Segurança Informática e nas Organizações

Guiões das Aulas Práticas

João Paulo Barraca[1] e Hélder Gomes[2]

[1]Departamento de Eletrónica, Telecomunicações e Informática
[2]Escola Superior de Tecnologia e Gestão de Águeda
Universidade de Aveiro

2015–2016

Conteúdo

2

Vulnerabilidades na Web

Resumo:

- Teste de ataques por injeção de *strings* SQL.
- Teste de ataques XSS (*Crosss Site Scripting*).

2.1 Introdução

Para realizar este trabalho vamos usar a aplicação **WebGoat**[1][2]. O WebGoat é uma aplicação Web que se destina ao ensino de segurança e na qual foram deliberadamente introduzidas vulnerabilidades. Foi desenvolvida pela OWASP[3], organização cujo objetivo é a sensibilização para a segurança.

2.2 Arranque do WebGoat

2.2.1 Alteração da instalação

A máquina virtual fornecida para a disciplina tem a versão 6.0 do WebGoat instalada. No entanto, alguns dos exercícios neste guião não funcionam nessa versão. Por essa razão deve proceder à instalação da versão anterior, a versão 5.4. Para esse efeito, descarregue da página da disciplina na plataforma de elearning (http://moodle.ua.pt) o script `installWebGoat5.4.sh`.

Usando um terminal, vá para a pasta para onde descarregou o script e altere as permissões do script para que o possa executar:

```
chmod u+x installWebGoat5.4.sh
```

Execute-o usando o seguinte comando (note que o script inclui comandos que têm de ser executados como sudo, pelo que lhe irá ser pedida a sua password):

```
./installWebGoat5.4.sh
```

O script irá demorar algum tempo a executar, uma vez que além de descarregar e instalar o WebGoat5.4 também tem de fazer a instalação do JDK7.

2.2.2 Iniciar o WebGoat

Para iniciar o WebGoat, abra uma consola de terminal e introduza os seguintes comandos:

```
cd /opt/WebGoat/WebGoat-5.4
sudo ./webgoat.sh start8080
```

[1] `https://www.owasp.org/index.php/Category:OWASP_WebGoat_Project`
[2] `https://code.google.com/p/webgoat`
[3] `http://www.owasp.org`

Este terminal fica dedicado ao WebGoat, e será para lá que todo o output será dirigido.

Para aceder ao WebGoat, navegue para o seguinte endereço: `http://localhost:8080/WebGoat/attack`

Quando lhe for pedida a credencial de login, o *username* é `guest` e a senha é `guest`. Clique no botão `Start WebGoat`.

Explore o WebGoat. Na coluna do lado esquerdo está um menu de acesso a um conjunto de exercícios e na parte inicial da página está um menu que pode aceder para obter mais informação sobre o exercício selecionado, tal como sugestões, soluções, etc.

2.3 Injeção de SQL

2.3.1 Injeção de *strings* SQL

O ataque por injeção de *strings* SQL é utilizado para comprometer bases de dados. Os métodos utilizados são simples, mas as suas consequências podem ser devastadoras.

Na coluna do lado esquerdo do WebGoat, clique em `Injection Flows` e depois selecione `String SQL Injection`. O ecrã apresentado permite aos utilizadores obter informação sobre os seus cartões de crédito, sendo sugerida a introdução do nome `Smith`. Introduza o nome sugerido e veja os cartões de crédito associados. A procura (*query*) utilizada para obter a informação foi a seguinte:

```
SELECT * FROM user_data WHERE last_name='Smith'
```

Neste caso, `Smith` foi o valor que introduziu, tendo a procura obtido todos os cartões de crédito do utilizador Smith.

1. Quantas linhas de resultado obteve?

2. São todas referentes ao utilizador Smith?

3. Como faria para obter a informação dos cartões de crédito de todos os utilizadores?

Experimente introduzir `Smith' OR '1'='1` e veja o resultado. Do ponto de vista de segurança, quais as consequências do resultado obtido?

Indique uma forma de eliminar a vulnerabilidade neste exercício.

2.3.2 Alteração de dados através de injeção de SQL

Na coluna do lado esquerdo do WebGoat, clique em `Injection Flows` e depois selecione `Modify Data with SQL Injection`. O ecrã apresentado permite aos utilizadores obter informação sobre os seus salarios, sendo sugerida a introdução do identificador de utente `jsmith` e mostrado o valor do seu salário.

1. Como faria para alterar o valor do salário deste utilizador?
2. Como faria para ver o valor de todos os salários?

2.3.3 Inserção de dados através de injeção de SQL

Na coluna do lado esquerdo do WebGoat, clique em `Injection Flows` e depois selecione `Add Data with SQL Injection`. O ecrã apresentado permite aos utilizadores obter informação sobre os seus salários, sendo sugerida a introdução do identificador de utente `jsmith` e mostrado o valor do seu salário, após clicar no botão Go!.

