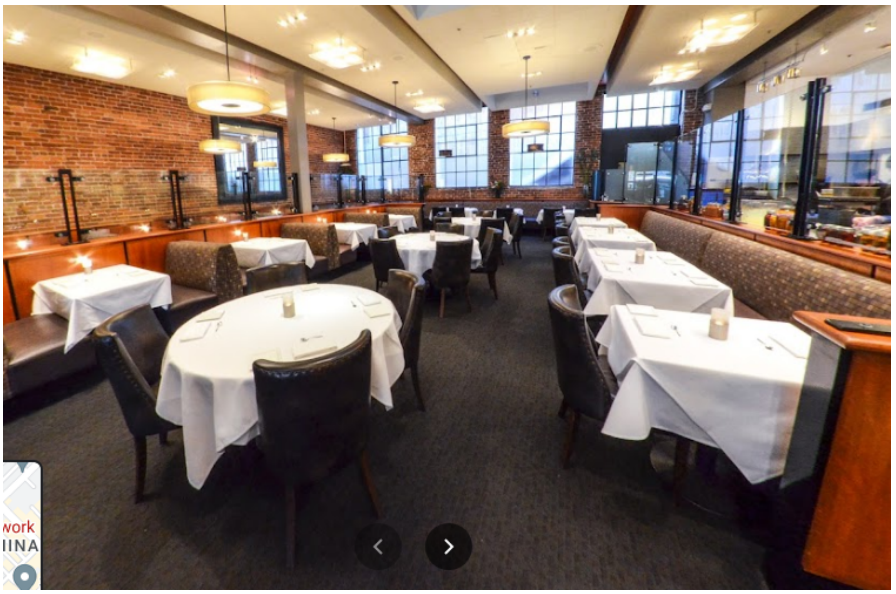
9.2. Google Maps (Street View)

Pesquisando no Google Maps sobre a localização da empresa, pude encontrar o local, que fica na 475 Brannan St, San Francisco, CA 94107, Estados Unidos, em um escritório no prédio Brannan. Analisando sua localidade, percebi que no quarteirão tem muitas lanchonetes, bares que com certeza alguns funcionários frequentam após o serviço, a maioria não se preocupa em tirar o crachá, e os lugares são de livre acesso a qualquer pessoa, então pessoas mal intencionadas, podem ir lá apenas para ouvir conversas, ter contatos com os funcionário da empresa que estão lá, buscando informações que possam o ajudar, em possíveis invasões.

Upwork - Google Maps

Restaurante Próximo:





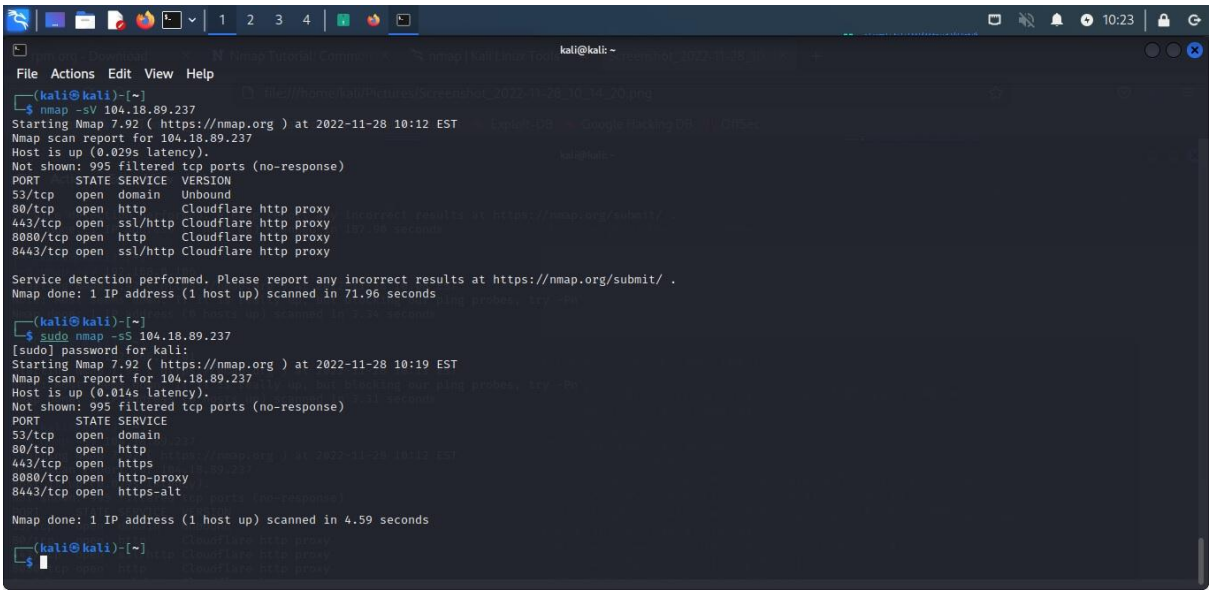
Podemos perceber aqui que as cadeiras são coladas, alguém pode sentar na cadeira de trás do funcionário e ouvir toda sua conversa.

Brickhouse Cafe: Bar & Grill - Google Maps

Bares são riscos maiores ainda, ambiente mais aglomerado e descontraído, facil de outras pessoas se aproximarem e ainda mais quando ingerem bebidas alcoólicas, que os deixam mais sucessíveis a persuasão, já que o córtex pré-frontal está inibido por conta do álcool e elas ficam sem filtros, podem falar muita coisas que eram sigilosas sem nem se tocar no que está fazendo.

