Reflected XSS

By
Rajan Nisargam

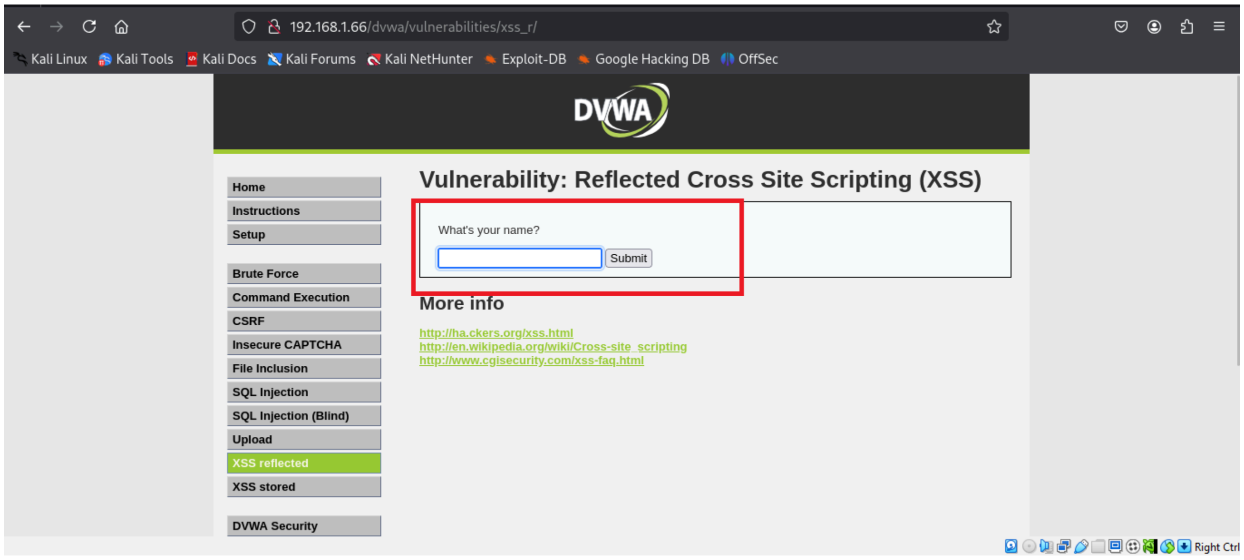
Reflected XSS:-

Reflected Cross-Site Scripting (Reflected XSS) is a type of XSS vulnerability where an attacker injects malicious scripts into a website, and the script is reflected off a web server in a response to a user request. Unlike **Stored XSS**, which permanently stores the malicious script in a database or server, **Reflected XSS** is executed immediately when a user interacts with a specially crafted URL or form submission.

How Reflected XSS Works

1. **Injection: The attacker crafts a malicious URL containing a script and tricks a victim into clicking it (e.g., via phishing emails, social media, or malicious ads).**
2. **Reflection: The vulnerable website includes the malicious script in its response without proper validation or encoding.**
3. **Execution: The victim's browser executes the script, allowing the attacker to steal cookies, session tokens, or perform actions on behalf of the user.**

Step to reprodus :

