Website Security Analysis Using Penetration Testing Method

by rumahjurnalunived@gmail.com 1

Submission date: 03-Jan-2022 12:56AM (UTC-0500)
Submission ID: 1737021727
File name: 428-1487-1-SM.doc (152K)
Word count: 2466
Character count: 16795

GATOT KACA JOURNAL
Jurnal Keilmuan Teknik: Aplikasi, Perencanaan, Rancang Bangun, Sistem, Simulasi, & Rekayasa

Analisis Keamanan Webstie Menggunakan Metode Peneteration Testing

Tio Rahmadi [1]; Khairil [2]; Reno Supardi [2]
[1,2] *Program Studi Informatika, Fakultas Ilmu Komputer, Universitas Dehasen Bengkulu*
Email: [1] tioorahmadi@gmail.com

How to Cite :
Rahmadi, T., Khairil., Supardi, R. (2021). Analisis Keamanan Webstie Menggunakan Metode Peneteration Testing. Gatotkaca Journal, 2(2). DOI:

ARTICLE HISTORY
Received [xx Month xxxx]
Revised [xx Month xxxx]
Accepted [xx Month xxxx]

KEYWORDS
Website Security, Cyber, Penetration Testing, Self Test, Zero Entry Hacking

ABSTRAK
Penetration testing merupakan salah satu metode untuk mengamankan website dari serangan orang atau hacker yang tidak bertanggung jawab. Dengan metode ini para pemilik website dapat mengetahui letak kerentanan yang terdapat pada website. Tujuan dari penelitian ini adalah menguji tingkat keamanan pada suatu website. Metode penetration testing yang digunakan yaitu metode Zero Entryhacking dengan 4 tahapan, yaitu reconnaissance (pengintaian), scanning (pemindaian), exploitation (eskploitasi), dan post exploitation and maintaining access (Pasca Eksploitasidan Mempertahankan Hak Akses). Hasil yang didapatkan dari penelitian ini adalah dapat diketahui bahwa website Pengadilan Tinggi Bengkulu memiliki 4 kerentanan yang berhasil dieksploitasi, terdapat 1 kerentanan yang masuk kategori High, dan 3 kerentanan yang dikategorikan medium, hasil uji eksploitasi yang berhasil dilakukan diukur menggunakan Common Vulnerability Scoring System (CVSS) sehingga dapat diketahui tingkat secara keseluruhan kerentanan website Pengadilan Tinggi Bengkulu memiliki skor 6.0(medium), yang artinya website Pengadilan Tinggi Bengkulu cukup aman terhadap serangan cyber.

ABSTRACT
Penetration testing is one method to secure websites from attacks by irresponsible people or hackers. With this method, website owners can find out where the vulnerabilities are on the website. This study aims to test the level of security on a website. The penetration testing method used is the Zero Entry hacking method with 4 stages, namely: reconnaissance, scanning, exploitation, and post exploitation and maintaining access. The results obtained from this study are that High Court of Bengkulu's website has 4 vulnerabilities that have been successfully exploited, there is 1 vulnerability that is in the High category, and 3 vulnerabilities that are categorized as medium, the results of the exploitation test that were successfully carried out were measured using the Common Vulnerability Scoring System (CVSS), therefore it can be seen that the overall level of vulnerability of High Court of Bengkulu's website has a score of 6.0 (medium), which means that High Court of Bengkulu's website is quite safe against cyber attacks.

PENDAHULUAN

Website dapat dengan mudah diakses oleh orang banyak dari manapun dan kapanpun, kemudahan akses ini terkadang membuat banyak orang atau suatu organisasi membangun sistem web server tanpa memperhatikan apakah web server yang dibangun sudah aman atau belum terhadap gangguan cyber. Sehingga sering terjadi gangguan dan merugikan bagi orang atau organisasi tersebut. Contoh serangan cyber yang paling umum adalah malicious codes, viruses, worms dan trojans, malware, stolen devices, phising, social engineering, dan serangan berbasis web. Adapun contoh serangan berbasis web secara umum yang paling sering dilancarkan yaitu, Structured Query Langueage (SQL) Injection, Distributed Denial of Service (DDoS), Cross Site Scripting (XSS), Defacement, Account Hijacking, dan Malwere.

