

**PRAKTIKUM
KEAMANAN INFORMASI 1
PERTEMUAN 10**

Web XSS INJECTION



Disusun oleh

Nama : Riva Mahyuli
NIM : 21/478709/SV/19365
Kelas : R1AA

**PROGRAM STUDI D-IV
TEKNOLOGI REKAYASA INTERNET
DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA
SEKOLAH VOKASI
UNIVERSITAS GADJAH MADA
2023**

Link : https://github.com/RIVAMAHYULI/Lap10_PrakKI_RivaMahyuli_478709.git

Modul 1 (Cross Site Scripting Injection)

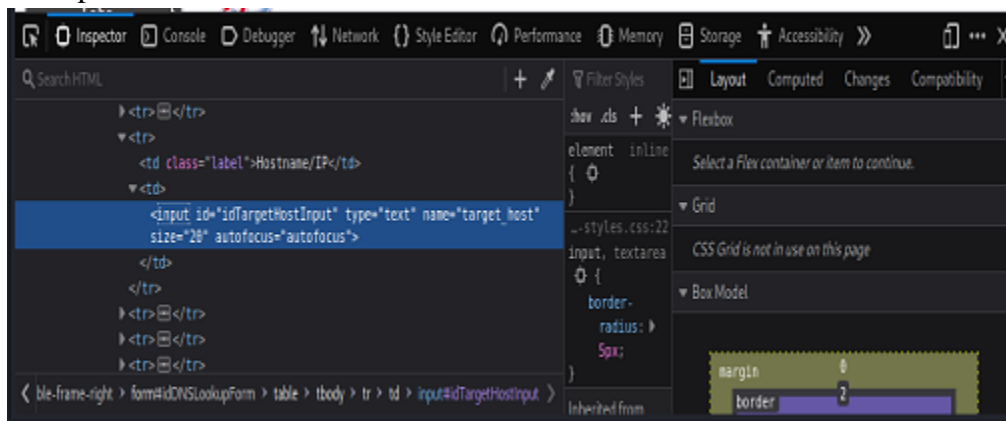
Langkah Kerja

Langkah 1: Login ke KaliLinux dengan IP yang telah disediakan.

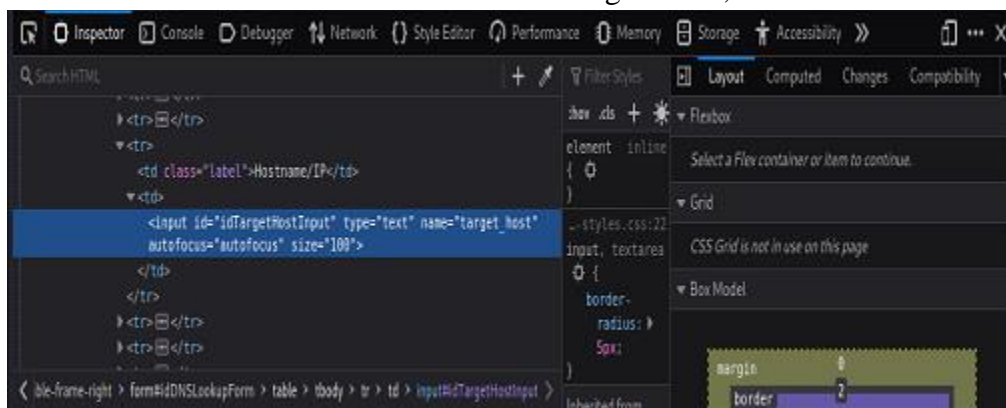
Langkah 2: Reflected Cross Site Scripting (XSS) Injection #1 - Popup Window

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



d. Uji Injeksi (XSS) - instruksi: Di Hostname/IP Textbox tempatkan string berikut: Klik Tombol Pencarian DNS



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

a. Uji Injeksi (XSS) - instruksi: - Di Hostname/IP Textbox tempatkan string berikut: Klik Tombol Pencarian DNS



