Portable Web Penetration Test Tool Memanfaatkan Single Board PC

Laksono Adiputro AR[1], Yudi Prayudi[2], Fietyata Yudha[3]
Jurusan Teknik Informatika Universitas Islam Indonesia
Yogyakarta
[1]13523023@students.uii.ac.id, [2]prayudi@uii.ac.id, [3]fietyata.yudha@uii.ac.id
Jurusan Teknik Informatika
Universitas Islam Indonesia
Yogyakarta

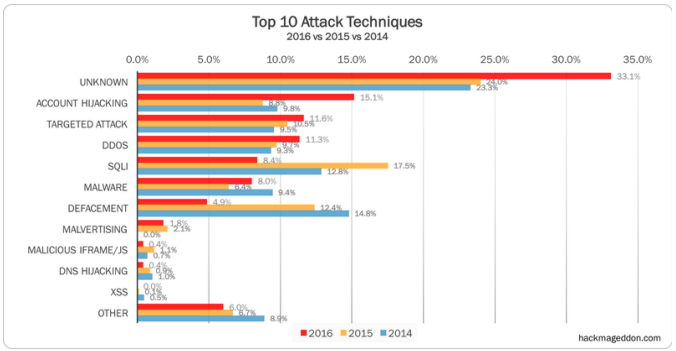
***Abstrak*—Sebagian besar penggunaan tools yang tersedia di Kali Linux masih bersifat manual, seperti halnya sqlmap, Pengguna masih harus mengetikkan sintaks untuk menjalankan tools tersebut. Hal tersebut tentunya kurang efektif dan efisien mengingat saat ini sudah banyak library atau framework yang dapat digunakan untuk mempermudah penggunaan tools tersebut. Adanya perangkat portable ini menjadi solusi keterbatasan tersebut dimana pengguna dapat melakukan pengujian keamanan dengan mudah dan ringkas. Perangkat portable ini diharapkan dapat membantu administrator atau pemilik layanan untuk melakukan pengujian secara berkala. Tujuan membangun perangkat pengujian celah keamanan ini adalah untuk membuat pengujian celah keamanan terhadap aplikasi berbasis web menjadi lebih efisien dan efektif. Aplikasi ini memiliki 2 jenis serangan untuk melakukan pengujian celah keamanan, diantaranya SQL Injection dan Cross-Site Scripting. Hasil yang dicapai berdasarkan pengujian White Box, pengujian Black Box, dan pengujian secara manual terhadap aplikasi ini adalah Perangkat Portable Pengujian Celah Keamanan pada Aplikasi Berbasis Web mampu membuat pengujian celah keamanan terhadap aplikasi berbasis web menjadi lebih efektif dan efisien.**

Kata kunci: Aplikasi Python, PyQt5, Pengujian celah keamanan, Single board PC.

I. PENDAHULUAN

Pengujian keamanan sistem komputer adalah suatu kegiatan yang dilakukan untuk menemukan celah keamanan yang terdapat pada sistem tersebut. Hasil pengujian ini dapat digunakan untuk memperbaiki sisi keamanan dari sistem untuk melindungi data-data dari serangan dan atau pencurian yang dilakukan oleh pihak-pihak yang tidak bertanggung jawab. Selama ini, untuk melakukan pengujian keamanan membutuhkan beberapa aplikasi yang dijalankan pada suatu sistem operasi. Dua contoh sistem operasi yang tersebut adalah kali linux dan parrotOs, kedua sistem operasi biasa digunakan oleh para penguji system keamanan komputer. Dalam hal ini, penguji adalah orang yang melakukan penetrasi testing atau pengujian sistem komputer dan menemukan celah keamanan pada sistem tersebut. [1].

Sistem komputer tidak pernah terhenti dari upaya adanya attack terhadap system. Sebagai contoh Gambar 1 menunjukkan data tentang sepuluh jenis serangan siber yang mengancam system keamanan computer. Berdasarkan Gambar 1 tersebut terdapat tiga contoh kasus nyata aktivitas serangan siber. Pertama adalah serangan yang dibuat oleh sekelompok hacker yang bernama TeamBerserk yang mengklaim keberhasilannya dalam mencuri dana sebesar $100,000.[2]



Gambar 1. Top 10 serangan siber

Kasus kedua adalah serangan DDoS di Amerika yang menyerang server Dyn, sebuah perusahaan infrastruktur sistem nama domain (DNS) internet. Serangan itu terjadi pada tanggal 21 Oktober 2016, dengan menginfeksi jaringan komputer menggunakan malware spesial yang diketahui bernama Mirai botnet sehingga membuat down situs Twitter, the Guardian, Netflix, Reddit, dan CNN [3]. Kasus serangan yang ketiga adalah serangan yang belum lama terjadi di tahun 2017 dan sempat viral di internet di Indonesia, serangan tersebut adalah *defeacement attack* atau mengubah tampilan laman web. Serangan tersebut yang menyebabkan sebuah situs penyedia jasa telekomunikasi dan internet Indonesia,yaitu telkomsel.com berubah tampilannya. Kejadian ini ternyata dilator belakangi oleh kekesalan para pelanggan terhadap tarif internet yang mahal dan dirasa merugikan pelanggan [4].

