Jurnal Informatika Universitas Pamulang **ISSN: 2541-1004**
Penerbit: Program Studi Teknik Informatika Universitas Pamulang **e-ISSN: 2622-4615**
Vol. 6, No. 2, Juni 2021 (225-231) **10.32493/informatika.v6i2.8635**

Pengujian Kualitas Aplikasi Web E-Learning Universitas Pamulang Menggunakan Metode Black Box

Fefbi Septa Kristara[1], Gusti Kanuraga[2], Rohmat[3], Dedi Yansah[4], Aries Saifudin[5], Yulianti[6]

Teknik Informatika, Universitas Pamulang, Jl. Raya Puspitek No. 46 Buaran, Serpong, Tangerang Selatan, Banten, Indonesia, 15417
e-mail: [1]fefbisepta86@gmail.com, [2]Gustikanuraga0@gmail.com, [3]Rohmatalmusawa@gmail.com, [4]dediyansah@gmail.com, [5]aries.saifudin@unpam.ac.id, [6]yulianti@unpam.ac.id

Submitted Date: December 29th, 2020 Reviewed Date: April 28th, 2021
Revised Date: August 10th, 2021 Accepted Date: August 11th, 2021

Abstrak

A website will always have vulnerabilities in its system. One of the vulnerabilities that often occur on a website is an input validation problem or error handling that usually occurs in an input form. Testing on the Pamulang University e-learning website is important to guarantee that the software produced is meet the requirements. This test is doing to measure how good is the quality of the Pamulang University e-learning website. Good quality service will give satisfaction to students as users who benefit the most from the website. Testing the Pamulang University e-learning website is done using the black box testing method with the fuzzing technique approach. This technique can display complete information regarding the response from the server when the input form is giving abnormal data. The information obtained will later be analyzed to determine possible vulnerabilities.

Keywords : black box; fuzzing; website; e-learning.

Abstrak

Sebuah website akan selalu memiliki kerentanan di dalam sistemnya. Salah satu kerentanan yang sering terjadi pada sebuah website adalah masalah *input validation* atau *eror handling* yang biasanya terjadi pada suatu form masukan. Pengujian kualitas pada website e-learning Universitas Pamulang sangat penting untuk dilakukan guna memberikan jaminan bahwa software yang dihasilkan telah sesuai dengan persyaratan. Pengujian ini dilakukan untuk mengukur seberapa baik kualitas website e-learning Universitas Pamulang. Kualitas layanan yang baik akan memberikan kepuasan terhadap mahasiswa sebagai pengguna yang paling banyak mengambil manfaat dari website tersebut. Pengujian website e-learning Universitas Pamulang dilakukan dengan menggunakan metode black blox testing dengan pendekatan teknik fuzzing. Teknik ini dapat menampilkan informasi secara lengkap, mengenai respon dari server ketika form masukan diberi data yang tidak normal. Informasi yang didapat nantinya akan dianalisa untuk mengetahui kerentanan yang mungkin terjadi .

Kata kunci: black box; fuzzing; website; e-learning

1 Pendahuluan

Pengujian suatu website dapat membantu menjaga kualitas dan mutu sebuah website (Wicaksono, Kusumaningsih, & Iswahyudi, 2020). Pengujian dapat menyebabkan pengguna percaya bahwa fungsionalitas aplikasinya sudah berfungsi dengan baik dan tidak ragu untuk menggunakannya (Susanto, Biqirrosyad, Junaidi, Sudrajat, & Desyani, 2021). Mengingat sekarang ini banyak sekali serangan yang dilakukan pada website oleh orang yang tidak bertanggung jawab. Hal semacam ini tentunya memberikan kerugian terhadap pemilik website dan pengguna website (Afandi, Iswahyudi, & Rachmawati, 2019). Dengan dilakukan pengujian kita dapat mengantisipasi serangan-serangan yang mungkin terjadi, karena kita bisa mengetahui kerentanan yang terjadi pada website dan bisa segera diperbaiki (Andria, 2020).

Website e-learning Universitas Pamulang adalah sebuah website yang cukup penting karena website ini digunakan oleh pihak Universitas Pamulang untuk melakukan kegiatan belajar mengajar secara online atau daring. Untuk bisa mengakses, mahasiswa membutuhkan sebuah akun yaitu username dan password untuk masuk ke sistem. Untuk itu perlu dilakukan pengujian pada form login ini, untuk mengetahui kerentanan yang mungkin terjadi.

Ada banyak sekali kerentanan yang bisa terjadi pada sebuah website (Sanjaya, Sasmita, & Arsa, 2020). Salah satu yang sering terjadi adalah *input validation* atau kerentanan website terhadap suatu form masukan. Teknik yang sering digunakan untuk mengeksploitasi kerentanan ini adalah sql-injection dan XSS (Cross Site Scripting) (Gultom & Harahap, 2015). Kerentanan ini cukup berbahaya, karena penyerang dapat mengambil data-data penting seperti data user dan cookie.

