

PENETRATION TESTING SISTEM INFORMASI PELAPORAN DAN KONSULTASI PADA WEBSITE XYZ MENGGUNAKAN STANDAR NIST 800-115

M. LUTFI YUSTISYIA



**TEKNOLOGI REKAYA PERANGKAT LUNAK
SEKOLAH VOKASI
INSTITUT PERTANIAN BOGOR
BOGOR
2024**

@Hak cipta milik IPB University

IPB University



PERNYATAAN MENGENAI LAPORAN PROYEK AKHIR DAN SUMBER INFORMASI SERTA PELIMPAHAN HAK CIPTA

Dengan ini saya menyatakan bahwa laporan proyek akhir dengan judul “Penetration Testing Sistem Informasi Pelaporan dan Konsultasi pada Website XYZ Menggunakan Standar Nist 800-115” adalah karya saya dengan arahan dari dosen pembimbing dan belum diajukan dalam bentuk apapun kepada perguruan tinggi mana pun. Sumber informasi yang berasal atau dikutip dari karya yang diterbitkan maupun tidak diterbitkan dari penulis lain telah disebutkan dalam teks dan dicantumkan dalam Daftar Pustaka di bagian akhir laporan proyek akhir ini.

Dengan ini saya melimpahkan hak cipta dari karya tulis saya kepada Institut Pertanian Bogor.

Bogor, Juli 2024

M.Lutfi Yustisyia J0303201044



ABSTRAK

M. LUTFI YUSTISYIA. *Penetration Testing* Sistem Informasi Pelaporan dan Konsultasi pada *Website XYZ* Menggunakan standar NIST 800-115. Dibimbing oleh NUR AZIEZAH.

Kemajuan teknologi telah menjadi bagian tak terpisahkan dalam kehidupan masyarakat, yang bergerak sejalan dengan perkembangan ilmu pengetahuan. Inovasi teknologi membawa manfaat positif dan kemudahan dalam berbagai aspek kehidupan, seperti akses mudah terhadap informasi melalui internet. Dengan adanya internet masyarakat dapat dengan mudah untuk mencari informasi. Informasi biasanya tersedia dalam *website*, namun kemudahan tersebut juga dapat menjadi sebuah ancaman untuk tersebarnya data pribadi. Tujuan penulisan ini adalah melakukan pengujian penetrasi untuk *website XYZ* dan menghasilkan rekomendasi dengan standar NIST 800-115. Metode pengujian yaitu pendekatan *blackbox* dan *greybox*. Metode ini dinilai relevan untuk diterapkan karena pengujian merupakan pihak luar dari perusahaan. Adapun hasil dari pengujian yang dilakukan *website XYZ* memiliki kerentanan level rendah dan sedang. Hal tersebut tentunya membantu perusahaan untuk melakukan pencegahan atas kebocoran data.

Kata kunci: *blackbox* , *greybox* , NIST 800-115, pengujian

ABSTRACT

M. LUTFI YUSTISYIA. Analysis of the Vulnerability of the Reporting and Consultation Information System on the *Website XYZ* Using standart NIST 800-115. Supervised by NUR AZIEZAH.

Technological advancement has become an integral part of people's lives, moving in tandem with the development of scientific knowledge. Technological innovations bring positive benefits and conveniences in various aspects of life, such as easy access to information through the internet. With the internet, people can easily search for information, which is usually available on websites. However, this convenience can also pose a threat to the spread of personal data. The purpose of this writing is to conduct penetration testing to test the *XYZ website* and produce recommendations according to the NIST 800-115 standard. The penetration testing used are the *blackbox* and *greybox* approaches. These methods are considered relevant because the tester is an external party to the company. The results of the testing showed that the *XYZ website* has low and medium-level vulnerabilities. This helps the company take preventive measures against data breaches.

Keywords: *blackbox* , *greybox*, NIST 800-115, testing

PENETRATION TESTING SISTEM INFORMASI PELAPORAN DAN KONSULTASI PADA WEBSITE XYZ MENGGUNAKAN STANDAR NIST 800-115

M. LUTFI YUSTISYIA

Laporan Proyek Akhir
Sebagai salah satu syarat untuk memperoleh gelar
Sarjana Terapan pada
Program Studi Teknologi Rekayasa Perangkat Lunak

**TEKNOLOGI REKAYA PERANGKAT LUNAK
SEKOLAH VOKASI
INSTITUT PERTANIAN BOGOR
BOGOR
2024**

@Hak cipta milik IPB University

IPB University



Judul Proyek Akhir : *Penetration Testing* Sistem Informasi Pelaporan dan Konsultasi pada *Website XYZ* Menggunakan Standar NIST 800-115
Nama : M.Lutfi Yustisyia
NIM : J0303201044

Disetujui oleh

Pembimbing:
Nur Aziezhah, S.Si., M.Si.



