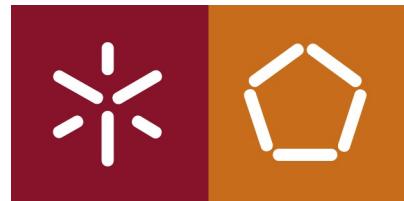


Universidade do Minho



Mestrado Integrado em Engenharia Informática
Engenharia de Segurança

Aula 12

Grupo 8



João de Macedo
A76268



João Aloísio
A77953



Nelson Gonçalves
A78173

24 de Maio de 2020

1 Injection

Inicialmente foi pedido para ser obtido o departamento do trabalhador "Bob Franco". Para isso foi feito o comando **SELECT DEPARTMENT FROM Employees WHERE first_name = 'Bob';**

No passo 3 foi pedido para alterar o valor de "DEPARTMENT" para "Sales" do empregado "Tobi". Para isso foi feito o comando **UPDATE Employees SET DEPARTMENT = 'Sales' WHERE first_name = 'Tobi';**

No passo 4 foi pedido para adicionar a coluna "phone" a tabela "employees". Para isso foi feito o comando **ALTER TABLE employees ADD phone varchar(20);**

No passo 5 foi pedido para alterar as permissões do grupo "UnauthorizedUser" e permitir que este alterem a tabela. Para isso foi deito o comando **GRANT ALTER TABLE TO UnauthorizedUser;**

No passo 9 foi dada hipóteses para obter a lista completa de utilizadores e para isso foi escolhida a opção "Smith' or '1' = '1".

No passo 10 foi pedido para descobrir que campo era vulnerável dos dois fornecidos. Foi descoberto através do 0, sendo o segundo campo o vulnerável inserindo assim os campos **0, 0 or 1=1**

No passo 11 foi pedido para obter a lista de empregados e para isso foram introduzidos os campos "s, ' or '1' = '1" tal como nos exercícios anteriores, sendo após a query ser analisada.

No passo 12 é pedido para alterar o valor do salário do empregado, sendo que após fechar ';' é possível introduzir uma query à tabela e alterar assim os valores **UPDATE employees SET salary=9999999 WHERE first_name='John'**

No passo 13 é pedido para eliminar a tabela "access_log" e para isso foi usado como anteriormente ';' e feita a query **DROP TABLE access_log;**

2 XSS

Ponto 2:

- Abrir 2 separadores na pagina do webgoat
- Abrir a consola do browser e inserir `alert(document.cookie);`
- Verificar que ambas as cookies são iguais e responder "yes"

ponto 7:

- Inserimos `<script>alert()</script>` na box do cartao de credito
- Obtemos um pop-up alert

- Obtemos tb a seguinte mensagem "Well done, but alerts are not very impressive are they? Please continue."

ponto 10:

- Abrir o debugger
- Ir par a diretoria View
- Abrir GoatRouter.js
- Ver as rotas : 'welcome': 'welcomeRoute', 'lesson/:name': 'lessonRoute', 'lesson/:name/:pageNum': 'lessonPageRoute', 'test/:param': 'testRoute', 'reportCard': 'reportCard'

ponto 11:

- Aceder a rota test
- colocar como parametro o webgoat.customjs.phoneHome()
- substituis o "/"em </script> por %2f
- aceder a "http://localhost:8080/WebGoat/start.mvc#test/ <script>webgoat.customjs.phoneHome()%2Fscript</script>".
- Na consola do browser obetmos a seguinte resposta "phoneHome Response is 661119233"