Dari tiga contoh kasus diatas menunjukkan bahwa pentingnya pengujian keamanan sistem komputer untuk memastikan sistem tersebut dalam keadaan aman dari serangan. Dalam pengujian sistem komputer membutuhkan banyak aplikasi penguji bahkan telah dibuat sistem operasi yang khusus untuk kepentingan pengujian sistem komputer, sebagai contoh kali linux dan parrot os. Meskipun dibuat khusus dan sering digunakan, kedua sistem operasi tersebut masih memiliki kekurangan.

Kali linux sebelumnya bernama Backtrack, adalah sistem operasi penetrasi testing paling populer yang digunakan oleh penguji. Namun untuk menjalankan perintah-perintahnya masih menggunakan terminal sehingga dirasa kurang praktis. Kemudian Parrot os yang memiliki kesamaan serupa kali linux,

yaitu merupakan sistem operasi penetrasi testing untuk pengujian keamanan sistem komputer, namun parrot os ternyata kurang populer dibandingkan dengan kali linux.

Kedua contoh sistem operasi penetrasi testing tersebut memang *powerful*, terutama kali linux. Bahkan tidak heran jika sistem operasi tersebut dibuat versi yang bisa dijalankan untuk smartphone berbasis android. Meskipun dapat dijalankan pada smartphone yang berbasis android, kali linux masih menggunakan terminal atau menulis manual perintah yang akan dijalankan sehingga kurang praktis. Untuk mengatasi permasalahan ini maka dirasa perlu kiranya dibuat sebuah alat yang dapat memberikan kemudahan kepada penguji system untuk melakukan aktivitas penetrasi testing tanpa harus melalui perangkat komputer. Solusi yang dapat diberikan adalah melalui sebuah desain alat portable yang memuat sistem operasi pengujian keamanan sistem komputer yang lebih praktis. Alat tersebut dapat dirancang sedemikian rupa hanya memuat perangkat sederhana berupa komputer papan tunggal, layar sentuh ukuran 3.5inci, powerbank yang nantinya digunakan sebagai rumah bagi sistem operasi yang akan dibuat. Keberadaan alat protable tersebut diharapkan akan memberikan kemudahan kepada penguji keamanan system untuk melakukan aktivitas pengujian dimanapun tanpa harus bergantung pada ketersediaan perangkat komputer.

II. LANDASAN TEORI

Terdapat beberapa pengetahuan dasar yang melandasi kegiatan penelitian ini. Pengetahuan dasar diperlukan untuk menjadi acuan solusi yang akan dibangun.

A. Vulnerability

Vulnerability adalah suatu titik lemah atau kerentanan dalam sebuah prosedur keamanan kontrol administratif, kontrol internet, dan lain-lain sebagai yang dapat dieksploitasi melalui suatu cara untuk memperoleh akses yang tidak sah terhadap informasi atau untuk mengganggu proses secara kritis [7]. Dalam sebuah sistem, vulnerability dapat dikatakan sebagai sebuah celah keamanan yang dapat dimanfaatkan oleh pihak tidak bertanggung jawab untuk melanggar kebijakan keamanan sistem. Setiap website berpotensi memiliki vulnerability, maka dari itu tidak ada jaminan bahwa suatu website benar-benar aman dari segala celah keamanan.

B. OWASP

OWASP (Open Web Application Security Project) merupakan komunitas terbuka diseluruh dunia yang berfokus pada peningkatan keamanan aplikasi perangkat lunak [8]. Hingga saat ini, panduan pengujian OWASP telah mencapai versi 4.0. Dan untuk pertama kalinya yakni pada tahun 2003, Yayasan OWASP merilis 10 daftar resiko keamanan aplikasi website yang paling kritis. Daftar tersebut disebut OWASP TOP 10. Seiring dengan perkembangan tekonologi dan meningkatnya kejahatan siber, Yayasan OWASP kembali merilis OWASP TOP 10 pada tahun 2004, 2007, 2010, 2013, dan terakhir pada tahun 2017. OWASP TOP 10 tidak hanya berisi daftar resiko keamanan aplikasi website yang paling kritis, namun juga berisi tentang penjelasan daftar resiko tersebut, cara mencegah celah keamanan tersebut, dan contoh skenario dari serangan tersebut.

C. Single Board PC

Single Board PC adalah sebuah perangkat komputer layaknya komputer biasa yang didalamnya terdapat cpu, ram, gpu, input, dan output yang membedakannya yaitu ukuran mininya.

D. Vulnerability Assesment

Vulnerability assessment adalah proses pengujian untuk menemukan dan mengukur tingkat seberapa tinggi resiko serta banyaknya kerentanan pada sebuah sistem. Pengujian ini biasa melibatkan penggunaan alat uji otomatis seperti pemindai keamanan web dan jaringan yang hasilnya akan dievaluasi oleh tim pengembang kemudian sistem diperbaiki untuk mengurangi resiko. Sedangkan pengujian penetrasi adalah kegiatan yang dilakukan untuk menguji sebuah sistem, pengujian ini dilakukan untuk menemukan celah keamanan pada sebuah sistem tersebut. Hasil dari pengujian penetrasi ini yang nantinya digunakan untuk memperbaiki sisi keamanan dari sistem [5].

