Security of Distributed Software

SS 2020 – 3. Tutorial

Valentin Siegert M.Sc.

Shovra Das M.Sc.

VSR.*Informatik*.TU-Chemnitz.*de*

Task 1

What is Session Hijacking?

The Session Hijacking attack consists of the exploitation of the web session control mechanism, which is normally managed for a session token.

The Open Web Application Security project

How do you get a Session-Token?

- Predictable Session Token
- Session Sniffing
- Client-side attacks (XSS)

https://mytuc.org/vwfx enables registered users to retrieve the PIN number of his mobile phone (e.g. using username Max and password Mustermann).

Find out the PIN number of user John.

2

Task 2

Install a MySQL database

1. Create a database named {URZ Nutzername}-svs with a table *personen*:
   - id: INT, Index: PRIMARY, AUTO_INC
   - name: CHAR(20)
   - age: INT
2. Addsome data
3. Write an SQL query, which returns all persons, whose name is *Max.*
4. Extend *personen.php* to send above query to DB.
5. Extend program with search functionality (use string concatenation)

What is SQL-Injection?

A SQL injection attack consists of insertion or "injection" of a SQL query via the input data from the client to the application

The Open Web Application Security project

What can be done with SQL Injection?

…read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system

How can a SQL-Query be injected?

- Form data

```
POST / HTTP/1.1
…
username=max&password=mustermann
```

- URL paramter

```
GET /login.php?username=max&password=mustermann HTTP/1.1
```

- Cookies

```
Cookie: username=max; id=114;
```

3 Task 3

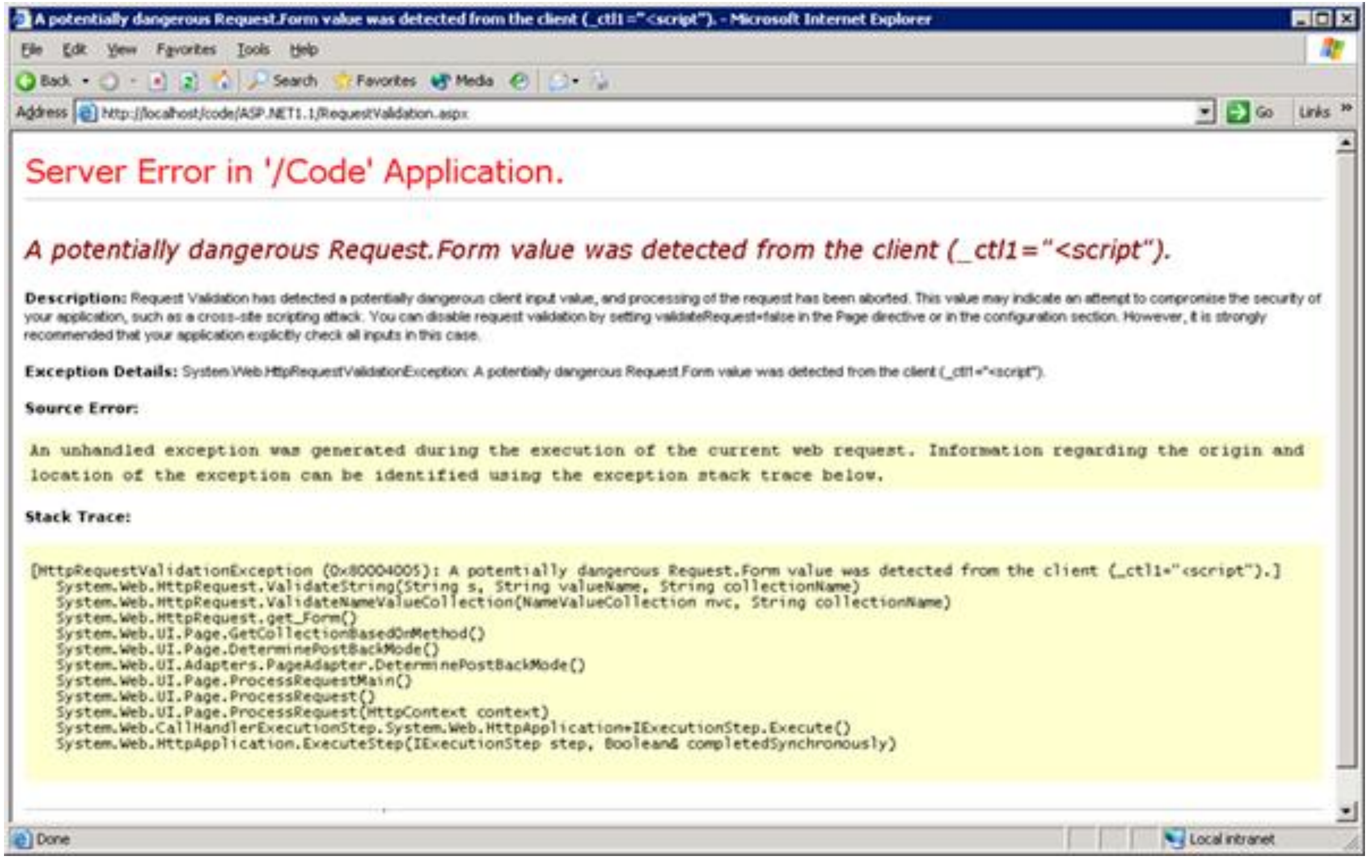
Open the page from task 2, cf. https://mytuc.org/vkdt