10. Softwares usados e Resultados e Vulnerabilidades relatada

Foi utilizado o software Nmap do Kali Linux para averiguar todas as portas do host do site em busca de uma possível porta aberta com um software desatualizado.

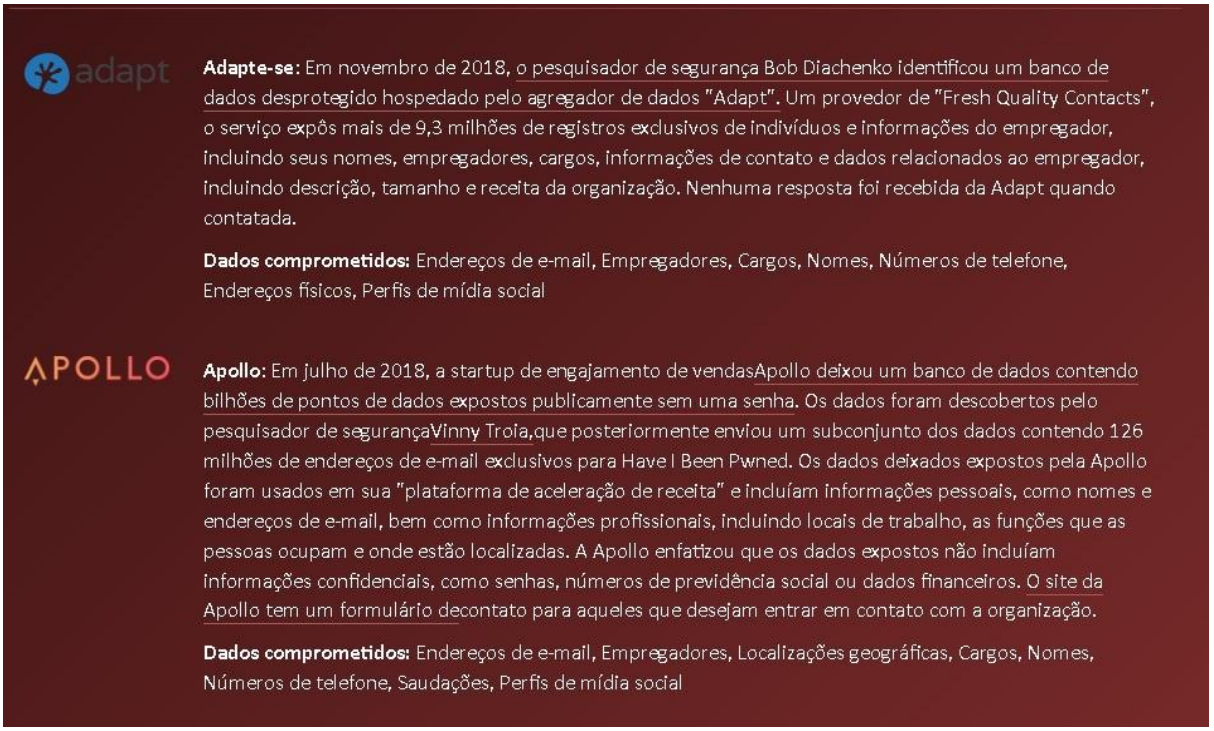


De acordo com os resultados, as únicas portas abertas são de serviços http e https, não há nenhum programa ou serviço com uma versão desatualizada que possa servir como brecha para invasões, logo as portas se encontram seguras.

11. Lista de e-mails que já tiveram dados vazados

Através de e-mails corporativos extraídos utilizando a ferramenta hunter.io, verificamos que alguns desses e-mails já foram expostos durante vazamentos de dados, de acordo com o site Have Been Pwned. Um desses e-mails, inclusive, é de uma Diretora Sênior da empresa na parte do Marketing; Segue a lista.

- katieevans@upwork.com
- Já foi exposto em 8 vazamentos diferentes.
- Dados comprometidos: E-mail, empregadores, cargos, nomes, números de telefone, endereços físicos, perfis de mídia social, senhas, idiomas falados, nome de usuário no site, entre outros.



Lumin **PDF**: Em abril de 2019, o serviço de gerenciamento de PDFLumin PDF sofreu uma violação de dados. A violação não foi divulgada publicamente até setembro, quando 15,5 milhões de registros de dados de usuários apareceram para download em um popular fórum de hackers. Os dados foram deixados expostos publicamente em uma instância do MongoDB, após o que o Lumin PDF foi supostamente "contatado várias vezes, mas ignorou todas as consultas". Os dados expostos incluíam nomes, endereços de e-mail, gêneros, idioma falado e um hash de senha bcrypt ou token de autenticação do Google. Os dados foram fornecidos ao HIBP por uma fonte que solicitou que fossem atribuídos a "JimScott.Sec@protonmail.com".