Dalam hal ini, [6] telah melakukan penelitian dengan membuat aplikasi bernama Ardilla. Aplikasi ini dapat digunakan untuk melakukan pengujian terhadap sebuah website dengan menggunakan jenis serangan SQL Injection dan Cross-Site Scripting (XSS). Aplikasi ini akan menghasilkan vektor serangan yang konkret dan ditulis dalam bentuk bahasa pemrograman PHP (Hypertext Prepocessor). Untuk menggunakan aplikasi Ardilla ini, pengguna harus menentukan jenis serangan yang akan digunakan antara serangan SQL Injection atau serangan Cross-Site Scripting (XSS)). Nantinya, hasil keluaran dari program Ardilla adalah vektor serangan. Pada uji coba yang dilakukan, Ardilla berhasil menemukan 68 celah keamanan pada 5 program. Masing-masing program memiliki kerentanan yang berbeda-beda. Namun, masih terdapat beberapa kekurangan pada penelitian ini salah satunya adalah program ini hanya menggunakan 2 jenis serangan, yaitu SQL Injection dan Cross-Site Scripting (XSS). Sampai saat ini aplikasi Ardilla belum terpublikasi untuk publik karena aplikasi tersebut masih dalam tahap pengembangan.

Berbeda dengan aplikasi Ardilla yang menggunakan 2 jenis serangan, [7] juga telah melakukan sebuah penelitian dengan membuat sebuah aplikasi pendeteksi celah SQL Injection untuk keamanan website. Untuk menjalankan aplikasi tersebut, pertama-tama pengguna harus memasukkan alamat website yang ingin diuji. Kemudian, pengguna memilih jenis pengujian yang akan digunakan. Aplikasi ini menyediakan 8 jenis pengujian, diantaranya uji komentar baris, uji komentar sebaris, uji perintah bertumpuk, uji kalimat jika, uji bilangan bulat, uji untaian, uji penggabungan hasil query, dan uji kesalahan. Setelah itu, program tinggal dijalankan dengan menekan tombol mulai. Pada saat proses pengujian dijalankan, aplikasi ini nantinya akan menampilkan semua halaman-halaman yang ada di dalam website tersebut dengan menggunakan teknik crawling web. Selain itu, aplikasi ini juga memungkinkan pengguna untuk melihat kode HTML (Hypertext Markup Language) atau script website dari halaman yang sedang

dianalisa. Hasil akhir yang akan ditampilkan oleh aplikasi ini adalah menampilkan halaman apa saja yang rentan terhadap SQL Injection.

E. SQL Injection

SQL (*Structured Query Language*) *Injection* merupakan suatu teknik peretasan yang memungkinkan penyerang mendapatkan akses yang tidak sah kedalam database kemudian menyerang atau mengubah data-data yang berada didalam database [6]. Berdasarkan data dari Akamai Q2 pada tahun 2016 [9], SQL Injection merupakan ancaman yang sering terjadi pada aplikasi web server setelah Local File Inclusion (LFI) dengan presentasi sebesar 44.11%, diikuti dengan Cross-Site Scripting (XSS) dengan presentasi sebesar 5.91% dan Remote File Inclusion (RFI) 2.27%. Teknik SQL Injection ini digunakan dengan cara memasukkan perintah-perintah SQL melalui alamat URL (Uniform Resource Locator) atau melalui kolom masukan yang nantinya akan dieksekusi oleh server ketika meminta data ke dalam database.

