

# 9. XSS (Stored)

Disusun oleh :

Chaerul Umam, M.Kom (chaerul@dsn.dinus.ac.id)

Hafiidh Akbar Sya'bani (akbar@dinustek.com)



## XSS/Cross-Site Scripting (Stored)

Pada tampilan awal DVWA klik bagian XSS (Stored)

**DVWA**

Home  
Instructions  
Setup / Reset DB

Brute Force  
Command Injection  
CSRF  
File Inclusion  
File Upload  
Insecure CAPTCHA  
SQL Injection  
SQL Injection (Blind)  
Weak Session IDs  
XSS (DOM)  
XSS (Reflected)  
**XSS (Stored)**  
CSP Bypass

### Vulnerability: Stored Cross Site Scripting (XSS)

Name \*

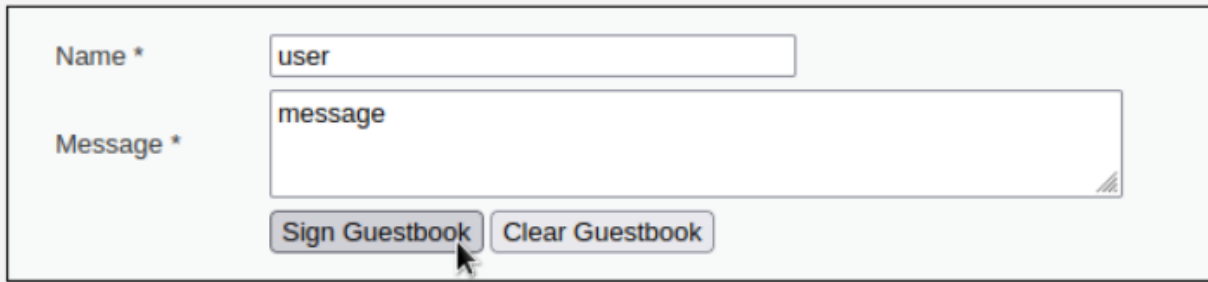
Message \*

#### More Information

- <https://owasp.org/www-community/attacks/xss>
- <https://owasp.org/www-community/xss-filter-evasion-cheatsheet>
- [https://en.wikipedia.org/wiki/Cross-site\\_scripting](https://en.wikipedia.org/wiki/Cross-site_scripting)
- <http://www.cgisecurity.com/xss-faq.html>
- <http://www.scriptalert1.com/>

Coba masukkan nama dan message lalu klik Sign Guestbook

## Vulnerability: Stored Cross Site Scripting (XSS)

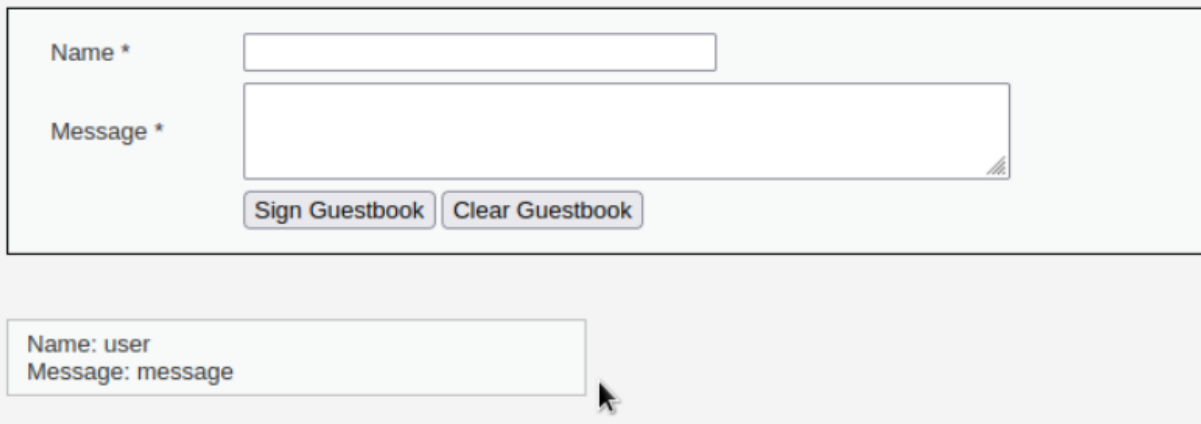


Name \*

Message \*

Nama dan pesan tadi akan masuk dan tersimpan pada website

## Vulnerability: Stored Cross Site Scripting (XSS)



Name \*

Message \*

Name: user  
Message: message

Tujuan dari stored XSS adalah agar script XSS dapat tersimpan dan membuat browser dari pengguna lain menjalankan scriptnya. Script untuk stored XSS biasa dimasukkan dalam komentar, kolom chat, thread forum, bahkan form identitas seperti nama atau alamat.

