

# DOM Based XSS in XVWA

Information Security Inc.

# Contents

- About DOM Based XSS (Type 0)
- DOM Based XSS in XVWA
- References

# About DOM Based XSS (Type 0)

- DOM based XSS also known as “type-0 XSS” is a special contrast class in Cross Site Scripting category in which the malicious script is executed as a result of tampering the DOM environment objects. The attack triggers within the page, but with no need of requests/response pair.
- About DOM Based XSS  
[https://www.owasp.org/index.php/DOM\\_Based\\_XSS](https://www.owasp.org/index.php/DOM_Based_XSS)



# What is XVWA

## © Xtreme Vulnerable Web Application (XVWA)

XVWA is a badly coded web application written in PHP/MySQL that helps security enthusiasts to learn application security. It's not advisable to host this application online as it is designed to be "Xtremely Vulnerable".

# DOM Based XSS in XVWA

## © Testing environment

- Kali linux (SMP Debian 4.6.4-1kali1) with XVWA docker image.  
IP:192.168.10.12
- Mysql database  
mysql Ver 14.14 Distrib 5.6.30, for debian-linux-gnu (x86\_64) using  
EditLine wrapper
- Apache webserver  
Server version: Apache/2.4.25 (Debian)
- Docker install script:   
dockerinstall.sh
- XVWA download, install and setup script:   
XVW.sh

# DOM Based XSS in XVWA

- Run XVWA docker image

# docker run --name xvwa -d -p 80:80 tuxotron/xvwa

- Setup the database

Access <http://192.168.10.12/xvwa/setup>

- DOM XSS access

Access [http://192.168.10.12/xvwa/vulnerabilities/dom\\_xss/](http://192.168.10.12/xvwa/vulnerabilities/dom_xss/)

# DOM Based XSS in XVWA

## © Vulnerability discovery

- Access

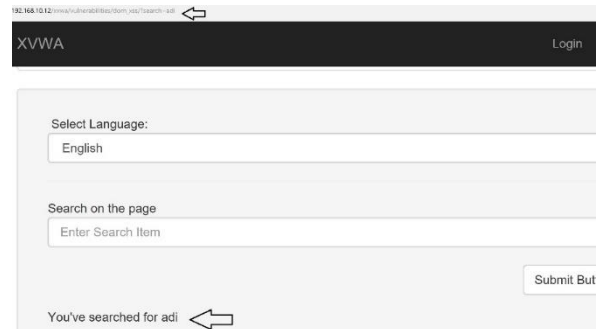
[http://192.168.10.12/xvwa/vulnerabilities/dom\\_xss/](http://192.168.10.12/xvwa/vulnerabilities/dom_xss/)

- Input

[http://192.168.10.12/xvwa/vulnerabilities/dom\\_xss/?search=adi](http://192.168.10.12/xvwa/vulnerabilities/dom_xss/?search=adi)

- Output

```
<br>
  ▶ <div align="right">☰</div>
</div>
</form>
<p></p>
<p id="srch">You've searched for adi</p>
</div>
```



# DOM Based XSS in XVWA

## © Vulnerability discovery

### • Output

Output is not showing in source code. But show in Inspect Element because input is not made by PHP or backend code. Its occur from JavaScript Code. So its not how in source code directly and just only work in browser.

Function search() explained: When ?search found in URL , the input after ?search= will show in the element that is defined by id=srch. Can use html tag for XSS purpose.

```
<script type="text/javascript">
  function search()
  {
    var myurl = document.URL;
    if(myurl.indexOf("?search=")>0)
    {
      document.getElementById('srch').innerHTML = "You've searched for "+unescape(myurl.substr(myurl.indexOf("?search=")+8));
    }
  }
</script>
```



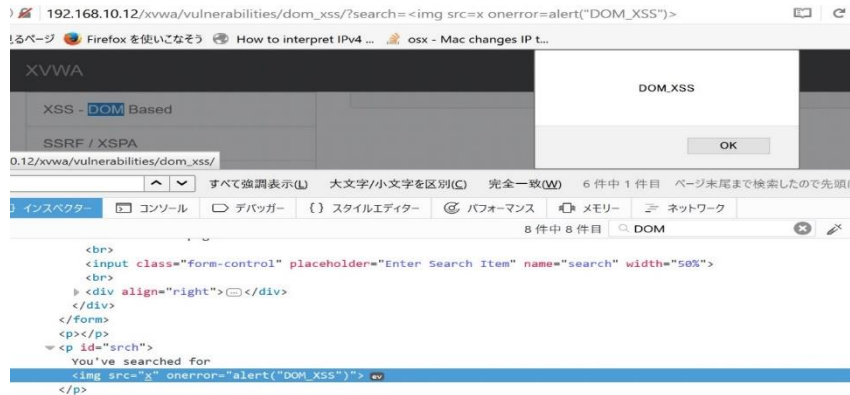
# DOM Based XSS in XVWA

## ◎ Vulnerability discovery

- Input

192.168.10.12/xvwa/vulnerabilities/dom\_xss/?search=<img src=x onerror=alert("DOM\_XSS")>

- Output



# References

- OWASP

[https://www.owasp.org/index.php/DOM\\_Based\\_XSS](https://www.owasp.org/index.php/DOM_Based_XSS)

[https://www.owasp.org/images/c/c5/Unraveling\\_some\\_Mysteries\\_around\\_DOM-based\\_XSS.pdf](https://www.owasp.org/images/c/c5/Unraveling_some_Mysteries_around_DOM-based_XSS.pdf)

- Github

<https://github.com/s4n7h0/xvwa>

[https://github.com/tuxotron/xvwa\\_lamp\\_container](https://github.com/tuxotron/xvwa_lamp_container)

- Wikipedia

[https://en.wikipedia.org/wiki/Document\\_Object\\_Model](https://en.wikipedia.org/wiki/Document_Object_Model)