

[Добавить материал](#)

Информационная безопасность

[Новости](#) [Мероприятия](#) [Статьи](#) [Отчеты](#) [Сравнения](#) [Интервью](#) [Видео](#)

[Эксперты](#) [Документы](#) [Еще](#)



# Уязвимость CSRF | Руководство для начинающих специалистов

Дата: 30.09.2020. Автор: Игорь Б . Категории:

[Статьи по информационной безопасности](#)



**В данной статье пойдет речь об основных понятиях, связанных с CSRF-атаками. Читатели также узнают о том, как злоумышленник способен заставить пользователей выполнить вредоносные действия, которые не входили в их планы.**

## Что такое файлы cookie и Session ID?



Прежде чем перейти к атакам CSRF и тому, как они выполняются, нужно узнать немного из терминологии, связанной с обеспечением

безопасности приложений.

## Cookies

**Cookies** — это небольшие текстовые файлы (с максимальным размером до 4 КБ). Они хранятся в браузере клиента в виде пары имя-значение. Файлы cookie в основном используются для отслеживания или мониторинга активности клиента в веб-приложении и хранят в себе конфиденциальные данные, такие как **имя пользователя, идентификатор сеанса, пароль**. Таким образом, они могут быть отправлены обратно на сервер для получения аутентификации.

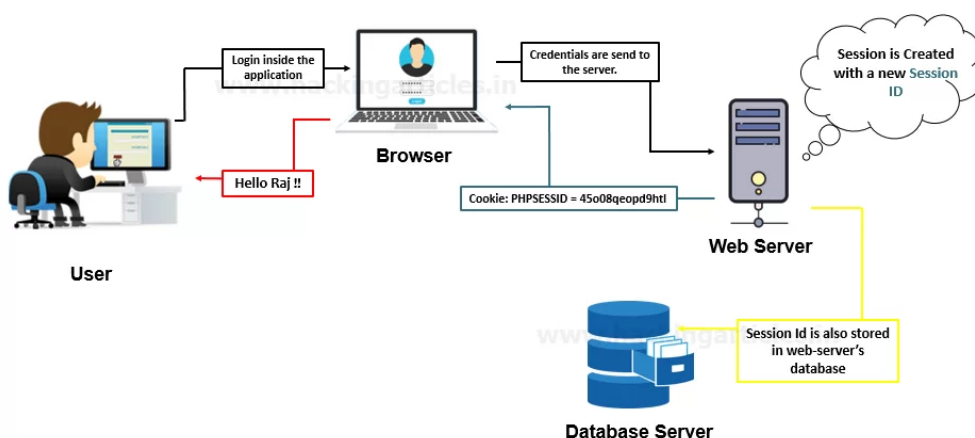
## Session ID

Как и файлы cookie, сеансы — это тоже небольшие файлы, однако они генерируются и хранятся на конце сервера. Каждый сеанс связан с идентификатором сеанса (**Session ID**). Всякий раз, когда пользователь входит в систему, сеанс получает свой идентификатор. Этот идентификатор сеанса сливается с файлом cookie и хранится в браузере клиента. Таким образом, он передается обратно на веб-сервер всякий раз, когда браузер отправляет HTTP-запрос.

Когда клиент выходит из системы или закрывает браузер, эти сеансы прекращаются. С каждым новым входом генерируется еще один сеанс с идентификатором.

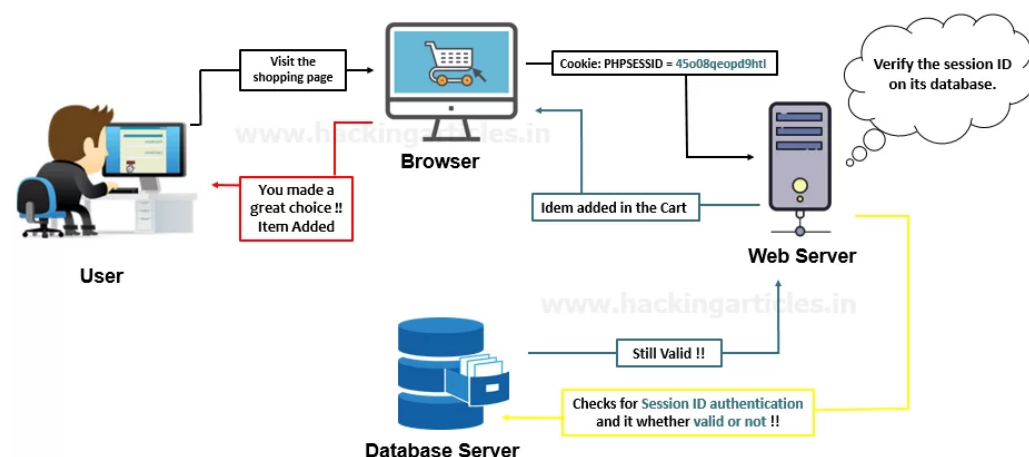
Стоит понять это на примере следующего сценария развития событий:

Когда новый пользователь создает свою учетную запись через веб-приложение, происходит следующее:



Пользователь открывает какой-то раздел того же приложения, и

идентификатор сеанса, хранящийся в его браузере, отправляется на сервер для проверки.



## Что такое SOP?

**SOP** — это аббревиатура **Same-Origin Policy**, что является одним из наиболее важных понятий в модели безопасности веб-приложений. В соответствии с этой политикой веб-браузер разрешает скриптам, находящимся на первой веб-странице, получить доступ к данным на второй веб-странице. Это происходит только в том случае, если обе веб-страницы работают на одном и том же порту, имеют одинаковый протокол и источник.

К примеру:

Веб-страница «<https://www.ignitetechnologies.com/ceh/module1.pdf>» может получить прямой доступ к контенту по адресу:

«<https://www.ignitetechnologies.com/network/RDP/module7.docx>». Но она не способна получить доступ к данным из следующего источника:

«<https://www.ignitetechnologies.com:8080/bug/xss.pdf>», поскольку порт был изменен.