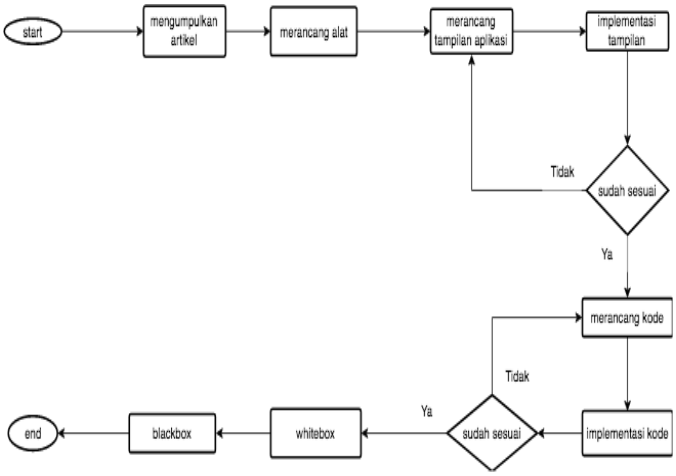
F. Cross-Site Scripting

Cross-Site Scripting (XSS) merupakan sebuah jenis serangan yang memanfaatkan kelemahan server dalam melakukan validasi terhadap masukan yang diberikan oleh pengguna. XSS memungkinkan penyerang mengeksekusi script-script didalam browser korban, sehingga dapat mengubah tampilan website atau mengarahkan pengguna ke situs-situs nakal [10]. Selain itu, jenis serangan ini juga memungkinkan penyerang untuk mencuri cookies pengguna lain. Ketika penyerang telah mendapatkan cookies dari pengguna lain, maka penyerang dapat memuat nilai sesi tersebut dan menggunakannya untuk masuk ke website yang digunakan oleh cookies tersebut. Banyak penyedia layanan yang tidak mengakui dan menganggap bahwa celah dari serangan Cross-Site Scripting (XSS) tidak begitu berbahaya, sehingga banyak dari mereka yang tidak melakukan langkah pencegahan terhadap serangan ini [11]. Menurut [12], Cross-Site Scripting (XSS) memiliki 2 jenis, yaitu Reflected XSS dan Stored XSS. Reflected XSS adalah jenis serangan XSS yang hanya berjalan pada halaman klien (client page). Jenis serangan ini biasanya digunakan oleh penyerang untuk mencari celah keamanan sebuah website dari sisi klien. Berbeda dengan Reflected XSS, Stored XSS merupakan jenis serangan XSS yang dapat berjalan disisi klien dan server. Hal tersebut dikarenakan script yang dimasukkan oleh penyerang akan tersimpan didalam database. Jenis serangan ini lebih berbahaya dibandingkan Reflected XSS, karena script yang telah dimasukkan oleh penyerang akan terus berjalan setiap pengguna memanggil halaman yang terinjeksi.

III. METODOLOGI PENELITIAN

Secara umum penelitian ini bertujuan untuk merancang sebuah perangkat pengujian keamanan aplikasi berbasis web dengan memanfaatkan single board komputer, lcd touchscreen, sdcard, dan baterai. Aplikasi yang dirancang diperuntukan bagi kepentingan pengujian khususnya pada sistem berbasis web dengan berpedoman pada metode OWASP top 10 tahun 2013.

Sementara metode penelitian yang digunakan untuk membuat aplikasi adalah sebagaimana pada Gambar 2.



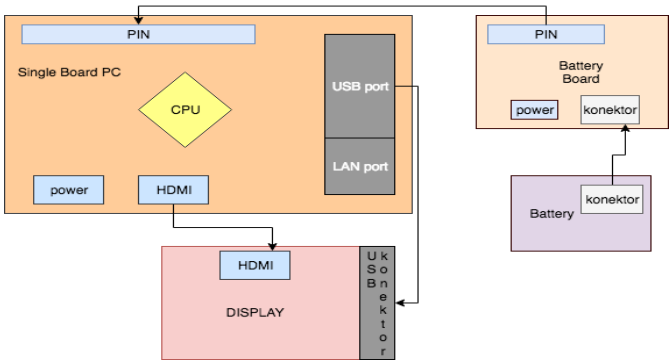
Gambar 2. Diagram alur pengerjaan perangkat

Salah satu tahapan dari penelitian ini adalah merancang tampilan aplikasi menggunakan modul PyQt5. Setelah merancang tampilan lalu mengimplementasikan tampilan sesuai dengan rancangan yang telah dibuat. Ketika tampilan sudah sesuai dengan yang diharapkan maka menuju tahapan selanjutnya atau tahapan ketiga yaitu tahap merancang kode. Source code ini yang nantinya akan berfungsi sebagai sarana untuk melakukan serangan SQL Injection dan serangan XSS. Kode yang sudah dirancang maka diimplementasikan agar sesuai dengan yang dibutuhkan.

Pada proses perancangan dan pembuatan perangkat terdapat beberapa komponen perangkat keras yang digunakan. Dalam perangkat keras peneliti menggunakan single board PC. Untuk menunjang daya digunakan baterai, sedangkan untuk menampilkan layar menggunakan lcd layar sentuh yang berukuran 5inch. Kemudian untuk pengujian perangkat menggunakan sebuah laptop.

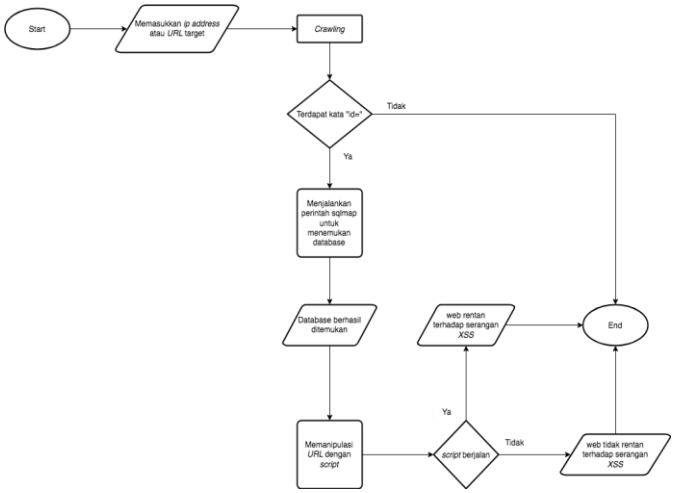
Pada proses perancangan dan pembuatan aplikasi terdapat beberapa komponen perangkat lunak yang digunakan. Dalam perangkat lunak sistem, peneliti menggunakan sistem operasi MacOs. Untuk merancang tampilan (interface) aplikasi, digunakan tools Pencil karena tools tersebut telah memiliki library GUI (Graphic User Interface) untuk memudahkan saat digunakan. kemudian pembuatan aplikasi, digunakan bahasa pemrogaman python versi 3.6 dan modul PyQt5 dikarenakan hasil yang lebih baik dan lebih jernih dibandingkan modul Tkinter. Sedangkan untuk text editor, digunakan JetBrain PyCharm. Dan untuk melakukan pengujian secara manual dibutuhkan browser Mozilla Firefox.