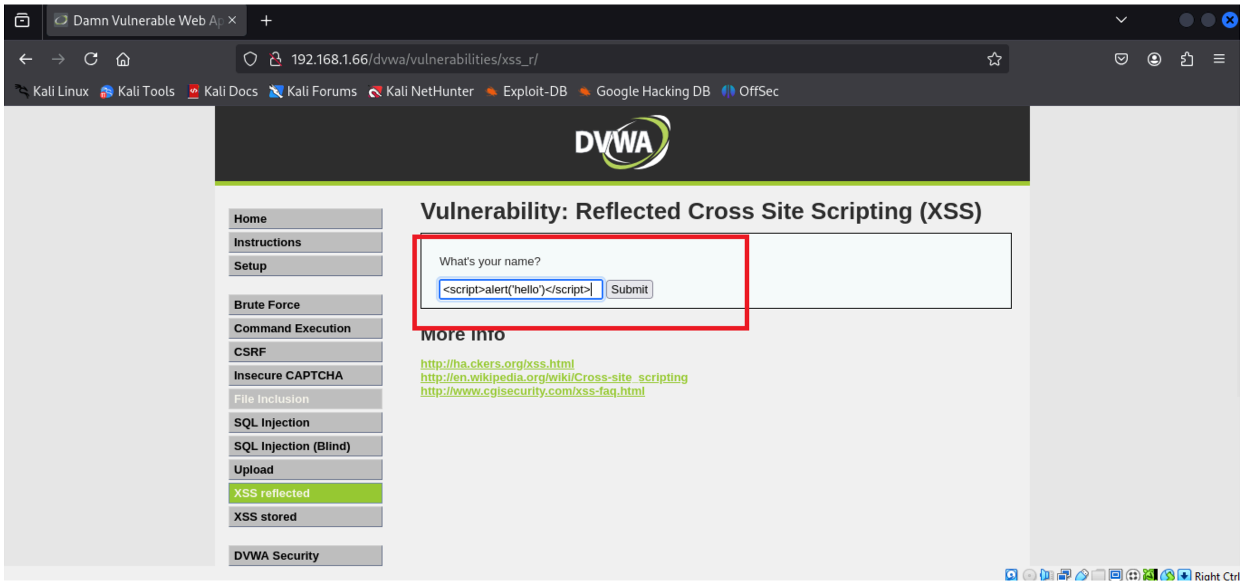


Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

More info

http://ha.ckers.org/xss.html
http://en.wikipedia.org/wiki/Cross-site_scripting
http://www.cgisecurity.com/xss-faq.html



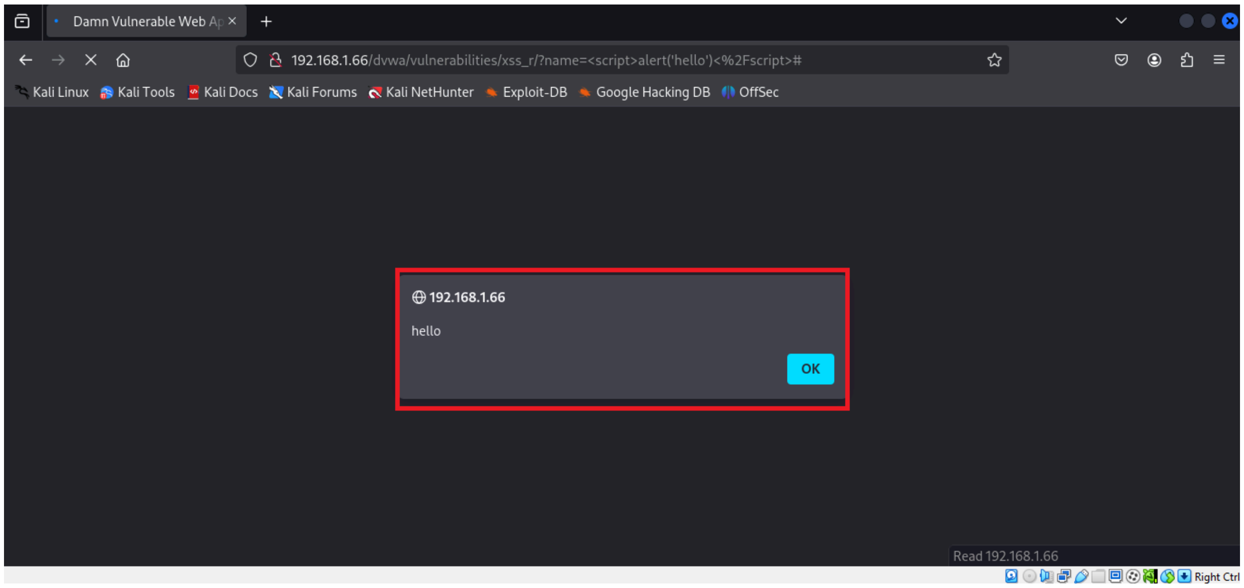
Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

