ANALISIS KELEMAHAN *CROSS SITE SCRIPTING* PADA PHP *NUKE* UNTUK KEAMANAN *WEBSITE*

The Analysis of the Weakness of Cross Site Scripting in PHP Nuke For Website Security

Imam Riadi[1], Jazi Eko Istiyanto[2]

Program Studi Ilmu Komputer
Program Pascasarjana Universitas Gadjah Mada

ABSTRACT

The problem of exploitation system of web portal through vulnerability of Cross Site Scripting of PHP Nuke 5.2 is becoming a crucial topic. It is found by CERT in september 2002. The appearance of the problem of the system web portal represent the shares is different from attending of open program system a system application of web portal whic is obtained easily and free of charge.

A group of one who can be told as attacker have the very circumstantial knowledge about the system of security of web portal. This matter supports a good program ability use of the PHP and its correctness learn the source code of document and antirety article have a similar purpose that is to look for the vulnerabilitas from an existing program. A system of web portal also has the risk factor and the high threat effect of incured by attack of Cross Site Scripting will water down the attacker conducting the infiltration into system of web portal use PHP Nuke application

CERT on 18 September 2002 through the information at her website wrote about vulnerability Cross Site Scripting from PHP Nuke. It criticize that file admin.php whic do not use authentication administrator at the command **copy** with the variable **$upload** so that attacker can exploit this weakness by copying the certain file in web portal as the attacker like. The researcher chose exploitation program of security through Cross Site Scripting as the object on the thesis. As a supported facility data from conveying problems of security and text book related to parsing parameter in PHP Programming.

Keywords : *Exploitation, Cross Site Scripting, Website, Analysis, Vulnerability, PHP Nuke.*

---

[1] Fakultas MIPA Universitas Ahmad Dahlan, Yogyakarta
[2] Fakultas MIPA Universitas Gadjah Mada, Yogyakarta

PENGANTAR

Saat ini *website* lebih kompleks dibandingkan sebelumnya, terdiri dari banyak isi yang dinamis sehingga memudahkan pengguna. Isi *website* yang dinamis akan dapat menampilkan hasil yang berbeda untuk pengguna sesuai dengan konfigurasi dan kebutuhan yang diinginkan. Salah satu teknologi baru yang mendorong pengembangan *website* secara dinamis untuk membangun web portal adalah PHP *Nuke*.

PHP *Nuke* adalah sebuah *software* pembangun *web portal* instan dengan menggunakan bahasa pemrograman PHP. Dengan teknologi ini *website* akan mempunyai sebuah sistem dimana pengunjung dapat mengirimkann sebuah artikel atau berita, berinteraksi dengan pengunjung lain, dan fungsi-fungsi lain yang dapat ditambahkan. Dengan demikian, *website* tersebut mempunyai sebuah komunitas *online*. Beberapa *web portal* yang menggunakan PHP *Nuke* mempunyai suatu ancaman serangan yang dapat merugikan pengguna. Dengan banyaknya kelemahan yang ada dalam PHP *Nuke* maka dapat menimbulkan permasalahan dalam keamanan *web portal* tersebut.

Kemudahan pengaksesan *website* dari berbagai tempat dan kesalahan konfigurasi akan menimbulkan resiko dalam masalah keamanan. Maka masalah keamanan *website* menjadi masalah yang pokok dalam suatu sistem *online* yang berbasis pada halaman *web*. Salah satu ancaman yang paling umum selain virus adalah pemanfaatan *scripts* untuk memperoleh akses ke dalam sistem. Dengan menggunakan *scripts* dapat menampilkan informasi dan menghubungkannya dengan basis data atau program seperti *e-commerce*.

Masalah keamanan *website* yang disebabkan oleh kelemahan dari pemrograman *scripting* sering dikenal dengan *Cross Site Scripting* (XSS). Kelemahan ini dapat terjadi ketika suatu layanan aplikasi *web* mengumpulkan informasi data dari seorang pengguna. Biasanya seorang penyerang (*attacker*) akan merubah informasi dari *link* menggunakan beberapa pengkodean sehingga tidak mencurigakan pengguna ketika menggunakan layanan tersebut.

Informasi tentang serangan *Cross Site Scripting* kurang mendapat perhatian dari para pengguna layanan *website* yang dinamis (Schremptf, 2000).