Pengadilan Tinggi Bengkulu sebagai lembaga peradilan di lingkungan Peradilan Umum yang lebih tinggi dari Pengadilan Negeri di provinsi Bengkulu memanfaatkan jaringan internet yaitu web sebagai media dalam menyampaikan informasi kepada pihak luar dan menghubungkan civitas-civitas yang ada guna memudahkan dalam penyampaian informasi. Pertukaran informasi yang terjadi dalam jaringan internet dapat berupa informasi penting atau pribadi yang hak aksesnya hanya dapat dilakukan oleh orang-orang tertentu. Website Pengadilan Tinggi Bengkulu menggunakan Virtual Private Server (VPS) sebagai server, web server yang

digunakan yaitu Apache v2.4 kemudian database yang digunakan yaitu MySQL v5.0, bahasa pemrograman yang digunakan yaitu PHP 5.6, dan Content Management System (CMS) yang digunakan yaitu v4.6.1. Versi CMS yang digunakan pada website Pengadilan Tinggi Bengkulu merupakan versi yang sedikit lawas yaitu WordPress 4.6 yang bermasalah terhadap masalah kerentanan Remote Code Execution (RCE). Menurut informasi yang didapatkan dari pihak Pengadilan Tinggi Bengkulu, untuk masalah kerentanan tersebut pihak pengadilan Tinggi Bengkulu telah memperbaikinya. Tidak menutup kemungkinan bahwa masih terdapat celah kerentanan yang belum terdeteksi oleh pihak Pengadilan Tinggi Bengkulu.

Untuk mengamankan website dari serangan hacker yang tidak bertanggung jawab, disarankan pemilik website melakukan selftest terhadap web server atau website mereka sendiri. Melalui selftest, para pemilik website akan mengetahui letak kerentanan dari sistem yang ada. Salah satu metode pengujian self test adalah penetration testing. Penetration testing (pentest) sama dengan aktivitas hacking namun dilakukan secara legal. Pengujian terhadap website dengan metode penetration testing adalah cara yang efektik dalam mengidentifikasi kerentanan sistem.

LANDASAN TEORI

Pengertian Analisis

Menurut Aufan Imron Rosadi (2018:4), analisis adalah aktivitas yang memuat sejumlah kegiatan seperti mengurai, membedakan, memilah sesuatu untuk digolongkan dan dikelompokkan kembali menurut kriteria tertentu kemudian dicari kaitannya dan ditafsirkan maknanya. Dalam pengertian yang lain, analisis adalah sikap atau perhatian terhadap sesuatu (benda, fakta, fenomena) sampai mampu menguraikan menjadi bagian – bagian, serta mengenal kaitan antarbagian tersebut dalam keseluruhan. Analisis dapat juga diartikan sebagai kemampuan memecahkan atau menguraikan suatu materi atau informasi menjadi komponen-komponen yang lebih kecil sehingga lebih mudah dipahami.

Pengertian Pengujian

Menurut Wahyu Nur Cholifah, dkk (2018:207). Pengujian adalah suatu aktifitas yang direncanakan dan sistematis untuk menguji atau mengevaluasi kebenaran yang diinginkan. Aktifitas pengujian terdiri dari satu set atau sekumpulan langkah dimana dapat menempatkan desain kasus uji yang spesifik.

Pengertian Keamanan

Menurut Kamus Besar Bahasa Indonesia (KBBI), dijelaskan bahwa keamanan merupakan suatu kondisi bebas dari bahaya. Istilah bahaya disini dapat diartikan gangguan, ancaman, kecelakaan ataupun hal lainnya yang sifatnya tidak diinginkan.

