

Software Testing pada Aplikasi Website PT Semen Tonasa menggunakan Metode Assessment Vulnerability

Software Testing on PT Semen Tonasa Website Application using Vulnerability Assessment Method

Reza Maulana¹⁾ Indrawan Liwanto²⁾, Christouvel Lucman³⁾

¹⁾Fakultas sains dan teknologi,prodi sisitem informasi, uin alauddin makassar

^{2,3)}Sekolah Tinggi Manajemen Informatika & Komunikasi Kharisma Makassar

^{2,3)}Jl. Baji Ateka No.20, Makassar, 90134, Telp. 0411-871555 – 871968, Fax. 0411-870098

E-mail: ¹⁾saya@rezamaulana.com ²⁾indrawan_14@kharisma.ac.id¹, ³⁾christouvel_14@kharisma.ac.id

Abstrak – Ancaman terhadap sebuah aplikasi website sangat mungkin terjadi dan sangatlah sulit untuk mengatakan bahwa aplikasi website akan aman dan bebas ancaman atau serangan dari attacker. Sebuah aplikasi website yang terhubung dengan koneksi jaringan komputer akan diakses semua pihak sehingga ancaman selalu ada mengintai. Cara analisa dari aplikasi website yakni dengan mencari kelemahan-kelemahan yang bisa menjadi pintu masuk seorang attacker. Istilah yang sering digunakan dalam menganalisa kelemahan aplikasi website yaitu analisa vulnerability assessment. Cara melakukan analisa ini yaitu dengan menggunakan teknik String Based Sql Injection. Dengan menggunakan teknik ini attacker dapat menganalisa serta mendapatkan kelemahan-kelemahan yang dimiliki aplikasi website.

Kata Kunci: Software Testing, Vulnerability, Website Testing, Security Test

Abstract –Threats to a website application is likely to occur and it is difficult to say that the application site will be safe and free of threats or attacks from the attacker. A website application that is connected to the computer's network connection will be accessible to all parties so that there is always a lurking threat. How to analysis of a website application that is by looking for weaknesses that could be the entrance to an attacker. The term is often used in analyzing the weaknesses of a website application that analyzes the vulnerability assessment. How to perform this analysis is by using the String Based Sql Injection techniques. By using this technique the attacker can analyze and get weaknesses from website application.

Keywords: Software Testing, Vulnerability, Website Testing, Security Test

PENDAHULUAN

Pengukuran kualitas perangkat lunak sangat diperlukan sebelum sebuah aplikasi akan dirilis atau diluncurkan, hal ini berfungsi untuk menguji maturitas dari sebuah perangkat lunak. Tujuan utama dari pengujian ini adalah untuk meyakinkan kepada pelanggan bahwa sistem tersebut layak untuk digunakan dan memenuhi kinerja persyaratan. Agar perangkat lunak dapat terjamin kualitasnya, maka diperlukan pengendalian, pengujian dan pengelolaan yang mengacu pada kualitas perangkat lunak. Jaminan kualitas perangkat lunak merupakan aktivitas

mendasar dalam berbagai bidang perusahaan yang menghasilkan produk yang digunakan oleh pengguna.

Peneliti mengetes aplikasi berbasis *website* yang dimiliki oleh PT Semen Tonasa berdasarkan *Security Test* pada *web* perusahaan yaitu *sementonasa.co.id*.

METODOLOGI PENELITIAN

Penelitian dilakukan dengan menggunakan metode Vulnerability. Penelitian dilakukan pada tanggal 13 Juni 2016.

Registrant Email:atjom@sementonasa.co.id	Billing State/Province:Sulawesi Selatan
Admin ID:01160472prsd	Billing Postal Code:90651
Admin Name:Atjo Muchlis	Billing Country:ID
Admin Organization:PT SEMEN TONASA	Billing Phone:+081.1466851
Admin Street1:Biringere – Pangkep	Billing Email:atjom@sementonasa.co.id
Admin City:Pangkep	Sponsoring Registrar ID:digitalreg
Admin State/Province:Sulawesi Selatan	Sponsoring Registrar Organization:Digital Registra
Admin Postal Code:90651	Sponsoring Registrar Postal Code:55281
Admin Country:ID	Sponsoring Registrar Country:ID
Admin Phone:+081.1466851	Sponsoring Registrar Phone:0274882257
Admin Email:atjom@sementonasa.co.id	Name Server:NS1.SEMENTONASA.CO.ID
Tech ID:01160472prsd	Name Server:NS2.SEMENTONASA.CO.ID
	DNSSEC:Unsigne

Gambar 1 Hasil *Ping* ke *Server*

Gambar 2 Letak Geografis *IP*

Setelah itu peneliti mencoba mengakses beberapa halaman situs sementonasa.co.id untuk mencari *string* alamat *web* yang rentan, seperti `.php?namavariabel=nilaivariabel`.