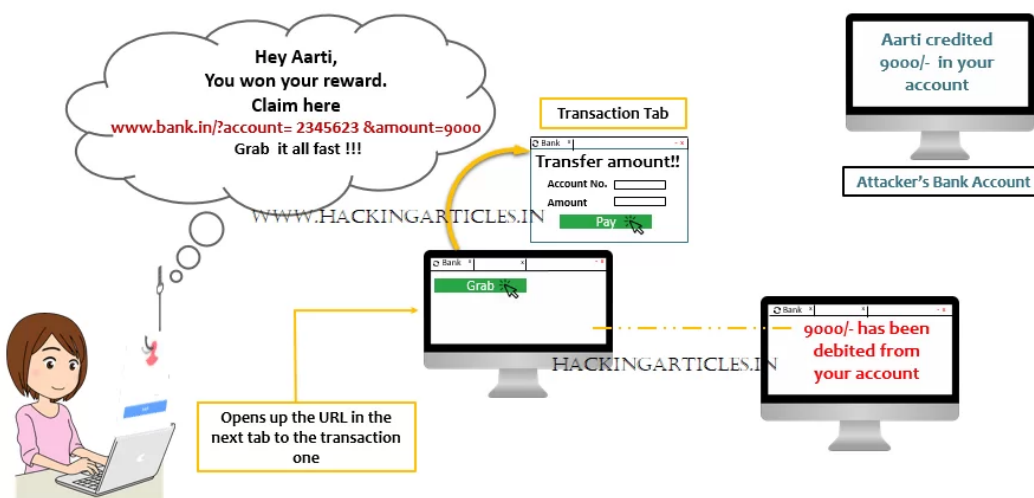
## Знакомство с CSRF-атаками

**CSRF** — это аббревиатура **Cross-Site Request Forgery**, также еще известная как **Client-Site Request Forgery**. Некоторые называют ее еще атакой в один клик. Злоумышленник заставляет пользователя выполнить вредоносные действия в веб-приложении, в котором он в данный момент аутентифицируется.

Чтобы лучше понять саму схему, необходимо взглянуть на следующий сценарий развития событий:

Пользователь «**Aarti**» получает письмо от злоумышленника, после того как он сделал банковский перевод на счет Raj Chandel. Пользователь оставил транзакцию незавершенной и проверяет свою почту на новой вкладке.

Там он увидел общий URL-адрес с содержанием, в котором говорилось, что «была получена определенная сумма в качестве вознаграждения». Теперь, когда пользователь открывает данный URL в новой вкладке, там его ждет форма захвата. Страница транзакции осталась на первой вкладке, а эта вредоносная – открыта на второй. Как только пользователь нажимает на кнопку «**Submit**», выполняется запрос. Указанная сумма будет списана со счета «**Aarti**» без его ведома.



## Влияние уязвимости CSRF на пользователя

CSRF — это атака, которая заставляет жертву выполнить вредоносный запрос на сервере от имени атакующего. Хотя CSRF-атаки не предназначены для кражи каких-либо конфиденциальных данных, поскольку злоумышленник не получает никакого ответа, они отличаются тем, что осуществляют изменения на сервере. К примеру:

- изменение адреса электронной почты или пароля жертвы;
- покупка продуктов;
- осуществление банковской операции;
- выход пользователя из своей учетной записи.

Таким образом, эта уязвимость была включена в **топ-10 OWASP** в 2013 году. Сейчас она обладает оценкой CVSS «**6,8**» и «**средней степенью тяжести**».



- **CWE-352:** Cross-Site Request Forgery (CSRF)

## Применение CSRF

Для этого раздела автор использовал уязвимое веб-приложение **bwAPP** и создал учетную запись с данными **Raj : ignite** для входа на веб-сервер.



**New User**  
www.hackingarticles.in  
Create a new user.

Login:  E-mail:

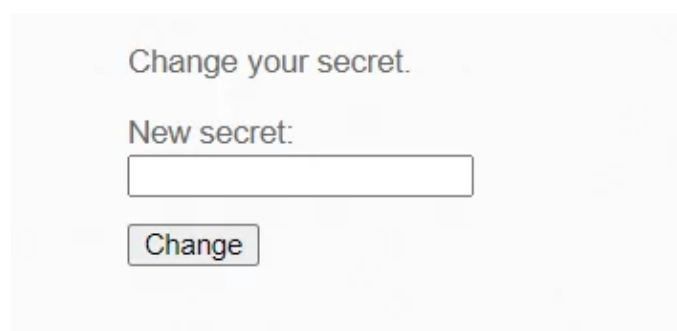
Password:  Re-type password:

Secret:

E-mail activation: ☐

## Манипулирование данными учетной записи пользователя

На приведенном выше изображении можно увидеть, что для создания нового пользователя юзер **«Raj»** установил секретное значение **«who are you»**. Его он может изменить, используя подсказки ниже:



Change your secret.

New secret:

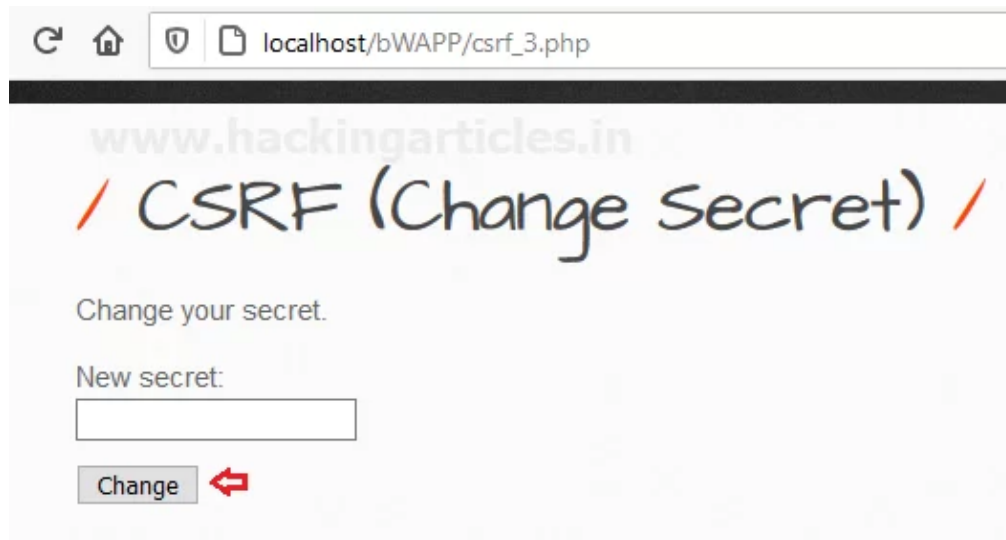
Но что, если секретное значение поменяется на нужное значение для атакующего без ведома пользователя.