`<script>alert('hello')</script>` Submit

More info

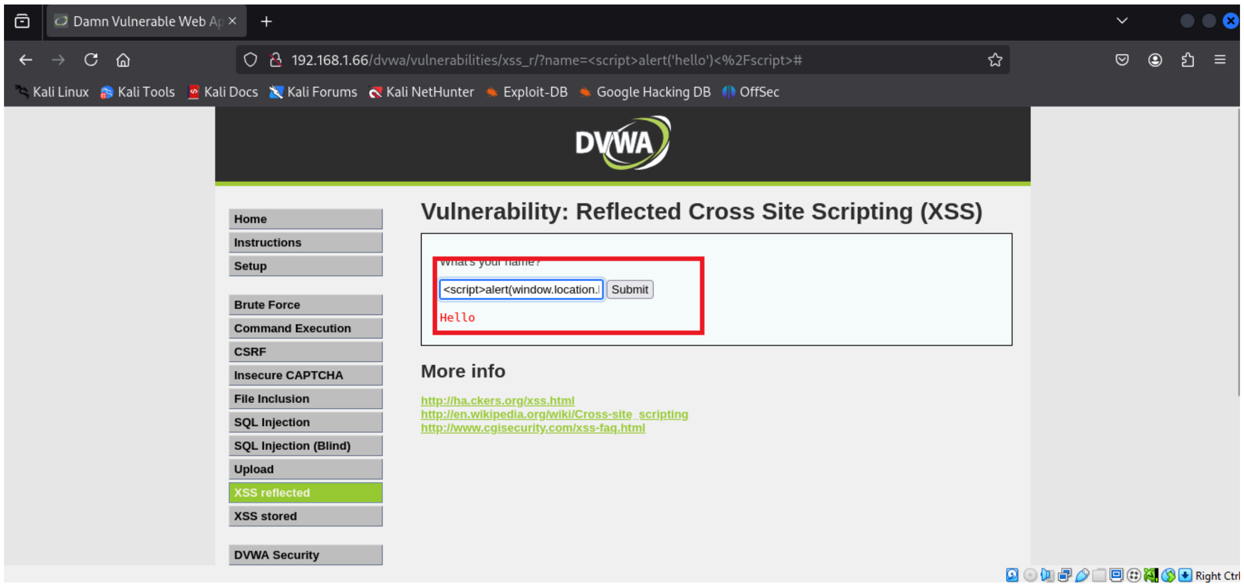
http://ha.ckers.org/xss.html
http://en.wikipedia.org/wiki/Cross-site_scripting
http://www.cgisecurity.com/xss-faq.html



192.168.1.66/dvwa/vulnerabilities/xss_r/?name=<script>alert('hello')<%2Fscript>#

192.168.1.66

hello



Damn Vulnerable Web Ap

192.168.1.66/dvwa/vulnerabilities/xss_r/?name=<script>alert('hello')<%2Fscript>#

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

DVWA

Home
Instructions
Setup

Brute Force
Command Execution
CSRF
Insecure CAPTCHA
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored

DVWA Security

Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

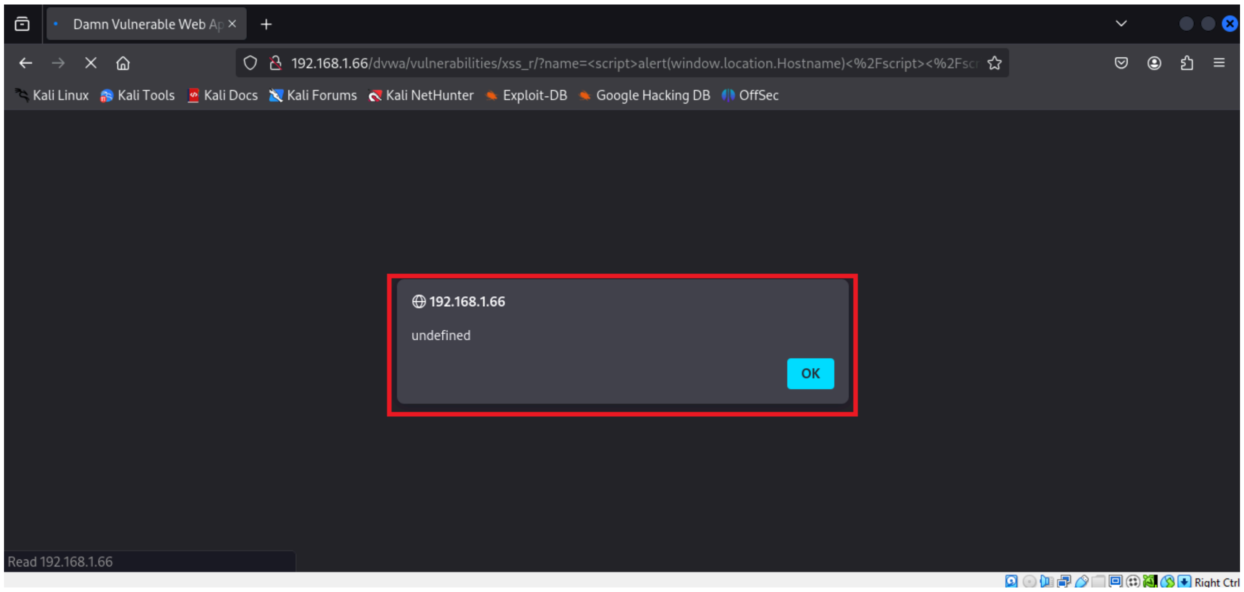
<script>alert(window.location.