Pada XSS ini coba masukkan script alert, namun karena field "Name" dibatasi jumlah karakternya, maka masukkan dalam field "Message"

```
<script>alert('xss')</script>
```

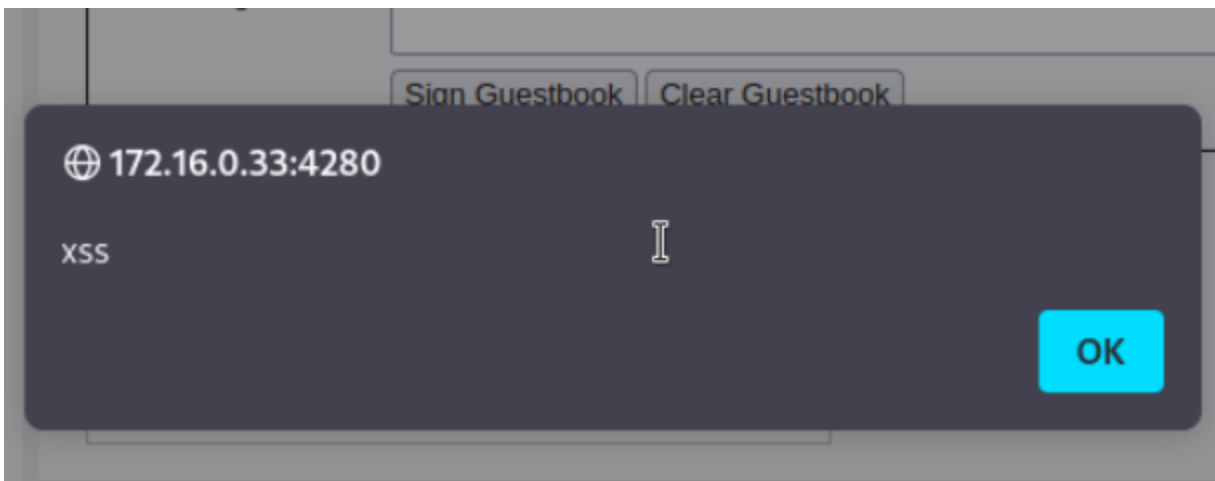
## Vulnerability: Stored Cross Site Scripting

Name \*

Message \*

Name: user  
Message: message

Setelah tombol Sign Guestbook ditekan, halaman selanjutnya akan memunculkan alert dari script yang dimasukkan tadi