Dados comprometidos: Tokens de autenticação, endereços de e-mail, gêneros, nomes, senhas, idiomas falados, nomes de usuário

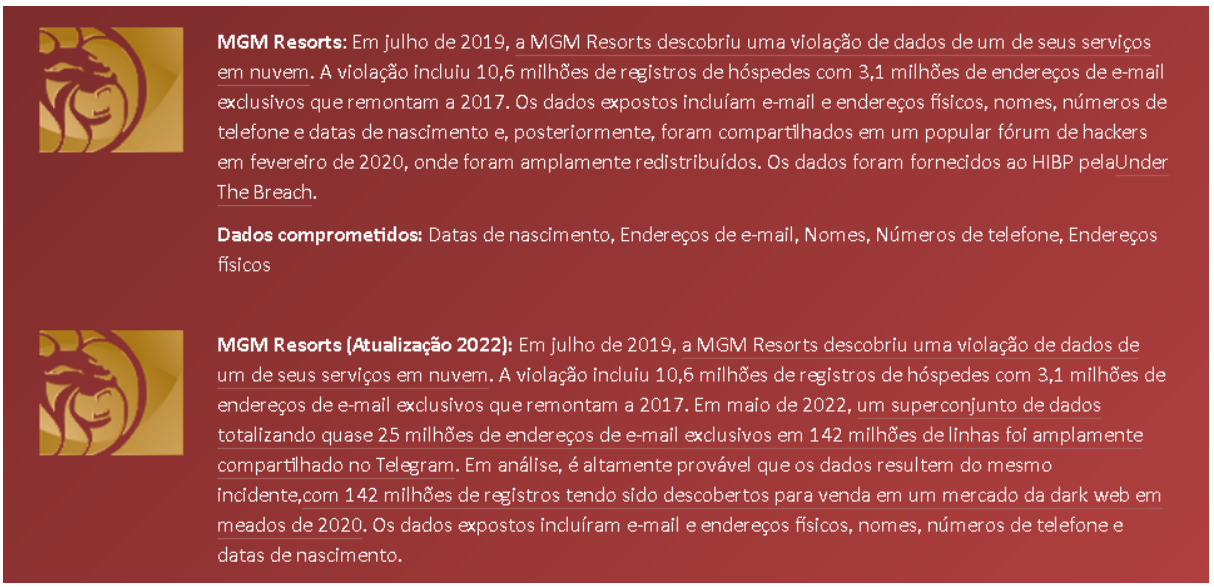
Exposição ao enriquecimento de dados do cliente PDL: Em outubro de 2019, os pesquisadores de segurança Vinny Troia e Bob Diachenko identificaram um servidor Elasticsearch desprotegido que continha 1,2 bilhão de registros de dados pessoais. Os dados expostos incluíam um índice indicando que eram provenientes da empresa de enriquecimento de dados People Data Labs (PDL) e continham 622 milhões de endereços de e-mail exclusivos. O servidor não era de propriedade da PDL e acredita-se que um cliente não conseguiu proteger adequadamente o banco de dados. As informações expostas incluíam endereços de e-mail, números de telefone, perfis de mídia social e dados de histórico de trabalho.

Dados comprometidos: Endereços de e-mail, Empregadores, Localizações geográficas, Cargos, Nomes, Números de telefone, Perfis de mídia social

Exactis: Em junho de 2018, a empresa de marketing Exactis inadvertidamente vazou publicamente 340 milhões de registros de dados pessoais. O pesquisador de segurançaVinny Troia, da Night Lion Security, descobriu que o vazamento continha vários terabytes de informações pessoais espalhadas por centenas de campos separados, incluindo endereços, números de telefone, estruturas familiares e extensos dados de perfil. Os dados foram coletados como parte do serviço da Exactis como um "compilador e agregador de dados premium de empresas e consumidores", que eles vendem para fins de criação de perfil e marketing. Um pequeno subconjunto dos campos expostos foi fornecido ao Have I Been Pwned e continha 132 milhões de endereços de e-mail exclusivos.

Dados comprometidos: Informações de status de crédito, Datas de nascimento, Níveis de educação, Endereços de e-mail, Etnias, Estrutura familiar, Investimentos financeiros, Gêneros, Status de propriedade residencial, Níveis de renda, Endereços IP, Estados civis, Nomes, Patrimônio líquido, Ocupações, Interesses pessoais, Telefones, Endereços físicos, Religiões, Idiomas falados

Dados raspados do LinkedIn: Durante o primeiro semestre de 2021, o LinkedIn foi alvo de invasores que coletaram dados de centenas de milhões de perfis públicos e depois os venderam on-line. Embora a raspagem não constituísse uma violação de dados nem acessasse quaisquer dados pessoais que não se destinassem a ser acessíveis ao público, os dados ainda eram monetizados e, posteriormente, amplamente divulgados em círculos de hackers. Os dados coletados contêm aproximadamente 400 milhões de registros com 125 milhões de endereços de e-mail exclusivos, bem como nomes, localizações geográficas, gêneros e cargos. O LinkedIn aborda especificamente o incidente em seu post sobreuma atualização sobre o relatório de dados raspados.