Cross-Site Scripting dapat terjadi ketika suatu aplikasi *web* menjalankan perintah-perintah tertentu dari seorang penyerang. Data ini biasanya diserang dengan memanfaatkan *hyperlink* atau menuliskan secara langsung perintah tertentu pada *browser*. Penyerang akan menjalankan *script* yang telah dimanipulasi untuk tujuan tertentu. Setelah data yang diinginkan diperoleh akan ditampilkan pada halaman yang diinginkan oleh penyerang.

Dengan pemahaman perintah dan variabel yang ada dalam bahasa pemrograman PHP, khususnya perintah **copy** dan variabel **$upload** yang kurang diperhatikan (kesalahan implementasi), dapat mengakibatkan serangan *Cross Site Scripting* pada sistem *web portal* yang menggunakan PHP *Nuke*. Dengan adanya serangan *Cross Site Scripting* mengakibatkan penyerang mampu melakukan eksploitasi sistem sehingga dapat memperoleh *account* administrator dari *web portal* tersebut (CERT, 2001; 2002a, b, c, dan 2003).

CARA PENELITIAN

Bahan Penelitian

- *Source code program diambil dari* www.*sourceforge*.net/*projects* sebagai bahan penelitian utama
- Pustaka-pustaka untuk melakukan pembuktian vulnerabilitas *Cross Site Scripting*.

Peralatan *Software*

- Windows XP *Profesional* digunakan sebagai *server web portal*
- Windows XP *Home Edition* digunakan sebagai *client*.
- PHP *Nuke* 5.2 tar
- Program editor seperti, *editplus*, PHP Editor, *notepad*, Vi, dll.

Peralatan *Hardware*

- Pentium III 450Hz RAM 128MB, HD 20GB, Terkoneksi pada sistem jaringan Intranet.
- *Notebook* Toshiba, Pentium IV 2,5 GHz, RAM 256MB, HD 30GB, terkoneksi pada jaringan Intranet

Prosedur Pelaksanaan

- Melakukan debug *source code file* **admin.php** dalam bahasa PHP untuk mengetahui algortima eksploitasi PHP *Nuke* 5.2 tar
- Membuat *patch* program *file* **admin.php** dalam *web portal* yang menggunakan PHP *Nuke* untuk mengatasi masalah kelemahan serangan *Cross Site Scripting*.

- Membuktikan kebenaran dari issue yang berkembang di Internet mengenai adanya Vulnerabilitas *Cross Site Scripting* pada PHP *Nuke* 5.2 tar dengan mencari landasan teori hasil algoritma yang diperoleh dari pustaka-pustaka yang ada (*text book*, dokumen, artikel, buletin, dll.)

Analisa Hasil

Hasil penelitian yang berupa *file* **admin.php** yang sudah di*patch*, sudah tidak terdapat kelemahan terhadap serangan *Cross Site Scripting* sehingga usaha penyerang (*attacker)* untuk mendapatkan *account* administrator *web portal* yang menggunakan PHP *Nuke* tidak bisa dilakukan lagi.

HASIL DAN PEMBAHASAN

Analisis program dilakukan melalui debug *source code* bahasa pemrograman PHP untuk eksploitasi vulnerabitlitas *Cross Site Scripting* pada **PHP *Nuke* 5.2.tar**. Algoritma program eksploitasi ada 3 fase dimulai dari mengakses *web portal* yang dituju (target), mengecek vulnerabilitas dan menyalin *file* **config.php** menjadi *file* yang bisa di*download* pada lokasi tertentu, men*download file* hasil salinan sampai dengan proses eksploitasi **PHP *Nuke* 5.2.tar.**

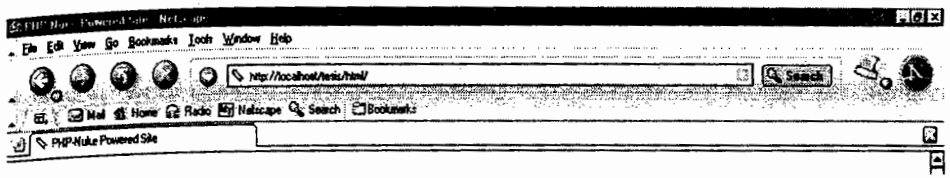
Disini akan nampak bagaimana penyerang berhasil melakukan penyalinan *file* **config.php** untuk mendapatkan *account* administrator. Dalam hal ini penyerang memanfaatkan keteledoran programmer aplikasi PHP *Nuke*, yaitu tidak adanya autentikasi administrator pada perintah **copy** dengan variabel **$upload** dalam *file* **admin.php** yang seharusnya menggunakan proses autentikasi administrator.