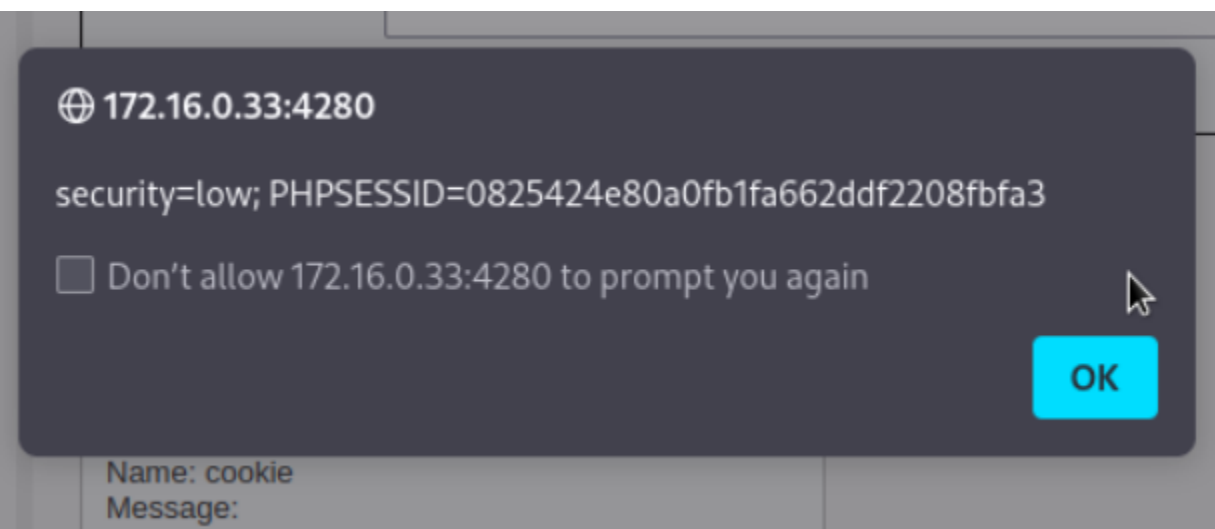
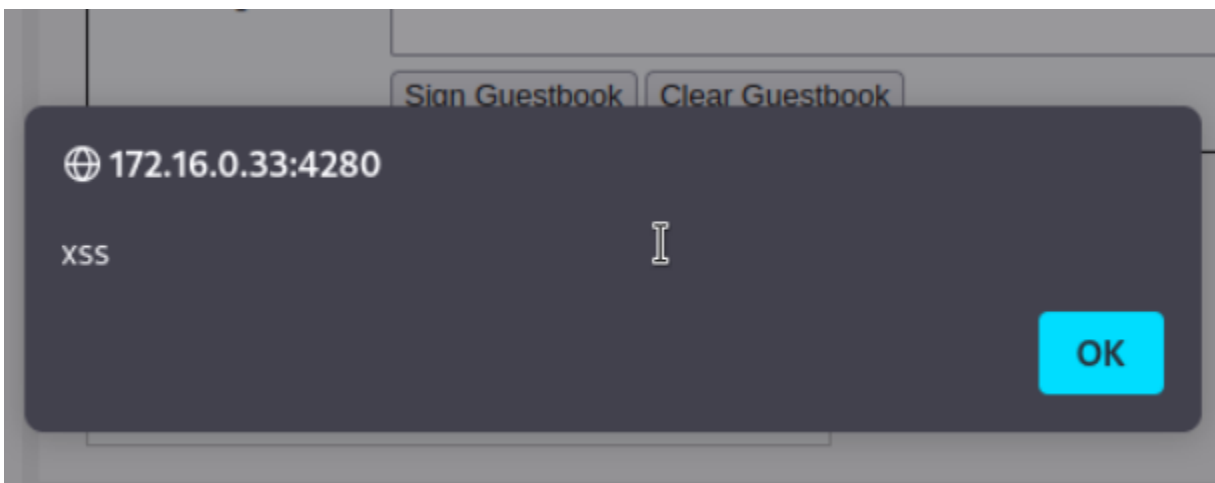
Pada tahap ini setiap kali user masuk ke halaman XSS (Stored) akan muncul alert karena ada script XSS didalamnya. Sekarang coba masukkan payload untuk menampilkan cookie

```
<script>alert(document.cookie)</script>
```

## Vulnerability: Stored Cross Site Scripting

Name *	<input type="text" value="cookie"/>
Message *	<input type="text" value="&lt;script&gt;alert(document.cookie)&lt;/script&gt;"/>
<input type="button" value="Sign Guestbook"/> <input type="button" value="Clear Guestbook"/>	

Sekarang setiap kali user membuka halaman XSS (Stored) browser akan menampilkan 2 alert, teks "xss" dan cookie



#### Note

- Metode ini hanya berfungsi pada website yang vulnerable
- Beberapa website memproteksi diri dari XSS dengan melakukan block pada berbagai payload XSS sehingga hasil payload tidak akan ditampilkan
- Payload pada artikel ini hanya payload dasar dan sudah pasti banyak diblock oleh website website
- Terkadang ada beberapa payload yang belum diblock oleh website sehingga masih ada celah untuk dilakukan XSS, banyak payload yang bisa dicoba untuk melakukan XSS seperti yang ada pada [list ini](#)
- XSS DOM dan Reflected hanya akan berjalan pada browser pelaku namun tidak pada browser pengguna lain, untuk membuat XSS yang dapat berjalan di browser pengguna lain gunakan script XSS yang tersimpan (stored)