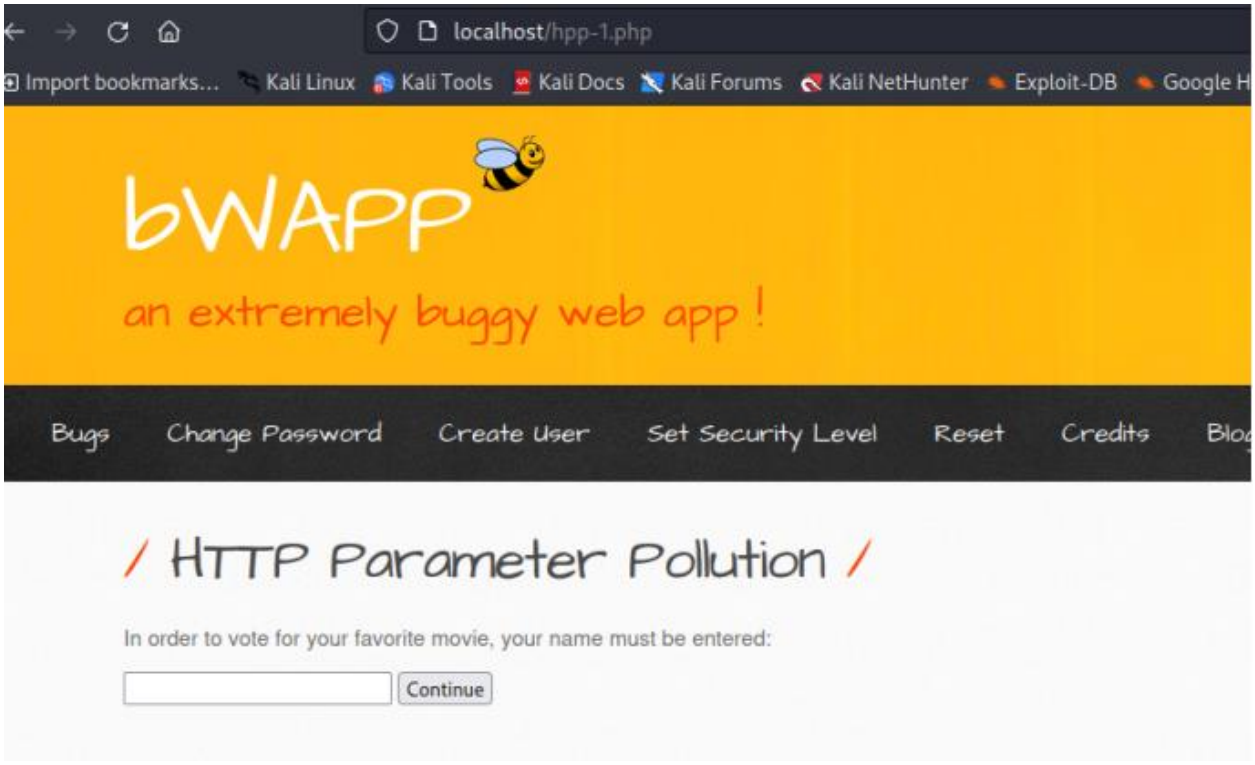
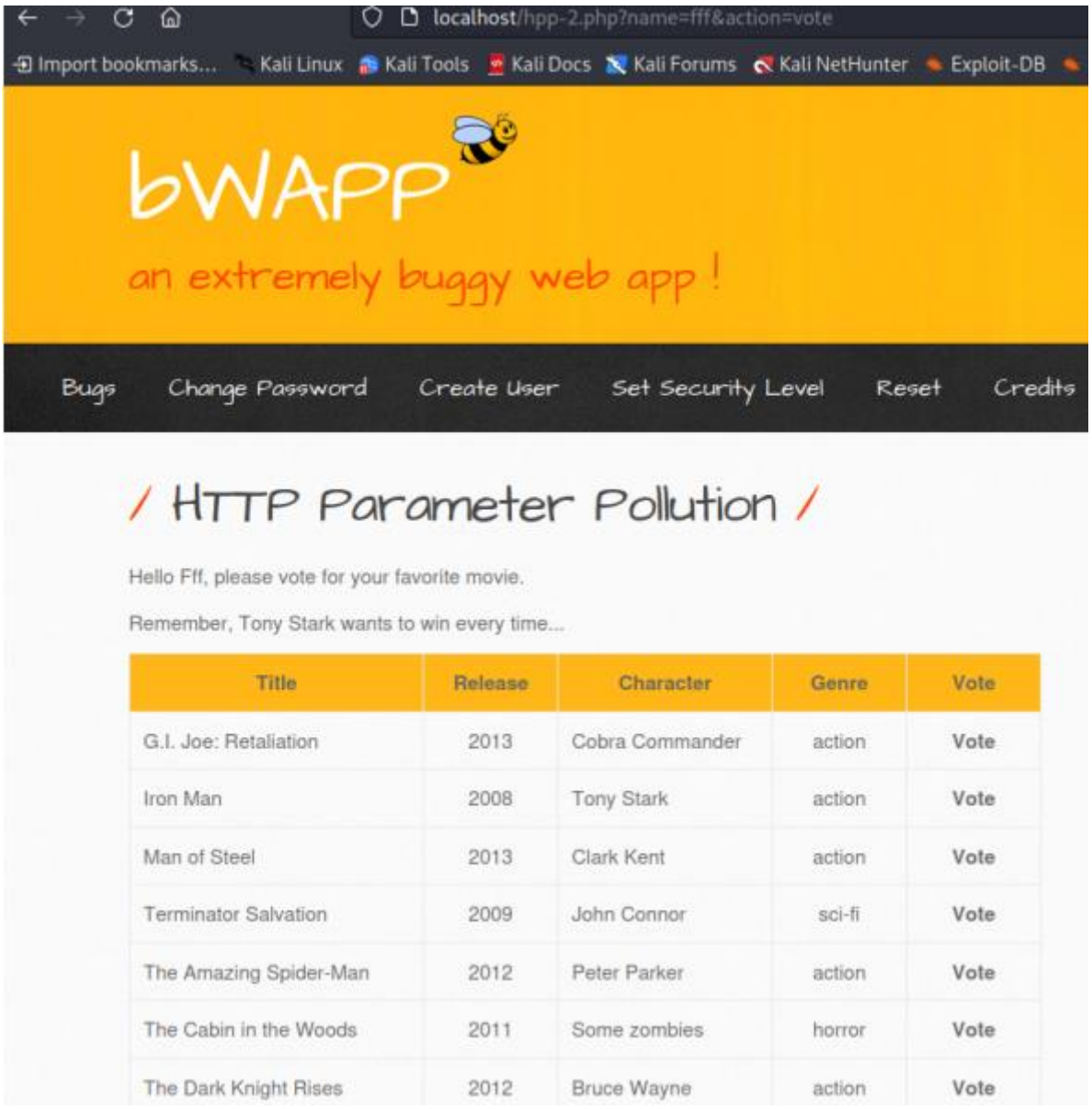
