Penetration Testing Sistem Keamanan Aplikasi Web Berbasis e-Commerce Pada Perusahaan Hptasik

Article · September 2015

1 author:

Iim Abdurrohim
Universitas Nasional Pasim
4 PUBLICATIONS **0** CITATIONS

SEE PROFILE

Penetration Testing Sistem Keamanan Aplikasi Web Berbasis E-Commerce Pada Perusahaan Hptasik

Iim Abdurrohim

Program Studi Teknik Informatika Universitas Nasional Pasim
Jl. Dakota No.8a Sukaraja Bandung 40172 Indonesia
iim2loey@gmail.com

Abstrak - *B*anyak perusahaan maupun instansi – instansi yang mempunyai masalah pada kemanan sistem *website* yang di kelola, kemanan sistem sering kali kurang di perhatikan, tidak sedikit juga *website* yang telah mendapati kerugian yang di akibatkan kelemahan sistem yang ada ,pencurian informasi pada *sistem*, pencurai data informasi *credit card* , alamat , no telepon, *username* ,*password* dan lain sebagainya. menggunakannya, oleh karena itu *penetration testing* kemanan sistem ini diharapkan dapat meningkatkan kemamanan pada *website* dengan mengetahui kelemahan sistem *website* yang ada dan melakukan perbaikan celah kemanan pada *website* terkait, *penetration testing* ini akan menggunakan metodologi yang mengacu pada pendekatan *ISSAF (Information Systems Security Assessment Framework)*, dengan tujuan untuk mencari kelemahan sistem *website* yang ada,.
Kata kunci : *penetration testing* , kemanan sistem *website , sql injection , open web application security project. Carding , deface.*

Abstract - *Many companies and institutions that have security problems on the website in the manage system, security system is often lacking in the notice, not least also a website that has found a loss that causes weakness of the existing system, the theft of information in the system, theft credit card information, address, telephone number, username, password, and so forth. use, therefore security penetration testing of this system is expected to improve security on the website by knowing the weaknesses of the existing system website and make improvements to the security holes related websites, penetration testing will use the methodology refers to the approach ISSAF (Information Systems Security Assessment Framework) , with the aim to find the weaknesses of existing website system.*
***Keywords** : penetration testing website, website security, sql injection, open web application security project, Carding , deface*

I. PENDAHULUAN

Masalah keamanan merupakan salah satu aspek penting dari sebuah sistem informasi. Seringkali masalah keamanan berada di urutan terakhir dalam daftar hal-hal yang dianggap penting. Apabila mengganggu peforma sistem, seringkali keamanan dikurangi atau bahkan ditiadakan. Informasi pada era ini sudah menjadi sebuah komoditas yang sangat penting. Bahkan ada yang mengatakan bahwa kita sudah berada di sebuah "information-based society". Kemampuan untuk mengakses dan menyediakan informasi secara cepat dan akurat menjadi sangat esensial bagi sebuah organisasi, baik yang berupa organisasi komersial (perusahaan), perguruan tinggi, lembaga pemerintahan, maupun individual. Hal ini memungkinkan dengan perkembangan pesat di bidang teknologi komputer dan telekomunikasi. Berbagai type celah keamanan pada website ada beberapa type vulnerability XSS (Cross-Site Scripting), vulnerability File Inclusioon, vulnerability SQL injection dan banyak lagi metode Attacker website lainnya, Sedangkan vulnerability yang paling banyak dan paling fatal adalah vulnerability SQL Injection, SQL Injection merupakan salah satu kelemahan yang paling dahsyat untuk dampak bisnis, karena dapat menyebabkan pembongkaran semua informasi yang sensitif yang tersimpan dalam sebuah aplikasi database, termasuk informasi berguna seperti username, password, nama, alamat, nomor telepon, dan rincian kartu kredit. Jadi vulnerability SQL injection adalah kelemahan yang terjadi ketika penyerang mampu mengubah Structured Query Language (SQL) di dalam database. Dengan mempengaruhi database, penyerang dapat memanfaatkan sintaks dan kemampuan dari SQL itu sendiri, serta kekuatan dan fleksibilitas yang mendukung fungsi database dan fungsi sistem operasi yang hanya dilakukan dalam database

Hipotesis-

Terdapatnya Vulnerabillity SQL Injection pada suatu website, yang dapat memungkinkan pengambilan data informasi pada database website untuk mendapatkan hak akses oleh seorang cracker/defacer, dengan melakukan proses penetrasi pada website hptasik.com. Yang di tujukan untuk mengetahui hasil dari adanya celah keamanan yang dapat berakibat fatal pada kemanan aplikasi website tersebut.

Identifikasi masalah -

Dengan adanya masalah pada kemanan sistem website banyak kerugian yang sangat besar yang di timbulkan dalam kasus, pencurian data , pencurian informasi , pencurian credit card , deface dan lain-lain. Untuk itu Masalah keamanan sistem website sangat perlu di perhatikan.