Perangkat yang akan dibuat nantinya menggunakan single board PC berbasis raspberry pi. Raspberry pi dipilih karena dukungannya yang cukup luas untuk melakukan pengembangan. Selain itu dukungan terhadap perangkat-perangkat tambahan lainnya juga cukup banyak. Perangkat yang dibuat akan ditenagai baterai dan juga dilengkapi dengan layar berukuran 5 inch. Baterai yang digunakan agar tujuan dari portabilitas perangkat tersebut terpenuhi. Hasil perancangan perangkat tersebut dapat dilihat pada Gambar 3.

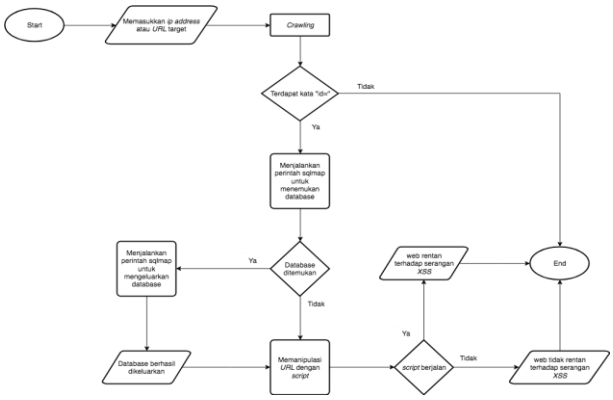


Gambar 3. Perancangan perangkat

Aplikasi Pengujian Celah Keamanan Nenggala memiliki dua alur diagram (flowchart) yaitu alur yang pertama dapat dilihat pada Gambar 4. Ketika pengguna membuka aplikasi Nenggala, hal pertama yang dilakukan adalah aplikasi meminta pengguna untuk memasukkan alamat target, baik berupa alamat URL maupun ip address. Selanjutnya aplikasi akan melakukan crawling untuk mencari tautan-tautan yang berada di halaman awal target. Jika terdapat tautan yang memiliki kata "id=", maka aplikasi menjalankan perintah sqlmap untuk menemukan database. Jika tidak terdapat tautan yang memiliki kata "id=", maka aplikasi akan akan berhenti melakukan proses pengujian. Lalu alur diagram yang kedua Aplikasi Pengujian Celah Keamanan Nenggala dapat dilihat pada Gambar 5. proses yang terjadi hampir sama dengan alur yang pertama hanya saja yang membedakan yaitu pada alur yang kedua aplikasi Nenggala menjalankan perintah sqlmap untuk mengeluarkan isi dari database target.



Gambar 4 *Flowchart* aplikasi tanpa *dump*



Gambar 5. Diagram alur aplikasi dengan dump

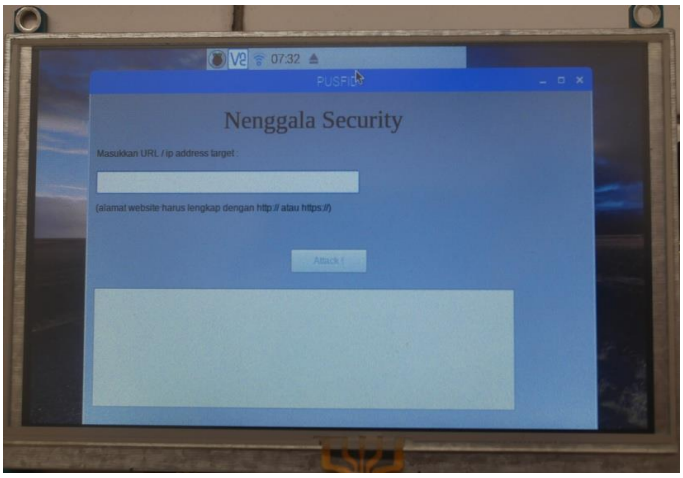
IV. IMPLEMENTASI DAN PENGUJIAN

Perangkat yang sudah dirancang pada tahapan kemudian diimplementasikan dengan kelengkapan implementasi sebagaimana pada Tabel 1.

TABEL1 TABEL PERANGKAT

No.	Item	Perangkat	Keterangan
1	Single Board PC	Raspberry pi 3	-
2	Baterai	GeekWorm	2500 mAh
3	Layar	Waveshare	5 inch
4	Sistem Operasi	Debian	Raspbian Jessie

Pada form alamat target, pengguna diminta untuk mengisi alamat target dengan benar yaitu diawali dengan "http://" atau "https://". Halaman awal terdapat 2 proses, yaitu proses keluar dan proses pengujian. Proses keluar merupakan proses yang akan membuat pengguna keluar dari aplikasi. Sedangkan proses pengujian adalah proses yang digunakan untuk menjalankan porses pengujian terhadap target. Proses keluar dijalankan dengan menekan tombol silang dan proses pengujian dijalankan dengan menekan tombol Attack!. Implementasi halaman awal dapat dilihat pada Gambar 6.