b. Memulai server apache2 Start Apache2

```
root@kali: ~/home/kali
# service apache2 status
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; disabled; vendor preset: disabled)
   Active: active (running) since Mon 2023-05-08 20:24:01 CDT; 6 days ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 151094 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Process: 200943 ExecReload=/usr/sbin/apachectl graceful (code=exited, status=0/SUCCESS)
  Main PID: 151105 (apache2)
    Tasks: 11 (limit: 4635)
   Memory: 24.8M
      CPU: 38.664s
  CGroup: /system.slice/apache2.service
          └─151105 /usr/sbin/apache2 -k start
            └─200955 /usr/sbin/apache2 -k start
              └─200956 /usr/sbin/apache2 -k start
                └─200957 /usr/sbin/apache2 -k start
                  └─200958 /usr/sbin/apache2 -k start
                    └─200959 /usr/sbin/apache2 -k start
                      └─216094 /usr/sbin/apache2 -k start
                        └─216095 /usr/sbin/apache2 -k start
                          └─216096 /usr/sbin/apache2 -k start
                            └─216097 /usr/sbin/apache2 -k start
                              └─216098 /usr/sbin/apache2 -k start

May 12 00:00:04 kali systemd[1]: Reloaded The Apache HTTP Server.
May 13 00:00:04 kali systemd[1]: Reloading The Apache HTTP Server.
May 13 00:00:04 kali apachectl[191118]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 10.33.102.200. Set the 'ServerName' directive globally to suppress this message
May 13 00:00:04 kali systemd[1]: Reloaded The Apache HTTP Server.
May 14 00:00:04 kali systemd[1]: Reloading The Apache HTTP Server.
May 14 00:00:04 kali apachectl[200113]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 10.33.102.200. Set the 'ServerName' directive globally to suppress this message
May 14 00:00:04 kali systemd[1]: Reloaded The Apache HTTP Server.
May 15 00:00:04 kali systemd[1]: Reloading The Apache HTTP Server.
May 15 00:00:04 kali apachectl[208952]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 10.33.102.200. Set the 'ServerName' directive globally to suppress this message
May 15 00:00:04 kali systemd[1]: Reloaded The Apache HTTP Server.
```

```
(root@kali)~[/home/kali]
# ps -eaf | grep apache2 | grep -v grep
root      151105      1    0 May08 ?        00:00:37 /usr/sbin/apache2 -k start
www-data  208955    151105    0 00:00 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  208956    151105    0 00:00 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  208957    151105    0 00:00 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  208958    151105    0 00:00 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  208959    151105    0 00:00 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  216894    151105    0 19:39 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  216915    151105    0 19:39 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  216916    151105    0 19:39 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  216917    151105    0 19:39 ?        00:00:00 /usr/sbin/apache2 -k start
www-data  216918    151105    0 19:39 ?        00:00:00 /usr/sbin/apache2 -k start
```

c. Buatlah direktori Apache Log Directory

```
(root@kali)~[/home/kali]
# mkdir -p /var/www/logdir
#
```

```
(root@kali)~[/home/kali]
# chown www-data:www-data /var/www/logdir
#
```

```
(root@kali)~[/home/kali]
# chmod 700 /var/www/logdir
#
```

```
(root@kali)~[/home/kali]
# ls -ld /var/www/logdir
drwx----- 2 www-data www-data 4096 May 15 20:10 /var/www/logdir
#
```

d. Konfigurasi CGI Cookie Script

```
(root@kali)~[/home/kali]
# cd /usr/lib/cgi-bin
```

```

(root@kali)~/usr/lib/cgi-bin
# wget https://github.com/cianni20/logit.git mv logit.pl.TXT logit.pl
--2023-05-15 20:17:17-- https://github.com/cianni20/logit.git
Resolving github.com (github.com)... 20.205.243.166
Connecting to github.com (github.com)|20.205.243.166|:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://github.com/cianni20/logit [following]
--2023-05-15 20:17:17-- https://github.com/cianni20/logit
Reusing existing connection to github.com:443.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'logit.git'

logit.git                                     [====>] 162.13K  --KB/s  in 0.08s

2023-05-15 20:17:18 (1.96 MB/s) - 'logit.git' saved [166017]

--2023-05-15 20:17:18-- http://mv/
Resolving mv (mv)... failed: No address associated with hostname.
wget: unable to resolve host address 'mv'
--2023-05-15 20:17:18-- http://logit.pl.txt/
Resolving logit.pl.txt (logit.pl.txt)... failed: Name or service not known.
wget: unable to resolve host address 'logit.pl.txt'
--2023-05-15 20:17:18-- http://logit.pl/
Resolving logit.pl (logit.pl)... 213.186.33.5
Connecting to logit.pl (logit.pl)|213.186.33.5|:80... connected.
HTTP request sent, awaiting response... 302 Moved Temporarily
Location: http://10.13.254.233:80/slogin/appoint.html?URL=http://logit.pl&f6appoint=https://internet.ugm.ac.id/en/ [following]
--2023-05-15 20:17:18-- http://10.13.254.233/slogin/appoint.html?URL=http://logit.pl&f6appoint=https://internet.ugm.ac.id/en/
Connecting to 10.13.254.233:80... connected.
HTTP request sent, awaiting response... 302 Moved Temporarily
Location: https://internet.ugm.ac.id/en/ [following]
--2023-05-15 20:17:18-- https://internet.ugm.ac.id/en/
Resolving internet.ugm.ac.id (internet.ugm.ac.id)... 10.13.243.12
Connecting to internet.ugm.ac.id (internet.ugm.ac.id)|10.13.243.12|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 10062 (9.8K) [text/html]
Saving to: 'index.html'

index.html                                     100%[=====>] 9.83K  --KB/s  in 0s

2023-05-15 20:17:18 (123 MB/s) - 'index.html' saved [10062/10062]

FINISHED --2023-05-15 20:17:18--
Total wall clock time: 1.6s
Downloaded: 2 files, 172K in 0.08s (2.08 MB/s)