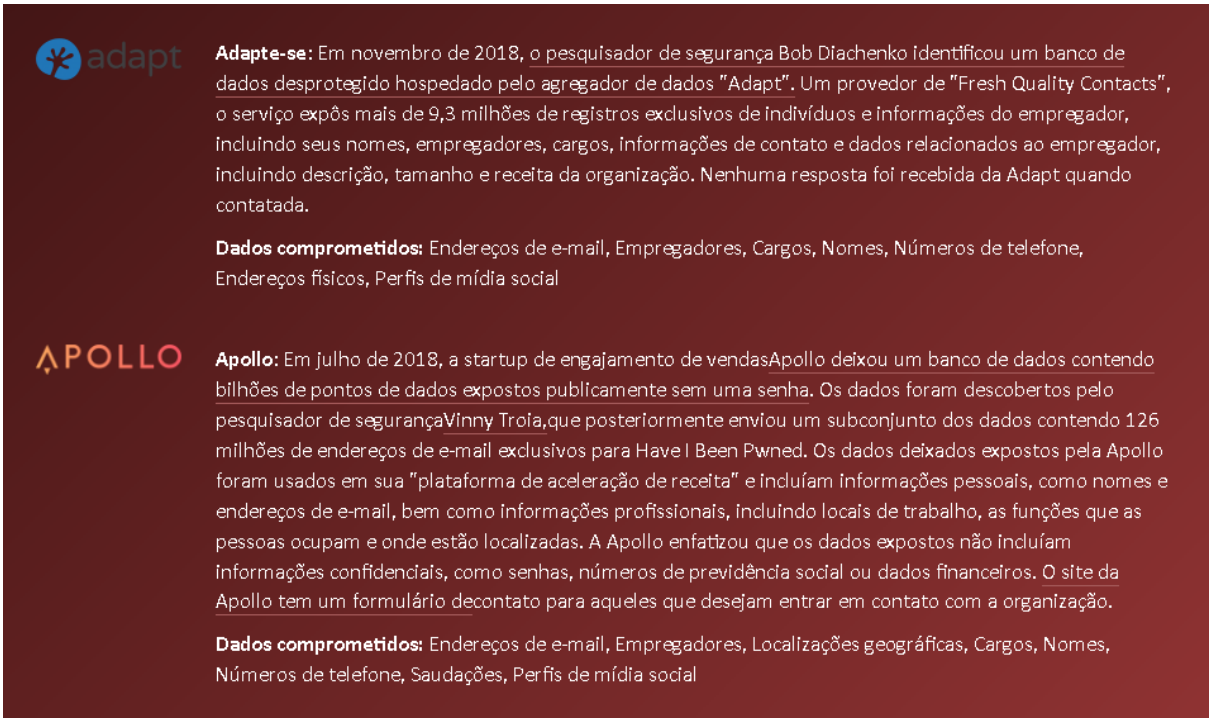


MGM Resorts: Em julho de 2019, a MGM Resorts descobriu uma violação de dados de um de seus serviços em nuvem. A violação incluiu 10,6 milhões de registros de hóspedes com 3,1 milhões de endereços de e-mail exclusivos que remontam a 2017. Os dados expostos incluíam e-mail e endereços físicos, nomes, números de telefone e datas de nascimento e, posteriormente, foram compartilhados em um popular fórum de hackers em fevereiro de 2020, onde foram amplamente redistribuídos. Os dados foram fornecidos ao HIBP pelaUnder The Breach.

Dados comprometidos: Datas de nascimento, Endereços de e-mail, Nomes, Números de telefone, Endereços físicos

MGM Resorts (Atualização 2022): Em julho de 2019, a MGM Resorts descobriu uma violação de dados de um de seus serviços em nuvem. A violação incluiu 10,6 milhões de registros de hóspedes com 3,1 milhões de endereços de e-mail exclusivos que remontam a 2017. Em maio de 2022, um superconjunto de dados totalizando quase 25 milhões de endereços de e-mail exclusivos em 142 milhões de linhas foi amplamente compartilhado no Telegram. Em análise, é altamente provável que os dados resultem do mesmo incidente,com 142 milhões de registros tendo sido descobertos para venda em um mercado da dark web em meados de 2020. Os dados expostos incluíram e-mail e endereços físicos, nomes, números de telefone e datas de nascimento.

- samanthadestefano@upwork.com
- Já foi exposto em 5 vazamentos diferentes
- Dados comprometidos: Endereço de e-mail, empregadores, cargos, nomes, números de telefone, endereços físicos, perfis de mídia social, senhas, entre outros.