Gambar 6. Implementasi antarmuka aplikasi

Jenis serangan pertama yang akan diujikan kepada alamat target adalah serangan SQL Injection. Kode program serangan SQL Injection secara keseluruhan dapat dilihat pada Gambar 7.

```
input(alamatURL)
BeautifulSoup(response, 'html5lib') ← soup
soup.find(kata : 'id=') ← kondisiSQLXSS
if (kondisiSQLXSS) then
  get('href') ← URL
    try:
        apa = []
        command = ('sqlmap -u ' + URLSql[0] + ' -dbs' +
' -batch')
        result                                    =
subprocess.Popen(command,stdout=subprocess.PIPE,
shell=True)
        tulis = open('file.txt', 'w')
        baca = open('file.txt', 'r')
        commandDB = ('sqlmap -u ' + URLSql[0] + ' -D ' +
database +
' -dump-all'+          '--batch')
        tulisDB = open('fileDB.csv', 'w')
    urllib.request.open(URL                          +
'<script>alert(222)</script>')
    soup.find(kata : 'alert') ← kondisiXSS
    if(kondisiXSS) then
      output("Website rentan terhadap serangan XSS")
    else
      output("Website  tidak  rentan  terhadap  serangan
XSS")
else
  output("Website tidak rentan")
```

Gambar 7. Kode program serangan SQL injection

Jenis serangan terakhir yang akan diujikan kepada alamat target adalah serangan Cross-Site Scripting (XSS). Kode program serangan Cross-Site Scripting secara keseluruhan dapat dilihat pada Gambar 8

```
try:
responseXSS=urllib.request.urlopen(URLXss[intXSS]+
"%22%3E%3Cscript%3Ealert%28222%29%3C%2Fscript%3E").read()
soupXSS = BeautifulSoup(responseXSS, 'html5lib')
kondisiXSS = soupXSS.find_all('script',
string=re.compile('alert'))
print(kondisiXSS)
if len(kondisiXSS) > 0:
  print(datetime.now().strftime("%d-%m-%Y %H:%M:%S") + " " +
  URLXss[intXSS] + " rentan terhadap serangan
  Cross-Site Scripting")
  self.textArea.insertPlainText(datetime.now()
  .strftime("%d-%m-%Y %H:%M:%S") + " " +
  URLXss[intXSS] + " rentan terhadap serangan
  Cross-Site Scripting\n")
                        tdkXSS.append("tidak")
                    intXSS = intXSS + 1
                except HTTPError as e:
                    print(datetime.now()
  .strftime("%d-%m-%Y %H:%M:%S") + " " +
  URLXss[intXSS], ":", e.code, e.reason)
                    intXSS = intXSS + 1
          except http.client.IncompleteRead as e:
          responseSQL = e.partial
            if len(tdkXSS) == 0:
        print(datetime.now().strftime("%d-%m-%Y %H:%M:%S") + " "
+
  URLAsli, "tidak rentan terhadap serangan
  Cross-Site Scripting")
  self.textArea.insertPlainText(datetime.now() >>>>>>>
  .strftime("%d-%m-%Y %H:%M:%S") + " " +
  URLAsli + " tidak rentan terhadap serangan
Cross-Site Scripting\n")
```

Gambar 8. Kode program serangan Cross-Site Scripting

Pertama-tama aplikasi akan membaca nilai berupa alamat website yang ada pada array “URLXSS”. Selanjutnya, aplikasi akan menyisipkan script alert (pemberitahuan) pada akhir alamat dan mengunjungi alamat yang telah disisipkan script tersebut. Setelah itu, terdapat sebuah variabel yang berfungsi untuk mencari kata “alert” pada tag script. Jika terdapat kata “alert” pada tag script di halaman target, maka aplikasi akan memberikan keluaran informasi bahwa alamat target rentan terhadap serangan Cross-Site Scripting (XSS). Sebaliknya, jika kondisi tersebut salah, maka aplikasi akan memberikan keluaran informasi bahwa alamat target tidak rentan terhadap serangan Cross-Site Scripting (XSS).

A. Hasil Pengujian

Pengujian terhadap beberapa jenis merupakan tahap pengujian untuk membuktikan apakah Aplikasi Pengujian Celah Keamanan pada Aplikasi Berbasis Web dapat digunakan untuk menguji segala jenis website (bersifat universal) atau tidak. Jenis-jenis website yang akan diuji, diantaranya wesbite yang dibangun dengan struktur HTML dan PHP biasa (website umum), website yang dibangun dengan menggunakan CMS (Content Management System) Wordpress, dan website yang dibangun dengan menggunakan framework terkini seperti Laravel dan CodeIgniter.

Perbedaan dasar dari ketiga jenis website tersebut dapat dilihat dari pemanggilan terhadap source gambar, source css, dan hyperlink. Website yang menggunakan struktur HTML dan PHP biasa, pada umumnya memanggil source gambar dan css langsung dari folder gambar dan css itu sendiri atau menambahkan tanda titik 2 kali (..) diawal, seperti "img/logo.png" atau "../css/style.css". Selain itu, alamat URL pada website yang menggunakan struktur HTML dan PHP biasa identik dengan kata "id=" diakhir alamat.