```

```

(root@kali)~/usr/lib/cgi-bin
# chown www-data:www-data logit.pl

```

```

(root@kali)~/usr/lib/cgi-bin
# chown 700 logit.pl

```

```

(root@kali)~/usr/lib/cgi-bin
# perl -c logit.pl
logit.pl syntax OK

```

Langkah 4 :Test Cross Site Script (XSS) Injection

a. Instructions: Hostname/IP masukan string:

Enter IP or hostname

Hostname/IP

Lookup DNS

Not Found

The requested URL was not found on this server.

Apache/2.4.46 (Debian) Server at localhost Port 80

b. Lihat File Log Skrip Cookie

← → ↺ 🏠

localhost/logdir/log.txt

Kali Linux

Kali Training

Kali Tools

Kali Forums

Kali Docs

NetHunter

Offensive Security

MSFU

Not Found

The requested URL was not found on this server.

Apache/2.4.46 (Debian) Server at localhost Port 80

c. Simulasikan Serangan Man-In-The-Middle. Dimana kita akan mengubah nilai dan menambahkan nilai di Cookie+

Cookies

username:samurai
uid:6
PHPSESSID:he37g44qhsfhhtkauqsg0it3pi
showhints:1

Details

Domain	localhost
First-Party	
Name	PHPSESSID
Value	he37g44qhsfhhtkauqsg0it3pi
Path	/
Context	Default
httpOnly	<input type="checkbox"/> sameSite No restriction
isSecure	<input type="checkbox"/>
isSession	<input checked="" type="checkbox"/>

Cookies

username:samurai
uid:6
PHPSESSID:he37g44qhsfhhtkauqsg0it3pi
showhints:1



Details

Domain	localhost
First-Party	
Name	showhints
Value	1
Path	/
Context	Default
httpOnly	<input type="checkbox"/> sameSite Lax
isSecure	<input type="checkbox"/>
isSession	<input checked="" type="checkbox"/>

Cookies

username:samurai
uid:6
PHPSESSID:he37g44qhsfihhtkauqsg0it3pi
showhints:1

Details

Domain	localhost		
First-Party			
Name	username		
Value	samurai		
URL	 0x4		
Path	/mutillidae/		
Context	Default		
httpOnly	<input type="checkbox"/>	sameSite	No restriction
isSecure	<input type="checkbox"/>		
isSession	<input type="checkbox"/>		
Expire	17-05-2023 20:59:48 		

Cookies

username:samurai

uid:6

PHPSESSID:he37g44qhsfhhtkauqsg0it3pi

showhints:1

Details

Domain

localhost

First-Party

Name

uid

Value

6

Path

/mutillidae/

Context

Default

HttpOnly

☐

sameSite

No restriction

isSecure

☐

isSession

☐

Expire

17-05-2023 21:01:45

d. setelah selesai menambah nilai di Cookie+, buka Mutillidae apakah tanpa klik Login/Register user sudah masuk?

localhost/mutillidae/

Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB

OWASP 2017

OWASP 2013

OWASP 2010

OWASP 2007

Web Services

Others

Labs

Documentation

Resources

Donate

Want to Help?

Video Tutorials

Announcements

Getting Started

Hints and Videos

What Should I Do?

Help Me!

Listing of vulnerabilities

Video Tutorials

Release Announcements

Latest Version

Helpful hints and scripts

Mutillidae LDIF File

TIP: Click [Hint and Videos](#) on each page

Klik Login / Register lalu Tempatkan satu kutipan (') di Kotak Teks Nama

Error Message	
Failure is always an option	
Line	238
Code	0
File	/var/www/html/mutillidae/classes/MySQLHandler.php
Message	/var/www/html/mutillidae/classes/MySQLHandler.php on line 238: You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near '''' at line 1 Query: SELECT username FROM accounts WHERE username='''; (1064) [mysql_sql_exception]
Trace	#0 /var/www/html/mutillidae/classes/MySQLHandler.php(328): MySQLHandler->doExecuteQuery() #1 /var/www/html/mutillidae/classes/SQLQueryHandler.php(279): MySQLHandler->executeQuery() #2 /var/www/html/mutillidae/includes/process-login-attempt.php(57): SQLQueryHandler->accountExists() #3 /var/www/html/mutillidae/index.php(225): include_once('...') #4 {main}
Diagnostic Information	Error querying user account
Click here to reset the DB	