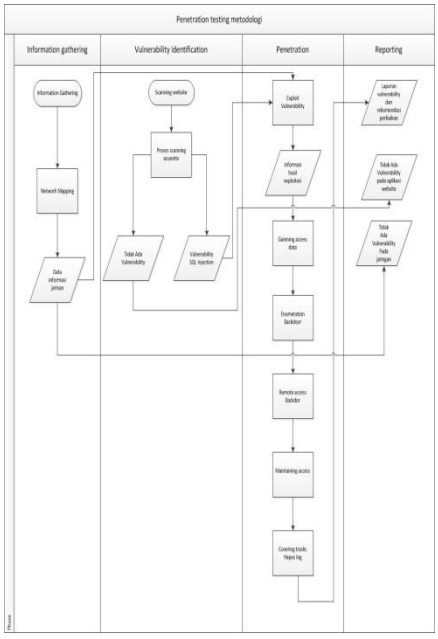
II. METODE PENELITIAN

Terdapat beberapa cara yang dapat digunakan dalam melakukan sebuah penelitian pengembangan teknologi informasi, tetapi penulis menggunakan dua cara dalam melakukan penelitian ini, yaitu:

A. Analisis Sistem

- Information Gathering
- Information Gathering difokuskan untuk dapat mengumpulkan informasi secukupnya mengenai sistem hptasik.com.
- Network Mapping
- Proses untuk mencari informasi jaringan pada web hptasik.com dengan menggunakan tool Nmap.

- Vulnerability identification
- Mencari informasi vulnerability pada web hptasik.com dengan menggunakan Acunetix web vulnerability scanner.
- Penetration
- Proses exploitasi pada vulnerability yang di temukan. Dalam kasus penelitian ini exploitasi pada vulnerability Sql Injection.
- Gaining access
- Mengolah data hasil dari exploitasi sebelumnya,untuk mengakses lebih jauh pada pada system target. Akses data admin dari hasil penetration.
- Enumerating further
- Proses upload file backdoor pada website hptasik.com.
- Compromising remote access
- Proses untuk mengakses lebih pada server target, dengan menggunakan backdoor yang telah di upload.
- Maintaining Access
- Proses setelah masuk sistem , untuk mencoba berbagai akses lebih jauh pada server hptasik.com.
- Covering tracks
- Menghapus log aktifitas yang telah dilakukan pada penetration untuk menghapus jejak pada log server hptasik.com.
- Reporting
- Laporan hasil penetration testing pada website hptasik.com dengan menyertakan rekomendasi untuk perbaikan pada vulnerability yang di temukan.



Tabel 1.3 Proses Penetration Testing Website

B. Perancangan Sistem

Hasil Penetration

Dalam proses Penetration testing Website hptasik.com untuk mencari suatu kelemahan system website beberapa hasil yang ditemukan dari penetration testing sebagai berikut :

Network mapping

Detemukan port jaringan yang terbuka, tetapi sistem dan jaringan pada server hptasik.com termasuk kategori aman,tidak ada exploitasi untuk jaringan dan sistem pada server hptasik.com

Scanning website

Terdapat vulnerability Sql Injection pada aplikasi web hptasik.com di temukan pada file cek_login.php

Penetration

Dengan adanya vulnerability Sql injection website, exploitasi berhasil masuk pada sistem, dengan pengambilan database pada web hptasik.com.

Enumeration further

Proses upload backdoor berhasil di lakukan, dengan mem-bypass filter jpg pada web hptasik.com.

Remote Access backdoor

Explorasi backdoor pada web hptasik.com berhasil di jalankan, tidak terdeteksi virus oleh server hosting.

Covering tracks

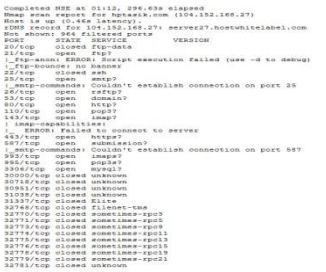
Proses menghapus jejak penetrasi berhasil di lakukan pada file log.txt pada web hptasik.com namun log server tidak bisa di hapus karena keterbatasan hak akses dari penyedia hosting.