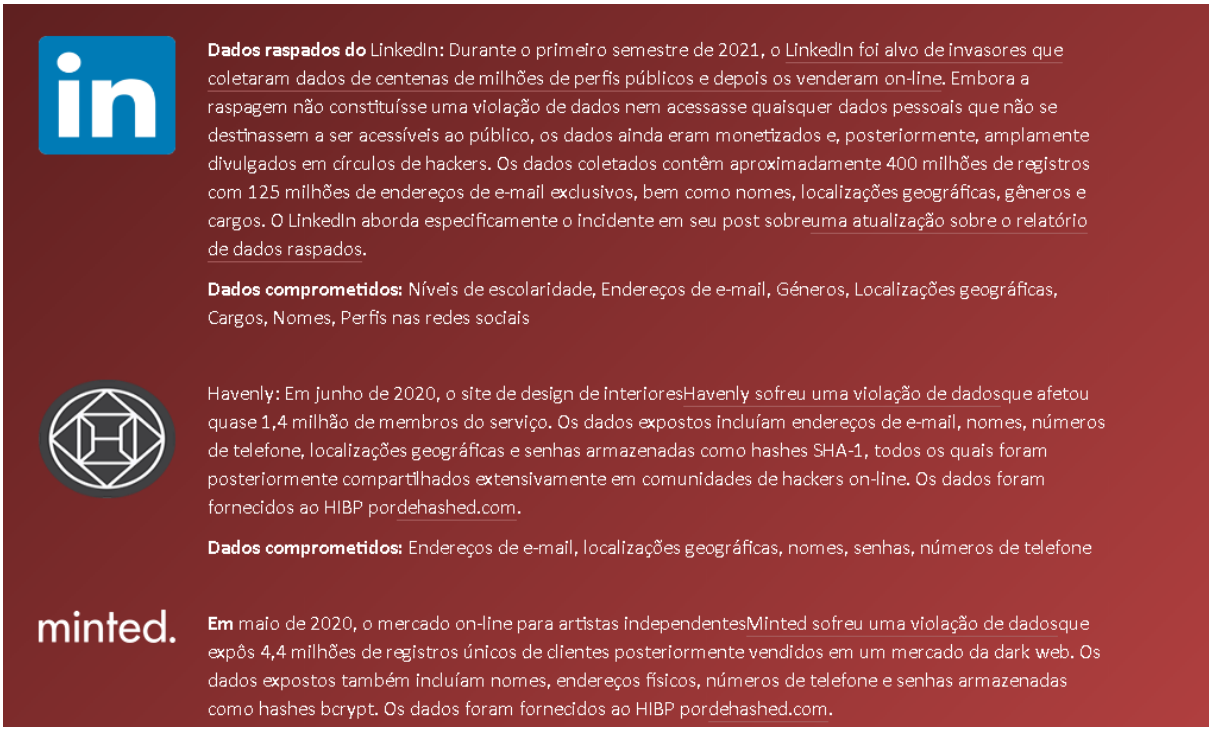


Adapte-se: Em novembro de 2018, o pesquisador de segurança Bob Diachenko identificou um banco de dados desprotegido hospedado pelo agregador de dados "Adapt". Um provedor de "Fresh Quality Contacts", o serviço expôs mais de 9,3 milhões de registros exclusivos de indivíduos e informações do empregador, incluindo seus nomes, empregadores, cargos, informações de contato e dados relacionados ao empregador, incluindo descrição, tamanho e receita da organização. Nenhuma resposta foi recebida da Adapt quando contatada.

Dados comprometidos: Endereços de e-mail, Empregadores, Cargos, Nomes, Números de telefone, Endereços físicos, Perfis de mídia social

Apollo: Em julho de 2018, a startup de engajamento de vendasApollo deixou um banco de dados contendo bilhões de pontos de dados expostos publicamente sem uma senha. Os dados foram descobertos pelo pesquisador de segurançaVinny Troia,que posteriormente enviou um subconjunto dos dados contendo 126 milhões de endereços de e-mail exclusivos para Have I Been Pwned. Os dados deixados expostos pela Apollo foram usados em sua "plataforma de aceleração de receita" e incluíam informações pessoais, como nomes e endereços de e-mail, bem como informações profissionais, incluindo locais de trabalho, as funções que as pessoas ocupam e onde estão localizadas. A Apollo enfatizou que os dados expostos não incluíam informações confidenciais, como senhas, números de previdência social ou dados financeiros. O site da Apollo tem um formulário decontato para aqueles que desejam entrar em contato com a organização.

Dados comprometidos: Endereços de e-mail, Empregadores, Localizações geográficas, Cargos, Nomes, Números de telefone, Saudações, Perfis de mídia social



Dados raspados do LinkedIn: Durante o primeiro semestre de 2021, o LinkedIn foi alvo de invasores que coletaram dados de centenas de milhões de perfis públicos e depois os venderam on-line. Embora a raspagem não constituísse uma violação de dados nem acessasse quaisquer dados pessoais que não se destinassem a ser acessíveis ao público, os dados ainda eram monetizados e, posteriormente, amplamente divulgados em círculos de hackers. Os dados coletados contêm aproximadamente 400 milhões de registros com 125 milhões de endereços de e-mail exclusivos, bem como nomes, localizações geográficas, gêneros e cargos. O LinkedIn aborda especificamente o incidente em seu post sobreuma atualização sobre o relatório de dados raspados.

Dados comprometidos: Níveis de escolaridade, Endereços de e-mail, Géneros, Localizações geográficas, Cargos, Nomes, Perfis nas redes sociais