Login Tanpa Kata Sandi, di username masukan ' or 1 = 1 - - '

Langkah 3: SQL Injection: Single Quote Test On Password Field

1. Periksa Elemen Kotak Kata Sandi

Klik Login/Daftar 2. Nama: samurai 3. Kata Sandi: Klik Kanan 4. Klik Elemen Inspect

Please sign-in

Username

Password

Login

Ganti string "kata sandi" dengan kata "teks"

```
<td>  
<input type="text" name="password" size="20">  
</td>
```

Lalu login lagi

Please sign-in

Username

Password

Login

Dont have an account? [Please register here](#)

Error Message

Failure is always an option

Line	238
Code	0
File	/var/www/html/mutillidae/classes/MySQLHandler.php
Message	/var/www/html/mutillidae/classes/MySQLHandler.php on line 238: You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near '''' at line 1 Query: SELECT username FROM accounts WHERE username='samurai' AND password='''; (1064) [mysqli_sql_exception]
Trace	#0 /var/www/html/mutillidae/classes/MySQLHandler.php(328): MySQLHandler->doExecuteQuery() #1 /var/www/html/mutillidae/classes/SQLQueryHandler.php(302): MySQLHandler->executeQuery() #2 /var/www/html/mutillidae/includes/process-login-attempt.php(68): SQLQueryHandler->authenticateAccount() #3 /var/www/html/mutillidae/index.php(225): include_once('...') #4 {main}
Diagnostic Information	Error querying user account

[Click here to reset the DB](#)

Langkah 4: SQL Injection: Single Quote Test On Password Field

Klik Login/Daftar 2. Nama: samurai 3. Kata Sandi: Klik Kanan 4. Klik Elemen Inspect

Please sign-in

Username

Password

Login

Dont have an account? [Please register here](#)

Ganti string "kata sandi" dengan kata "teks"

```
<td>  
<input type="text" name="password" size="20">  
</td>
```

Login lagi

Please sign-in

Username

Password

Error Message

Failure is always an option	
Line	238
Code	0
File	/var/www/html/mutillidae/classes/MySQLHandler.php
Message	/var/www/html/mutillidae/classes/MySQLHandler.php on line 238: You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near ''' at line 1 Query: SELECT username FROM accounts WHERE username='samurai' AND password='' or 1=1--'; (1064) [mysqli_sql_exception]
Trace	#0 /var/www/html/mutillidae/classes/MySQLHandler.php(328): MySQLHandler->doExecuteQuery() #1 /var/www/html/mutillidae/classes/SQLQueryHandler.php(382): MySQLHandler->executeQuery() #2 /var/www/html/mutillidae/includes/process-login-attempt.php(68): SQLQueryHandler->authenticateAccount() #3 /var/www/html/mutillidae/index.php(225): include_once('...') #4 {main}
Diagnostic Information	Error querying user account
Click here to reset the DB	

Langkah 5: SQL Injection: Single Quote Test On Password Field

Please sign-in

Username

Password

Login

Dont have an account? [Please register here](#)

Ganti string "kata sandi" dengan kata "teks" - Setelah size=, ganti string "20" dengan "50" - Setelah maxlength=, ganti string "20" dengan "50" - Minimalkan Firebug

```
<input type="text" name="password" size="50">  
</td>
```

Login lagi

Please sign-in

Username

samurai

Password

' or (1=1 and username='samurai')--|

Login

Dont have an account? [Please register here](#)

Memverifikasi Hasil (Punya Samurai?)

OWASP Mutillidae II: Keep Calm and Pwn On

Version: 2.11.4 Security Level: 0 (Hosed) Hints: Enabled Logged In User: **samurai**

[Home](#) | [Logout](#) | [Toggle Hints](#) | [Toggle Security](#) | [Enforce TLS](#) | [Reset DB](#) | [View Log](#) | [View Captured Data](#)

OWASP 2017

OWASP 2013

OWASP 2010

OWASP 2007

Web Services

Others

Labs

Documentation

Resources

Donate

Want to Help?

Video Tutorials

Announcements

Getting Started

Hints and Videos

What Should I Do?

Help Me!

Listing of vulnerabilities

Video Tutorials

Release Announcements

Latest Version

Helpful hints and scripts

Mutillidae LDIF File

TIP: Click [Hint and Videos](#) on each page