Information gathering

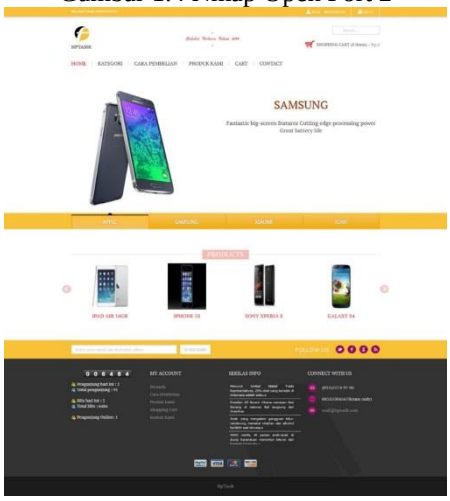
Nmap adalah sebuah peralatan pencari informasi, lebih khusus mencari informasi port yang terbuka dalam sebuah jaringan. Nmap di disain khusus untuk melakukan ping menuju port - port yang terbuka, dan kembali lagi kepada hacker dengan membawa informasi Disini Penulis akan melakukan Network Mapping pada situs yang beralamat http://hptasik.com/ .

```
C:\nmap>nmap -v -A hptasik.com

Starting Nmap 6.47 ( http://nmap.org ) at 2015-03-10 01:02 SE Asia Standard Time
NSE: Loaded 118 scripts for scanning.
NSE: Script Pre-scanning.
Initiating Ping Scan at 01:02
Scanning hptasik.com (104.152.168.27) [4 ports]
Completed Ping Scan at 01:02, 0.81s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 01:02
Completed Parallel DNS resolution of 1 host. at 01:02, 0.73s elapsed
Initiating SYN Stealth Scan at 01:02
Scanning hptasik.com (104.152.168.27) [1000 ports]
Discovered open port 143/tcp on 104.152.168.27
Discovered open port 587/tcp on 104.152.168.27
Discovered open port 25/tcp on 104.152.168.27
Discovered open port 443/tcp on 104.152.168.27
Discovered open port 53/tcp on 104.152.168.27
Discovered open port 993/tcp on 104.152.168.27
Discovered open port 110/tcp on 104.152.168.27
Discovered open port 3306/tcp on 104.152.168.27
Discovered open port 21/tcp on 104.152.168.27
Discovered open port 995/tcp on 104.152.168.27
Discovered open port 80/tcp on 104.152.168.27
Discovered open port 26/tcp on 104.152.168.27
Increasing send delay for 104.152.168.27 from 0 to 5 due to 20 out of 66 dropped probes since last increase.
Completed SYN Stealth Scan at 01:06, 240.70s elapsed (1000 total ports)
Initiating Service scan at 01:06
Scanning 12 services on hptasik.com (104.152.168.27)
Completed Service scan at 01:07, 5.02s elapsed (12 services on 1 host)
Initiating OS detection (try #1) against hptasik.com (104.152.168.27)
Retrying OS detection (try #2) against hptasik.com (104.152.168.27)
Initiating Traceroute at 01:07
Completed Traceroute at 01:07, 9.04s elapsed
Initiating Parallel DNS resolution of 8 hosts. at 01:07
Completed Parallel DNS resolution of 8 hosts. at 01:07, 0.75s elapsed
NSE: Script scanning 104.152.168.27.
Initiating NSE at 01:07
NSE Timing: About 28.57% done; ETC: 01:09 (0:01:18 remaining)
NSE Timing: About 57.14% done; ETC: 01:09 (0:01:02 remaining)
```

Gambar 1.3 Nmap Open Port 1



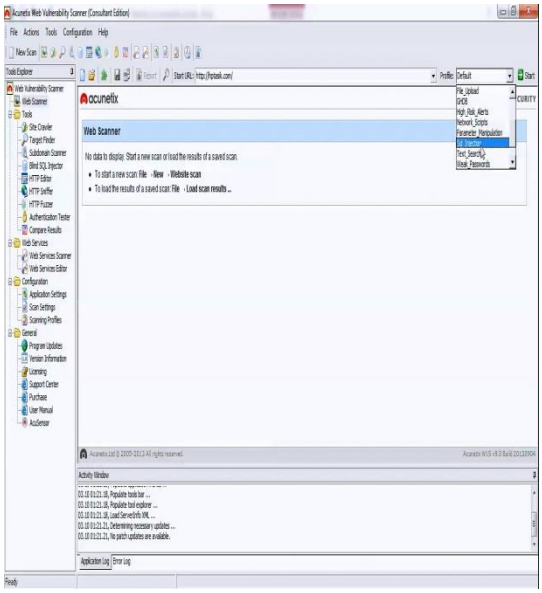
Gambar 1.4 Nmap Open Port 2



Gambar 1.5 Tampilan Web hptasik.com

C. *Scanning Website*

Proses scanning website menggunakan tool Acunetix web vulnerability scanner fungsi nya untuk mencari vulnerability pada website, mode canning ada beberapa jenis ditujukan untuk pencarian vulnerability tertentu, jika memilih default sebagai scanning nya acunetix akan men – scanning semua vulnerability pada website, disini penulis memilih metode pencarian vulnerability dengan tipe SQL Injection.



Gambar 1.6 Tampilan Acunetix Web Vulnerability scanner

Di kolom Start Url di Acunetix penulis memasukan Website yang akan di Scan, di sini penulis memasukan url nya dengan alamat Website http://hptasik.com/ di kolom Profile Acunetix Penulis Memilih Profile “SQL Injection” fungsing nya adalah untuk di tujukan khusus untuk mencari Vulnerability SQL Injection . apa yang akan di cari, disini penulis akan mncari Vulnerability SQL Injection. Dengan memilih Profile Acunetix nya dengan “SQL Injection” dan klik tombol “Start” untuk memulai proses Scanning.

D. *Vulnerability identification*

Setelah proses Scanning Website , Acunetix Akan memberikan Result/Laporan dari Vulnerability yang di temukan.