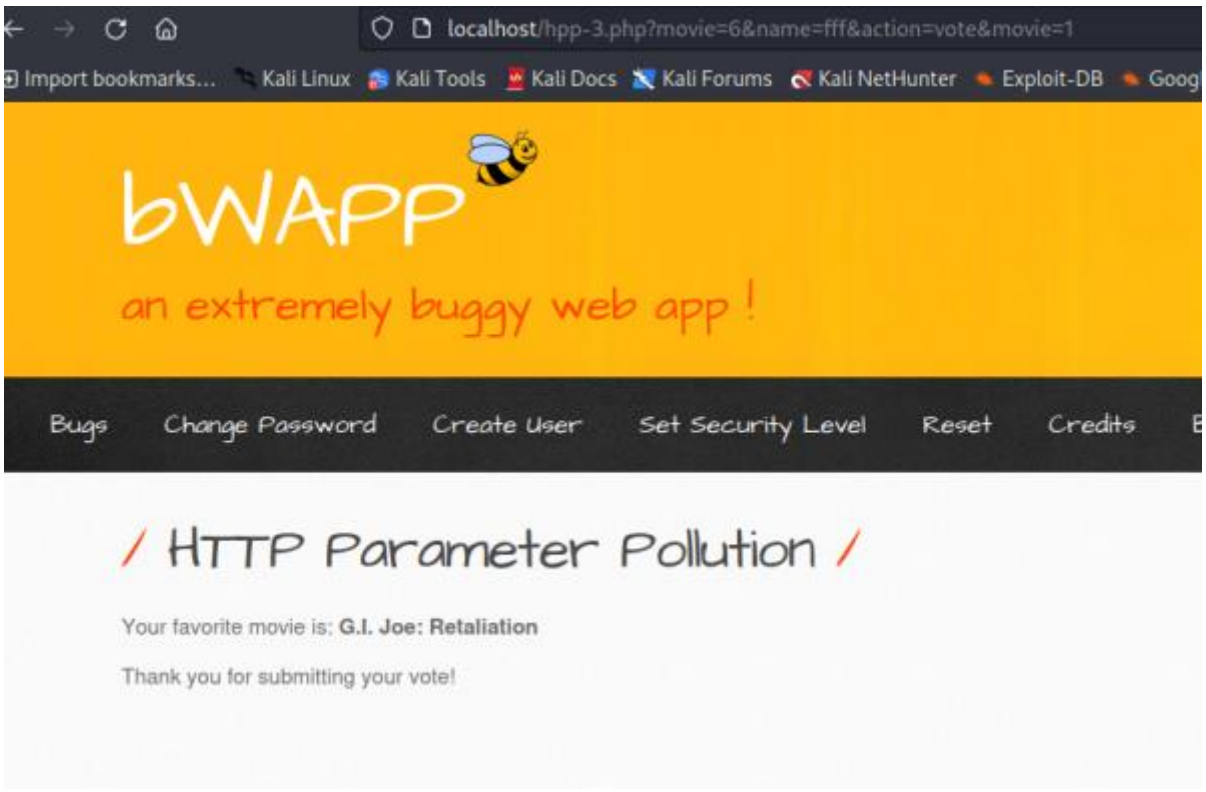
1.