Algoritma Program Eksploitasi

Fase ke1 : Mengakses *Web Portal* yang dituju

Dalam percobaan fase ke-1, diilustrasikan langkah-langkah yang harus dilakukan dalam mengakses *web portal* yang dituju, sebagai berikut :

```
http://localhost/tesis/html
```



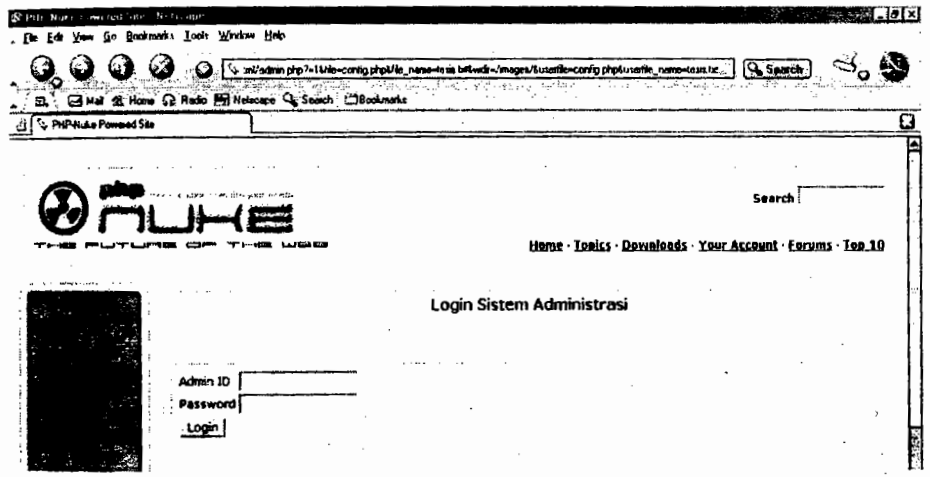
Gambar 4.1. Proses pengaksesan *web portal*

Pada fase ke-1, merupakan bentuk pengaksesan *web portal* menggunakan *browser* untuk mengakses *web portal* yang akan dijadikan target.

Fase ke 2 : Mengecek Kelemahan dan Menyalin *File* config.php

Dalam percobaan fase ke-2, diilustrasikan langkah-langkah yang harus dilakukan dalam mengakses *web portal* yang dituju dengan menambahkan beberapa perintah tertentu pada *browser* sebagai berikut.

```
http://localhost/tesis/html/admin.php?upload=1&file=config.php&
file_name=tesis.txt&wdir=/&userfile=config.php&userfile_name=tesis.txt
```



Gambar 4.2. Proses pengecekan dan penyalinan *file*

Deretan perintah yang dituliskan pada browser diatas adalah untuk melakukan pengecekan vulnerabilitas *Cross Site Scripting* pada *file* **admin.php**. Dari ilustrasi tersebut diatas terdapat vulnerabilitas *Cross Site Scripting*, yang diakibatkan oleh variabel **$upload** dan perintah **copy** yang ada dalam *file* **admin.php** tidak melakukan proses autentikasi administrator, sehingga penyerang dapat memanfaatkan kelemahan isi *script* file **admin.php** seperti ilustrasi berikut ini.

```
$basedir = dirname($SCRIPT_FILENAME);
$textrows = 20;
$textcols = 85;
$udir = dirname($PHP_SELF);
if(!$wdir) $wdir="/";
if($cancel) $op="FileManager";
if($upload) {
   copy($userfile,$basedir.$wdir.$userfile_name);
   $lastaction = "". _UPLOADED." $userfile_name --> $wdir";
   $wdir2="/";
   chdir($basedir . $wdir2);
   Header("Location: admin.php?op=FileManager");
   exit;
}
```

dengan menuliskan pada *browser* alamat diikuti parsing parameter tertentu, maka penyerang akan dapat melakukan proses penyalinan *file*.