Result High

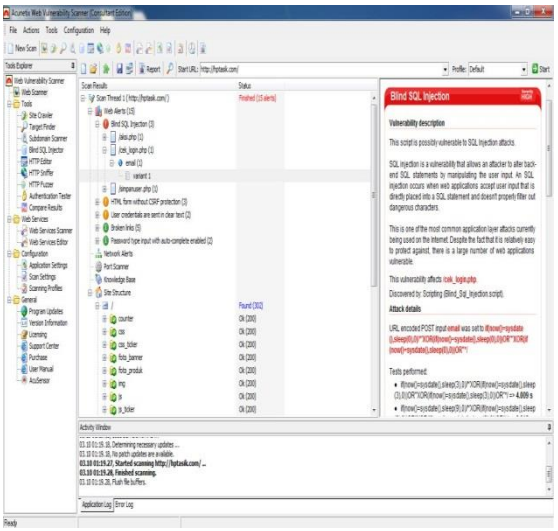
Memberitahukan Vulnerability Sangat berbahaya dan memungkinkan Attacker dapat memamfaatkan nya , untuk masuk kepada system website.

Result Medium

Memberitahukan Vulnerability cukup berbahaya, namun masih cukup susah untuk proses Exploit pada tingkat Medium Result.

Result Low

Memberitahukan Vulnerability cukup aman , dalam Result ini berbentuk Result seperti hasil Crawling pada website contoh nya, Direktori image, url , (.txt) , broken link dll. Tapi tidak bersifat dapat di Exploit. Termasuk kategori Aman.



Gambar 1.7 Result Vulnerability Acunetix

Dari Hasil Result Vulnerability Acunetix telah ditemukan vulnerability SQL Inecjtion pada file php “cek_login.php” dengan method POST pada parameter “email”.

```
POST /cek_login.php HTTP/1.1
Content-Length: 166
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
```

```
Referer: http://hptasik.com/
Cookie:
PHPSESSID=75fb78c484959cf97da6093501a3916a
Host: hptasik.com
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/28.0.1500.63 Safari/537.36
Accept: */*

email=if(now()%3dsysdate()%2csleep(0)%2c0)/*'XOR(if(now()%3dsysdate()%2csleep(0)%2c0))OR'%22XOR(if(now()%3dsysdate()%2csleep(0)%2c0))OR%22*/&password=g00dPa%24%24w0rD
```

Tabel 1.4 Http Header SQL Injection

Table di atas menunjukan sebuah *Vunlnerability* terdapat pada url "*/cek_login.php*" untuk *url* lengkap nya. *"http://hptasik.com/cek_login.php" SQL Injection* terdapat di *Source php "cek_login.php"* dengan *Paramater* nya "*email="* *value* nya "*sample%40email.tst" method post*

E. Implementasi

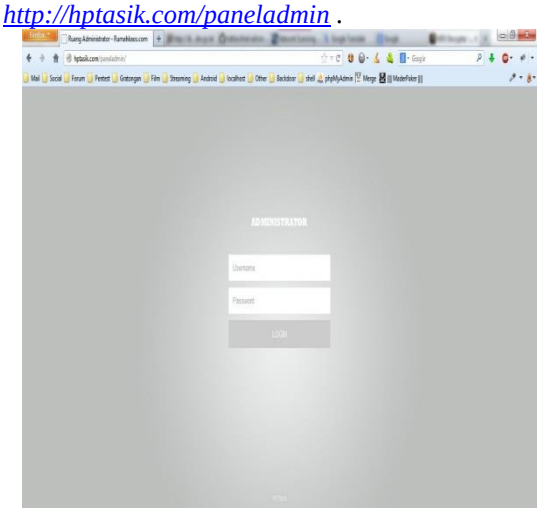
Login Admin Finder

Dalam proses Login Admin Finder penulis menggunakan Tool AdminFinder.py untuk pencari directory login admin. Sebelum nya penulis sudah memiliki data Admin dari proses SQL Injection dengan SQLMap. Tahap login , penulis akan mencoba login dengan data dari hasil SQLMap sebelum nya, dengan data Username(admin), Password(admin666). Proses pencarian admin login page dengan tool adminfinder.py.

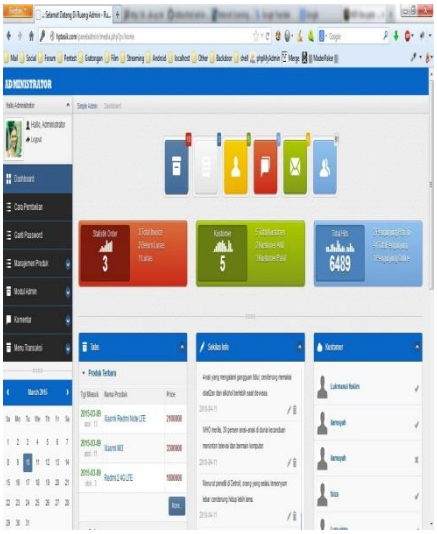
```
Web Site for Scan?: www.hptasik.com
      Checking website www.hptasik.com...
      [$] Yes... Server is Online.
Enter site source code:
1 PHP
2 ASP
3 CFM
4 JS
5 CGI
6 BRF

Press 1 and 'Enter key' for Select PHP

> 1
       [+] Scanning www.hptasik.com...


       [#] Checking www.hptasik.com/admin/...
       [#] Checking www.hptasik.com/administrator/...
       [#] Checking www.hptasik.com/admin1/...
       [#] Checking www.hptasik.com/admin2/...
       [#] Checking www.hptasik.com/admin3/...
       [#] Checking www.hptasik.com/admin4/...
       [#] Checking www.hptasik.com/admin5/...
       [#] Checking www.hptasik.com/usuarios/...
       [#] Checking www.hptasik.com/usuario/...
       [#] Checking www.hptasik.com/administrator/...
       [#] Checking www.hptasik.com/moderator/...
       [#] Checking www.hptasik.com/webadmin/...
       [#] Checking www.hptasik.com/paneladmin/...


>>>www.hptasik.com/paneladmin/ Admin page found!
Press enter to continue scanning.
```

Gambar 2.5 adminfinder

Login admin telah di temukan oleh *tool adminfinder.py* pada page http://hptasik.com/paneladmin .