Kemudian menurut Muhammad Subagja Sastra Wardaya (2019:18), keamanan dalam konteks komputer dijelaskan bahwa suatu sistem dapat dikatakan aman apabila dalam segala keadaan, sumber daya yang digunakan dan yang di akses adalah sesuai dengan kehendak pengguna.

Website/Web Application

Menurut Aliefyan Arbi, (2020:2), Website adalah sebuah kumpulan halaman pada suatu domain di internet yang dibuat dengan tujuan tertentu dan saling berhubungan serta dapat diakses secara luas melalui halaman depan (home page) menggunakan sebuah browser menggunakan URL website. Ciri yang paling mendasar dari Website yaitu memiliki informasi/content yang statis dengan kata lain jarang mengalami perubahan.

Aplikasi web (Web Application) merupakan sebuah perangkat lunak komputer yang dikodekan dalam bahasa pemrograman yang mendukung perangkat lunak berbasis web seperti HTML, CSS, JavaScript, Ruby, Python, Php, Java serta bahasa pemrograman lainnya. Web Application adalah sesuatu yang sedikit berbeda, Seperti aplikasi desktop (Word, Photoshop, Skype), web application bersifat dinamis dan terus berkembang.

Zero Entry Hacking (ZEH) Methodology

Menurut (Engerbetson, 2013:18), Zero Entry Hacking(ZEH) Methodology merupakan suatu metodologi yang digunakan dalam Penetration Testing. Metode ini cocok digunakan untuk pemula dalam melakukan Penetration Testing, karena hanya terdiri dari 4 tahap yaitu, Reconnaissance (Pengintaian Sistem), Scanning (Pemindaian), Exploitation (Mendapatkan Akses), Post Exploitation (Pasca Eksploitasi).

Pengertian Common Vulnerability Scoring System (CVSS)

Diambil langsung dari situs Forum of Incident Response and Security Teams (FIRST:2019). Common Vulnerability Scoring System (CVSS) menangkap karakteristik teknis utama dari kerentanan perangkat lunak, perangkat keras, dan firmware. Keluarannya mencakup skor numerik yang menunjukkan tingkat keparahan kerentanan relatif terhadap kerentanan lainnya.

CVSS terdiri dari tiga grup metrik:Base, Temporal, Environmental. Skor Dasar mencerminkan tingkat keparahan kerentanan sesuai dengan karakteristik intrinsiknya yang konstan dari waktu ke waktu dan mengasumsikan dampak kasus terburuk yang wajar di berbagai environment yang diterapkan. Metrik Temporal menyesuaikan tingkat keparahan Basis kerentanan berdasarkan faktor-faktor yang berubah dari waktu ke waktu, seperti ketersediaan kode eksploitasi. Metrik Environmental menyesuaikan keparahan Base dan Temporal ke environment komputasi tertentu. Mereka mempertimbangkan faktor-faktor seperti adanya mitigasi di lingkungan itu.

METODE PENELITIAN

Metodo penelitian yang akan digunakan pada penelitian ini yaitu metode Zero Entry Hacking. Metode ini merupakan suatu metodologi yang digunakan dalam penetration testing yang terdiri dari pengintaian sistem(reconnaissance), yang bertujuan untuk mencari informasi dari website yang tersedia di internet. Kemudian pemindaian (scanning) yaitu tahap penguji menggunakan berbagai macam tools dan mencoba berusaha mencari kerentanan-kerentanan yang terdapat pada website target.

Selanjutnya eksploitasi lubang keamanan (exploitation), merupakan tahap dimana penguji mencoba menguji kerentanan yang didapatkan pada tahap sebelumnya. Yang terakhir yaitu post eksploitasi (post exploitation), merupakan tahap melaporkan hasil uji yang telah dilakukan dan memberikan rekomendasi untuk mengatasi kerentanan yang ditemukan.