Стоит понять, как это проверить.

Настала пора открыть целевой IP-адрес в своем браузере и воспользоваться опцией **«Choose Your Bug»** для **«Cross-Site-Request-Forgery (Change Secret)»**.

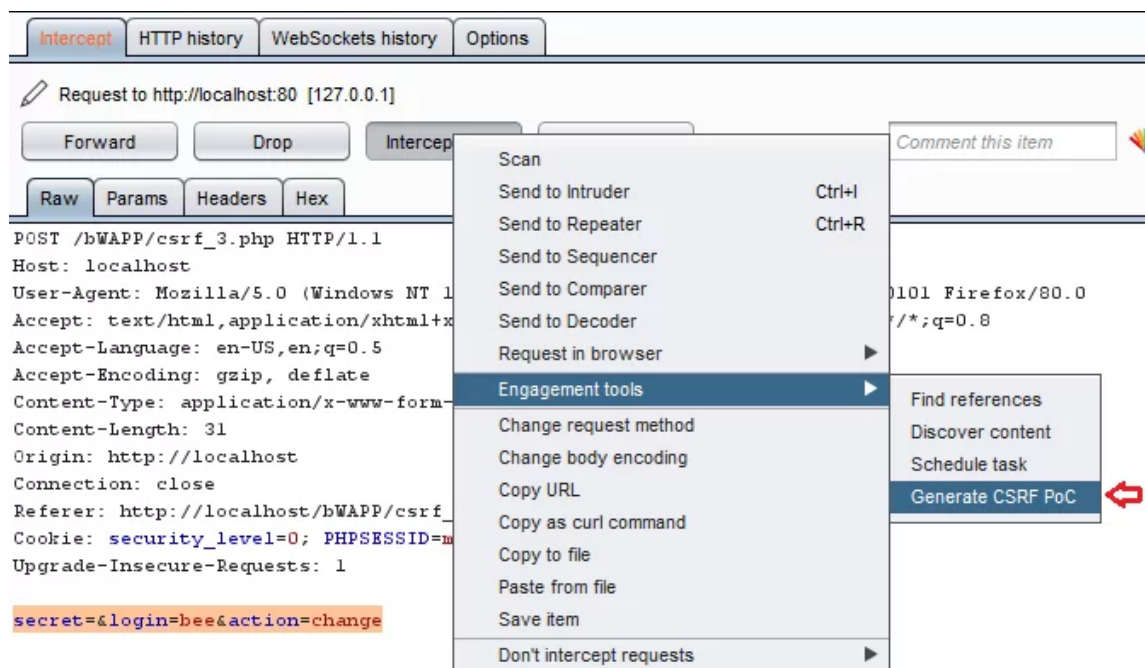


Здесь пользователь будет перенаправлен на веб-страницу, которая уязвима для CSRF атаки. Читатели могут увидеть, что **есть возможность изменить секретное значение**.



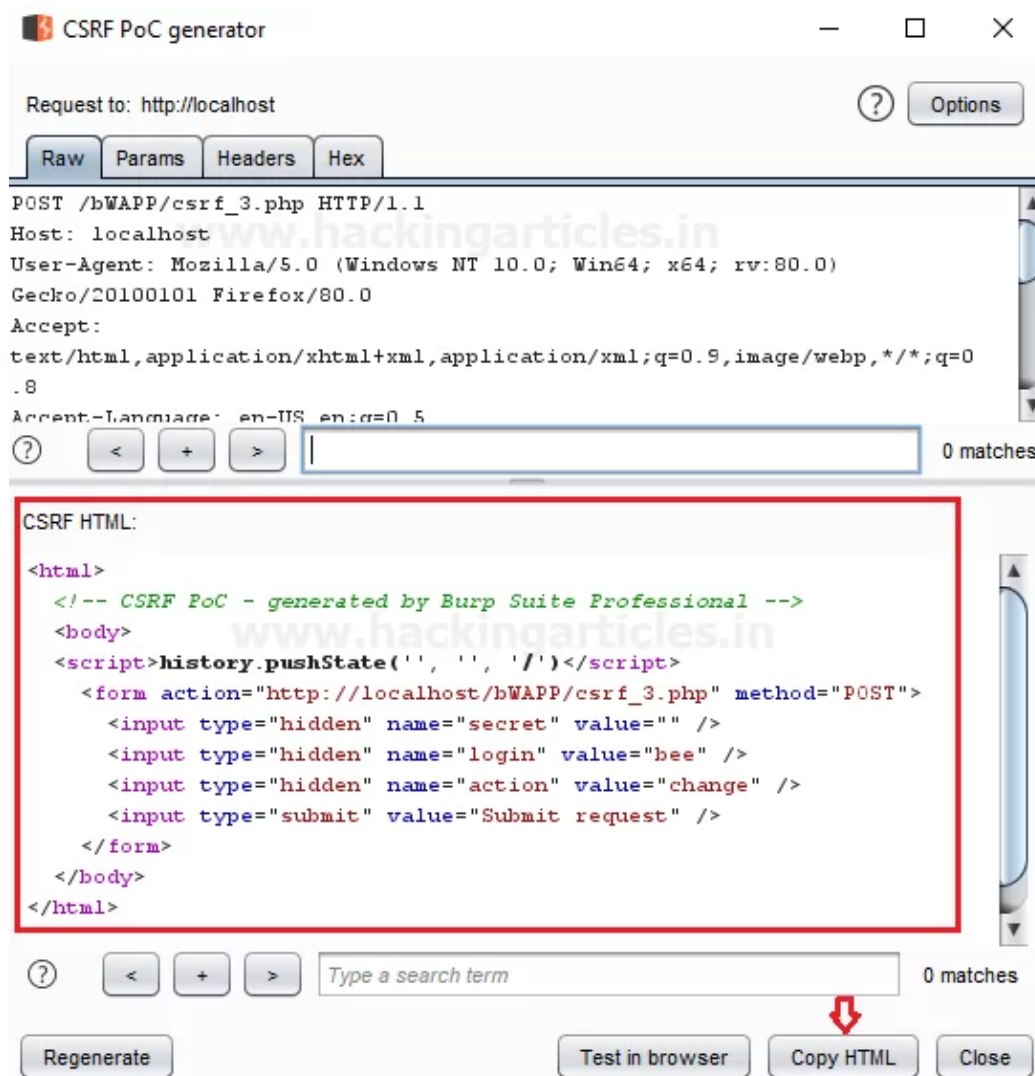
Теперь стоит нажать на кнопку **«Change»** и захватить этот HTTP-запрос.