Submit

```
Hello
```

More info

http://ha.ckers.org/xss.html
http://en.wikipedia.org/wiki/Cross-site_scripting
http://www.cgisecurity.com/xss-faq.html



Damn Vulnerable Web Ap

192.168.1.66/dvwa/vulnerabilities/xss_r/?name=<script>alert(window.location.Hostname)<%2Fscript><%2Fsc

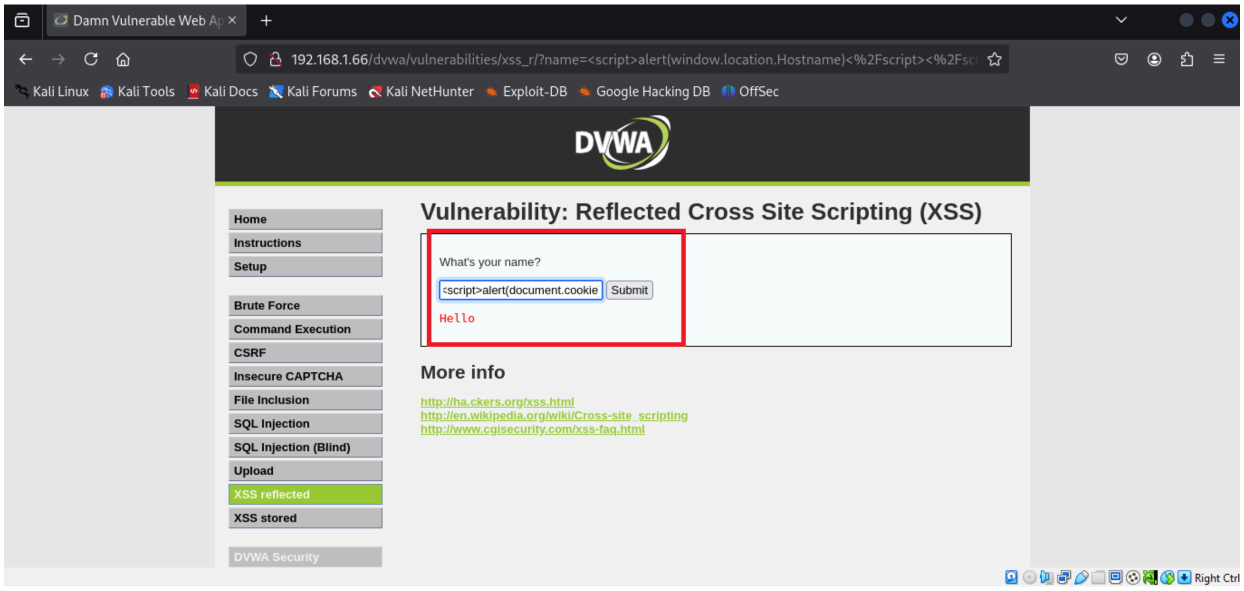
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

192.168.1.66

undefined

OK

Read 192.168.1.66


Damn Vulnerable Web Ap

192.168.1.66/dvwa/vulnerabilities/xss_r/?name=<script>alert(window.location.Hostname)<%2Fscript><%2Fsc

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name?