Lain halnya dengan website yang dibangun dengan menggunakan CMS. Website yang dibangun dengan menggunakan CMS pada umumnya memiliki kata "wp" pada alamat source yang digunakan, seperti "www.abc.xyz/wp-content/image/logo.png". Sedangkan, untuk mengetahui website yang dibangun dengan menggunakan framework Laravel atau CodeIgniter adalah dengan melihat source gambar dan hyperlink yang digunakan. Source gambar dan hyperlink yang digunakan pada umunya diawali dengan base path. Base path ini merupakan path yang namanya mirip seperti alamat URL. Contoh souce gambar pada framework Laravel adalah "https://www.abc.xyz/storage/product-variants/logo.jpeg".

Website yang akan dijadikan target pada pengujian ini, diantaranya "http://www.f10products.co.za" yang dibangun menggunakan HTML dan PHP biasa (website umum), "http://www.tobiweb.id/" yang dibangun menggunakan Framework CodeIgniter, dan "https://www.needrom.com/" yang dibangun menggunakan CMS Wordpress. Untuk hasil pengujian terhadap beberapa jenis website dapat dilihat pada

Dari hasil pengujian diatas, Aplikasi Pengujian Celah Keamanan pada Aplikasi Berbasis Web menemukan celah pada "http://www.f10products.co.za" . Celah tersebut dapat ditemukan karena website tersebut masih menggunakan HTML dan PHP biasa dalam pembangunan struktur web nya. Dengan struktur HTML dan PHP biasa, Aplikasi Pengujian Celah Keamanan pada Aplikasi Berbasis Web mampu dengan mudah mendapatkan alamat yang mengandung kata "id=". Berbeda dengan "http://www.tobiweb.id/" tidak ditemukan kerentanan dari Aplikasi Pengujian Celah Keamanan pada Aplikasi Berbasis Web. Hal tersebut dapat terjadi karena dengan menggunakan struktur framework (baik Laravel, maupun CodeIgniter) dalam membangun sebuah website, developer (pengembang) dapat mengatur alamat link agar kata "id=" dapat disembunyikan. Selain itu, pengembang juga memiliki hak penuh dalam mengatur keamanan dari website tersebut. Jadi, Aplikasi Pengujian Celah Keamanan pada Aplikasi Berbasis Web dapat digunakan untuk melakukan pengujian terhadap website yang dibangun dengan HTML biasa dan website yang dibangun dengan CMS Wordpress.

B. Perbandingan terhadap Aplikasi Sejenis

Pada tahap ini, aplikasi akan dibandingkan dengan aplikasi sejenis yang telah ada sebelumnya, yaitu SqlMap. Perbandingan ini dilakukan untuk mengetahui kelebihan dan kekurangan dari Aplikasi Pengujian Celah Keamanan pada Aplikasi Berbasis Web. Walaupun algoritma yang digunakan oleh kedua aplikasi tersebut berbeda dengan algoritma yang digunakan oleh Aplikasi Pengujian Celah Keamanan pada Aplikasi Berbasis Web, namun secara garis besar kedua aplikasi tersebut memiliki fungsi untuk mencari informasi apakah alamat website yang dimasukkan oleh pengguna rentan terhadap serangan yang dimiliki masing-masing aplikasi atau tidak.

SqlMap merupakan salah satu alat atau aplikasi yang sering digunakan oleh para peretas untuk mencari celah keamanan pada sebuah sistem. Pada dasarnya alat ini menggunakan teknik SQL Injection untuk menyerang targetnya. Alat ini memiliki beberapa kelebihan, diantaranya aplikasi ini dapat melakukan SQL Injection dengan beberapa metode, seperti Union Query SQL Injection, Error-Based SQL Injection, Boolean-Based SQL Injection, dan Time-Based SQL Injection. Selain itu, aplikasi ini juga dapat berjalan untuk beberapa jenis database, seperti MySQL, Oracle, PostgreSQL, dan masih banyak lagi. Kelebihan tersebut tentunya semuanya dapat dimanfaatkan oleh Aplikasi Pengujian Celah Keamanan pada Nenggala. Namun, kelebihan Aplikasi Pengujian Celah Keamanan pada Aplikasi Nenggala yang belum tentu dimiliki oleh SqlMap adalah aplikasi tersebut dapat menerima target dari pengguna berupa alamat utama sebuah website. Tidak seperti SqlMap yang mengharuskan pengguna memasukkan alamat target secara spesifik (mengandung kata "id=").

Untuk mengetahui perbandingan Aplikasi Pengujian Celah Keamanan pada Aplikasi Nenggala terhadap sistem operasi sejenis lebih rinci, maka Rincian tabel perbandingan dapat dilihat pada Tabel 2.

TABEL 2 TABEL PERBANDINGAN SISTEM OPERASI

Spesifikasi	**RaspbianOs**	**Kali Linux**
CPU	4x ARM Cortex-A53, 1.2GHz	4 processor core i7, 2.5GHz
GPU	Broadcom VideoCore IV	Intel Iris Pro
RAM	1GB LPDDR2 (900 MHz)	2GB LPDDR3 (1600MHz)
Waktu Booting	17 detik	19 detik
Waktu menjalankan pengujian	55 detik	4860 detik

Dari perbandingan di atas, dapat disimpulkan hasil perbandingan dari ketiga aplikasi, yaitu Aplikasi Pengujian Celah Keamanan pada Aplikasi Berbasis Web lebih mudah digunakan dibandingkan tools SqlMap dan SET dengan presentasi sebesar 88%. Selanjutnya, tools SqlMap membutuhkan waktu paling lama dalam melakukan pengujian dibandingkan tools SET dan Aplikasi Pengujian Celah Keamanan pada Aplikasi Berbasis Web. Dan tools SET

memiliki kemampuan yang paling baik dalam melakukan pengujian dibandingkan tools SqlMap dan Aplikasi Pengujian Celah Keamanan pada Aplikasi Berbasis Web.

