JEITECH – Journal of Electrical Engineering and Information technology
Department of Electrical Engineering University of Mataram
Vol. 2, No. 1, March 2024, pp. 33-45 ; E-ISSN: 2987-7830

Penetration Testing untuk Menguji Sistem Keamanan pada Website dengan Metode Black-Box

Muhammad Arif Madani [1], Lalu A. Syamsul Irfan Akbar [1]
[1] Jurusan Teknik Elektro - Universitas Mataram, 83127 - Lombok, Indonesia

ARTICLE INFO

Article history:

Received February 11, 2024
Revised March 25, 2024
Accepted March 27, 2024

Keywords:

Penetration Testing;
OWASP Top 10;
WSTG Guide;
Keamanan Website;
Website;

ABSTRACT

The use of websites has a significant role in increasing efficiency, transparency, and public participation in public administration processes. Websites have become effective tools for providing accurate and up-to-date information about public policies, programs, and services. Although the use of websites has contributed positively, challenges such as website security need to be improved. The goal to be achieved in this study is to conduct penetration testing with the Black Box method by referring to the Open Web Application Security Project (OWASP) Top 10-2021. The number of subdomains tested was 3 identified subdomains. All vulnerability assessments are carried out in 4 stages consisting of foot printing, scanning, exploitation, and reporting. This penetration testing refers to Web Security Guide (WSTG) guidance document version 4.2. The result of this study was the discovery of 3 vulnerabilities with a distribution of 1 High, 1 Low, and 1 Informational. The final process of this research is in the form of recommendations that can be used as a reference for website application developers to deal with vulnerabilities, especially loss of service availability and data leakage.

Corresponding Author:

Lalu A. Syamsul Irfan Akbar, Jurusan Teknik Elektro - Universitas Mataram, 83127 - Lombok, Indonesia
Email: irfan@unram.ac.id

1. PENDAHULUAN

Keamanan sistem informasi menjadi suatu hal yang sangat penting. Menurut data laporan Honeynet BSSN tahun 2019, terdapat 98 juta serangan siber ke Indonesia menggunakan berbagai macam teknik serangan siber, oleh karena itu serangan siber saat ini menjadi suatu serangan yang sangat masif di Indonesia [1].

Website biasanya banyak menyimpan data pengguna yang nantinya bisa diolah untuk keperluan Data Science, Statistik, dan laporan. Data ini biasanya hasil dari pendaftaran pengguna pada website tersebut ataupun dari tempat lain yang aplikasinya saling berhubungan. Terdapat beberapa website yang tidak mengharuskan penggunanya untuk melakukan pendaftaran. Namun terdapat juga beberapa website yang mengharuskan penggunanya daftar terlebih dahulu untuk menggunakan fitur-fitur yang tersedia di dalamnya [2]. Kemudahan akses ini membuat banyak orang maupun instansi membangun sistem webserver tanpa memperhatikan apakah webserver yang dibangun sudah aman atau belum terhadap gangguan. Gangguan tersebut diantaranya berupa serangan maliciousCode atau malware. MaliciousCode atau malware merupakan jenis serangan yang paling banyak menyerang website [3].

Melakukan analisis celah keamanan merupakan salah satu bentuk deteksi dini terhadap ancaman di masa mendatang serta untuk menjamin confidentiality (kerahasiaan), integrity (konsistensi, akurasi, dan validitas data), availability (ketersediaan) atau biasa disebut dengan CIA Triad yang merupakan komponen dasar keamanan informasi. Celah keamanan dapat dijumpai dalam sebuah sistem maupun jaringan, salah satunya sistem aplikasi berbasis web. Dalam melakukan analisis celah keamanan suatu website diperlukan metode pengujian yang memuat kerangka pengujian sesuai standar keamanan yang ada [4].

Pengujian penetrasi pada website bertujuan untuk mencari celah-celah keamanan pada website yang nantinya dapat dikategorikan sebagai risiko kerentanan keamanan. Tahapantahapan yang digunakan untuk melakukan penetration testing pada suatu website terdiri dari berbagai modul yang akan disesuaikan dengan

standarisasi atau framework yang telah tersedia. Framework wajib digunakan oleh penguji agar hasil pengujian bersifat valid dan dapat dipertanggung jawabkan. Hasil pengujian keamanan tersebut nantinya ditampilkan dalam bentuk laporan evaluasi dengan saran terhadap perbaikan celah keamanan yang ditemukan. Saran yang diberikan penguji diharapkan membentuk suatu website yang memiliki tingkat keamanan yang tinggi [5]

2. METODE PENELITIAN

Metodologi ini mengacu pada penetration testing metode blackbox yang diasumsikan pada pengujian yang tidak mengetahui sama sekali infrastruktur sistem bangun yang dimiliki pada terget. Dengan demikian seorang security audit melakukan serangan pada webserver yang bertujuan mengumpulkan informasi yang dibutuhkan [6]

Parameter yang digunakan pada OWASP TOP 10 adalah sebagai berikut :