1. Como faria para inserir um salário para si?
2. Como faria para ver o valor de todos os salários?

2.4 *Cross-Site Scripting* (XSS)

2.4.1 Ataque XSS por armazenamento

O ataque XSS por armazenamento, ilustrado na Figura 2.1, permite a um utilizador colocar conteúdo numa página num sítio na Web que pode fazer com que outro utilizador, ao aceder a essa página, carregue outra página não desejada ou conteúdo não desejado.

Na coluna do lado esquerdo do WebGoat, clique em `Cross-Site Scripting (XSS)` e depois selecione `Stored XSS Attacks`. A página apresentada permite a gravação de uma mensagem.

Na caixa `Title`, introduza o título da mensagem. Por exemplo, introduza `XSS Example`. Na caixa `Message`, introduza o seguinte conteúdo HTML:

```
<script language="javascript" type="text/javascript">
alert("Vais ser atacado!"); </script>
```

Clique no botão `Submit` e depois clique na mensagem que acabou de submeter, o *link* está em baixo a seguir à caixa de texto.

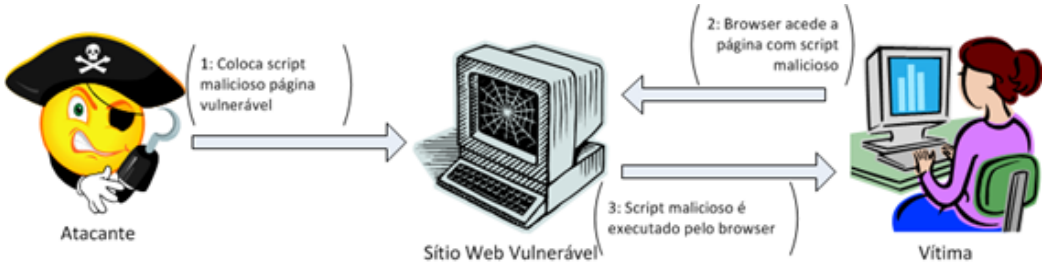

Figura 2.1: Ataque XSS por armazenamento

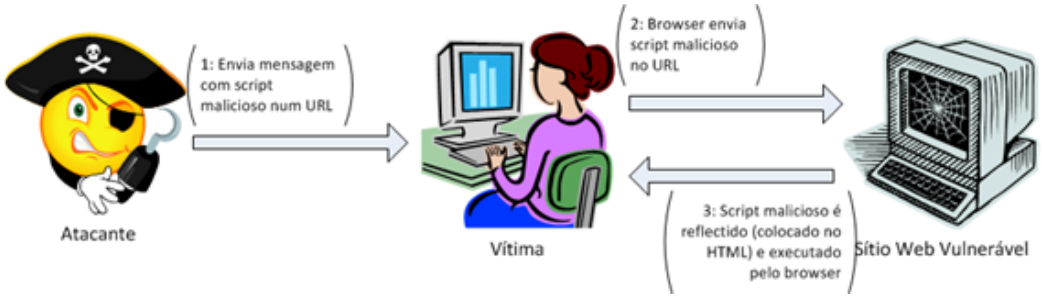

Figura 2.2: Ataque XSS por reflexão

1. O que é que acontece a quem clicar na mensagem que introduziu?

2. Quais são as implicações do ponto de vista da segurança do utilizador?

2.4.2 Ataque XSS por reflexão

O ataque XSS por reflexão, ilustrado na Figura 2.2, permite a um atacante utilizar uma página vulnerável para refletir um guião (*script*) para o navegador da vítima. Porém, primeiro tem de convencer a vítima a selecionar uma hiperligação com um URL com um guião malicioso.

Para demostrar este ataque, selecione o seguinte *link*: Para demostrar este ataque, usando a máquina virtual, aceda à página da disciplina na plataforma de elearning e faça o download do documento `Demo XSS Reflexão.docx`.

O documento contém um link, Demo XSS, com o seguinte script: `http://localhost:8080/WebGoat/attack?show=Params&Screen=%3cscript%3ealert(%22Viva!%20Aqui%20estou%20eu.%22);%3c/script%3e`

No documento, clique no link Demo XSS.

Nota: Eventualmente poderá ser necessário clicar uma segunda vez no *link* atrás para o ataque surtir efeito.

Após tê-lo feito ir-se-á abrir uma nova aba no seu navegador, onde o ataque decorrerá.

1. Qual o elemento vulnerável na página que foi explorado neste ataque?
2. Diga qual a diferença entre este ataque e um ataque de *Phishing*?

2.5 Exercícios adicionais

Explore os vários tipos de ataques que a plataforma WebGoat disponibiliza.

Nota: Para alguns dos ataques poderá ser necessário utilizar um *proxy* para interceptar as mensagens entre o navegador e o servidor Web. A máquina virtual vem com o *proxy* Paros instalado. Para o iniciar, numa consola vá para a pasta `~/tools/paros` e execute o comando `./startserver.sh`. A consola fica bloqueada até que a execução do Paros termine.

2.6 Soluções

Para os desafios colocados na Secção 2.3.2 podem ser usadas as seguintes soluções:

1. `jsmith'; update salaries set salary='30000' where userid='jsmith`
2. `jsmith' or '1'='1`