Gambar 2.6 Panel Admin



Gambar 2.7 Menu Admin

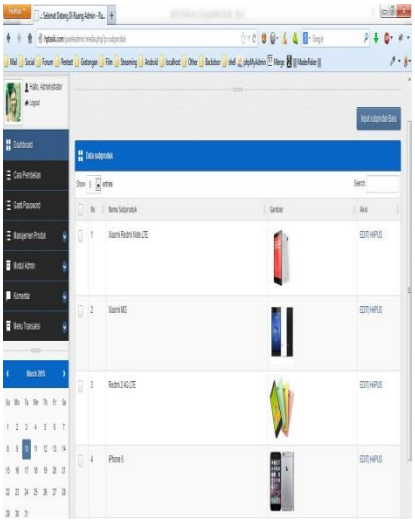
III. HASIL DAN PEMABAHASAN

Pada bagian ini disampaikan tentang objek penelitian dan analisis sistem yang sedang berjalan, juga bentuk rancangan sistem yang penulis lakukan dari penelitian ini.

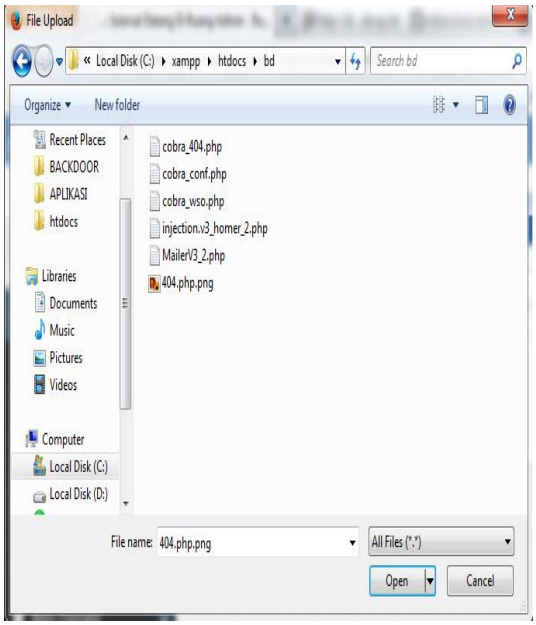
A. Backdoor Website

Proses Backdoor Website adalah membuat pintu masuk untuk seseorang tanpa harus melalu Login Page Admin dan autentifikasi lainnya, Backdoor Website sering di lakukan oleh para Cracker untuk membuat pintu Website tersendiri , disini penulis akan melanjutkan proses upload Backdoor pada Website pada menu admin dengan menggunakan addons Mozilla LiveHttpHeaders , LiveHttpHeaders adalah addons Mozilla digunakan untuk mengulang reqauest pada website dengan merubah kiriman yang akan di kirimkan tetapi memiliki cookies,header dan data dari hasil rekaman data sebelum nya. Upload backdoor akan masukan pada menu sub produk pada

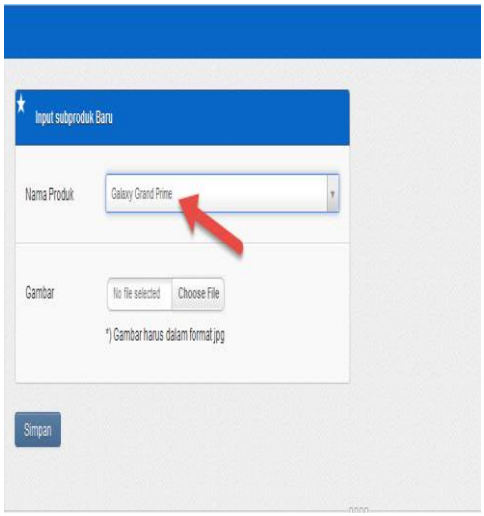
halaman admin , dengan mem bypass file upload png oleh LiveHttpHeaders.