1. A1 - Injection Celah injeksi, seperti SQL,OS dan LDAP injection terjadi ketika data yang berbahaya dikirim ke interpreter sebagai bagian dari perintah atau query. Data berbahaya milik penyerang dapat mengelabui interpreter untuk mengeksekusi perintah yang tidak diinginkan atau mengakses data secara ilegal.
2. A2 - Broken Authentication Fungsi aplikasi yang berhubungan dengan otentikasi dan manajemen sesi sering tidak diterapkan dengan benar, sehingga memungkinkan penyerang untuk mengambil password-password, kunci-kunci, token-token sesi, atau untuk mengeksploitasi celah implementasi lainnya untuk mengambil identitas pengguna.
3. A3 - Sensitive Data Exposure Banyak aplikasi web yang tidak melindungi data rahasia dengan baik. Seperti kartu kredit, nomor PIN, dan kewenangan-kewenangan otentikasi. Penyerang akan mencuri atau merubah data yang diproteksi dengan lemah, untuk melakukan tindak pencurian identitas, kejahatan lewat kartu kredit, pencurian identitas, atau kejahatan lainnya. Data rahasia pantas terlindungi dengan baik menggunakan sandi enkripsi ketika tinggal atau dalam transit, sebagai pencegahan khusus atas tidak kejahatan ketika ketika tampil di browser.
4. A4 - XML External Entities (XXE) Banyak bahasa XML versi lebih tua atau yang tidak dikonfigurasi dengan baik mengevaluasi referensi entitas eksternal dalam dokumen XML. Entitas eksternal dapat digunakan untuk mengungkapkan file internal menggunakan URL file, pembagian file internal, pemindaian port internal, eksekusi kode jarak jauh, dan penolakan serangan layanan.
5. A5 - Broken Access Control Pembatasan pada apa yang diizinkan oleh pengguna yang diautentikasi sering kali tidak dilakukan dengan benar. Penyerang dapat mengeksploitasi kelemahan ini untuk mengakses fungsionalitas dan / atau data yang tidak sah, seperti mengakses akun pengguna lain, melihat file sensitif, memodifikasi data pengguna lain, mengubah hak akses, dll.
6. A6 - Security Misconfiguration Keamanan yang baik memerlukan konfigurasi keamanan yang terperinci dan telah menyeluruh pada framework aplikasi, aplikasi pada server, web server, database dan sistem operasi. Semua pengaturan ini harus didefinisikan, diimplementasikan dan dipelihara, karena terdapat banyak aplikasi yang dirilis tanpa konfigurasi default yang aman. Termasuk menjaga semua software untuk tetap terbarukan (up to date)
7. A7 - Cross-Site Scripting (XSS) Celah XSS terjadi ketika sebuah aplikasi mengambil data berbahaya dan mengirimkannya ke web browser dengan tanpa memvalidasi atau melepaskan konten tersebut dengan benar. XSS mengijinkan penyerang mengeksekusi script di browser target sehingga dapat leluasa mengambil alih data pengguna, merubah tampilan website target, atau mengarahkan korban ke laman yang berbahaya.
8. A8 - Insecure Deserialization Eksploitasi deserialization adalah agak sulit, seperti di luar rak eksploitasi jarang bekerja tanpa perubahan atau menyesuaikan eksploitasi kode yang mendasarinya.
9. A9 - Using Components with Known Vulnerabilities Komponen, seperti libraries, frameworks, dan modul perangkat lunak lainnya, dijalankan dengan hak yang sama seperti

aplikasi. Jika komponen rentan dieksploitasi, serangan semacam itu dapat memfasilitasi hilangnya data serius atau pengambilalihan server. Aplikasi dan API yang menggunakan komponen dengan kerentanan yang diketahui dapat merusak pertahanan aplikasi dan memungkinkan berbagai serangan dan berdampak.

10. A10 - Insufficient Logging & Monitoring Logging / Pencatatan dan pemantauan yang tidak memadai, ditambah dengan integrasi yang hilang atau tidak efektif dengan respons insiden, memungkinkan penyerang untuk menyerang sistem lebih lanjut, mempertahankan exploitasi, beralih ke lebih banyak sistem, dan mengutakatik, mengekstrak, atau menghancurkan data. Sebagian besar studi pelanggaran menunjukkan waktu untuk mendeteksi pelanggaran lebih dari 200 hari, biasanya terdeteksi oleh pihak eksternal daripada proses internal atau pemantauan [7].

Tools yang digunakan pada penelitian ini merupakan tools auotmation dan tools manual seperti:

1. BURP Tools (manual), dapat memberi gambaran umum tentang fungsionalitas dan konten aplikasi web target di mana ini berisi peta situs yang memberikan informasi terperinci tentang target sehingga memungkinkan untuk menetapkan ruang lingkup pengujian penetrasi testing.
2. Dirb (automation), adalah pemindai konten Web, yaitu mencari objek web yang ada atau tersebunyi. Dirb berkerja dengan meluncurkan serangan berbasis dictionary terhadap server web dan menganalisis tanggapan. Dirb bertujuan untuk membantu audit aplikasi web profesional. Dirb bekerja dengan memindai direktori dan kemudian melintasi di dalam direktori tersebut untuk memindai lebih banyak subdirektori.
3. Common Vulnerability Scoring Sysem atau CVSS, adalah sebuah framework yang dapat digunakan oleh publik untuk mengkomunikasikan dan kerentanan perangkat lunak. CVSS terdiri dari tiga bagian bagian, yaitu Base Score, Temporal Score dan Environmental Score. Base Score yaitu mewakili kualitas intrinsik kerentanan yang konstan sepanjang waktu dan diseluruh lingkungan pengguna, Temporal Score menggambarkan karakteristik kerentanan yang berubah seiring waktu dan Environmental score mewakili karakteristik kerentanan unik bagi pengguna lingkungan [8].

