Segurança em Computação
Trabalho Individual I

João Paulo Taylor Ienczak Zanette

25 de março de 2019

O objetivo deste trabalho é que você exercite a forma de pensar de um profissional de segurança em computação. Por isso voce deve produzir um relatório analisando algum sistema que você usa corriqueiramente quanto a sua segurança, lembre de avaliar pelo menos:

- Ativos?
- Adversários?
- Gerenciamento de Risco?
- Contra medidas?
- Custo/Beneficio?

A avaliação deste trabalho vai exigir que você escolha um sistema com um grau de complexidade pelo menos médio. Sistemas de baixa complexidade implicam em nota máxima de 60%. Cada item avaliado corresponde a 20% da nota final do trabalho. A avaliação de cada item requer uma discussão embasada nos fundamentos discutidos em aula e um grau de profundidade médio (pelo menos 3 parágrafos por item avaliado), exigindo que o alunos discorra coerentemente sobre o tópico.
A entrega deve ser feita obrigatoriamente em PDF (o sistema não vai deixar entregar de outra forma). Atrasos sofrerão punição de 50% da nota independente da data de entrega.

1 Sobre o Sistema Escolhido

O sistema escolhido para este trabalho foi o **Sistema de Controle Acadêmico da Graduação** (CAGR), visto que, enquanto sistema da graduação, há bastante uso especialmente em períodos de matrícula, já que é necessário que esta seja feita nele, e ele é quem apresenta quais matérias o aluno conseguiu ou não, a grade de horários com salas em cada dia, professores, turmas e suas vagas, dentre outras informações de uso comum dos universitários da UFSC. Esta análise será estendida também ao **Fórum da Graduação**, um subsistema do CAGR para discussão entre alunos, com tópicos separados em fóruns de disciplinas ou do curso.

Toda a análise neste relatório será feita **do ponto de vista do aluno**.

2 Análise

2.1 Ativos

2.1.1 Geral

Por se tratar do sistema oficial da graduação, há informações bastante importantes (institucionalmente) de cada aluno. Nem todas elas, porém, tem um valor monetário direto. Para boa parte delas, o uso indevido acarreta em problemas administrativos e transtornos para os alunos. Sumarizando a parte principal do CAGR:

- Dados cadastrais (detalhado nas Seções 2.1.2 e 2.1.3);
- Pedidos de matrícula (inclusões, exclusões e alterações);
- E-mail e senha[1]

Dos pedidos de matrícula, é importante que o aluno não tenha sua matricula fora da regularidade por conta de alterações indesejadas nos pedidos de suas disciplinas. Além ainda da regularidade, vale apontar o transtorno de ser redirecionado para turmas e disciplinas que não compactuam com os objetivos do aluno, incluindo casos como estar sobrecarregado de disciplinas contra a própria vontade. Desfazer/corrigir essas mudanças demandaria ao aluno tratar diretamente com autoridades como o Coordenador de Curso e principalmente da boa vontade de professores entenderem a situação e poderem tomar medidas como aumento do número de vagas em suas turmas para que o aluno pudesse cursar as disciplinas que havia voluntariamente pedido. Vale apontar que há casos em que o professor não teria como alimentar a demanda de vagas, uma vez que necessita de espaço e tempo em aula para coordenar a turma. Ou seja, o pedido de matrícula de um aluno deve ser protegido.

Quanto ao e-mail e senha, não é necessário elaborar muito sobre sua necessidade de proteção: o não recebimento de e-mails (por conta de um invasor configurar um e-mail que não seja algum de acesso do aluno) pode levar o aluno a perder informações importantíssimas que prejudicariam sua vida acadêmica (perda de provas por alterações de data, ou entregas de trabalho, etc.). A senha seria ainda mais catastrófica, uma vez que um atacante tendo acesso a ela é possível fazer todas as alterações indesejadas citadas até o momento, e ainda configurar uma senha que não é a do aluno (fazendo com que este tenha que resolver o caso com a instituição, gerando situações inconvenientes). Há de lembrar ainda a possibilidade da senha configurada ser a mesma de outras contas do aluno, outras ainda mais pessoais (plataformas de *chat* instantâneo, repositório de arquivos na nuvem — e.g. Google Drive —, etc.).

Vale lembrar que, se noticiada publicamente, uma invasão dessas mancharia a visão do público sobre a instituição, ainda mais sendo uma instituição pública em um país em que é comum a descrença quanto a recursos relacionados ao governo.

2.1.2 Dados cadastrais institucionais

Dados institucionais incluem:

- E-mail institucional;
- Currículo do aluno (notas e frequência nas disciplinas em cada semestre).