HTTP Parameter Pollution – Расщепление запроса




localhost/hpp-2.php?name=fff&action=vote
Import bookmarks...
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
bWAPP
an extremely buggy web app !
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
/ HTTP Parameter Pollution /
Hello Fff, please vote for your favorite movie.
Remember, Tony Stark wants to win every time...
Title
Release
Character
Genre
Vote
G.I. Joe: Retaliation
2013
Cobra Commander
action
Vote
Iron Man
2008
Tony Stark
action
Vote
Man of Steel
2013
Clark Kent
action
Vote
Terminator Salvation
2009
John Connor
sci-fi
Vote
The Amazing Spider-Man
2012
Peter Parker
action
Vote
The Cabin in the Woods
2011
Some zombies
horror
Vote
The Dark Knight Rises
2012
Bruce Wayne
action
Vote


localhost/hpp-3.php?movie=6&name=fff&action=vote
Import bookmarks...
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
bWAPP
an extremely buggy web app !
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
/ HTTP Parameter Pollution /
Your favorite movie is: The Cabin in the Woods
Thank you for submitting your vote!



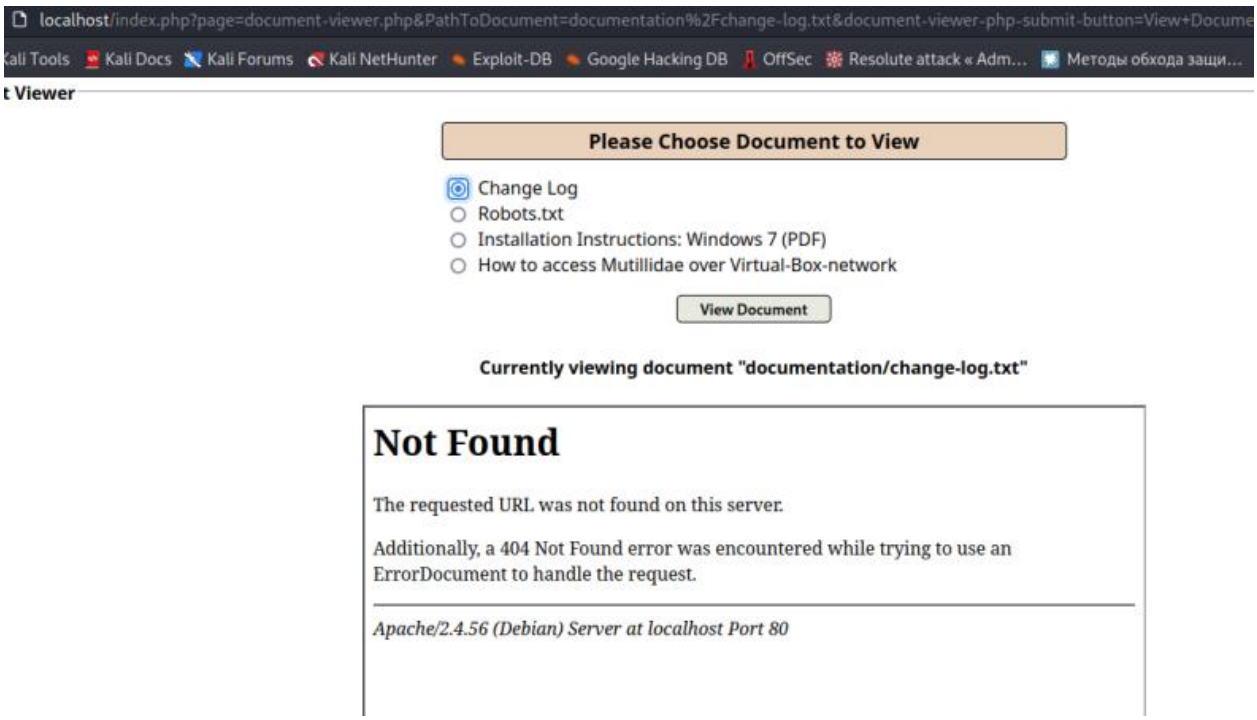

На данном ресурсе есть возможность подмены выбора за счёт того, что учитывается последнее значение параметра.

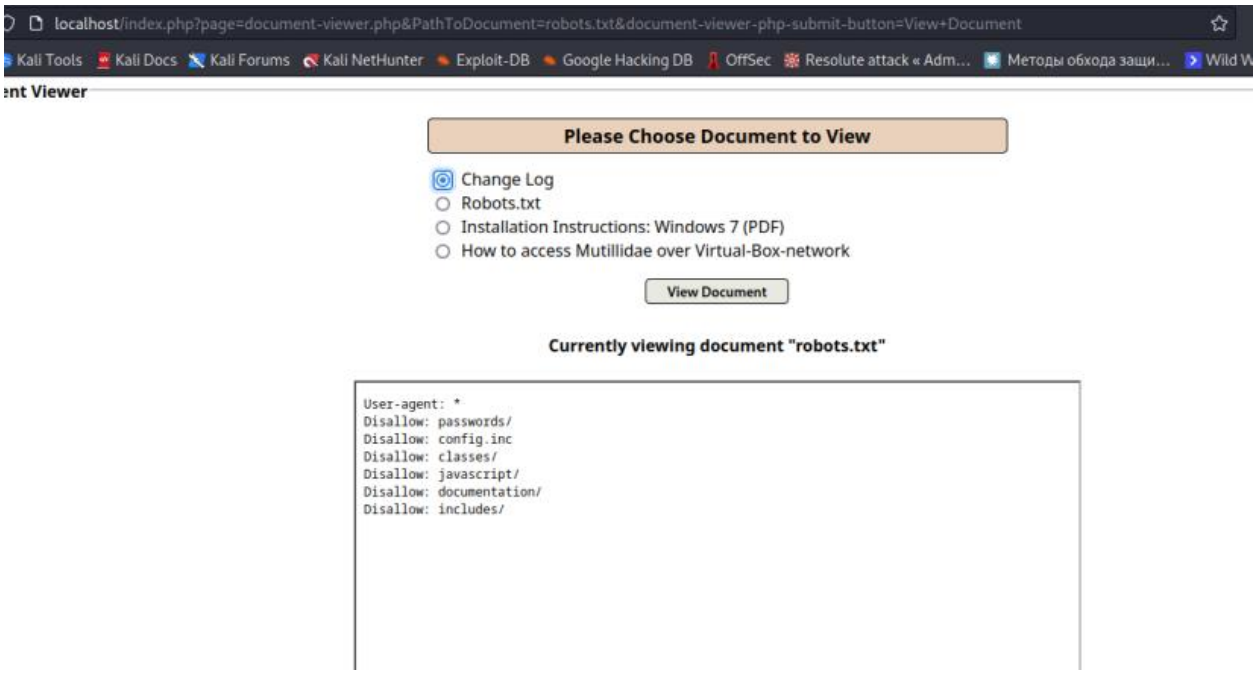
Может быть использовано для "подмены" результата в пользу конкретного варианта/

