

# XSS Attacks

Reflected XSS



**ZDResearch**

[www.zdresearch.com](http://www.zdresearch.com)

ZDResearch Advanced Web Hacking

# DVWA Reflected XSS

- How is an XSS Attack possible in the high security level of DVWA Reflected XSS challenge?
- Test it in both [white-box](#) and [black-box](#)

Exdemy.com  
Personal property of Keith Samborski  
I\_my69@yahoo.com



# DVWA Reflected XSS - Solution

- DVWA blacklists script tag
  - We need to find another method to run javascript in other tags
- Also in HTML pages every element support events which they handled by a javascript function
  - `<ELEMENT onEVENT=JAVASCRIPT>`
- For example:
  - `<img src=x onerror=alert('xss')>`





Exdemy.com  
Personal property of Keith Samborski  
l\_my69@yahoo.com

ZDRResearch Advanced Web Hacking

***ZDRResearch***

[www.zdresearch.com](http://www.zdresearch.com)

Copyright © Exdemy.com