Gambar 2.8 Menu Sub Produk Upload

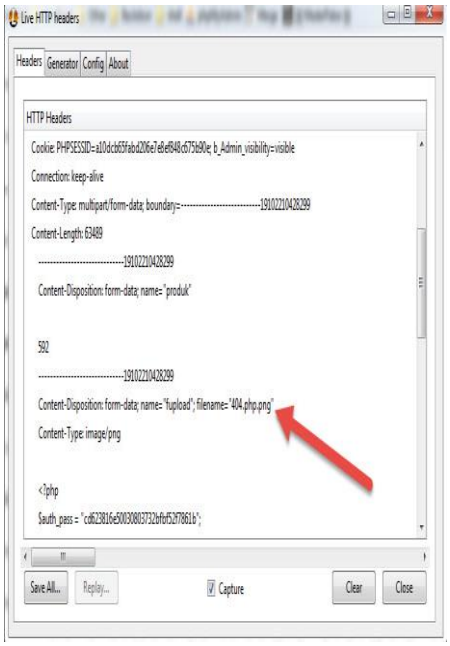


Gambar 3.1 Backdoor 404.php.png

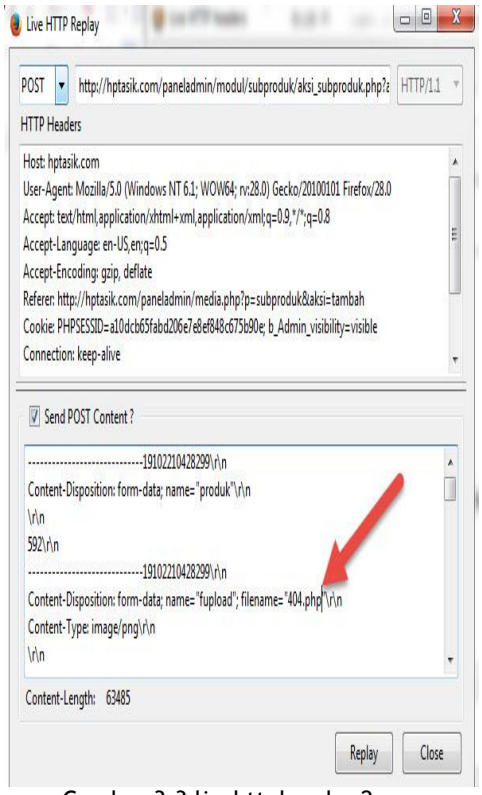


Gambar 2.9 Produk yang akan di upload backdoor

Backdoor yang di upload di rubah *extensi .php* menjadi *.php.png* untuk mem *bypass* upload pada form foto sub produk, nama file *backdoor* menjadi *404.php.png*.

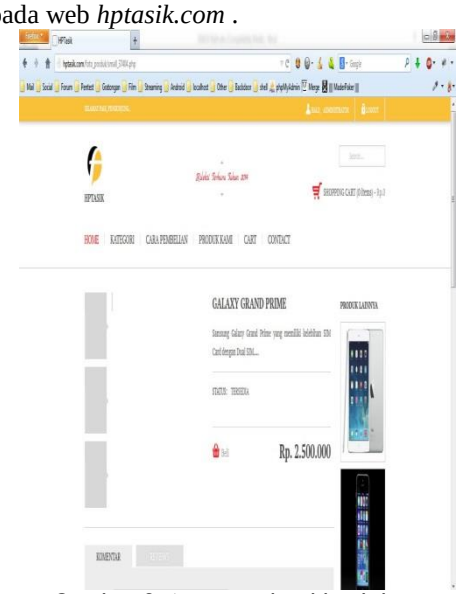


Gambar 3.2 livehttpheader 1



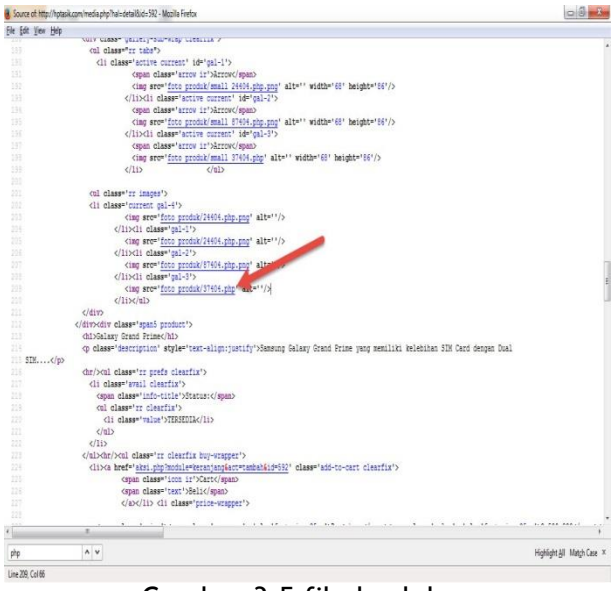
Gambar 3.3 livehttpheader 2

Rubah *extensi 404.php.png* menjadi *404.php* pada *livehttpheader* dan klik tombol *replay* untuk mengirim *request* kembali. Untuk mencari *backdoor* yang sudah di upload pada kategori *"Galaxy Grand Prime"* klik menu *"Galaxy Grand Prime"* pada web *hptasik.com* .