На приведенном ниже изображении можно увидеть, что пользователь успешно захватил запрос. Настала пора создать поддельную HTML-форму, для этого следует щелкнуть правой кнопкой мыши в любом месте экрана и выбрать инструменты взаимодействия, а затем нажать на кнопку **«Generate CSRF PoC»**.



CSRF PoC автоматически генерирует страницу HTML-формы. Теперь нужно нажать на кнопку **«Copy HTML»**, чтобы скопировать весь HTML-код и позже отправить эти данные в текстовый файл.



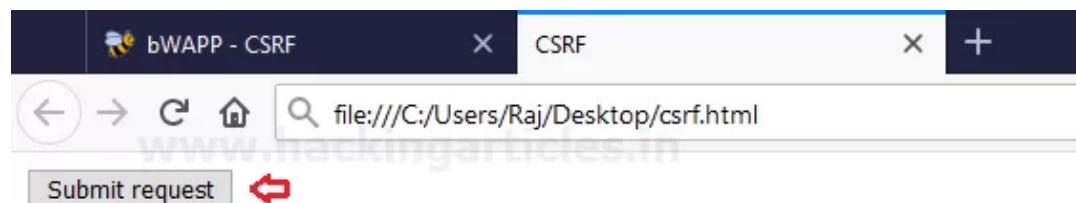


**Отлично!!** Стоит поманипулировать параметром **secret value=""** с помощью «**hackingarticles**», а затем сохранить этот файл как «**csrf.html**». Кроме того, нужно указать имя пользователя «**Raj**», для которого и будет изменено секретное значение.

```
<html>
<!-- CSRF PoC - generated by Burp Suite Professional -->
<body>
<script>history.pushState('', '', '/')</script>
<form action="http://192.168.0.10/bWAPP/csrf_3.php" method="POST">
  <input type="hidden" name="secret" value="hackingarticles" />
  <input type="hidden" name="login" value="Raj" />
  <input type="hidden" name="action" value="change" />
  <input type="submit" value="Submit request" />
</form>
</body>
</html>
```

Теперь пользователь прибегнет к социальной инженерии, чтобы поделиться этим файлом (csrf.html) с жертвой.

Как только жертва откроет csrf.html, там она увидит кнопку «**Submit**». Когда жертва нажмет на нее, ее секрет будет изменен.



На приведенном ниже изображении можно увидеть, что пользователь получил сообщение: «**Секрет был изменен**». Кроме того, успешная CSRF-атака способна изменить адрес электронной почты, имя пользователя и личную информацию юзера.



## CSRF: смена пароля

Возможность изменения пароля присутствует практически в каждом веб-приложении, но во многих случаях эти приложения не обеспечивают ее безопасности. Стоит попробовать использовать эту функцию вместе с уязвимостью CSRF, чтобы изменить пароль пользователя без его ведома.

Человек вернется в раздел «**Choose Your Bug**», выберет «**Cross-Site-Request-Forgery (Change Password)**» и нажмет на кнопку «**Hack**».



# / CSRF (Change Password) /

Change your password.

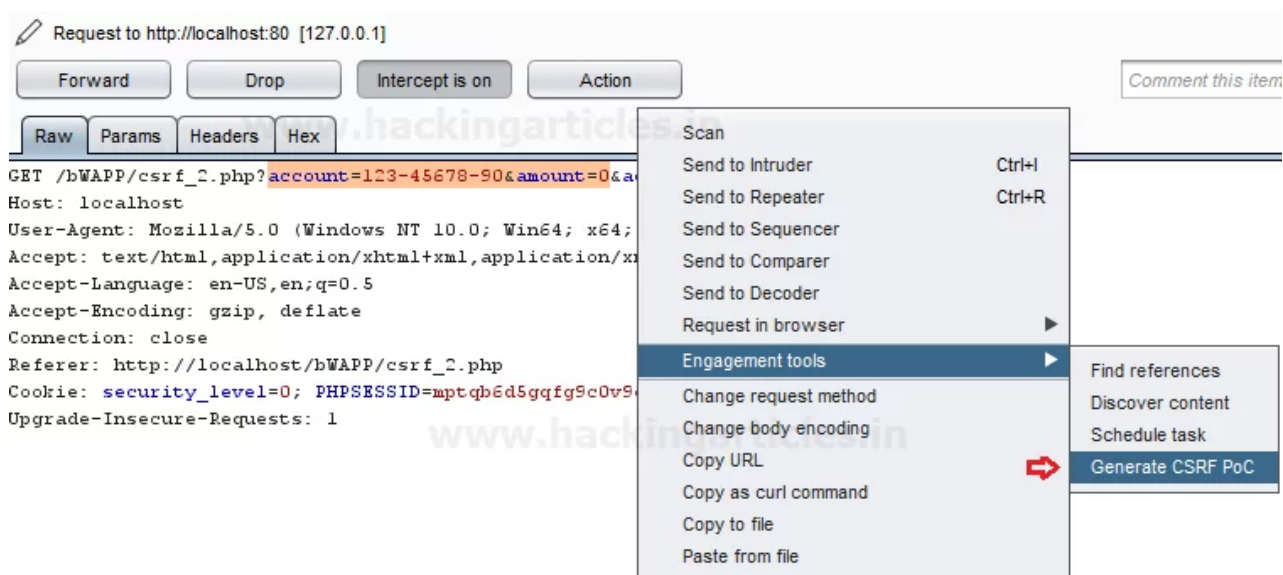
New password:

Re-type new password:

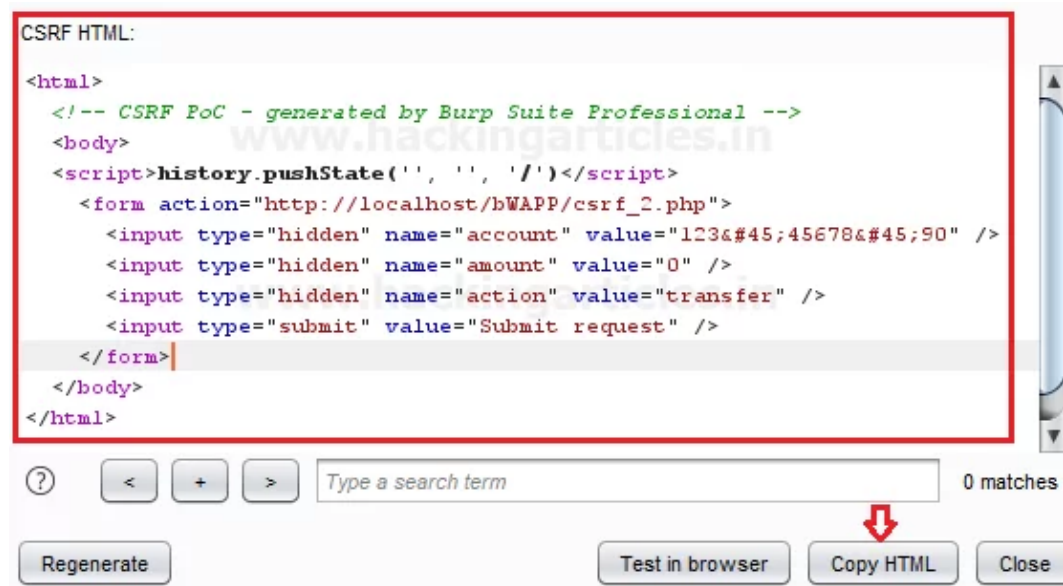
**Change** ↩

Теперь надо снова нажать на кнопку «**Change**» и захватить HTTP-запрос в **Burpsuite**.

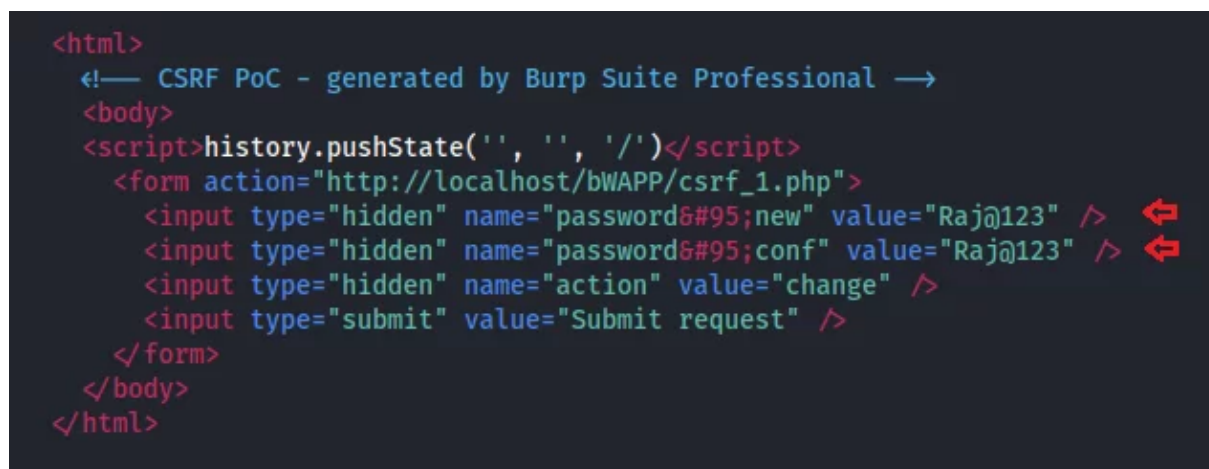
На приведенном ниже изображении можно увидеть, что пользователь успешно захватил запрос. Надо осуществить ту же процедуру для создания поддельной HTML-формы.



Теперь пользователь нажмет на кнопку «**Copy HTML**», чтобы скопировать весь HTML-код и позже отправить эти данные в текстовый файл.

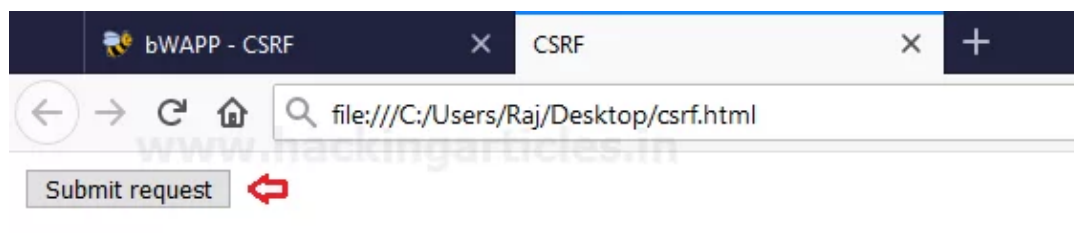


После того как пользователь вставил HTML-код в файл, нужно добавить новое значение пароля (пароль злоумышленника) и значение подтверждения пароля, а затем сохранить этот текстовый документ как **csrf.html**.