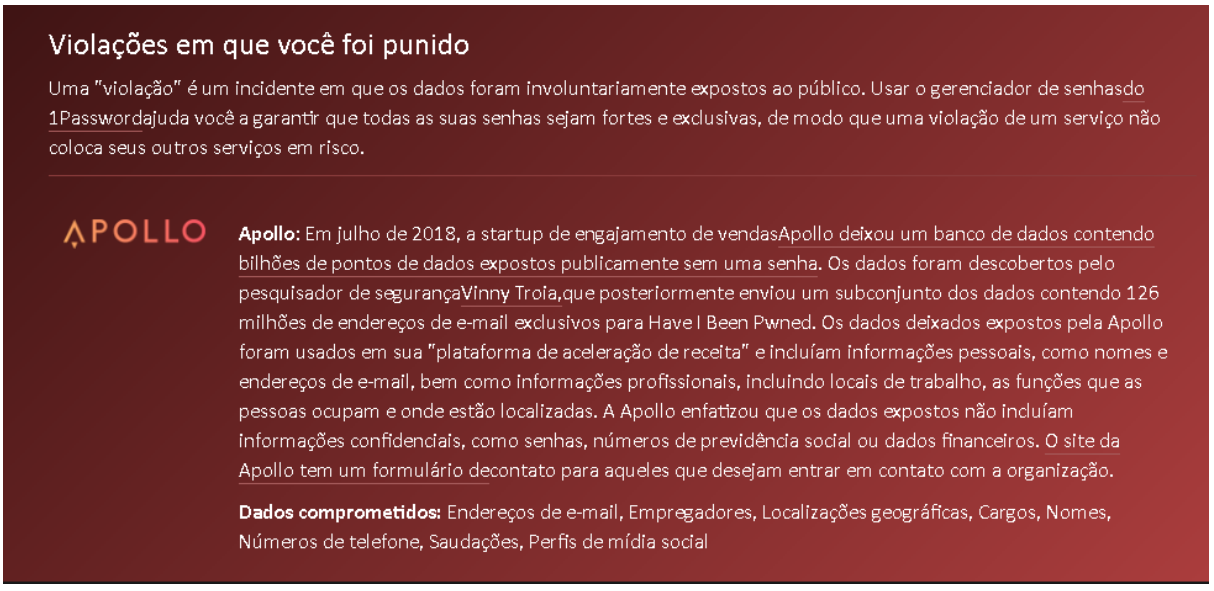
Havenly: Em junho de 2020, o site de design de interioresHavenly sofreu uma violação de dadosque afetou quase 1,4 milhão de membros do serviço. Os dados expostos incluíam endereços de e-mail, nomes, números de telefone, localizações geográficas e senhas armazenadas como hashes SHA-1, todos os quais foram posteriormente compartilhados extensivamente em comunidades de hackers on-line. Os dados foram fornecidos ao HIBP pordehashed.com.

Dados comprometidos: Endereços de e-mail, localizações geográficas, nomes, senhas, números de telefone

minted.

Em maio de 2020, o mercado on-line para artistas independentesMinted sofreu uma violação de dadosque expôs 4,4 milhões de registros únicos de clientes posteriormente vendidos em um mercado da dark web. Os dados expostos também incluíam nomes, endereços físicos, números de telefone e senhas armazenadas como hashes bcrypt. Os dados foram fornecidos ao HIBP pordehashed.com.

- freelancersuccess@upwork.com
- Foi exposto em somente um único vazamento.
- Dados expostos: Endereço de e-mail, empregadores, localização geográfica, cargo, nome, número de telefone, perfil de redes sociais.



Violações em que você foi punido

Uma "violação" é um incidente em que os dados foram involuntariamente expostos ao público. Usar o gerenciador de senhasdo 1Passwordajuda você a garantir que todas as suas senhas sejam fortes e exclusivas, de modo que uma violação de um serviço não coloca seus outros serviços em risco.