Langkah untuk menganalisis potensi kerentanan pada website:

1. Pengumpulan Informasi Tahap pengumpulan informasi merupakan proses mengumpulkan informasi secara umum berkaitan dengan target yang akan diuji. Informasi yang dikumpulkan berupa data mengenai IP target, registrant dan admin, informasi mengenai reverse DNS dan IP lookup, dan informasi lainnya yang diperlukan.
2. Identifikasi Kerentanan Sistem Identifikasi kerentanan sistem atau vulnerability assessment adalah proses identifikasi dan kuantifikasi kerentanan keamananan pada suatu lingkungan keamanan sistem infomasi. Dapat diartikan juga sebagai suatu evaluasi mendalam terhadap keamanan sistem infomasi yang aktif digunakan.
3. Uji Penetrasi Uji penetrasi (penetration testing) atau peretasan etis, adalah praktik pengujian aset teknologi informasi untuk menemukan kerentanan keamanan yang dapat dieksploitasi oleh penyerang. Pengujian penetrasi dapat diotomatisasi dengan perangkat lunak atau dilakukan secara manual.
4. Analisis dan Pelaporan Pada tahap ini biasanya dilaporkan tentang langkah kerja yang dilakukan, celah keamanan yang ditemukan serta usulan perbaikan. Tahapan selanjutnya biasanya tindak lanjut, yang biasanya harus dilakukan bersama-sama dengan admin untuk memperbaiki sistem [3].

2.1. Subjek Penelitian

Subjek pada penelitian ini adalah pada 3 website aplikasi yang dikelola oleh pemerintah provinsi NTB. Penelitian dilakukan dengan melakukan pengujian terhadap aplikasi (source code) dan webserver sebagai tempat berjalanya aplikasi.

2.2. Metode OWASP Top 10

Penetration testing dengan metode OWASP TOP 10 dilakukan dengan beberapa tahapan, yaitu [9]:

1. Footprinting Tahap awal yang dilakukan adalah mengumpulkan segala informasi mengenai website yang memiliki domain *.ntbprov.go.id yang akan dilakukan penetration testing.
2. Scanning Setelah mendapatkan segala informasi mengenai website target, proses selanjutnya adalah melakukan proses scanning. Proses scanning ini dilakukan untuk mencari port atau celah keamanan yang ada pada website yang dapat disusupi.
3. Uji keamanan website Melakukan pengujian pada website yang memiliki domain *.ntbprov.go.id menggunakan metode OWASP TOP 10.
4. Pembuatan laporan hasil pengujian Laporan berisi penjabaran dan penjelasan dari hasil pengujian yang telah dilakukan menggunakan metode OWASP TOP 10 disertai solusi untuk celah keamanan yang ditemukan.

2.3 Panduan WSTG

The Web Security Testing Guide atau WSTG versi stabil adalah sebuah panduan komprehensif pengujian keamanan perangkat lunak berbasis web yang merupakan salah satu proyek oleh OWASP. Kerangka kerja ini berisi tentang tahapan-tahapan pengujian keamanan pada setiap Software Development Life Cycle (SDLC) yang sedang dilakukan. WSTG telah tersedia dalam beberapa versi, salah satu versi yang telah dirilis adalah versi stabil [10]

3. HASIL DAN PEMBAHASAN

Hasil dan pembahasan berisi tentang langkah-langkah penelitian yang dilakukan beserta hasilnya. Berikut ini uraian hasil penelitian:

3.1 Tahap Pengumpulan Informasi

Tahap pengumpulan informasi (information gathering) bertujuan untuk mengumpulkan informasi umum mengenai website yang menjadi target menggunakan perangkat (tool). Hasil informasi yang didapat dilihat pada Tabel 1 berikut ini:

Tabel 1. Temuan Port.

Service	IP address	Open ports	Ports details
Http	103.18.117.186	80/tcp	Nginx
Https	103.18.117.186	443/tcp	Nginx
Domain	103.18.117.186	53/tcp	N/A
Ident	103.18.117.186	113/tcp	N/A

3.2 Identifikasi Kerentanan Sistem dan Uji Penetrasi

Proses identifikasi kerentanan dilakukan dengan memindai kerentanan keamanan pada website. Alat OWASP TOP 2021 digunakan untuk memindai kerentanan di domain utama situs web target. Hasilnya seperti terlihat pada Tabel 2:

Tabel 2. Temuan Tingkat Kerentanan.

Severity	Critical	High	Medium	Low	Informational
Number of issues	0	1	0	1	1

3.2.1 Low Severity

a) Rate Limiting

Rate limiting bertujuan untuk mencegah penyalahgunaan layanan atau fitur-fitur tertentu dengan membatasi jumlah permintaan yang dapat dilakukan oleh pengguna dalam periode waktu tertentu. Tanpa adanya pembatasan tingkat, aplikasi web dapat menjadi rentan terhadap serangan brute force atau penggunaan berlebihan yang dapat merugikan stabilitas atau kinerja aplikasi.

Dalam konteks WSTG, uji keamanan "Missing Rate Limit" bertujuan untuk menemukan kelemahan di mana aplikasi web tidak memberlakukan pembatasan tingkat pada operasi-operasi yang memerlukan kontrol akses atau operasi yang dapat disalahgunakan. WSTG dapat melibatkan berbagai jenis operasi seperti percobaan login, permintaan API, atau operasi-operasi lain yang dapat dieksploitasi jika tidak dibatasi.

a. Dampak yang ditimbulkan*:*

Penyerang dapat menggunakan kerentanan ini untuk melakukan serangan mailer spam voting dimana dapat menambah jumlah voting tanpa adanya Batasan dalam mengambil jumlah voting.

b. Detail Temuan:

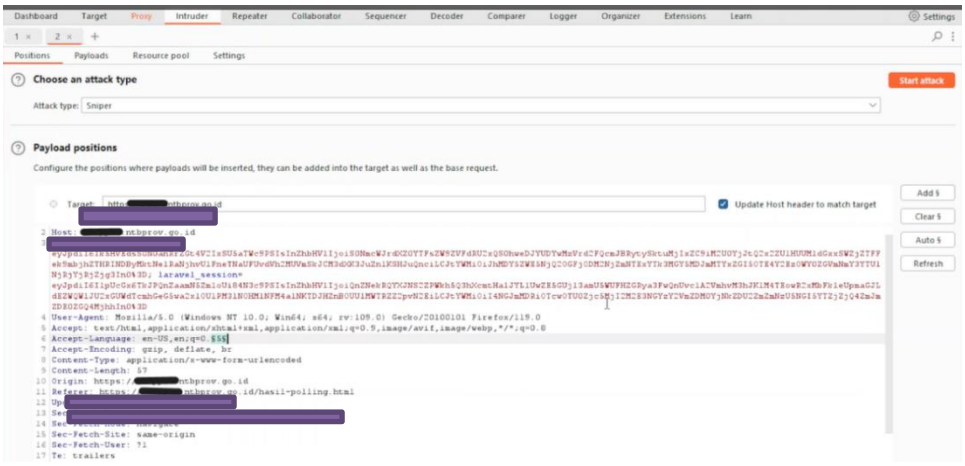
Admin menyediakan opsi voting, tetapi tidak ada jenis permintaan yang membatasi, sehingga penyerang dapat melakukan serangan dengan membanjiri jumlah vote. Kerentanan ini dapat menjadi ancaman terhadap reputasi pemilik website.

c. Tahap Pengujian*:*

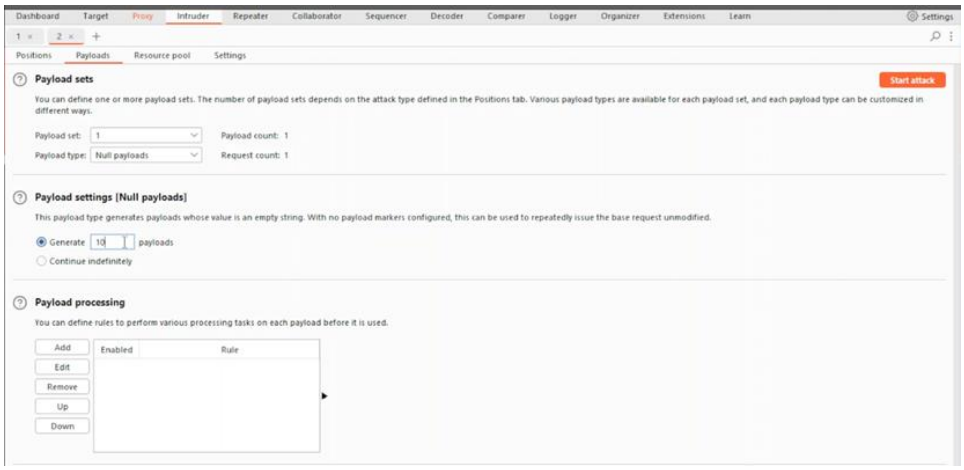
- User akan melakukan opsi Voting untuk memilih poling yang ada pada website
  HTTP request:

```
POST /hasil-polling.html HTTP/2

Host: xyz.ntbprov.go.id

Cookie:                                __dtsu=10401696996282EA727416E4CF618686;
_ga_WFC21TWQHW=GS1.1.1698584892.5.1.1698586734.0.0.0;
_ga=GA1.1.480797266.1696996735;
_ga_JQ825SZKGL=GS1.1.1696996946.1.1.1696996982.0.0.0;
_ga_EGKQD2W8P9=GS1.1.1698558403.4.0.1698558403.0.0.0;                XSRF-
TOKEN=eyJpdiI6ImZVTm5NU2hQZWxKaWlsR3plcjBWekE9PSIsInZhbHVlIjoiL2x1RkR6d2JS
ZVJoSW1pbE10NHRDcTJ1cFh4VkptaDYzNVUxRmFFZnBpRXNOdHVXUlNOc1U3R3lNUkFUQ3d3WT
hmdHdqR0x0NW9XT1p6VU9sRFpVbGhPK3lvNDREb1FFeVR4QmJ0MGxjL1BaMGUwRVZkYnNIWk5L
aVkvYkw4czciLCJtYWMiOiJiNmFjMWY5ZDQxZGQ3Y2E5ZDhjNDgxZjA1OTIzNTE4Zjlh0DQzNW
NjMGQ3NDZjMTUyYzIyYmVhMTIwMDUyNzEyIn0%3D;
laravel_session=eyJpdiI6IjR4K2hORC9rODhIMzUrWnRKQWw3alE9PSIsInZhbHVlIjoicT
cvY2ZKLy8xSnc0cUZFakRKQkhjSFd2TEluS3BJT0twQ3NaVXV0YityN3BhaS9GNFRTeWEvM0FW
a2I2NGJhN0hvVHlIUVg2WDd5bU9BU05OMzMyQnptQWwvenBscFFPaTZRQXJERC9VTW4yTWp2ZW
RWcERPMllLdUdUelRWclUiLCJtYWMiOiI3OWQ3MzlmY2ExY2FhZDRjNGIyZjE0MDBhNTJmNzVk
YjZiMWM2YjUxMDRiMTdjZDQ4MTk2NzQzZjkzNDc2YWE4In0%3D

User-Agent:  Mozilla/5.0  (Windows  NT  10.0;  Win64;  x64;  rv:109.0)
Gecko/20100101 Firefox/119.0

Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/web
p,*/*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Content-Type: application/x-www-form-urlencoded

Content-Length: 57

Origin: https://xyz.ntbprov.go.id

Referer: https://xyz.ntbprov.go.id/

Upgrade-Insecure-Requests: 1

Sec-Fetch-Dest: document
```