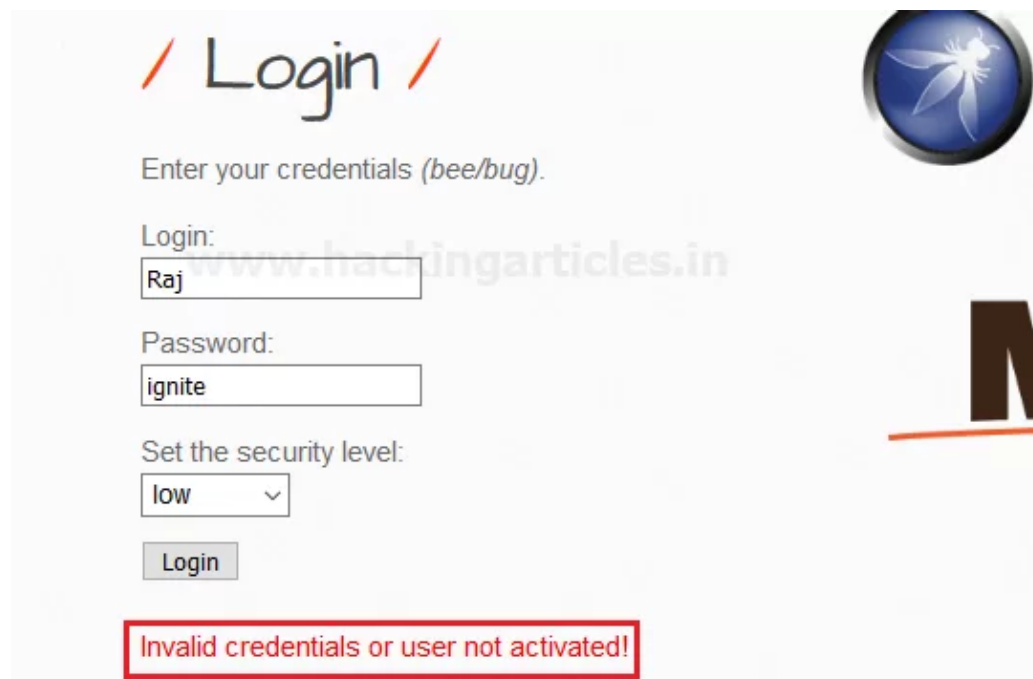
Теперь пользователь снова будет использовать социальную инженерию, чтобы поделиться файлом csrf.html с жертвой.

Как только жертва откроет csrf.html, там она увидит кнопку «**Submit**». Когда жертва нажмет на нее, ее пароль будет изменен.



На приведенном ниже изображении можно увидеть, что с помощью CSRF-атаки был изменен пароль, установленный пользователем «Raj».

**Отлично!!** Теперь, когда жертва попытается войти в систему со старым паролем, она получит сообщение об ошибке.



**Login**

Enter your credentials (bee/bug).

Login:

Password:

Set the security level:

**Invalid credentials or user not activated!**

## CSRF: банковский перевод

Возможно, читатели слышали о некоторых случаях, когда деньги списывались с банковского счета жертвы без ее ведома. Интересно, как CSRF связан с этим? Стоит взглянуть на следующий сценарий атаки.

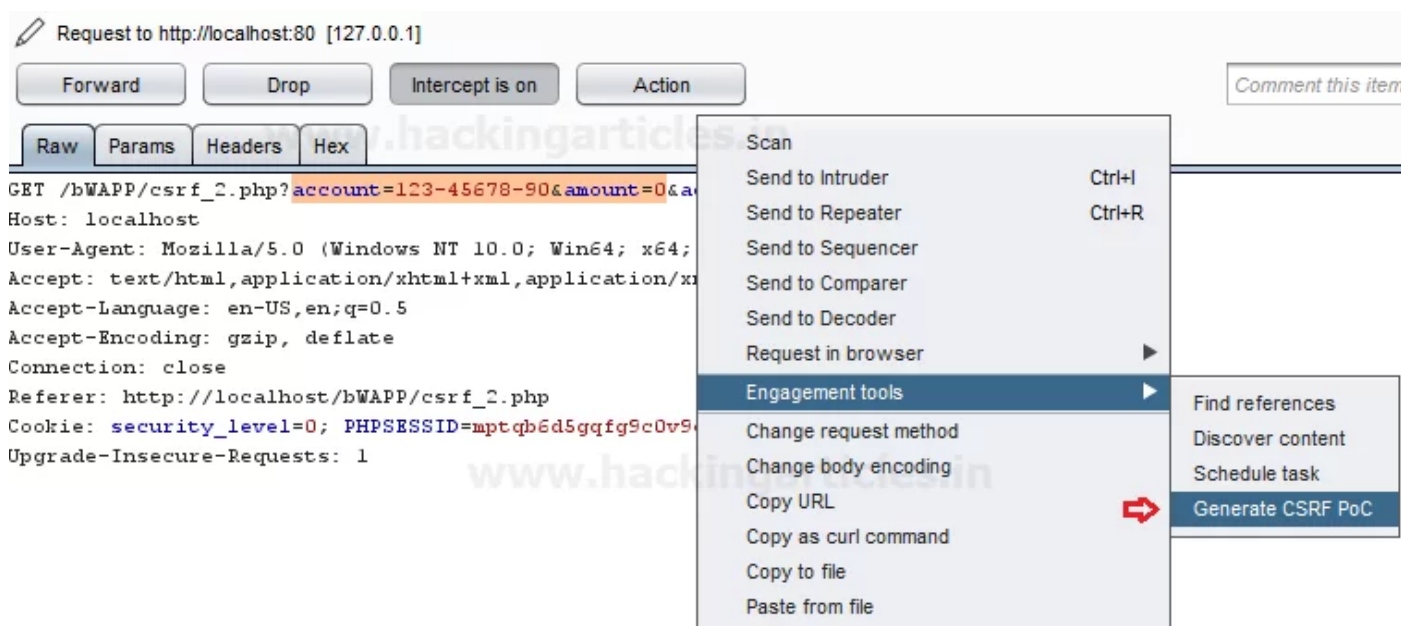
Нужно войти в систему **bWAPP**, затем выбрать уязвимость «**Cross-Site Request Forgery (Transfer Amount)**» и нажать на кнопку «**Hack**».

На приведенном ниже скриншоте можно увидеть, что у пользователя «Raj» €1000 на его счете.