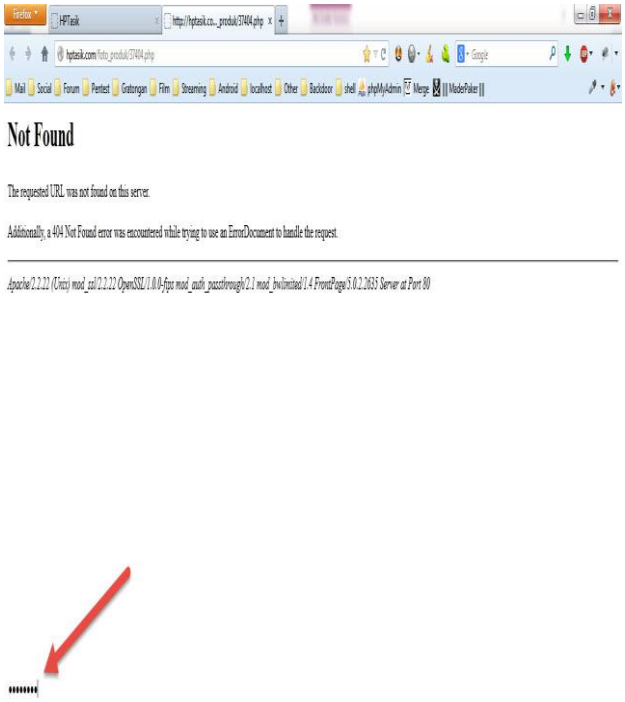


Gambar 3.4 page upload backdoor

Pada Page klik Kanan "View Page Source" untuk mencari file ".php" backdoor telah terupload pada direktori "foto_produk/37404.php" untuk url lengkap nya "http://hptasik.com/foto_produk/37404.php".

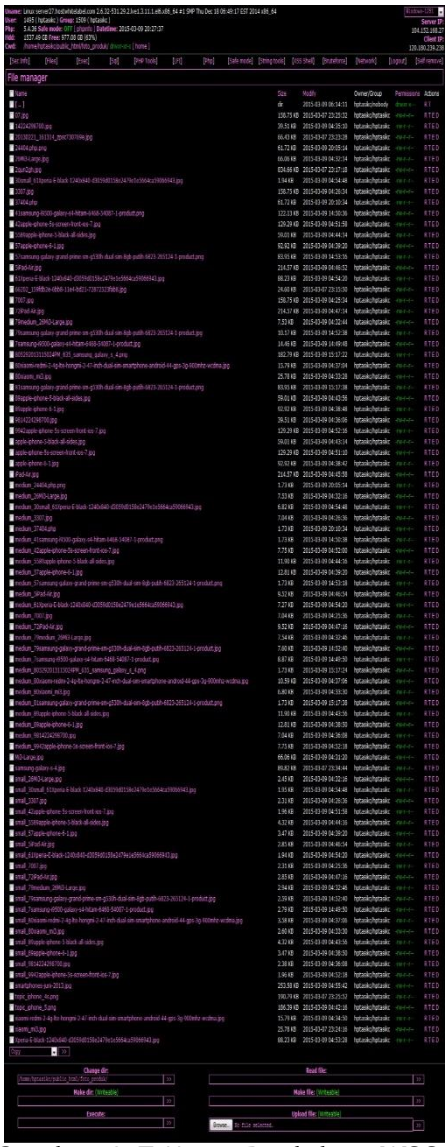


Gambar 3.5 file backdoor

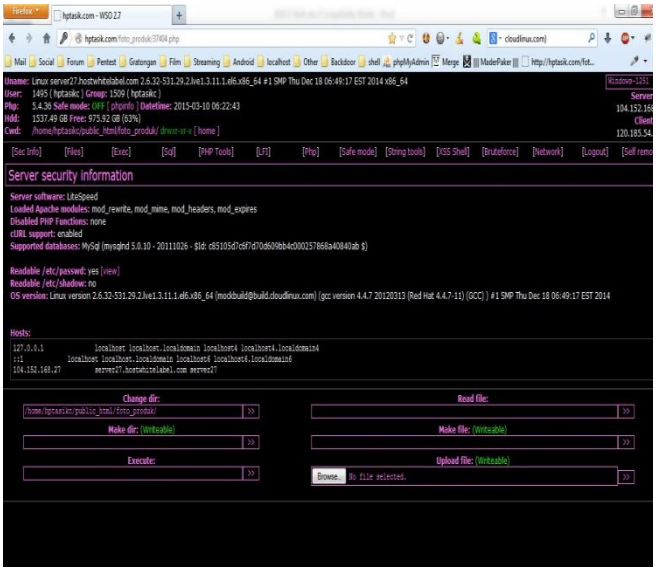


Gambar 3.6 backdoor WSO (*Edited)*

Tampilan WSO yang sudah sedikit di edit oleh penulis, merubah tampilan login menjadi seperti *404 Not Found*, dan di *encrypt* source agar tidak terdeteksi oleh anti virus dari pengelola server *Website*, sekarang penulis akan login ke menu *WSO* dengan *password* (*sauce182)* .



