Segurança em Computação
Trabalho Individual I

João Paulo Taylor Ienczak Zanette

17 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 mesno 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 extendida 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. 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, a matrícula de um aluno é um ativo de extrema responsabilidade de ser protegido contra alterações indesejadas.

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.).

2.1.2 Dados cadastrais institucionais

TODO

2.1.3 Dados cadastrais pessoais

Dados pessoais incluem:

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

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

2.2 Adversários

Os interessados nos ativos do CAGR podem envolver:

- Inimigos pessoais do aluno que estariam interessados em alguma forma de sabotagem a ele;
- Interessados em roubo de informações (para marketing direcionado, uso ilícito de informações pessoais, chantagem, ...);
- What else?

2.3 Gerenciamento de Risco

Ver sobre segurança do vBulletin

2.4 Contra medidas

Ver se as contra-medidas são para quando já aconteceu o ataque ou se são medidas preventivas.

2.5 Custo/Beneficio

Considerando que o CAGR é um sistema web, o custo de se realizar um ataque é potencialmente baixo (desconsiderando possíveis consequências). 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 ao balanceamento custo/benefício, 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.

Há um ponto a ser considerado, porém: por se tratar de uma instituição federal, se o atacante for identificado, as consequências legais podem ser maiores.

3 Conclusões

TODO