Pertama peneliti mengakses situs *whois.net* kemudian menginput alamat *web* Semen Tonasa untuk mendapat informasi mengenai alamat tersebut.

sementonasa.co.id/berita.php?thn=2014

sementonasa.co.id is already registered*

Domain ID:PANDI-DO42379	Tech Name:Atjo Muchlis
Domain Name:SEMENTONASA.CO.ID	Tech Organization:PT SEMEN TONASA
Created On:13-Feb-2004 13:22:59 UTC	Tech Street1:Biringere - Pangkep
Last Updated On:30-Sep-2014 00:57:04 UTC	Tech City:Pangkep
Expiration Date:01-Oct-2016 23:59:59 UTC	Tech State/Province:Sulawesi Selatan

```

C:\Users\Indra Livanto>ping sementonasa.co.id

Pinging sementonasa.co.id [222.124.178.89] with 32 bytes of data:
Reply from 222.124.178.89: bytes=32 time=96ms TTL=55
Reply from 222.124.178.89: bytes=32 time=112ms TTL=55
Reply from 222.124.178.89: bytes=32 time=69ms TTL=55
Reply from 222.124.178.89: bytes=32 time=100ms TTL=55

Ping statistics for 222.124.178.89:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 69ms, Maximum = 112ms, Average = 92ms

C:\Users\Indra Livanto>_

```

sementonasa.co.id/berita.php?thn=20'-14

Status:ok Registrant ID:01160472prsd	Tech Postal Code:90651
Registrant Name:Atjo Muchlis	Tech Country:ID
Registrant Organization:PT SEMEN TONASA	Tech Phone:+081.1466851
Registrant Street1:Biringere – Pangkep	Tech Email:atjom@sementonasa.co.id
Registrant City:Pangkep	Billing ID:01160472prsd
Registrant State/Province:Sulawesi Selatan	Billing Name:Atjo Muchlis
Registrant Postal Code:90651	Billing Organization:PT SEMEN TONASA
Registrant Country:ID	Billing Street1:Biringere - Pangkep
Registrant Phone:+081.1466851	Billing City:Pangkep

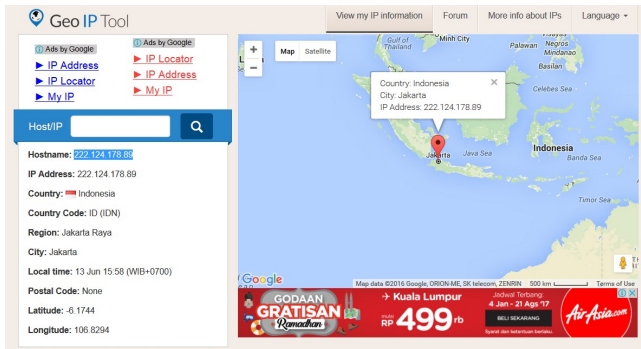


Selanjutnya peneliti mencoba *ping* ke *server* sementonasa.co.id untuk mencari tahu apakah ada *reply* dari server atau tidak dan juga untuk mendapatkan *IP* server, yang nantinya akan digunakan untuk mencari tahu letak geografis dari *IP* yang digunakan.

Gambar 3 Alamat dan Tampilan *Web*

Setelah ditemukan, peneliti menggunakan teknik *String Based Sql Injection* untuk mencari tahu apakah ada kelemahan pada *string* alamat tersebut.

Gambar 4 Alamat yang telah diubah dan Hasil



Tampilannya



Gambar 5 Alamat yang telah diubah dan Hasil

KESIMPULAN

Hasil dari penelitian menunjukkan bahwa suatu aplikasi website harus memiliki tingkat keamanan yang tinggi agar data penting website tidak mudah diakses, dimodifikasi, maupun dihapus. Untuk kedepannya diharapkan penelitian ini dapat berguna untuk meningkatkan keamanan pada aplikasi website. Penulis juga berharap semoga penelitian ini dapat berguna bagi pembaca.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Reza Maulana, S.Kom., M.T. selaku dosen mata kuliah *Software Testing* yang telah membimbing dalam kegiatan ilmiah ini. Tak lupa juga Penulis mengucapkan terima kasih kepada teman-teman sekelas yang telah membantu dalam penelitian ini.

DAFTAR PUSTAKA

Amin, Zaid., (2012), Analisa Vulnerabilitas Host pada keamanan jaringan computer di PT. SUMEKS TIVI Palembang (PALTV) Menggunakan Router Berbasis Unix. Jurnal Teknologi dan Informatika (TEKNOMATIKA) Vol 2 No 3 September 2012.

eprints.dinus.ac.id/12051/1/jurnal_11901.pdf

Gupta, Anika, dkk., (2013), Vulnerability Assessment and Penetration Testing, International Journal of Engineering Trends and Technology-Volume 4 Issue 3-2013.

Hidayat, Jonny., (2014), CEH Certified Ethical Hacker. Jasakom Publishers

S'to., (2014), Kali Linux 200% Attack. Jasakom Publishers

Dari hasil tersebut dapat diketahui bahwa adanya *error* pada aplikasi website Semen Tonasa.

HASIL DAN PEMBAHASAN

Setelah mendapat *error* tersebut, Peneliti melakukan percobaan lebih lanjut dengan memanfaatkan *error* yang ada dan kemudian mendapatkan *database mysql* milik *server*.

- tonasa
- information_schema
- mysql
- p15
- test
- tonasa1

Hasil dari percobaan tersebut menunjukkan bahwa tingkat keamanan pada aplikasi *website* Semen Tonasa sangat lemah, *database* dengan mudah dapat diakses.

Hal ini tentu saja dapat berakibat sangat fatal jika data didapatkan oleh pihak yang tidak bertanggung jawab. Data bisa saja dimodifikasi/dihapus atau disisipkan virus yang dapat merusak komputer *server*.

Sekalipun suatu data hanya bersifat informatif, tetapi jika data tersebut dapat diakses maka dapat disimpulkan aplikasi *website* tersebut telah gagal dalam hal *Security Test*.

Zam,Efvy,(2011),Trik Megamankan Website dari
Aksi Hacking.Elex Media Komputindo