HASIL DAN PEMBAHASAN

Hasil dan Pembahasan

Dari hasil uji penetrasi yang dilakukan penulis menemukan 6 domain yang menggunakan domain pt-bengkulu.go.id tools yang digunakan yaitu dnsenum. Domain pt-bengkululu.go.id didaftarkan dan dikelola oleh pihak Kementrian Komunikasi dan Informatika(Kominfo), dan hosting yang digunakan yaitu PT. Beon Intermedia, informasi ini dapat diketahui melalui tools whois. Penulis juga menemukan kerentanan yang berhasil dieksploitasi pada domain pt-bengkulu.go.id yang dikelompokkan berdasarkan CIA triad. Kerentanan yang mengancam aspek Confidentiality merupakan kerentanan yang mengancam kerahasiaan suatu informasi. Kerentanan yang berhasil diuji antara lain AWStats Script, Cookie Without HTTP only Flag, Sehingga total kererentanan yang mengancam aspek Confidentiality terdapat 2 kerentanan. Selanjutnya kerentanan yang mengancam aspek Integrity.

Aspek Integrity merupakan aspek agar data atau informasi tidak dapat diubah oleh pihak yang tidak bertanggung jawab. Kerentanan yang berhasil diuji antara lain XMLRPC Pingback, X-frame-option-headers not set. Sehingga total kerentanan yang mengancam aspek Integrity berjumlah 2 kerentanan. Namun penulis tidak menemukan kerentanan yang mengancam aspek availability pada website dengan domain pt.bengkulu.go.id. Dari hasil pengujian yang telah dilakukan, penulis memberikan skor pada kerentanan yang berhasil diuji berdasarkan Common Vulnerability Scoring System (CVSS) yang dapat dilihat pada tabel 1.

Tabel 1. Pengukuran nilai kerentanan

No	URL	Jenis Kerentanan	Hasil Uji	Rekomendasi	Skor

1	ptbengkulu.go.id/xmlrpc .php	XMLRPC *pingback*	*Pingback* berhasil dilakukan	Mematikan fitur XMLRPC jika tidak terlalu diperlukan	7.2
2	pt- bengkulu.go.id/cgi-bin/awstats.pl	*AWStats Script*	Berhasil menemukan *url* sensitif	Membatasi hak akses terhadap direktori ini	5.8
3	pt.bengkulu.go.id	*Cookie Without HttpOnly Flag*	*Cookie* berhasil diakses melalui *console* sisi *client.*	Mengatur *header* menjadi *HttpOnly*	5.8
4	pt-bengkulu.go.id	*X-Frame-Options Headers not Set*	Aplikasi *website* berhasil di *iframe*	Mengatur *X-Frame-options : Deny*	5.3

Berdasarkan hasil pengukuran nilai kerentanan yang berhasil dieksploitasi yang dapat dilihat pada tabel 1. Rata-rata skor kerentanan yang terdapat pada website pt-bengkulu.go.id, website ini memiliki skor 6.0 yang termasuk kategori medium yang artinya website pt-bengkulu.go.id cukup aman terhadap serangan cyber.

Post Exploitation and Maintaining Access (Pasca Eksploitasi dan Mempertahankan Hak Akses)

Pada tahap ini penulis akan melampirkan hasil uji yang telah dilakukan Penulis tidak melakukan Maintaining Access. Penulis melaporkan hasil uji untuk mempermudah dalam melihat keseluruhan kerentanan mana saja yang merupakan akibat dari kegagalan Confidentiality, Integrity, dan Availability. Laporan ini akan memprioritaskan kerentanan mana saja yang perlu diperbaiki terlebih dahulu, dan merekomendasikan perbaikan kepada pihak Pengadilan Tinggi Bengkulu.