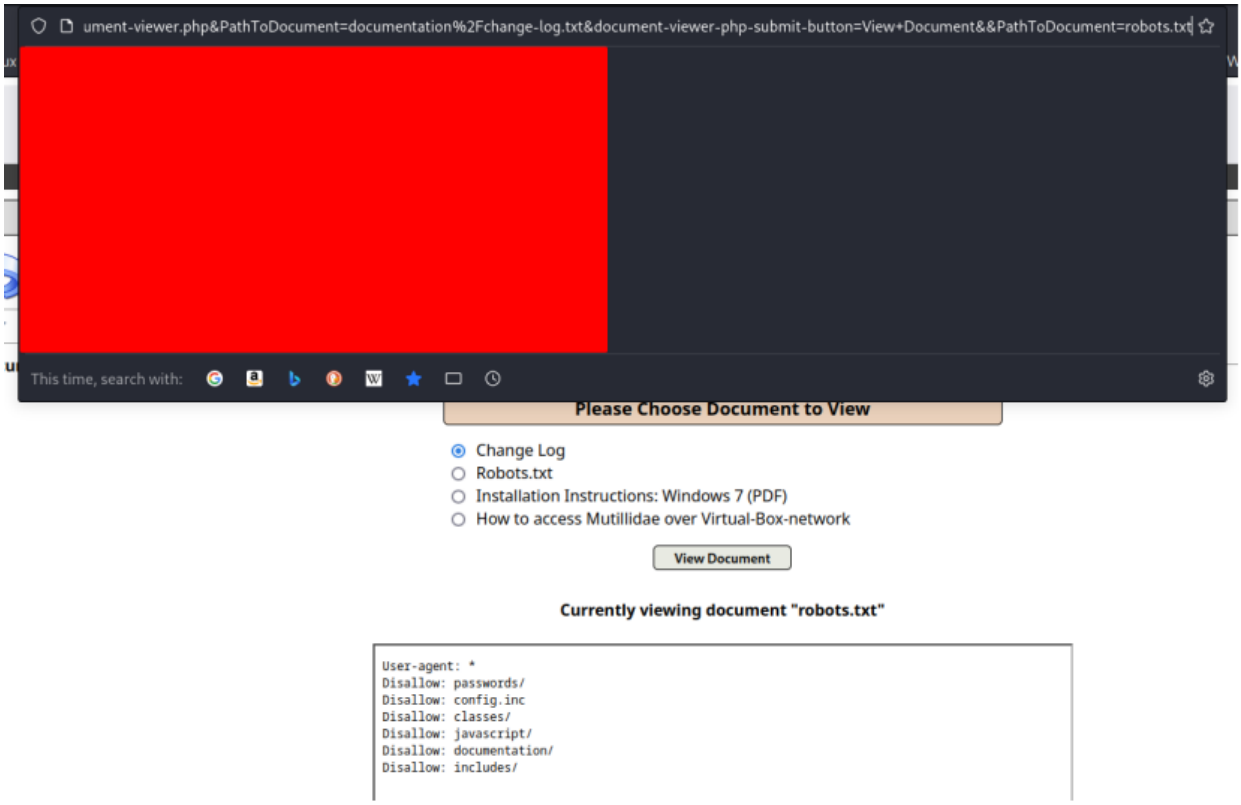
2.

