Voulnerability:

|  |  |
| --- | --- |
| Nr | 1 |
| Name oft he attack | SQLi – my offers |
| Exploitation | Override httpsession variable shopUserID  <script type="text/javascript">  function SetUserName()  {  var userId = "1 or 1=1";  '<%Session["UserName"] = "' + userId + '"; %>';  alert('<%=Session["shopUserID"] %>');  }  </script> |
| Opportunities for the attacker | Get baskets of other users or all by passing userID = «1 or 1=1» |
| Software error | The userID is passed as plain text to the query in class DBAccessSeller::getOwnProducts |
|  |  |

|  |  |
| --- | --- |
| Nr | 2 |
| Name oft he attack | SQLi – account edit |
| Exploitation | Override httpsession variable shopUserID  <script type="text/javascript">  function SetUserName()  {  var userId = "1 or 1=1";  '<%Session["UserName"] = "' + userId + '"; %>';  alert('<%=Session["shopUserID"] %>');  }  </script> |
| Opportunities for the attacker | Get other clients secret information |
| Software error | The id is passed as plain text to the query in class DBAccessAdmin::getClient  By passing 1 or 1=1 get all information from clients |
|  |  |

|  |  |
| --- | --- |
| Nr | 3 |
| Name oft he attack | SQLi – edit seller |
| Exploitation | Send Id such that other dml is executed for instance: delete any other record on table:  Id = 1; delete from purchase; |
| Opportunities for the attacker | Do any other manipulation on the db as you want with the passed parameter. Just end the delete statement and introduce another one |
| Software error | The id is passed as plain text to the query in class DBAccessAdmin::deleteSeller  By passing 1 or 1=1 get all information from clients or other mutations:  Id = 1; delete from purchase; |
|  |  |

|  |  |
| --- | --- |
| Nr | 4 |
| Name oft he attack | SQLi – add seller |
| Exploitation | The name can be given that way, such that the insert into statement gets finish vaild and then add another insert command and escape the rest oft he query with – at the end.  Any table updates or inserts are possible here |
| Opportunities for the attacker | Update data without having privileges (autorisation field) |
| Software error | The id is passed as plain text to the query in class DBAccessAdmin::addSeller  By passing name = «test','pw',7 ) – » |
|  |  |

|  |  |
| --- | --- |
| Nr | 5 |
| Name oft he attack | SQLi – add Offer |
| Exploitation | The name i staken plain out oft he request and only checked against not empty. Therefore we can edit the sql since ist used straight forward in the insert statement. |
| Opportunities for the attacker | Edit price as you want |
| Software error | DBAccessSeller is using name as plaintext in sql: passing following value as name parameter leads to price of 0  Name= name', 'anyText', 0, 100); -- |
|  |  |

|  |  |
| --- | --- |
| Nr | 6 |
| Name oft he attack | SQLi – delete Offer |
| Exploitation | The id is used as condition fort he record delete operation. By passing other ids we can simply delete other offers. As well as all at once |
| Opportunities for the attacker | Delete any offer in database / product |
| Software error | DBAccessSeller::deleteOffer is using id as plaintext in sql: passing following value as id parameter leads to deletion of any records  id= 1 or 1=1 |
|  |  |