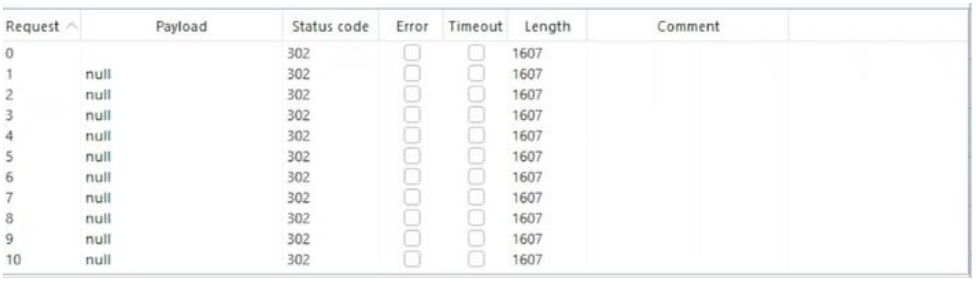
- Buka BurpSuite, aktifkan Intercept, kemudian kembali ke halaman Vote. Klik “Vote”
- Setelah respon ditangkap oleh Burpsuite, lakukan pengaturan pada Intruder untuk menambahkan satu digit angka ke Intruder. Lanjutkan ke bagian Payloads, ubah jenis payload menjadi “Null Payloads” dengan mengubah request sebanyak 10 kali serangan. Kemudian “Mulai Serangan”



Gambar 1. HTTP Request di Intruder

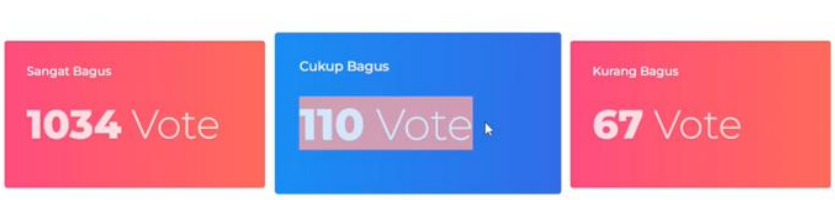


Gambar 2. Payload Settings

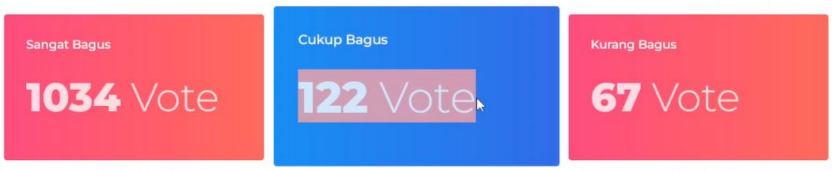


Request	Payload	Status code	Error	Timeout	Length	Comment
0		302			1607	
1	null	302			1607	
2	null	302			1607	
3	null	302			1607	
4	null	302			1607	
5	null	302			1607	
6	null	302			1607	
7	null	302			1607	
8	null	302			1607	
9	null	302			1607	
10	null	302			1607	

Gambar 3. HTTP Respons



Gambar 4. Hasil sebelum Vote



Gambar 5. Hasil sesudah Vote

d. Rekomendasi Penanganan:

Untuk mengatasi kekurangan ini, pengembang web harus memastikan bahwa ada mekanisme pembatasan tingkat yang efektif diimplementasikan di seluruh aplikasi untuk melindungi terhadap jenis serangan yang disebabkan oleh frekuensi tinggi dari permintaan yang tidak sah.

3.2.2 High Severity

b) Insecure Direct Object References - Possible Edit and Remove Documents

Insecure Direct Object Reference (IDOR) adalah sebuah kerentanan keamanan pada aplikasi web yang dapat memungkinkan penyerang untuk mengakses atau memanipulasi objek secara langsung tanpa otorisasi yang tepat.

Pada dasarnya, IDOR terjadi ketika aplikasi tidak memvalidasi atau mengotentikasi dengan benar hak akses pengguna terhadap objek tertentu, seperti file, database, atau rekaman data lainnya. Sebagai contoh, pertimbangkan suatu aplikasi yang menggunakan parameter ID untuk mengidentifikasi dan menampilkan data pengguna tertentu. Jika aplikasi tidak memvalidasi secara benar apakah pengguna yang mengakses objek tersebut memiliki hak akses yang sesuai, maka penyerang dapat mencoba mengganti parameter ID untuk mendapatkan akses tidak sah.

a. Dampak:

Penyerang dapat menghapus dan mengubah semua file tersimpan yang tersedia. File-file tersebut dapat berisi informasi sensitif seperti data event atau pribadi. Itu dapat mengarah pada penghapusan dan perubahan data secara langsung berdampak pada kerahasiaan dokumen perusahaan/instansi.

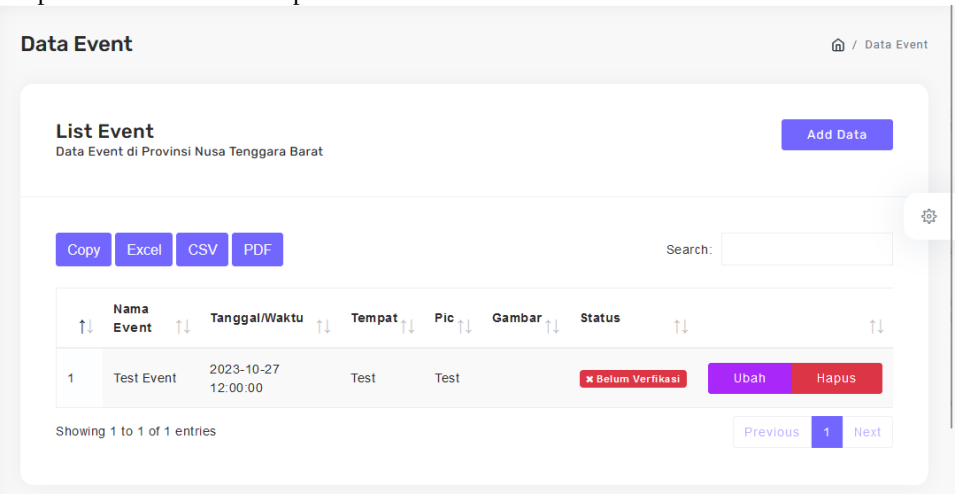
b. Detail Temuan:

Insecure Direct Object References adalah jenis kerentanan umum yang memungkinkan permintaan dibuat untuk objek tertentu melalui halaman atau layanan tanpa verifikasi yang tepat atas hak pemohon atas konten. Dalam hal ini, sistem kontrol akses memungkinkan anggota biasa yang mengetahui titik akhir API apa yang harus diterapkan untuk mendapatkan posting pribadi anggota selain itu juga dapat berdampak data yang tersimpan dapat terhapusa ataupun diubah oleh pihak yang tidak memiliki akses yang sah.

c. Tahap Pengujian:

Edit Data:

- Ikuti tautan (https://URL/admin/events/[ID]/edit) dan perhatikan bahwa Anda bisa mendapatkan file berdasarkan parameter ID di URL.



Gambar 6. Data Event

HTTP request:

```
GET /admin/events/490/edit HTTP/2

Host: vwx.ntbprov.go.id

Cookie: __dtsu=10401696996282EA727416E4CF618686;
_ga_WFC21TWQHW=GS1.1.1698594175.6.1.1698594213.0.0.0;
_ga=GA1.1.480797266.1696996735;
_ga_JQ825SZKGL=GS1.1.1696996946.1.1.1696996982.0.0.0;
_ga_EGKQD2W8P9=GS1.1.1698558403.4.0.1698558403.0.0.0; XSRF-
TOKEN=eyJpdiI6IjlHbnRHNW1nVUhNT1E5TFhXZTBYZGc9PSIsInZhbHVlIjo
iQnFQV2N2YmRyZHRQQTROYXlobStwQkpMMzhvZ3hJTk9ORVJ5c1B0N0dQVGxl
SzFjb1hvc28zQ01wWTJYU1VVV04xSHg4SVBMYzdCV2NSd0g1OHU2YTFnRllKS
Vk3M25UeERCQllEZVdUYWFzMEdIMnY1U3k5VmZyeDlHWmNsNmsiLCJtYWMiOi
JkMTJhODcwZDMwMTI3MTMzODA4MjRlYzFhMDAxZTY2MzUwZjI3YWQ4M2U0ZjE
2ZjUyMTMyNjE5NzRkZjY4ZTBkIn0%3D;
vwx_session=eyJpdiI6ImwrMFBlazNmZTRCSDdoQ0FBYnZyTUE9PSIsInZhb
HVlIjoiSEg1SU9NbG9ZNkFyRXhreFF5WWl5TCt4SWErQ0NURGtxRnpJSmUrR1
E2TVk1MUpLYkk5ZlBUcGNBbkJya1o3dmQvekIyODd6dlFtT2drUWhrMlZwUEd
ybTNGYno1NmR6MUpBWUFvUFl6cU13ZXRQMUJOQUVBa3RGVGZRSHY0dGEiLCJt
YWMiOiI4ODFjMDRkN2YzZDU1NmViN2ViZGNhN2NlMTNhMGZlOTY4OTQ5NDc1Y
zM0ZTFmMWYxMmFkZjVhMmQxMzc2ZjU1In0%3D

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:109.0) Gecko/20100101 Firefox/119.0

Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/a
vif,image/webp,*/*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Referer: https://vwx.ntbprov.go.id/admin/events
```

- Hapus event yang Anda miliki, kemudian tangkap request menggunakan Burp Suite.

HTTP request:

```
DELETE /admin/events/479 HTTP/2

Host: vwx.ntbprov.go.id

Cookie: __dtsu=10401696996282EA727416E4CF618686;
_ga_WFC21TWQHW=GS1.1.1698594175.6.1.1698594331.0.0.0;
_ga=GA1.1.480797266.1696996735;
_ga_JQ825SZKGL=GS1.1.1696996946.1.1.1696996982.0.0.0;
_ga_EGKQD2W8P9=GS1.1.1698558403.4.0.1698558403.0.0.0; XSRF-
TOKEN=eyJpdiI6IklIdmpIa3dOQUNuaDBTMXMrUDBOVkE9PSIsInZhbHVlIjoid3ZBVGpIUlNQY
kVkVTNrMjY5WFVQbnJKdGljZGYrQzc1aXhUVWp1bFNoZGFYdjFWOGQ1bXRVMVZTQ203ZmtxUENF
TmM1TytKcUNUWGF1SFdFZSs5N2diY1NpWDhxWmhRNGpIL3llMkdObXZ5ZDZKRkZSVXBQalJpTEp
YQWNhNjAiLCJtYWMiOiI0MzFjMzJiOGEyYTM3ZTFkNTZlODdjOGI2NmM0YjFhMjNkZjExNzg3ND
FkNmMwNGQ1MjRhMTk1NTE5NTQxMTczIn0%3D;
vwx_session=eyJpdiI6ImgySGpCZi9aSlNaTFVDVFNXZzRsRWc9PSIsInZhbHVlIjoiNm1rV1p
UQmxSbnp4S0NuVDBIWWM3UVFrbHRlTHljcVdFZnB3YmlOaER6WDlsd0ovZGdBbGNFQSt0ZHExY0
9LUU00TFFDRkhib0xremU1dGg2dE1WcTZIR2RmUDV6NGVtVVRMMEFIcytFalQ3cThNQjgzY3dLc
3ZyT2NKdXJLOGwiLCJtYWMiOiIyYjljODBmY2JjNWUzZGFjOGYyZTZmN2NkMmI1ODZjYTg5YWI0
ZTk5Zjk1NWMxNDdiMWFlMzg0ZGE5ZTFhNjU1In0%3D

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0)
Gecko/20100101 Firefox/119.0

Accept: */*

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

X-Csrf-Token: DoFq0et1yHYmCbB2CnMeh4CmeUOtRx7zDkEJ5iFs

X-Requested-With: XMLHttpRequest

Origin: https://vwx.ntbprov.go.id

Referer: https://vwx.ntbprov.go.id/admin/events

Sec-Fetch-Dest: empty

Sec-Fetch-Mode: cors

Sec-Fetch-Site: same-origin

Te: trailers
```