Для начала был просмотрен код страницы

```
<legend>Document Viewer</legend>
<form   action="index.php"
        method="GET"
        enctype="application/x-www-form-urlencoded"
        id="idDocumentForm">
    <input type="hidden" name="page" value="document-viewer.php" />
    <table>
        <tr id="id-bad-path-to-document-tr" style="display: none;">
            <td class="error-message">
                Validation Error: HTTP Parameter Pollution Detected. Input cannot be trusted.
            </td>
```


localhost/index.php?page=document-viewer.php&PathToDocument=documentation%2Fchange-log.txt&document-viewer-php-submit-button=View+Docume
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Resolute attack « Adm...
Методы обхода защи...
t Viewer
Please Choose Document to View
Change Log
Robots.txt
Installation Instructions: Windows 7 (PDF)
How to access Mutillidae over Virtual-Box-network
View Document
Currently viewing document "documentation/change-log.txt"
Not Found
The requested URL was not found on this server.
Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request.
Apache/2.4.56 (Debian) Server at localhost Port 80


localhost/index.php?page=document-viewer.php&PathToDocument=robots.txt&document-viewer-php-submit-button=View+Document
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Resolute attack « Adm...
Методы обхода защи...
Wild W
ent Viewer
Please Choose Document to View
Change Log
Robots.txt
Installation Instructions: Windows 7 (PDF)
How to access Mutillidae over Virtual-Box-network
View Document
Currently viewing document "robots.txt"
User-agent: *
Disallow: passwords/
Disallow: config.inc
Disallow: classes/
Disallow: javascript/
Disallow: documentation/
Disallow: includes/




При выборе первого варианта, адресная строка браузера выдаёт:

http://localhost/index.php?page=document-viewer.php&PathToDocument=documentation%

2Fchange-log.txt&document-viewer-php-submit-button=View+Document&PathToDocument=robots.txt

При выборе второго варианта:

http://localhost/index.php?page=document-viewer.php&PathToDocument=robots.txt&documentviewer-php-submit-button=View+Document

При подстановке PathToDocument=robots.txt в конец запроса к первому варианту:

http://localhost/index.php?page=document-viewer.php&PathToDocument=documentation%

2Fchange-log.txt&document-viewer-php-submit-button=View+Document&PathToDocument=robots.txt

Предоставляет доступ ко второму варианту.

Таким образом, можно подделать информацию о запросе на сайт, в том числе с возможностью подделки запроса на системы аутентификации и авторизации.

3.

В момент добавления лота в корзину, есть возможность добавления, изменив стоимость. Далее в момент оплаты будет выставлен счёт на ту сумму, которая была указана злоумышленником.

**Где найдена уязвимость**

Уязвимость найдена по адресу

https://URL/shop

Наименование продукта: <Название онлайн-магазина>

**Технические детали обнаружения и воспроизведения**

Уязвимость была обнаружена, в ходе анализа истории запросов, появляющихся на пути добавления товара в корзину до этапа оплаты.

**Выводы и рекомендации по устранению:**

Уязвимость позволяет изменить конечную стоимость продукта при добавлении в корзину.

Не требует дополнительных уязвимостей для эксплуатации.

**Рекомендации по устранению:**

Установить проверку входящего параметра price и id