Pengukuran Nilai Kerentanan

Dari hasil uji yang telah dilakukan sebelumnya penulis akan memberikan skor pada kerentanan yang berhasil dieksploitasi berdasarkan CVSS, rumus yang digunakan untuk mengukur nilai kerentanan dapat dilihat pada tabel 4.14, dan range score

Hasil Uji Eksploitasi

Untuk memudahkan pihak Pengadilan Tinggi Bengkulu memperbaiki celah kerentanan yang berhasil dieksploitasi, penulis memperlihatkan tabel yang berisikan jenis kerentanan, hasil uji, rekomendasi, dan skor terhadap kerentanan tersebut sehingga pihak Pengadilan Tinggi Bengkulu dapat memprioritaskan kerentanan yang harus diperbaiki terlebih dahulu. Hasil uji eksploitasi dapat dilihat pada tabel 2.

Tabel 2. Hasil uji eksplolitasi

No	URL	Jeni Kerentanan	Hasil Uji	Rekomendasi	Skor
1	ptbengkulu.go.id/xmlrpc .php	XMLRPC *pingback*	*Pingback* berhasil dilakukan	Mematikan fitur XMLRPC jika tidak terlalu diperlukan	7.2

2	pt- bengkulu.go.id/cgi-bin/awstats.pl	*AWStats Script*	Berhasil menemukan *url* sensitif	Membatasi hak akses terhadap direktori ini	5.8
3	pt.bengkulu.go.id	*Cookie Without Http Only Flag*	*Cookie* berhasil diakses melalui *console* sisi *client.*	Mengatur *header* menjadi *HttpOnly*	5.8
4	pt-bengkulu.go.id	*X-Frame-Options Headers not Set*	Aplikasi *website* berhasil di *iframe*	Mengatur *X-Frame-options : Deny*	5.3

KESIMPULAN DAN SARAN

Kesimpulan

Setelah melakukan penetration testing pada website Pengadilan Tinggi Bengkulu, dapat diambil beberapa kesimpulan yang antara lain adalah sebagai berikut.

1. Kerentanan pada website Pengadilan Tinggi Bengkulu dapat diketahui dengan meggunakan metode Penetration Testing berdasarkan pedoman Zero Entry Hacking yang menggunakan 4 tahap dalam pengujiannya, tahap yang digunakan antara lain Reconnaissance (Pengintaian), Scanning (Pemindaian), Exploitation (Eksploitasi), Post Exploitation and Maintaining Access (Mempertahankan Akses dan Pasca Eksploitasi). Kemudian memberikan penilaian terhadap kerentanan yang berhasil dieksploitasi menggunakan Common Vulnerability Scoring System (CVSS), sehingga dapat diketahui bagaimana dampak kerentanan terhadap aspek Confidentiality, Integrity, dan Availability (CIA) dan dapat memetakan kerentanan berdasarkan tingkatan medium, high dan critical.
2. Setelah dilakukan analisis dan pengujian terhadap kerentanan yang ditemukan, website Pengadilan Tinggi Bengkulu memiliki 4 kategori kerentanan yang dapat dieksploitasi. Terdapat kerentanan yang masuk kategori pada kategori High yaitu XMLRPC Pingback Attack, dan kategori Medium yaitu AWStats Script, Cookie Without HTTP Only Flag set, X-Frame-Options-Headers not set.
3. Secara keseluruhan, tingkat kerentanan website Pengadilan Tinggi Bengkulu dengan domain pt-bengkulu.go.id memiliki skor 6.0 yang termasuk pada kategori medium yang artinya website Pengadilan Tinggi Bengkulu dapat dikatakan cukup aman terhadap serangan cyber.

Saran

Berdasarkan penelitian yang telah dilakukan, keamanan website Pengadilan Tinggi Bengkulu masih belum memenuhi prinsip keamanan CIA Triad yaitu Confidentiality, dan Integrity. Hal tersebut dapat dilihat dari beberapa keberhasilan eksploitasi kerentanan yang telah dilakukan. Terdapat beberapa saran yang dapat diterapkan untuk mengamankan website pada Pengadilan Tinggi Bengkulu. Beberapa saran tersebut adalah sebagai berikut:

1. Meningkatkan keamanan website berdasarkan aspek CIA Triad.
2. Menerapkan rekomendasi untuk mengatasi kerentanan yang telah ditemukan..

