## Panduan Pemakaian Modul Pengaman Web

## 1. Instalasi

• Include file filter.php kedalam file php yang berpotensi mempunyai celah keamanan. Contoh :

include "web\_security/filter.php";

- Import database yang telah disediakan.
- Sesuaikan configurasi database di file *config.php* .

## 2. Setting

- Setting dilakukan di panel admin yang berada pada folder dimana modul berada.
- Default login untuk panel admin adalah user admin dan password admin.
- Input Chet Sheet untuk celah SQL Injection, XSS, File Inclution dan Command execution. Secara default telah ada bebeara chet sheet didalamnya, fitur ini digunakan untuk menambah atau mengurangi chet sheet yang telah ada. Pengaturan tersebut berada pada menu *pengamanan* :

		and the device of the second state of the second state of the second state of the second state of the second st		
	Web Security	Logout		
ne sqli				
Tambah String Daftar String				
NO	String	Delete		
1	,	Delete		
2	•	Delete		
3	-	Delete		
4	select	Delete		
	e sqli aL INJECTION mbah String iftar String NO 1 2 3 4	e sqli SALINJECTION mbah String Itar String 1 ' 2 ' 3 4 select		

• Input pengaturan maksimal request, serta lama waktu pemblokiran dan juga nama-nama parameter yang akan dilindungi dari serangan brute force. Pengaturan tersebut berada pada menu *pengamanan* dan submenu *Brute Forcing* :

Web Security Panel	+					
🔹 🔹 S 🕘 localhost/	/pengujian/web_sec/inc 🏠	🔻 🖸 🧕 💺 🛛 🐱 🗣 Google	🔍 🕂 🚻 🙆 🤲 🎕			
Panel Admin		Web Security	Logout			
👤 Sai	Home bf					
PENGAMANAN	<u></u>					
SQL Injection	BRUTE FORCING					
XSS     File Inclution	Maximal Request					
Brute Forcing 3 Simpan						
File Upload	Lama Blokir (Jam)					
	24	Simpan				
ADMIN	Tambah Parameter					
THT Pembatasan Akses		Tambahkan				
	NO	Parameter	Delete			
Copyright © 2013 Web Security	1	username	Delete			
	2	password	Delete			
	3	login	Delete			
	4	user	Delete			
	5	mail	Delete			

• Input alamat-alamat IP yang diperbolehkan untuk mengakses panel admin. Berada pada menu Admin dan submenu *pembatasan akses* :

Web Security Panel - Mo	zilla Firefox			$\bigcirc \bigcirc \bigcirc \bigcirc$	
🗌 Web Security Panel	+				
🔹 🕞 S 🙆 localhos	<b>t</b> /pengujian/web_sec/inc	🕆 📧 🥘 🐇 🛛 🛚 🕏 Google	🔍 🦊 Yau 🙆 🤲	<u> </u>	
Panel Admin		Web Security		Logout	
2 Sai	Home				
PENGAMANAN SQL Injection	IP				
File Inclution Brute Forcing File Upload	Tambah IP Yang Diperbolehkan Tambahkan				
Command Execution	Daftar IP Yang Diperb	olehkan	Delete	_	
ADMIN ## Pembatasan Akses	1	127.0.0.1	Delete		
Le Users	2	192.168.56.1	Delete		
Copyright © 2013 Web Security					

• Input pengaturan user yang bisa mengakses panel admin. Pengaturan tersebut berada pada menu Admin dan submenu *Users* :

Panel Admin		Web Sec	urity	Log
Sai	Home us			
ENGAMANAN SQL Injection	USERS			
XSS File Inclution	Tambah Users	Decoverd	Tranhabl	
File Upload     Command Execution	Daftar Users	Password	Tambani	kan
DMIN	NO	Username	Password	Delete
III Pembatasan Akses	1	sai	ful	Delete
	2	Sai	Sai	Delete
	3	s4i	fu7	Delete
copyright © 2013 Web Security	4	admin	admin	Delete

## 3. Output

• Output berupa log yang berada pada folder log. Berikut contoh log :

slazht@slazht: /var/www/pengujian/web_sec/log	● ● ● 〕
127.0.0.1 : [2014-01-29 10:13:23] : xss POST - "/pengujian/batikmoduler-g	w/?mod
=cari&act=search" - ",blus,XXXL,< Rp. 100.000,cari, "	
127.0.0.1 : [2014-01-29 10:14:16] : fi GET - "/pengujian/pdam/?daf=php://	filter
/convert.base64-encode/resource=daftar" - "php://filter/convert.base64-enc	ode/re
source=daftar, "	
127.0.0.1 : [2014-01-29 10:22:53] : fu "Terjadi usaha untuk mengupload fi	le php.
.php "	
127.0.0.1 : [2014-01-29 10:26:08] : fu "Terjadi usaha untuk mengupload fi	le php.
.php "	
127.0.0.1 : [2014-01-29 10:27:11] : fu "Terjadi usaha untuk mengupload fi	le php.
.php "	
127.0.0.1 : [2014-01-29 10:28:08] : fu "Terjadi usaha untuk mengupload fi	le php.
.php "	
127.0.0.1 : [2014-01-29 10:45:10] : fu "Terjadi usaha untuk mengupload fi	le php.
.php "	
127.0.0.1 : [2014-01-29 10:45:10] : xss POST - "/pengujian/inalgosystem/a	dmin/i
ndex.php?type=mn2⊂=sub8&act=add&edit=31" - "rgggregerg,31,sfgsgrgwrg,20	14-01-
29,rgwrgwrgrg,Web,, "	
127.0.0.1 : [2014-01-29 10:45:27] : fu "Terjadi usaha untuk mengupload fi	le php.
.php "	
127.0.0.1 : [2014-01-29 10:45:27] : xss POST - "/pengujian/inalgosystem/a	dmin/i
ndex.php?type=mn2⊂=sub8&act=add&edit=31" - "rgggregerg,31,sfgsgrgwrg,20	14-01-
29,rgwrgwrgrg,Web,, "	
slazht@slazht:/var/www/pengujian/web_sec/log\$	

• Output berupa chart yang berada panel admin. Berikut contoh chart yang digenerate oleh modul pengaman web :

Web Security Panel	ezilla Firerox					
🔹 🔹 S 🙆 localho	st/pengujian/web_s	ec/ind: 🛱 🔻 🖸	) 😣 🐛 [	<mark>8</mark> <del>▼</del> Google (	🔍 🦊 Yau	🙆 * 🔞
Panel Admin			Web Secu	ırity		Logou
Sal	Home History					
PENGAMANAN SQL Injection XSS File Inclution Brute Forcing File Upload Command Execution ADMIN Pembatasan Akses	2700 2400 2100 1800 1500	Char	t History	y Seran	.gan	
L Users ≎opyright © 2013 Web Security	900 600 300 0 2014-01-26	2014-01-28	2014-01-30	2014-02-01	2014-02	2-03 2014-02-
	XSS SQL In COMMAND EXECUTION 636	jection File I UPLOAD FILE 27	FILE INCLUTION	pload Comma soli 2601	Execution xss 59	Brute Force BRUTE FORCE 29