V. KESIMPULAN DAN SARAN

Berdasarkan rumusan yang telah dibuat dan hasil penelitian yang sudah dilakukan maka dapat ditarik kesimpiulan sebagai berikut

1. Berhasil dirancang perangkat pengujian sistem komputer dengan memanfaatkan single board komputer, lcd touchscreen, sdcard, dan powerbank.
2. Berhasil dirancang aplikasi Nenggala pengujian sistem komputer dengan menggunakan metode owasp top 10 tahun 2013 yang berjalan pada perangkat raspberry pi.
3. Berhasil menguji aplikasi penetrasi testing yang telah dirancang dengan cara membandingkan aplikasi sejenis. Hasil dari perbandingan tersebut yaitu aplikasi Nenggala menjalankan proses mengeluarkan database lebih cepat dengan waktu 55 detik.

Dari penelitian yang telah dilakukan masih terdapat beberapa kekurangan dan kelemahan yang dapat dikembangkan lebih lanjut. Hal yang dapat dikembangkan dari penelitian ini yaitu :

1. Mengatasi kendala lambatnya waktu untuk booting dengan cara melakukan uninstall aplikasi-aplikasi yang tidak diperlukan.
2. Mengembangkan solusi dengan memanfaatkan bahasa pemrograman atau library yang dapat menampilkan proses yang berjalan secara real-time pada halaman GUI aplikasi.
3. Mengembangkan teknik web crawling yang tidak hanya dapat melakukan crawling pada halaman awal dari sebuah website, melainkan mampu melakukan crawling secara mendalam pada sebuah alamat website.

Pengembangan dari aplikasi ini juga diharapkan dapat menambahkan jenis serangan untuk melakukan pengujian pada aplikasi berbasis web, contohnya man in the middle attack.

REFERENSI

[1] J. Ismail, "Penetration Test - Pengujian Sistem Keamanan," 2014. [Online]. Available: http://julismail.staff.telkomuniversity.ac.id/penetration-test/. [Accessed: 04-Nov-2017].

[2] M. Kumar, "Hacker stole $100,000 from Users of California based ISP using SQL Injection," 2013. [Online]. Available: https://thehackernews.com/2013/10/hacker-stole-100000-from-users-of.html. [Accessed: 04-Nov-2017].

[3] N. Woolf, "DDoS attack that disrupted internet was largest of its kind in history, experts say," *The Guardian*, 2016. [Online]. Available: The Guardian, https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet. [Accessed: 19-Mar-2018].

[4] A. Nugraha, "Hack Deface Web Telkomsel.com, Tamparan keras buat perusahaan pengelola teknologi," 2017. [Online]. Available: http://www.arthanugraha.com/hack-deface-web-telkomsel-com-tamparan-keras-buat-perusahaan-pengelola-teknologi/. [Accessed: 04-Nov-2017].

[5] I. Muscat, "The difference between Vulnerability Assessment and Penetration Testing - Acunetix," 2017. [Online]. Available: https://www.acunetix.com/blog/articles/difference-vulnerability-assessment-penetration-testing/. [Accessed: 25-Mar-2018].

[6] A. Kiezun et al., "Automatic creation of SQL injection and cross-site scripting attacks," *Proc. - Int. Conf. Softw. Eng.*, pp. 199–209, 2009.

[7] A. M. Elu, "Rancang Bangun Aplikasi Pendeteksian Vulnerability Structured Query Language (Sql) Injection Untuk Keamanan Website," *Jurnal Teknologi Informasi*, vol. 7, no. 22, pp. 111–124, 2013.

[8] M. Meucci and A. Muller, "Testing Guide 4.0," Open Web Application Security Project (OWASP), 2014. [Online]. Available: OWASP https://www.owasp.org/images/1/19/OTGv4.pdf

[9] D. Fernandez, J. Arteaga, and E. Caltum, "Akamai's State of Internet / Security Q2 2016 Report," 2016.

[10] M. D. Gower and R. A. Shanks, "The effect of chain transfer agent level on adhesive performance and peel master-curves for acrylic pressure sensitive adhesives," *Macromol. Chem. Phys.*, vol. 205, no. 16, pp. 2139–2150, 2004.

[11] H. Tolle, T. A. Kurniawan and A. Zakaria, "Peningkatan Keamanan Web terhadap Serangan Cross-Site Scripting (XSS)," *TEKNO*, vol. 9, no. 1, 2012.

[12] S. Irwan and N. Arif, "Investigasi Web Attack Menggunakan Intrusion Detection System (IDS) dan Access Log," Doctoral dissertation, Program Studi Teknik Informatika FTI-UKSW, 2014.

[13] D. M. Oktaviani, "Sistem Rekomendasi Penyewaan Sound System Pada Ud . Dyah Audio Berbasis Web Menggunakan Metode Euclidean Distance," *Artik. Skripsi*, pp. 1–15, 2015.