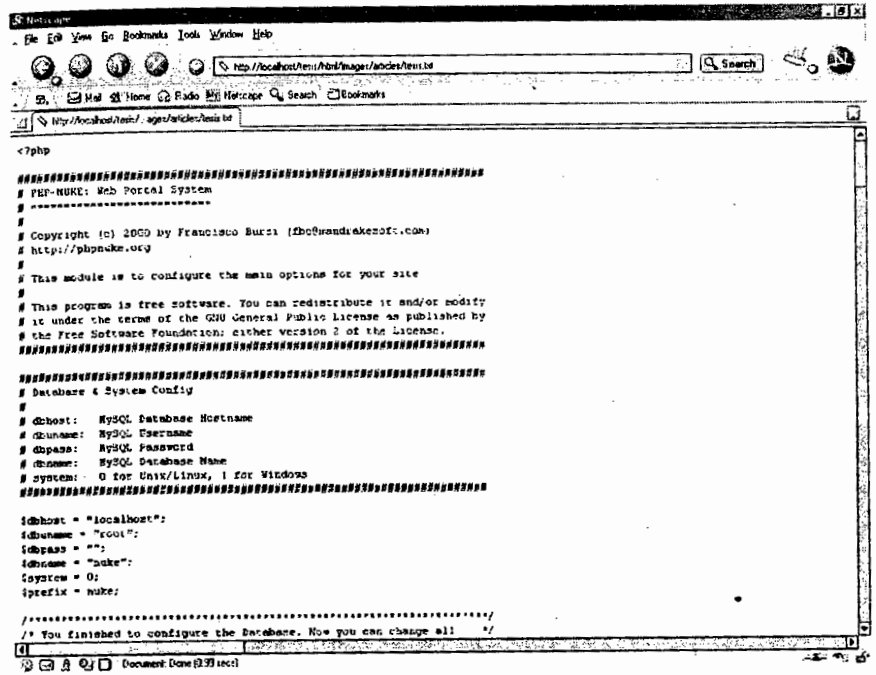
```
http://localhost/tesis/html/admin.php?upload=1&file=config.
php&file_name=tesis.txt&wdir=/&userfile=config.php&
userfile_name=tesis.txt
```

Pada perintah diatas terlihat bahwa perintah copy dengan diikuti parsing parameter tertentu dapat melakukan proses penyalinan *file* config.php menjadi *file* tesis.txt pada direktori images pada direktori PHP *Nuke*.

Fase ke 3 : Men*download file* hasil salinan

Dalam percobaan phase ke-3, diilustrasikan langkah-langkah untuk melihat atau men*download file* hasil salinan **config.php** yang dapat dilakukan seperti berikut ini.

```
http://localhost/tesis/html/images/articles/tesis.txt
```



Gambar 4.3. Proses *download file* hasil salinan

Dengan mengakses secara langsung *file* pada tempat direktori kita menyalin *file* **config.php**, maka akan ditampilkan isi *file* **tesis.txt** yang berisi sama persis dengan *file* **config.php**, dimana dalam *file* **config.php** tersimpan *username*, *password* dan nama *database* yang dapat digunakan penyerang untuk memasuki *web portal* dengan hak akses administrator *web* tersebut.

Dari hasil analisis yang dilakukan untuk mengatasi masalah kelemahan *Cross Site Scripting* pada *web portal* yang menggunakan PHP *Nuke*, didapatkan hasil penelitian seperti berikut.

a. *File* **admin.php** terutama pada proses *upload* ditambahkan suatu variabel **$admintest** yang berfungsi untuk memeriksa autentikasi administrator. Variabel **$admintest** adalah salah satu variabel

dalam *file* **admin.php** yang berfungsi untuk menangani proses login administrator *web portal*. Perubahan dapat dilakukan seperti berikut ini :

```
"if($upload) {"
```