HTTP respons:

```
HTTP/2 302 Found

Server: nginx

Date: Sun, 29 Oct 2023 16:11:43 GMT

Content-Type: text/html; charset=UTF-8

X-Powered-By: PHP/8.0.30

Cache-Control: private, must-revalidate

Pragma: no-cache

Expires: -1

Set-Cookie: XSRF-
TOKEN=eyJpdiI6ImREdmZnL2pUWVJqS1MyVXk5VWNlZGc9PSIsInZhbHVlIjoieHpUNmFSSXJGU
TFmRnlYcUI1c0hxTHNSUGhObnd1M0x6QVlDZFBhZDQvaGlNTTlYRlM5TVFvOVlnZmxkekxRRDJ1
VVN3b3dPUEdURXNaSmlYK1V2QVhVLzdIRmVlMmpORnlTWW16L2tCa1BGbVdVbXRHWTROK240NXl
FcDcvdGYiLCJtYWMiOiI0OWFmYjA4ZDJjN2UzMjdkMWQ5ZGUwZTNmZGY5N2MwNDM2OTZjZjEzYW
E4MmRlY2JiY2UyMjVlNmNlMmZlYzUzIn0%3D; expires=Sun, 29-Oct-2023 18:11:43
GMT; Max-Age=7200; path=/; samesite=lax

Set-Cookie:
vwx_session=eyJpdiI6Ik1FdmlRK2czQWxMNE9PL1Y4ODZjbEE9PSIsInZhbHVlIjoiWXB4NUN
ha1Y3bnJNY3VIZ1Nrd1RjWUtZcEZxZEtGeFpsUndVNVo1akp1YVVQWFlNYTZSdlRlM0Y0VlRhbG
JIWElpWkhSRmRWWjBjVDg1dG9oQkYvUXo0RC9KYkxuWHcxNlVsd0xrajMyN2V6T0lhaG11aWlLQ
W9NamZBQjlJWHQiLCJtYWMiOiJjNGM2MDIwNzVkZmQ0YjQ1NzQyMTI3MTY2N2U3YmJlZjE5Zjg2
YjM2MzNiZjFjOWI1MTE1NjM3MDQzMGRjMzdlIn0%3D; expires=Sun, 29-Oct-2023
18:11:43 GMT; Max-Age=7200; path=/; httponly; samesite=lax

Location: https://vwx.ntbprov.go.id/admin/events

X-Powered-By: PleskLin

<!DOCTYPE html>
<html>
    <head>
        <meta charset="UTF-8" />
        <meta http-equiv="refresh"
content="0;url='https://vwx.ntbprov.go.id/admin/events'" />

        <title>Redirecting to
https://vwx.ntbprov.go.id/admin/events</title>
    </head>
    <body>
        Redirecting to <a
href="https://vwx.ntbprov.go.id/admin/events">https://vwx.ntbprov.go.id/adm
in/events</a>.
    </body>
</html>
```

d. Rekomendasi Penanganan:

Pada tahapan ini dilakukan untuk perbaikan bugs dan update code guna mengamankan website sebagai berikut:

1. Implementasikan Mekanisme Otentikasi dan Otorisasi yang Kuat: Pastikan aplikasi menggunakan mekanisme otentikasi yang kuat untuk mengidentifikasi pengguna dan mekanisme otorisasi yang memastikan hanya pengguna yang sah yang memiliki akses ke objek atau data sensitif.
2. Gunakan Pengidentifikasi yang Tidak Terduga: Gunakan pengidentifikasi yang tidak mudah ditebak atau ditebak oleh penyerang. Hindari menggunakan ID berturut-turut atau ID yang terkait dengan informasi pengguna lainnya yang dapat diakses secara publik.
3. Lakukan Validasi dan Kontrol Akses di Sisi Server: Pastikan validasi dan kontrol akses dilakukan di sisi server, bukan hanya di sisi klien. Ini akan membantu mencegah manipulasi parameter atau data yang dikirimkan oleh klien untuk mengakses objek yang tidak seharusnya diakses.
4. Terapkan Prinsip Least Privilege: Berikan hak akses terendah yang diperlukan untuk setiap pengguna. Hindari memberikan akses penuh atau hak akses yang tidak diperlukan pada objek atau data tertentu.
5. Enkripsi Referensi atau Identifikasi Objek: Gunakan enkripsi atau teknik hashing untuk mengamankan referensi atau identifikasi objek. Ini akan mempersulit penyerang untuk menebak atau memanipulasi referensi atau identifikasi objek yang digunakan dalam aplikasi.
6. Uji Keamanan Secara Rutin: Lakukan pengujian keamanan secara rutin untuk mengidentifikasi celah keamanan IDOR dan kerentanan lainnya, sehingga akan membantu mendeteksi dan memperbaiki masalah sebelum penyerang memanfaatkannya [11]

4. KESIMPULAN

Ada beberapa kesimpulan yang dapat diambil dari analisis data yang diperoleh Penetration Testing yang telah dilakukan sebelumnya:

Penetration Testing memiliki beberapa langkah untuk mengetahui tingkat kerentanan sesuai standar OWASP TOP yaitu dapat mengidentifikasi celah-celah yang bisa menjadi target serangan hacker untuk masuk ke sebuah website secara ilegal selanjutnya dengan menggunakan metode Common Vulnerability Scoring System (CVSS) cara ini bisa digunakan untuk dapat menentukan tingkat kerentanan dan menghasilkan skor yang mencerminkan tingkat kerentanan pada website dan pada CVSS terdapat kualifikasi tingkat kerentanan yang dibagi ke dalam representasi rendah, sedang, tinggi, dan kritis untuk membantu sebuah organisasi menilai dengan benar dan memprioritaskan proses manajemen kerentanan website.