1. What you can enter into the search field to find all persons in the table?
2. What can you enter to find out, if the current database contains a non-empty table *gehaelter*?
3. Answer the following:
    a. Which mistakes are exploited during SQL-Injection attacks?
    b. Which possibilities to inject SQL queries do you know?
    c. Which defense mechanisms against SQL injection exist?

SQL-Injection Protection:

- Filter or mask special chars
- Check input values for properties
- Black-/Whitelisting of parameters
- Seperation of Data and SQL-Queries
- Fine Distinction of user rights
- Disable unused DB functionalites
- Apply Web Application Firewalls

Web Application Firewall



A potentially dangerous Request.Form value was detected from the client (_ctl1="<script"). - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://localhost/code/ASP.NET1.1/RequestValidation.aspx
Go Links
Done
Local intranet

Server Error in '/Code' Application.

A potentially dangerous Request.Form value was detected from the client (_ctl1="<script").

Description: Request Validation has detected a potentially dangerous client input value, and processing of the request has been aborted. This value may indicate an attempt to compromise the security of your application, such as a cross-site scripting attack. You can disable request validation by setting validateRequest=false in the Page directive or in the configuration section. However, it is strongly recommended that your application explicitly check all inputs in this case.

Exception Details: System.Web.HttpRequestValidationException: A potentially dangerous Request.Form value was detected from the client (_ctl1="<script").

Source Error:

```
An unhandled exception was generated during the execution of the current web request. Information regarding the origin and
location of the exception can be identified using the exception stack trace below.
```

Stack Trace:

```
[HttpRequestValidationException (0x80004005): A potentially dangerous Request.Form value was detected from the client (_ctl1="<script").]
   System.Web.HttpRequest.ValidateString(String s, String valueName, String collectionName)
   System.Web.HttpRequest.ValidateNameValueCollection(NameValueCollection nvc, String collectionName)
   System.Web.HttpRequest.get_Form()
   System.Web.UI.Page.GetCollectionBasedOnMethod()
   System.Web.UI.Page.DeterminePostBackMode()
   System.Web.UI.Adapters.PageAdapter.DeterminePostBackMode()
   System.Web.UI.Page.ProcessRequestMain()
   System.Web.UI.Page.ProcessRequest()
   System.Web.UI.Page.ProcessRequest(HttpContext context)
   System.Web.CallHandlerExecutionStep.System.Web.HttpApplication+IExecutionStep.Execute()
   System.Web.HttpApplication.ExecuteStep(IExecutionStep step, Boolean& completedSynchronously)
```

4

Task 4

At https://mytuc.org/yngk one can find a form to request user data.

One valid pair of username and password is user1 and pass1.

Find out, which further users exist in the table.

Your feedback on today‘s session:

mytuc.org/tgxs

Questions?

valentin.siegert@informatik.tu-chemnitz.de

VSR.*Informatik*.TU-Chemnitz.*de*