Gambar 3.7 Menu Backdoor WSO

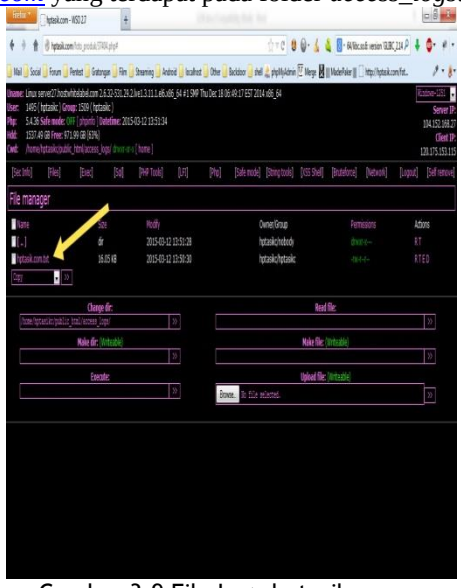


Gambar 3.8 Menu Backdoor WSO 2

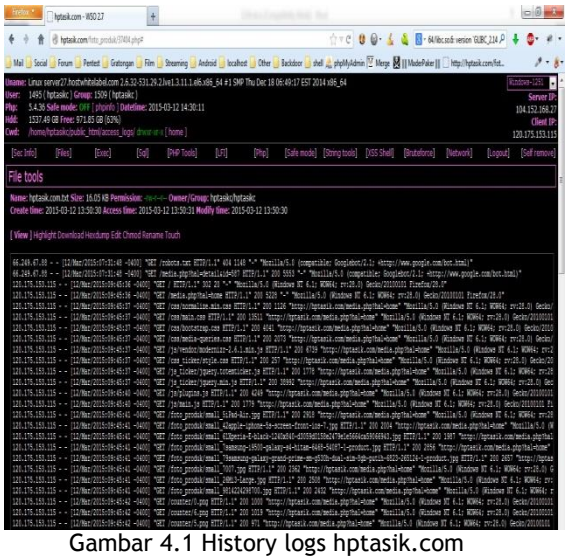
Melalui *Backdoor Website*, *Cracker* bisa mengakses penuh *Website*, dari mulai *deface* ,merubah *source code* , penggantian data pada *database* , *drop database*, memasang *PHP Keylogger* , *Back Connect* , *exploit kernel* dan lain - lain Tergantung tujuan *Cracker* itu sendiri.

B. Covering tracks / Hapus jejak

Covering track, adalah aktifitas menghapus log aktifitas kita pada mesin target. Seperti yang di ketahui, dalam melakukan *covering tracks*, beberapa file yang perlu diperhatikan adalah menghapus *logs* dari aktifitas kita, menyamarkan nama file *backdoor* yang kita tanamkan dan berbagai teknik lainya , dalam kasus ini penulis mengghapus aktifias *logs* dari web www.hptasik.com yang terdapat pada folder *access_logs*.



Gambar 3.9 File Logs hptasik.com



Gambar 4.1 History logs hptasik.com

Setelah file logs *hptasik.com.txt* di temukan. Proses selanjutnya adalah menghapus isi file *logs* tersebut untuk

menghapus semua aktifitas yang telah dilakukan. Supaya tidak di ketahui oleh pemilik *website*.

IV. KESIMPULAN

SQL Injection merupakan teknik hacking paling populer pada aplikasi web dengan prinsip melewatkan perintah-perintah SQL lewat aplikasi web untuk dieksekusi oleh database back-end. Kelemahan akan muncul apabila inputan user tidak disaring/difilter dengan sempurna dan akhirnya dieksekusi. Oleh karena itu diperlukan suatu pengamanan yang extra hati – hati pada SQL statement pada database yang ada pada suatu website-website kita, agar perintah-perintah SQL injection tersebut dapat disaring dengan baik. Demikian halnya dengan Setting server dengan benar memang akan mengamankan e-commerce web dari serangan *Deface* , *Drop Database, dll*. Semuanya tergantung dari kita bagaimana cara kita untuk selalu turus update dalam penanganan masalah ini. Karena tentunya para-para *cracker* tersebut selalu mengembangkan *bug-bug* mereka untuk dapat menemukan lubang-lubang pada jaringan kita. Oleh karena itu sebelum kita menjadi *defender* yang kuat, alangkah baiknya kita mengetahui dan mempelajari terlebih dahulu serangan-serangan para *cracker* tersebut, serta kita bisa menjadi *pentester* pada sistem kita sendiri.

DAFTAR PUSTAKA

[1] Emily Chow, 1 july 2011 , Ethical Hacking and Penetration Testing.
[2] Randy Glasbergen , Certified Ethical Hacking v5 Module 12 : Web Application Vulnerabilities
[3] OWASP Foundation , OWASP : Modern Information Gathering
[4] Anjar Priandoyo, 2006 : Vulnerability assessment
[5] Kementerian Komunikasi dan Informatika , GOV-CSIRT, 2012
[6] Aileen G. Bacudio, Xiaohong Yuan, Bei-Tseng Bill Chu, Monique Jones, International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, November 2011
[7] Shubham Srivastava , International Journal of Computer Science & Engineering Survey (IJCSES) Vol.3, No.3, June 2012: A Survey Of Sql Injection Countermeasures
[8] Shanmughaneethi , IOSR Journal of Computer Engineering (IOSRJCE) Detection of SQL Injection Attack in Web Applications using Web Services
[9] Shubham Srivastava , (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (4) , 2012,4747 - 4750 : Web Security and Classification of Different Types of Attack for Web
[10] Joseph Giron , 2009 , Web Shells