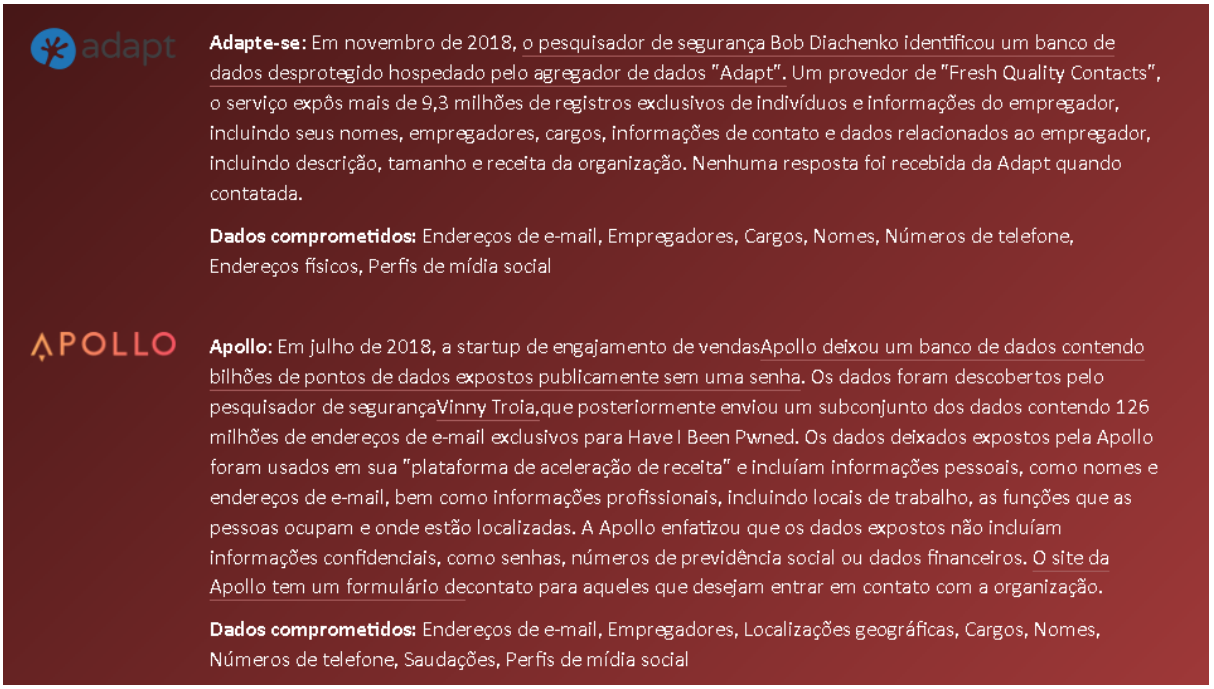
APOLLO

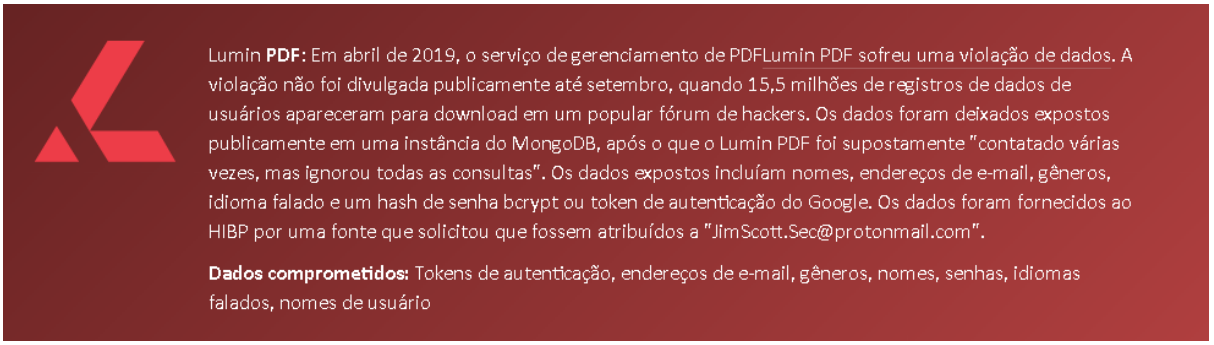
Apollo: Em julho de 2018, a startup de engajamento de vendasApollo deixou um banco de dados contendo bilhões de pontos de dados expostos publicamente sem uma senha. Os dados foram descobertos pelo pesquisador de segurançaVinny Troia,que posteriormente enviou um subconjunto dos dados contendo 126 milhões de endereços de e-mail exclusivos para Have I Been Pwned. Os dados deixados expostos pela Apollo foram usados em sua "plataforma de aceleração de receita" e incluíam informações pessoais, como nomes e endereços de e-mail, bem como informações profissionais, incluindo locais de trabalho, as funções que as pessoas ocupam e onde estão localizadas. A Apollo enfatizou que os dados expostos não incluíam informações confidenciais, como senhas, números de previdência social ou dados financeiros. O site da Apollo tem um formulário decontato para aqueles que desejam entrar em contato com a organização.

Dados comprometidos: Endereços de e-mail, Empregadores, Localizações geográficas, Cargos, Nomes, Números de telefone, Saudações, Perfis de mídia social

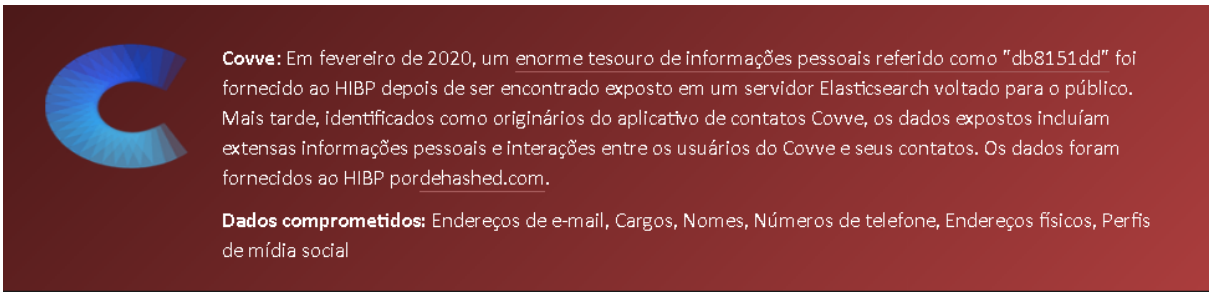
- support@upwork.com
- Já foi exposto em 4 vazamentos diferentes.
- Dados expostos: Endereço de e-mail, cargo, nome, número de telefone, endereço físico, perfil de rede social, endereço IP, dados parciais do cartão de crédito, senha, entre outros.

- charlieclark@upwork.com
- Exposto em 3 vazamentos diferentes.
- Dados comprometidos: Endereço de e-mail, cargo, nome, número de telefone, endereço físico, perfil de redes sociais, senha entre outros.