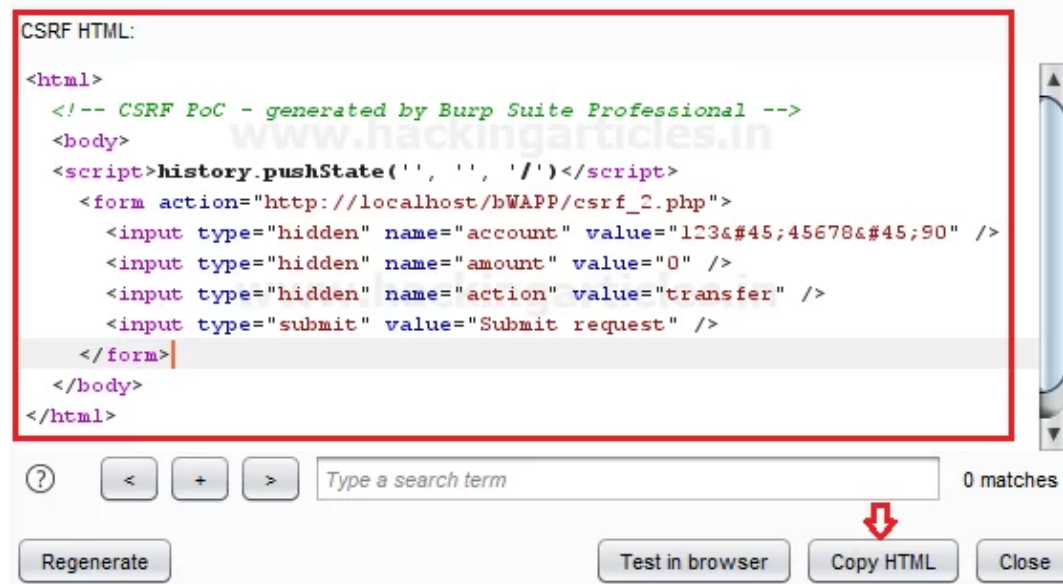


Стоит попробовать перевести какую-то сумму, так как номер счета уже есть в файле.

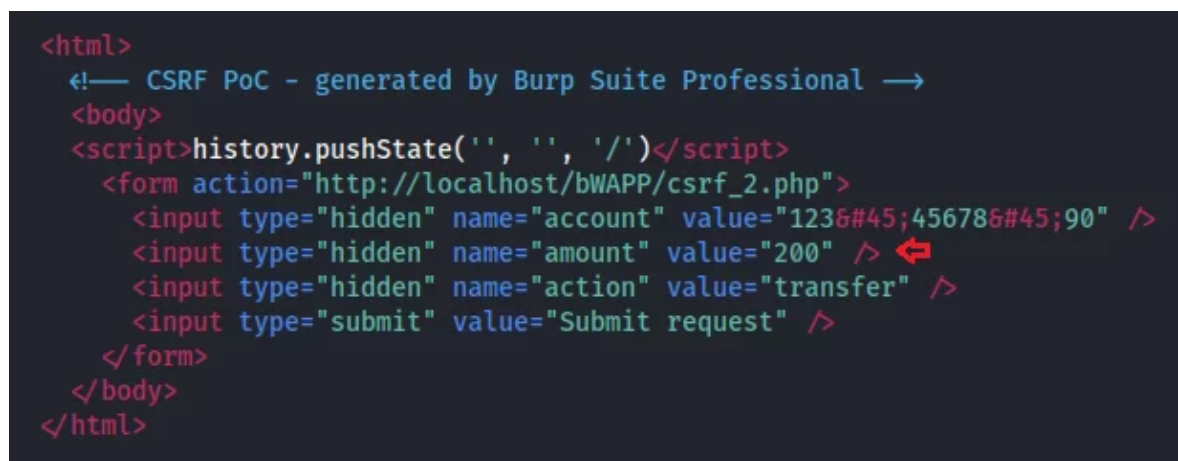
Процедура атаки CSRF аналогична описанной выше: нужно использовать **burp suite** для захвата отправленного запроса, а затем поделиться им в разделе «**Engagement tools**».



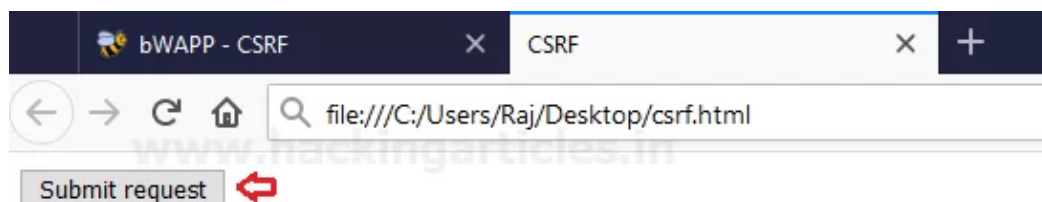
Будет автоматически создана HTML-форма для перехваченных данных. Нужно просто нажать на кнопку «**Copy HTML**» и вставить эти данные в текстовый файл.



**Отлично!!** Настало время манипулировать **value** field и добавить сумму "200" (желаемая сумма), которую нужно перевести. После этого следует сохранить текстовый документ как **csrf.html** и поделиться им с жертвой.



Как только жертва откроет этот файл и нажмет кнопку «**Submit**», сумма (введенная злоумышленником) будет переведена.



На приведенном скриншоте видно, что на счету пользователя осталось €800, а это значит, что с его счета было списано €200.



CSRF (Transfer Amount)

www.hackingarticles.in

Amount on your account: 800 EUR

Account to transfer:  
123-45678-90

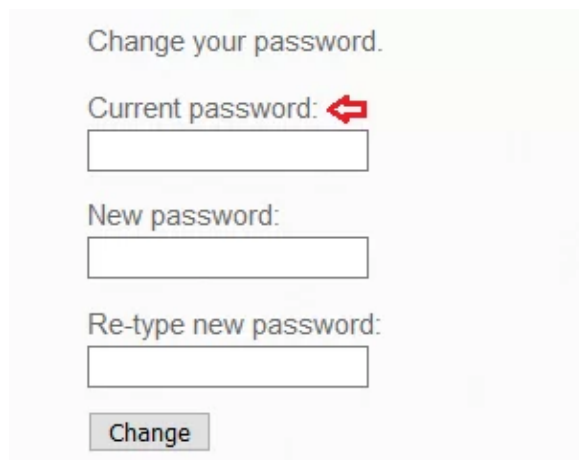
Amount to transfer:  
0

Transfer


Таким образом, с помощью таких базовых методов злоумышленник может внести серьезные изменения в данные учетной записи жертвы.