3 Quebra na Autenticação

Não conseguimos resolver este problema:

```
Applications Places System Sun May 24, 18:45
File Edit View Search Terminal Tabs Help user@CSI: ~
user@CSI:~$ sudo docker run -p 9090:9090 -t webgoat/webwolf
Waiting for database to be available...

:: Spring Boot :: (v2.2.2.RELEASE)

2020-05-24 17:43:39.709 INFO 7 --- [           main] org.owasp.webwolf.WebWolf          : Starting WebWolf v8.1.0 on 21160fb40d0e with PID 7 (/home/webwolf/webwolf.jar started by webwolf in /)
2020-05-24 17:43:39.712 DEBUG 7 --- [           main] org.owasp.webwolf.WebWolf           : Running with Spring Boot v2.2.2.RELEASE
2020-05-24 17:43:39.714 INFO 7 --- [           main] org.owasp.webwolf.WebWolf           : No active profile set, falling back to default profiles: default
2020-05-24 17:43:41.520 INFO 7 --- [           main] .s.d.r.c.RepositoryConfigurationDelegate : Bootstrapping Spring Data JPA repositories in DEFAULT mode.
2020-05-24 17:43:41.623 INFO 7 --- [           main] .s.d.r.c.RepositoryConfigurationDelegate : Finished Spring Data repository scanning in 92ms. Found 2 JPA repository interfaces.
2020-05-24 17:43:42.317 INFO 7 --- [           main] trationDelegatesBeanPostProcessorChecker : Bean 'org.springframework.transaction.annotation.ProxyTransactionManagementConfiguration' is not eligible for getting processed by all BeanPostProcessors (for example: not eligible for auto-proxying)
2020-05-24 17:43:42.813 WARN 7 --- [           main] io.undertow.websockets.jsr          : UT026010: Buffer pool was not set on WebSocketDeploymentInfo, the default pool will be used
2020-05-24 17:43:42.858 INFO 7 --- [           main] io.undertow.servlet                 : Initializing Spring embedded WebApplicationContext
2020-05-24 17:43:42.859 INFO 7 --- [           main] o.s.web.context.ContextLoader        : Root WebApplicationContext: initialization completed in 2979 ms
2020-05-24 17:43:43.576 INFO 7 --- [           main] o.h.hibernate.jpa.internal.util.LogHelper : HHH000204: Processing PersistenceUnitInfo [name: default]
2020-05-24 17:43:43.704 INFO 7 --- [           main] org.hibernate.Version                : HHH0000412: Hibernate Core {5.4.9.Final}
2020-05-24 17:43:43.976 INFO 7 --- [           main] o.h.hibernate.annotations.common.Version : HHH000401: Hibernate Commons Annotations {5.1.0.Final}
2020-05-24 17:43:44.362 WARN 7 --- [           main] o.h.e.j.e.i.JdbcEnvironmentInitiator : Connection refused (Connection refused)
2020-05-24 17:43:44.418 INFO 7 --- [           main] org.hibernate.dialect.Dialect       : HHH000400: Using dialect: org.hibernate.dialect.MYSQLDialect
2020-05-24 17:43:45.434 WARN 7 --- [           main] o.h.engine.jdbc.spi.SqlExceptionHelper : SQL Error: -101, SQLState: 08001
2020-05-24 17:43:45.435 ERROR 7 --- [           main] ConfigServletWebServerApplicationContext : java.net.ConnectException: Connection refused (Connection refused)
2020-05-24 17:43:45.440 INFO 7 --- [           main] ConditionEvaluationReportLoggingListener : Exception occurred during context initialization - cancelling refresh attempt
2020-05-24 17:43:45.462 INFO 7 --- [           main] org.springframework.beans.factory.BeanCreationException: Error creating bean with name 'entityManagerFactory' defined in class path resource [org/springframework/boot/autoconfig/orm/jpa/HibernateJpaConfiguration.class]: Invocation of init method failed; nested exception is org.hibernate.exception.JDBCConnectionException: Unable to open JDBC Connection for DDL execution
2020-05-24 17:43:45.462 INFO 7 --- [           main] ConditionEvaluationReportLoggingListener : 

Error starting ApplicationContext. To display the conditions report re-run your application with 'debug' enabled.
2020-05-24 17:43:45.474 ERROR 7 --- [           main] o.s.boot.SpringApplication            : Application run failed

org.springframework.beans.factory.BeanCreationException: Error creating bean with name 'entityManagerFactory' defined in class path resource [org/springframework/boot/autoconfig/orm/jpa/HibernateJpaConfiguration.class]: Invocation of init method failed; nested exception is javax.persistence.PersistenceException: [PersistenceUnit: default] Unable to build Hibernate SessionFactory; nested exception is org.hibernate.exception.JDBCConnectionException: Unable to open JDBC Connection for DDL execution
at org.springframework.beans.factory.support.AbstractAutowireCapableBeanFactory.initializeBean(AbstractAutowireCapableBeanFactory.java:1796) ~[spring-beans-5.2.2.RELEASE.jar!/:5.2.2.RELEASE]
at org.springframework.beans.factory.support.AbstractAutowireCapableBeanFactory.doCreateBean(AbstractAutowireCapableBeanFactory.java:595) ~[spring-beans-5.2.2.RELEASE.jar!/:5.2.2.RELEASE]
at org.springframework.beans.factory.support.AbstractAutowireCapableBeanFactory.createBean(AbstractAutowireCapableBeanFactory.java:517) ~[spring-beans-5.2.2.RELEASE.jar!/:5.2.2.RELEASE]
```

Figura 1

4 Componentes vulneráveis

Ponto 5:

Neste ponto conseguimos ver que usando o mesmo código fonte do *WebGoat* mas diferentes versões do componente *jquery-ui*, uma é explorável e outra não. Apenas foi copiado o comando *OK<script>alert('XSS')</script>* para a janela de diálogo.

Ponto 12:

Aqui foi adicionado o comando <java.lang.Integer>96</java.lang.Integer>