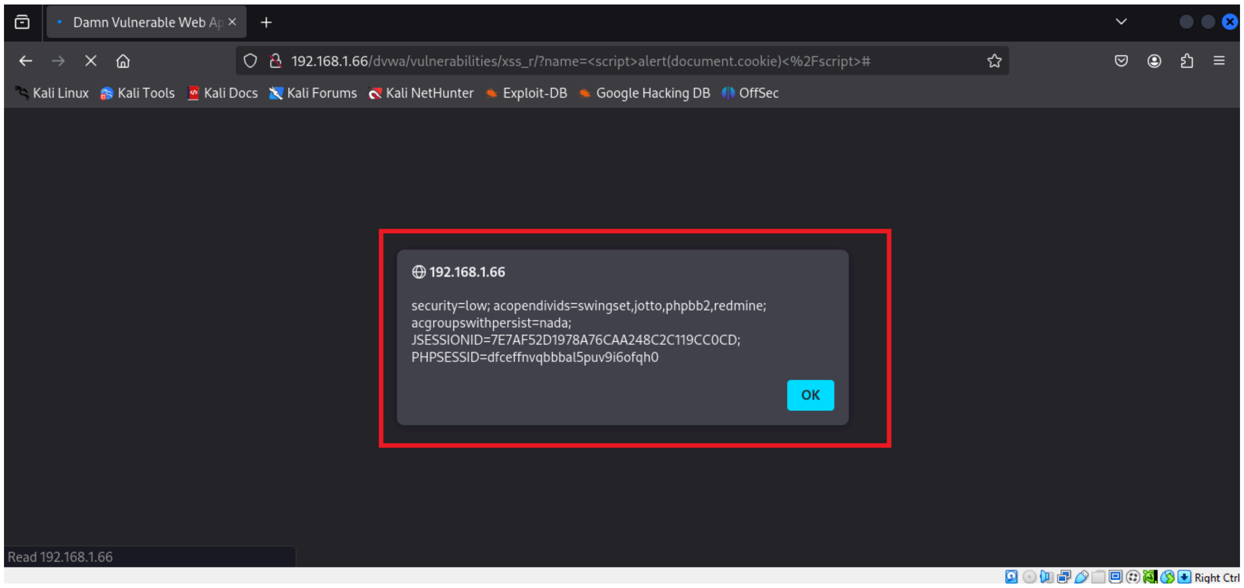
<script>alert(document.cookie

Submit

Hello

More info

http://ha.ckers.org/xss.html
http://en.wikipedia.org/wiki/Cross-site_scripting
http://www.cgisecurity.com/xss-faq.html


Damn Vulnerable Web Ap

192.168.1.66/dvwa/vulnerabilities/xss_r/?name=<script>alert(document.cookie)<%2Fscript>#

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

192.168.1.66

```
security=low; acopendivids=swingset,jotto,phpbb2,redmine;
acgroupswithpersist=nada;
JSESSIONID=7E7AF52D1978A76CAA248C2C119CC0CD;
PHPSESSID=dfceffnvqbbbal5puv9i6ofqh0
```

Impact of Reflected XSS

Reflected XSS can have serious security consequences for both users and organizations. Below are the key impacts:

1. Session Hijacking

- Attackers can steal session cookies using `document.cookie` and gain unauthorized access to a victim's account.
- Example: If a user is logged into a banking site, an attacker can steal their session and perform fraudulent transactions.

2. Phishing Attacks

- Attackers can craft URLs that inject fake login forms, tricking users into entering credentials.
- This can lead to credential theft and account takeovers.

3. Data Theft

- Malicious scripts can read and exfiltrate sensitive information like personal details, email addresses, or payment information.
- Attackers can send this data to an external server.

4. Malware Distribution

- Attackers can use XSS to inject malicious scripts that download and execute malware on the victim's device.
- Example: Redirecting users to fake software update pages that install keyloggers or ransomware.

5. Defacement of Web Pages

- Hackers can modify website content temporarily, displaying misleading information or propaganda.
- This affects the credibility and reputation of the organization.

6. Browser Exploitation

- XSS can be used to exploit browser vulnerabilities, leading to full system compromise in some cases.

7. Unauthorized Actions on Behalf of the User

- Attackers can make requests on behalf of the victim, such as transferring funds, changing account settings, or posting malicious content.

Real-World Example

- In 2017, **British Airways** suffered an attack where hackers injected malicious JavaScript using XSS, leading to the theft of **380,000 payment card details**.

Mitigation Strategies

- **Input Validation**: Ensure that user input does not contain malicious scripts.
- **Output Encoding**: Encode output before rendering it in HTML (`&lt;script&gt;` instead of `<script>`).
- **Use Content Security Policy (CSP)**: Restrict inline scripts and external script sources.
- **Use HTTPOnly and Secure Cookies**: Prevent cookie theft via JavaScript.
- **Sanitize User Input**: Use security libraries like OWASP Java Encoder.