Diketahui oleh

Ketua Program Studi:
Medhanita Dewi Renanti, S.Kom., M.Kom.
NPI 20180 719830512 2 001
Dekan Sekolah Vokasi:
Dr. Ir. Aceng Hidayat, M.T.
NIP 19660 717199203 1 003



Tanggal Ujian :
30 Juli 2024

Tanggal Lulus :



PRAKATA

Puji dan syukur penulis panjatkan kepada Allah subhanaahu wa ta'ala atas segala karunia-Nya sehingga karya ilmiah ini berhasil diselesaikan. Tema yang dipilih dalam penelitian yang dilaksanakan sejak bulan Agustus 2023 sampai bulan Februari 2024 ini ialah *Penetration Website*, dengan judul "*Penetration Testing Sistem Informasi Pelaporan dan Konsultasi pada Website XYZ Menggunakan Standar NIST 800-115*".

Terima kasih penulis ucapkan kepada pembimbing, Nur Aziezah, S.Si., M.Si.. Yang telah membimbing dan banyak memberi saran. Ungkapan terima kasih juga disampaikan kepada ayah, ibu, serta seluruh keluarga yang telah memberikan dukungan, doa dan kasih sayangnya.

Semoga karya tulis ilmiah ini bermanfaat bagi pihak yang membutuhkan dan bagi kemajuan ilmu pengetahuan.

Bogor, Juli 2024

M. Lutfi Yustisyia



DAFTAR ISI

DAFTAR TABEL	ix
DAFTAR GAMBAR	ix
DAFTAR LAMPIRAN	ix
PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Tujuan	2
1.4 Manfaat	2
1.5 Ruang Lingkup	2
II TINJAUAN PUSTAKA	3
2.1 Website	3
2.2 Cyber Security	3
2.3 Cyber Crime	3
2.4 NIST 800-115	3
2.5 Oracle VM VirtualBox	3
2.6 Kali Linux	4
2.7 Nikto	4
2.8 OWASP ZAP	4
2.9 Burp Suite	4
2.10 FoxyProxy	5
2.11 Blackbox	5
2.12 Greybox	5
III METODE	6
3.1 Lokasi dan Waktu Proyek Akhir	6
3.2 Kerangka Berpikir	6
3.3 Prosedur Kerja	6
IV HASIL DAN PEMBAHASAN	11
4.1 Planning	11
4.2 Discovery	12
4.3 Attack	14
4.4 Reporting	16
V KESIMPULAN DAN SARAN	23
5.1 Kesimpulan	23
5.2 Saran	23
DAFTAR PUSTAKA	24
LAMPIRAN	26
RIWAYAT HIDUP	30

DAFTAR TABEL

1. Spesifikasi <i>Software</i>	11
2. Spesifikasi <i>Hardware</i>	11
3. Jadwal Pengujian	12
4. Daftar kerentanan	13
5. fitur yang diuji	14
6. Update daftar kerentanan	17
7. Rekomendasi <i>website XYZ</i>	18
8. <i>Score Vulnerability</i>	22

DAFTAR GAMBAR

1. Kerangka berpikir	6
2. NIST 800-115	6
3. Skenario Umum Scanning Nikto	7
4. Skenario umum penggunaan OWASP ZAP	8
5. Pendekatan <i>Blackbox</i> menggunakan burpsuite	9
6. Pendekatan <i>Greybox</i> menggunakan <i>payload</i>	9
7. Port website XYZ	12
8. Kerentanan hasil <i>scanning</i> OWASP ZAP	13
9. Hasil penyerangan <i>clickjacking</i>	14
10. Header Request	15
11. <i>Input payload</i>	16
12. <i>Cross site scripting</i>	16
13. Perubahan Kategori Kerentanan 2017-2021	17
14. <i>Score Vulnerability</i>	22

DAFTAR LAMPIRAN

1. <i>Setting certificate FoxyProxy</i>	27
2. <i>Setting Network untuk terhubung ke OWASP</i>	27
3. <i>Setting Certificate OWASP ZAP</i>	28
4. <i>Clickbandit</i>	28
5. <i>Copy Clickbandit to Clipboard</i>	29
6. <i>Paste Code Clickbandit</i>	29