## Недостатки CSRF

- Атака будет успешной только тогда, когда злоумышленник знает, какой параметр и какие значения «перемешиваются» в HTML-форме;
- Даже такая атака нуждается в социальной инженерии, поскольку иногда HTML-формы требуют ранее использованных значений в качестве «**текущего пароля**», чтобы изменить его.



Change your password.

Current password: 

New password:

Re-type new password:

Change

## Митигирование

- Использование **токенов Anti—CSRF**;
- Использование атрибутов файлов cookie одного сайта для сеансовых файлов, которые могут быть отправлены только в том случае, если запрос сделан из источника, связанного с этим файлом;
- Не использовать GET-запросы для изменения операций;
- Идентификация источника должна осуществляться через заголовок Origin/Referer;
- Одноразовый токен должен быть реализован для защиты CSRF на основе взаимодействия с пользователем;
- Защита от атак XSS, так как любая из них может быть использована для усиления CSRF.






Автор [переведенной статьи](#): Chiragh Arora.

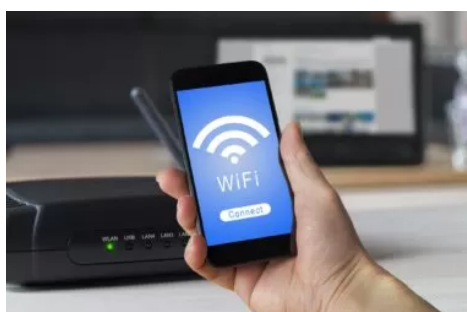
**Важно!** Информация исключительно в учебных целях. Пожалуйста, соблюдайте законодательство и не применяйте данную информацию в незаконных целях.



 Группа компаний Angara и CyberPeak объединили усилия для защиты неструктурированных данных

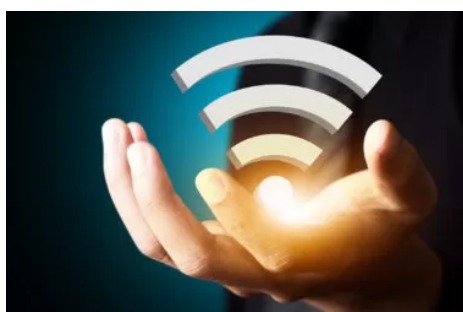
День антивируса Dr.Web в Челябинске

## Похожие записи



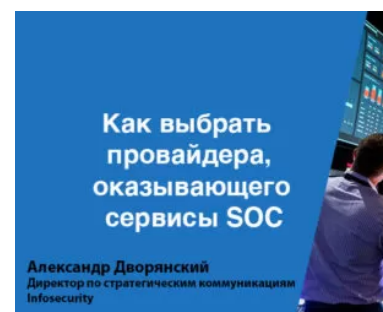
**Взлом паролей  
беспроводных сетей:  
Airgeddon**

03.08.2021



**Взлом паролей  
беспроводных сетей**

29.07.2021



**Как выбрать  
провайдера,  
оказывающего серви  
SOC**

22.07.2021



### Об авторе Игорь Б

Автор на портале cisoclub.ru. Добавляйте ваш материал на сайт в разделе "Разместить публикацию".

[Читать все записи автора Игорь Б](#)



**Добавить комментарий**



Ваш адрес email не будет опубликован. Обязательные поля помечены \*

Комментарий

Имя \*

Email \*

☐ Сохранить моё имя, email и адрес сайта в этом браузере для последующих моих комментариев.

☒ Хочу подписаться на новости!

Отправить комментарий



Информационный портал и профессиональное сообщество специалистов по информационной безопасности.	Категории	Метки	Контакты
Тел.: +7 495 147 49 47  Информация  ИБ клуб	Главное	уязвимости	Нашли ошибку?
	Новости	Microsoft Corp.	Пожалуйста, напишите нам.
	Мероприятия	информационная безопасность	Если вы хотите разместить публикацию, перейдите на страницу <a href="#">Добавить материал</a> .
	Статьи	Red Hat Inc.	
	Отчеты	Oracle Corp.	
	Интервью	Novell Inc.	
	Видео	Adobe Systems Inc.	
	Сравнения	Cisco Systems Inc.	
		Google Inc.      Windows	

Разрешается цитирование материалов на других сайтах при наличии ссылки на источник. Использование какого-либо материала допускается только по согласованию с редакцией портала. Мы не гарантируем точность, полноту и полезность любого материала. Мнение авторов материалов может не совпадать с позицией редакции портала. Пользователи и иные заинтересованные лица в случае выявления нарушения интеллектуальных прав и иных противоправных действий других пользователей, обязуются прежде всего сообщить редакции портала о подобных нарушениях по электронной почте [info@cisoclub.ru](mailto:info@cisoclub.ru) © cisoclub.ru, 2020-2021.

6+



Личный кабинет

Эксперты

АО «НПО РусБИТех»

Если вы хотите

Участники

Документы

The CentOS Project

**вступить в клуб,**  
пожалуйста,  
[зарегистрируйтесь](#)  
(вход [тут](#)).

Разместить  
публикацию

Вакансии

Canonical Ltd.

киберпреступность

Контакты

Уязвимости

information security

Партнеры

Рейтинг

Apple Inc. DEF

Если вы хотите  
воспользоваться

Реклама

Обучение

security conference

**платными услугами,**  
[напишите нам](#), указав  
компанию, которую вы  
представляете, а также  
продукт/услугу,  
которые вы хотите  
рекламировать.

О проекте

Бесплатно

Astra Linux CON

hacker conference

Прочее

DEFCON ubuntu

def con Android

хакеры Intel Corp.

hackers

Персональные данные

Mozilla Corp. Cisco

Gentoo Foundation Inc.

conference speakers

Red Hat Enterprise Linux

PR сервис от CISO CLU  
в Telegram:  
[t.me/cisoclub\\_pr](#).