DAFTAR PUSTAKA

Aliefyan Arbi, 2018. Analisis Keamanan Sistem Informasi Akademik dengan Web Penetration Testing. Undergraduate Theses of Informatic Technique, 2018.

Dwi Bayu Rendro, dkk, 2020. Analisis Monitoring Sistem Keamanan Jaringan Komputer Menggunakan Software NMAP (Studi Kasus di SMK Negeri 1 Kota Serang). Jurnal Prosisko, 2020 (7), 108-115

DNSdumpster. 2019. DNSdumpster. https://dnsdumpster.com/

Engerbetson, 2013. The Basics of Hacking And Penetration Testing Second Edition.
USA, Syngress. 178 hal.

First (2019), Common Vulnerability Scoring System (CVSS). https://www.first.org/cvss/specification-document
Feri Wibowo, dkk (2019). Uji Vulnerability pada Website Jurnal Ilmiah Universitas Muhammadiyah Purwokerto Menggunakan OpenVAS dan Acunetix WVS. Jurnal Informatika. 2019 (6), 212-218.
Gitanjali Simran T dan Sasikala D (2019). Vulnerability Assessment of Web Applications using Penetration Testing. International Journal of Recent Technology and Engineering (IJRTE). 2019 (4), 1552-1556.
Guntoro dkk. 2020. Analisis Keamanan Web Server Open Journal System (OJS) Menggunakan Metode ISSAF dan OWASP (Studi Kasus OJS Universitas Lancang Kuning). Jurnal Ilmiah Penelitian dan Pembelajaran Informatika, 2020 (5), 45-55.
Hernawan & Kho 2019. Bug Hunting 101. (Web Application Security). Jawa Barat, AlfursanID. 231 hal.
ICANN, (2017). WHOIS Primer. https://whois.icann.org/en/primer Kali, (2021), Weevely, https://tools.kali.org/maintaining-access/weevely
Sqlmap, https://en.kali.tools/?p=1
Patil, D.K. and Patil, K. 2016. Automated Client-side Sanitizer for Code Injection Attacks. International Journal of Information Technology and Computer Science, 2016 (4), 86-95.
Rama Sahtyawan, 2019. Penerapan Zero Entry Hacking Didalam Security Misconfiguration pada Vulnerability Assessment and Penetration Testing (VAPT). Jurnal of Information System Management, 2019(1), 18-22.
Rizky Dwiananda Lukita Putra dan Is Mardianto, 2019. Exploitation with Reverse_tcp method on Android Device Using Metasploit. Jurnal Edukasi dan Penelitian Informatika. 2019(5), 106-112.
Ric Messier, 2019. Certified Ethical Hacker (CEH) v10 Study Guide. United Kingdom. Sybex. 592 hal.
Sean-Philip Oriyano, 2016, Certified Ethical Hacker (CEH) v9 Study Guide, United Kingdom, Sybex. 786 hal.
Wahyu Nur Cholifah, 2018. Pengujian Black Box Testing Pada Aplikasi Action & Strategy Berbasis Android dengan Teknologi Phonegap, Jurnal String, 2018 (3), 106-110
Warsun Najib dkk, 2020. Tinjauan Ancaman dan Solusi Keamanan pada Teknologi Internet of Things (Review on Security Threat and Solution of Internet of Things Technology). Jurnal Nasional Teknik Elektro dan Teknologi Informasi. 2020 (9), 375-384.
WPScan, 2021. WordPress Vulnerability Scanner. https://wpscan.com/wordpress- security-scanner

Website Security Analysis Using Penetration Testing Method

ORIGINALITY REPORT

9%	9%	3%	3%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	repository.ittelkom-pwt.ac.id Internet Source	4%
2	ayusamsi.blogspot.com Internet Source	3%
3	mahesa.id Internet Source	3%

Exclude quotes	Off	Exclude matches	< 3%
Exclude bibliography	Off		