dirubah menjadi

```
"if (($upload) && ($admintest)) {"
```

b. *File* **admin.php** terutama pada proses *upload* ditambahkan suatu fungsi pengalihan (*redirect*) ke halaman tertentu sesuai dengan keinginan *programmer* apabila diketahui ada pengguna selain administrator. Perubahan dapat dilakukan seperti berikut ini :

```
$basedir = dirname($SCRIPT_FILENAME);
$textrows = 20;
$textcols = 85;
$udir = dirname($PHP_SELF);
if(!$wdir) $wdir="/";
if($cancel) $op="FileManager";
if($upload)
{
 if (!$admintest)
 {
   Header("Location: index.php"); // <----- fungsi redirect
   exit;
 }
 else
 {
   copy($userfile,$basedir.$wdir.$userfile_name);
   $lastaction = "".UPLOADED." $userfile_name --> $wdir";
   $wdir2="/";
   chdir($basedir . $wdir2);
   Header("Location: admin.php?op=FileManager");
   exit;
}}
```

c. *File* **admin.php** terutama pada proses *upload* ditambahkan pemeriksaan *cookies* untuk menentukan kewenangan *user* dalam melakukan proses penyalinan *file*. Perubahan dapat dilakukan seperti berikut ini.

```
$basedir = dirname($SCRIPT_FILENAME);
$textrows = 20;
$textcols = 85;
$udir = dirname($PHP_SELF);
if(!$wdir) $wdir="/";
if($cancel) $op="FileManager";
if(($upload) && ($admin)) //<---- baca cookie
{
   copy($userfile,$basedir.$wdir.$userfile_name);
   $lastaction = "".UPLOADED." $userfile_name --> $wdir";
   $wdir2="/";
chdir($basedir . $wdir2);
   Header("Location: admin.php?op=FileManager");
   exit;
}
```

KESIMPULAN

Kesimpulan yang dapat diambil dari hasil analisis program eksploitasi kelemahan *Cross Site Scripting* pada **PHP *Nuke* 5.2.tar** adalah sebagai berikut :

1. *File* **admin.php** pada **PHP *Nuke* 5.2.tar** mempunyai kelemahan terhadap serangan *Cross Site Scripting*, yaitu pada perintah **copy** dan variabel **$upload** tidak ada proses autentikasi administrator.
2. *Patch* program *file* **admin.php** dibuat berdasarkan kelemahan yang ditemukan dengan menambahkan pengecekan autentikasi administrator.
3. Informasi pada *website Computer Emergency Response Team* (CERT® Advisory, VU#933955) mengenai terdapatnya lubang keamanan *file* **admin.php** terhadap serangan *Cross Site Scripting* pada *web portal* yang menggunakan **PHP-*Nuke*-5.2.tar** adalah benar.

DAFTAR PUSTAKA

Anonymous, 1998, ***Maximum Security : A Hacker Guide To Protecting Your Internet Site and Network,*** Second Edition, Sams Publishing.

Apache Software Foundation, 2002, ***Apache Manual,*** http://www.apache.org/

CERT® Advisory, VU#933955, 18 September 2002a, ***"PHPNuke 'admin.php' script does not adequately authenticate users, thereby allowing malicious user to copy, move, or upload files".***

CERT® Advisory, VU#739211, 18 September 2002b, ***"PHP-Nuke does not adequately authenticate users thereby allowing attackers to change user information".***

CERT® Advisory, VU#488684, 9 Oktobrt 2003, ***"Hummingbird CyberDOCS contains multiple cross-site scripting vulnerabilities".***

CERT® Advisory, VU#240329, 10 Februari 2002c, ***"Apache HTTPD server vulnerable to cross site scripting on error page when using wildcard DNS".***

CERT® Advisory, VU#847803, 25 Juli 2001, ***"Php variables passed from the browser are stored in global context".***

Fransisco Burzi, ***PHP Nuke Manual,*** www.phpnuke.org

Rahardjo, Budi, 1999, ***"Keamanan Sistem Informasi Berbasis Internet",*** PT. Insan Komunikasi Informasi, Bandung.

Rasmus Lerdof, 2002, ***PHP Manual,*** http://www.php.net/

Schremptf, H., 2000, ***Cross Site Scripting,*** http://www.microsoft.com/Technet/security/ExSumCS.asp,

SPI Dynamics, , 2002, ***Cross Site Scripting,*** Atlanta.

Stallings, William, 2000, ***Network Security Essentials Application and Standards,*** Prentice Hall, Inc, New Jersey.

Suryatmoko, S, 2003, ***Membuat Web Portal dengan PHP Nuke,*** Elex Media Komputindo, Jakarta.