Penetration Testing dalam penelitian ini membantu dalam pengambilan keputusan untuk menghindari serangan-serangan siber dengan efektif berdasarkan data-data tersebut di atas; penelitian sistem keamanan website yang menggunakan metode penetration testing terbukti optimal karena terdapat celah untuk masuk ke user ID yang seharusnya tidak dapat diakses oleh orang lain. Selain itu, penetration testing membantu dalam menentukan rancangan website yang ideal.

Setelah melakukan uji penetration testing pada website, sistem firewall pada website ini cukup baik sehingga cukup menyulitkan dalam mengeksploitasi sistem, namun pada website tidak dikonfigurasi dengan baik sehingga aplikasi tidak memvalidasi atau mengotentikasi dengan benar hak akses pengguna terhadap objek tertentu, seperti file, database, atau rekaman data lainnya, user ID bisa dapat diketahui orang lain yang bisa menjadikan penyerang mengubah atau memanipulasi data melalui celah user ID tersebut.

Peneliti lebih menekankan pada website sebaiknya lebih memperhatikan hal-hal seperti: Implementasi pemeriksaan akses yang memadai untuk setiap objek yang ingin diakses oleh pengguna. Gunakan pengenal yang lebih kompleks, seperti GUID, untuk membuatnya praktis tidak mungkin ditebak oleh penyerang. Sebisa mungkin, hindari mengungkapkan pengenal dalam URL dan POST body. Pastikan aplikasi memeriksa izin pengguna setiap kali ada upaya akses. Gantilah pengenal numerik yang dapat dihitung dengan pengenal acak yang lebih kompleks. Hal ini dapat membantu mengurangi risiko menebak pengenal.

DAFTAR PUSTAKA

[1] D. F. Priambodo, A. D. Rifansyah, and M. Hasbi, "Penetration Testing Web XYZ Berdasarkan OWASP Risk Rating," *Teknika*, vol. 12, no. 1, pp. 33–46, Feb. 2023, doi: 10.34148/teknika.v12i1.571.

[2] R. Febriana, "Blackbox Testing Sistem Informasi Absensi Pegawai Karawang Dengan Metode Top 10 Owasp Attack," *J. Ilm. Wahana Pendidik.*, vol. 2022, no. 12, pp. 327–334, doi: 10.5281/zenodo.6945632.

[3] I. Uji *et al.*, "Implementation of Penetration testing on Websites to Improve Security of Information Assets UPN 'Veteran' Yogyakarta," *J. Inform. dan Teknol. Inf.*, vol. 20, no. 2, pp. 153–162, 2023, doi: 10.31515/telematika.v20i2.7757.

[4] B. T. K. & M. A. S. Dewi, "Kajian Literatur: Metode dan Tools Pengujian Celah Keamanan Aplikasi Berbasis Web," *Automata*, vol. 3, no. 1, pp. 1–8, 2022.

[5] I. D. G. G. Dharmawangsa, G. M. A. Sasmita, and I. P. A. E. Pratama, "Penetration Testing Berbasis OWASP Testing Guide Versi 4.2 (Studi Kasus: X Website)," *JITTER J. Ilm. Teknol. dan Komput.*, vol. 4, no. 1, p. 1613, 2023, doi: 10.24843/jtrti.2023.v04.i01.p06.

[6] D. Teguh Yuwono *et al.*, "DETEKSI SERANGAN VULNERABILITY PADA OPEN JURNAL SYSTEM MENGGUNAKAN METODE BLACK-BOX," 2021.

[7] Y. Yudiana, A. Elanda, and R. L. Buana, "Analisis Kualitas Keamanan Sistem Informasi E-Office Berbasis Website Pada STMIK Rosma Dengan Menggunakan OWASP Top 10," *CESS (Journal Comput. Eng. Syst. Sci.*, vol. 6, no. 2, p. 185, 2021, doi: 10.24114/cess.v6i2.24777.

[8] A. I. Rafeli, H. B. Seta, and I. W. Widi, "Pengujian Celah Keamanan Menggunakan Metode OWASP Web Security Testing Guide (WSTG) pada Website XYZ," *Inform. J. Ilmu Komput.*, vol. 18, no. 2, p. 97, 2022, doi: 10.52958/iftk.v18i2.4632.

[9] A. Dharmawan, Y. Prihati, and H. Listijo, "Penetration testing menggunakan OWASP top 10 pada domain xyz.ac.id," *Jelc*, vol. 8, no. 1, pp. 1–9, 2022.

[10] F. Ahmad and F. Rahma, "Hardening Sistem Informasi XYZ Menggunakan Framework OWASP," 2021.

[11] U. Muhammadiyah Sidoarjo, R. Ananda Putra, and I. Alnaurus Kautsar, "Detection and Prevention of Insecure Direct Object References (IDOR) in Website-Based Applications Deteksi dan Pencegahan Insecure Direct Object References (IDOR) Pada Aplikasi Berbasis Website," *Semin. Nas. Call Pap. Fak. Sains dan Teknol.*, vol. 4, no. June, 2023.