2.1.3 Dados cadastrais pessoais

Dados pessoais incluem:

- CPF e RG;
- Tipo sanguíneo;
- Cidade natural;

[1] Não são institucionais, mas são essenciais para ter acesso para ler e alterar todas as outras informações.

- Nome dos pais;
- Procedência escolar:
  - Ano de conclusão;
  - Escola;
  - Curso (quando há técnico integrado, por exemplo);
  - Cidade em que cursou.

2.2 Adversários

Um dos interessados nos dados guardados no CAGR pode ser um inimigo pessoal de um aluno. Tendo acesso aos dados, pode acontecer alguma forma de sabotagem ou humilhação pública. Por exemplo, no semestre 2015.2 do curso de Ciência da Computação, alguém obteve acesso ao CAGR de um aluno sem o consentimento dele (que possivelmente esqueceu algum computador da instituição logado) e postou no fórum da graduação (em que os professores possuem acesso e potencialmente recebem e-mail do que é postado nele) intitulado "Trote Opressor e Ofensivo", que fazia uma falsa denúncia de homofobia e bullying no nome do tal aluno. Uma postagem dessas pode por em jogo, além da imagem dos veteranos do curso, futuros eventos de recepção para calouros.

Atualmente também são valiosas informações para diferentes empresas e instituições. Pode ser considerado um adversário alguém interessado em roubo de informações seja para vender ou para uso direto. São informações importantes para quem busca contratar recém-formados ou graduandos, por exemplo.

Outros adversários podem envolver tanto quem queira sabotar resultados de processos seletivos (por exemplo, para pós-graduação, alterando o histórico escolar de algum aluno) quanto quem mesmo?.

2.3 Gerenciamento de Risco

Considerando que o CAGR é um sistema web, o custo de se realizar um ataque é potencialmente baixo (desconsiderando possíveis consequências jurídicas). Por exemplo, um *SQL Injection* teria apenas o custo de conhecer a estrutura interna dos bancos de dados do sistema e achar qual campo não é sanitizado. Quanto ataques via *buffer-overflow*, como o CAGR é feito em Java, ele depende quase totalmente da implementação das bibliotecas utilizadas.

Outro detalhe, o CAGR é um sistema direcionado à instituição UFSC, e portanto *potencialmente* não tem *mirrors* espalhados pelo país. Logo, o custo de se realizar um ataque é compensado pelo ganho de se ter acesso à única fonte daquelas informações (salvo *backups*). Isso significa tanto no fato de que obstrução de informações tem maior impacto quanto no de que, tendo acesso a uma informação, potencialmente se tem acesso a todas as outras.

Além disso, centralização pode facilitar ataques como *Denial of Service*. Esse ataque poderia não trazer estragos muito grandes, já que o servidor poderia ser religado pouco depois. Porém, isso poderia gerar transtornos aos alunos (tempo de matrícula, emissão de atestado de matrícula, etc.) e deve-se protegido contra, ainda que não seja um impacto ireto na instituição mas sim em seus clientes.

2.4 Contra medidas

De contra-medidas relacionadas a *software*, a primeira a se pensar, tratando-se de um sistema Web, é a sanitização de entradas de usuário, incluindo via URL (não permitir, por exemplo, um campo "idAluno" na URL não ser validado com o usuário *logado* e dar acesso a dados de outros alunos).

Para evitar ataques como *buffer-overflow*, é importante manter as bibliotecas atualizadas, já que atualizações de segurança são essenciais e nem sempre é possível ficar observando qual atualização de cada biblioteca terá alguma alteração importante.

Da parte de infraestrutura, o sistema do CAGR deve ter *backups*, para evitar perda de informação quando ocorrer alguma invasão com o propósito de destruir informações, e *logs* para tanto indentificar possíveis atacantes quanto desfazer operações indesejadas.

2.5 Custo/Beneficio

Apesar de os custos de se realizar um ataque no CAGR não sejam altos, os benefícios dificilmente compensariam. Boa parte deles são muito direcionados a pessoas específicas em situações específicas. Nas melhores hipóteses (do ponto de vista do atacante), se consegue a senha de algum usuário que possa utilizar a mesma senha em outros lugares.

Mesmo um *Denial of Service* não teria tantos benefícios. Inclusive, este possivelmente teria um dos custos mais altos, afinal o CAGR é feito para suportar acesso de todos os alunos da UFSC — mais de 46 mil — durante todo o semestre, a ganhos não muito significativos: atrasaria a publicação de médias finais, ou iria atrapalhar o processo de matrícula, porém nada de concreto se conseguiria.