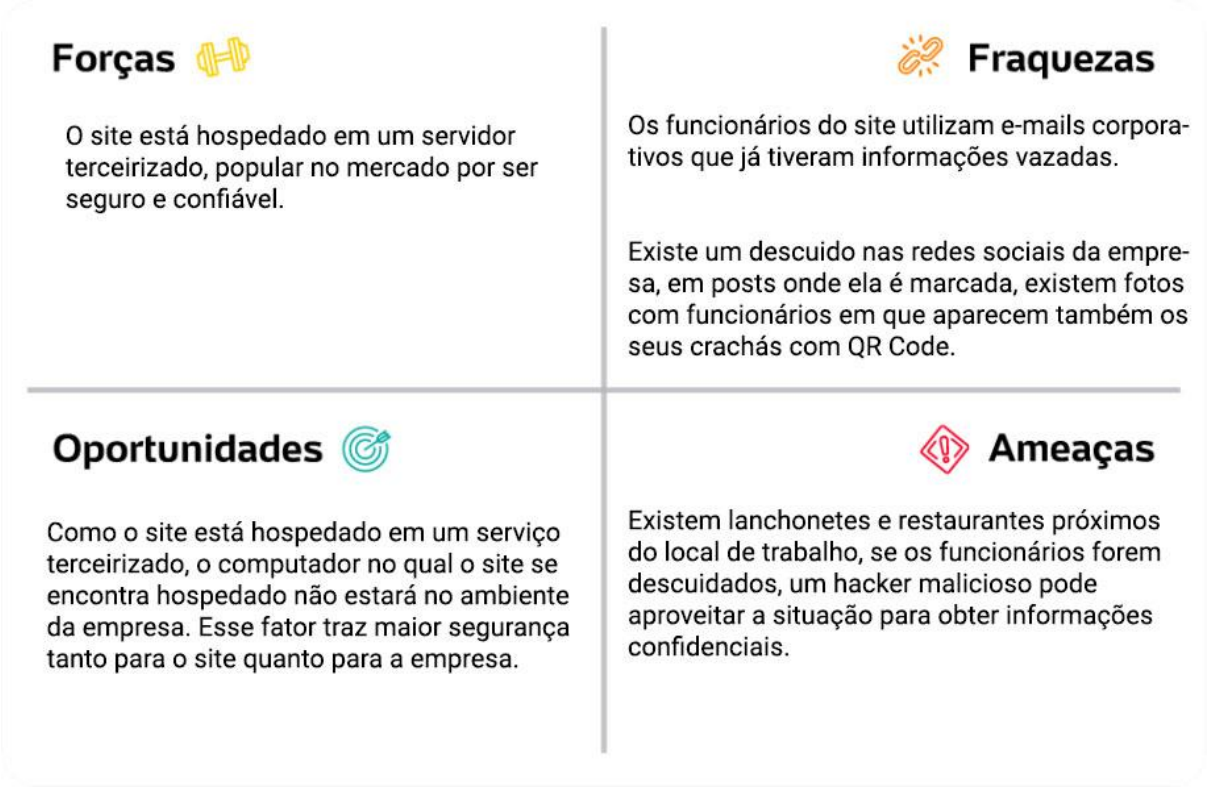




- partners@upwork.com
- Exposto em um único vazamento
- Dados vazados: Endereço de e-mail, cargo, nome, número de telefone, endereço físico, perfil de redes sociais.



12. Quadro SWOT da segurança do site



13. CONCLUSÃO

Foram realizados diversos testes de segurança e tentativas de manipulação no processo de registro de evidências providas pela plataforma. Nesta análise foram encontradas diversas proteções de segurança para evitar ataques simples e sofisticados no processo de coleta de informações fornecido pela plataforma, bem como em outros pontos do sistema. A partir do estudo realizado foi constatado que a upwork possui medidas efetivas para evitar a manipulação do conteúdo registrado durante e depois de seu processo de registro de evidências digitais, coletando as informações conforme constam em sua origem. Também foi constatada a efetividade da segurança sobre os dados armazenados e outros pontos detalhados na metodologia descrita em seguida. Porém, os e-mails corporativos são uma das principais portas de entrada para ameaças de segurança à infraestrutura de TI da empresa. Para minimizar os riscos é preciso fortalecer a proteção dos dados da organização e ampliar a educação dos colaboradores sobre a utilização adequada deste meio de comunicação.

14. Sugestões para o Contratante

14.1. Política de senha

- Adotar uma política forte de senha no trabalho, realizar a mudança de senha a cada mês ou semana e elas não podem repetir.
- Evitar usar senhas geradas automaticamente por outros sites ou pelo navegador.
- Jamais salve sua senha no navegador.
- Habilitar autenticação em 2 Fatores

14.2. Número de tentativas sem restrições (LOCK OUT)

Ao tentar fazer login na Upwork, o usuário pode errar a senha 5 vezes, na sexta tentativa em diante é necessário passar por um CAPTCHA antes de tentar logar. Tendo em vista que hoje em dia existem burladores de CAPTCHA, esse método de segurança não ajuda e recomendamos um bloqueio temporário escalonado (no quinto erro, o usuário não pode logar depois de 5 minutos, no sexto erro ele deve esperar 10 minutos e assim por diante.)

14.3. Políticas de segurança sugeridas para a companhia:

- Não utilizar e-mails que já foram vazados;
- Usar Filtros no E-mail e Anti-Spam
- Evitar muita exposição do local de trabalho e de crachás nas redes sociais;
- Não utilizar e-mails óbvios como admin@admin.com para conta administrativas do site;
- Não abrir arquivos de e-mails, os quais não conhecemos o remetente;
- Evitar falar do trabalho (principalmente quando são informações confidenciais); em espaços públicos ou com pessoas desconhecidas por perto;
- Ter um boa periodização de backups, para caso seja vítima do ataque ransomware;
- Estar com todos os software devidamente atualizados;

A política de segurança é algo que deve fazer parte diariamente do corpo da empresa, desde sua liderança até os prestadores de serviços. É algo que deve estar bem organizado, para manter um ambiente corporativo seguro, tanto para a empresa, como para seus clientes, e a melhor forma de fazer isso é treinando e capacitando seus funcionários, fazendo com que eles estejam sempre cientes de toda política, como funciona a segurança da empresa, o que devem evitar, e isso vem através de palestras, segundo, fornecendo um ambiente agradável para os funcionários, que já são adotados em diversas empresas, um ambiente de descompressão onde as pessoas podem comer, conversar com os outros funcionários, evitando que fiquem em bares, onde pode expor informações que não eram para serem expostas.