Dari uraian di atas *black box testing* dengan teknik fuzzing bisa jadi alternatif untuk pengujian yang efektif. Pengujian black box dilakukan berdasarkan masukan dan luaran tanpa memperhatikan rincian program sehingga penguji tidak perlu memiliki pengetahuan pemrograman (Shaleh, Prayogi, Pirdaus, Syawal, & Saifudin, 2021). *Black box testing* adalah salah satu pengujian yang dilakukan setelah website dipublikasi (Wahyuningrum & Januarita, 2015). Para penguji di sini tentunya tidak mengetahui atau tidak punya akses di suatu website, karena para penguji bertindak sebagai pengguna yang sedang menggunakan aplikasi (Wahyudi, 2019). *Fuzzing* adalah salah satu teknik dalam *black box testing* yang diujikan pada form input suatu website dengan mengirimkan data-data yang tidak normal untuk mengetahui respon server.

Teknik fuzzing ini akan dilakukan pada website e-learning Universitas Pamulang di form login dengan memasukan data-data yang tidak normal pada form login yang berupa sebuah sintaks SQL dan script javascript. Pengujian ini bertujuan untuk mengetahui apakah system login bisa menangani masukan-masukan dengan data-data yang tidak normal, seperti yang dimaksud di atas.

2 Metodologi

Pengujian yang akan dilakukan menggunakan metode *black box testing*, yaitu pengujian yang berfokus pada masukan dan luaran tanpa memperhatikan proses di dalam aplikasi (Nurudin, Jayanti, Saputro, Saputra, & Yulianti, 2019). Pengujian black box yang akan dilakukan menggunakan teknik fuzzing. Fuzzing adalah teknik untuk menguji kerentanan web yaitu *input validation* atau *eror handling*, dengan cara memasukan nilai yang tidak normal ke suatu form input suatu website (Riadi, Yudhana, & Wahyu, 2020). Nilai yang dimasukkan bisa berupa sintaks DBMS (Database Management System) atau berupa script javascript untuk memanipulasi form input (Guntoro, Costaner, & Mustawati, 2020), nantinya akan dianalisa respon balasan dari server yang muncul di client side.

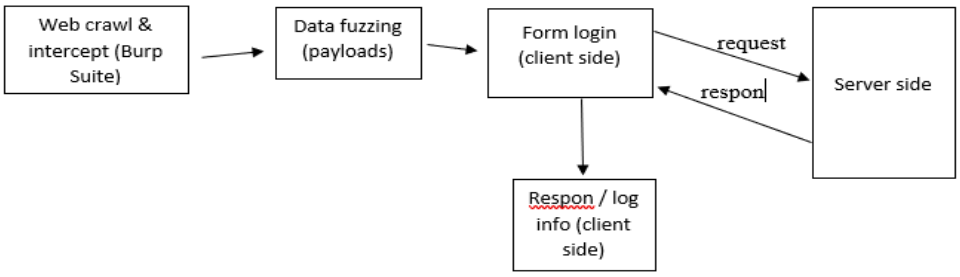
Form yang akan diuji pada website e-learning Universitas Pamulang adalah form login. Form login memerlukan 2 data masukan yaitu username dan password untuk masuk ke website e-learning. Form login ini menggunakan method post, yang artinya form ini akan melakukan request data ke server lalu server akan mengembalikan data yang diminta ke user.

Untuk melakukan fuzzing perlu identifikasi form input untuk pengumpulan informasi bagaimana form login tersebut memproses masukan yang diberikan menggunakan web interceptor. Menyiapkan data fuzzing, data yang digunakan adalah script untuk manipulasi form input, kami dapat dari github. Setelah data disiapkan lalu, memasukan data *fuzzing* pada form login menggunakan tool otomatis (intruder burp suite). Amati respon dari server yang ditampilkan di client lalu kita analisa, apakah ada kemungkinan untuk dieksploitasi.

3 Hasil Dan Pembahasan

Untuk melakukan tes fuzzing kita membutuhkan sebuah alat bernama ‘burpsuite’. Alat ini digunakan untuk mengotomatisasi tes fuzzing yang akan dilakukan. Berdasarkan bagan fuzzing test pada Gambar 1, maka pengujian yang dilakukan adalah:

1. Melakukan crawl website e-learning Universitas Pamulang di form login untuk mendapatkan informasi bagaimana metode yang digunakan yang nantinya akan digunakan untuk memasukan payloads atau data fuzzing.



Gambar 1 Bagan fuzzing test

```
POST /login/index.php HTTP/1.1
Host: e-learningab.unpam.ac.id
Connection: close
Content-Length: 21
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: https://e-learningab.unpam.ac.id
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://e-learningab.unpam.ac.id/login/index.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: _ga=GA1.1.515561953.1602769887; MoodleSession=85okocmr9vh97a05ln2bjdp81d; _ga_SDV98CJGSQ=GS1.1.1602769887.1.0.1602769894.0; _ga_BGB5YE9KT9=
GS1.1.1602769896.1.1.1602769903.0

username=x&password=x
```

Gambar 2 Crawl website e-learning Universitas Pamulang

Kami mendapatkan informasi tentang method http yang digunakan, dan form login untuk masukan username dan password. Gambar 2 menunjukkan sebuah form yang diminta (request) ke server.

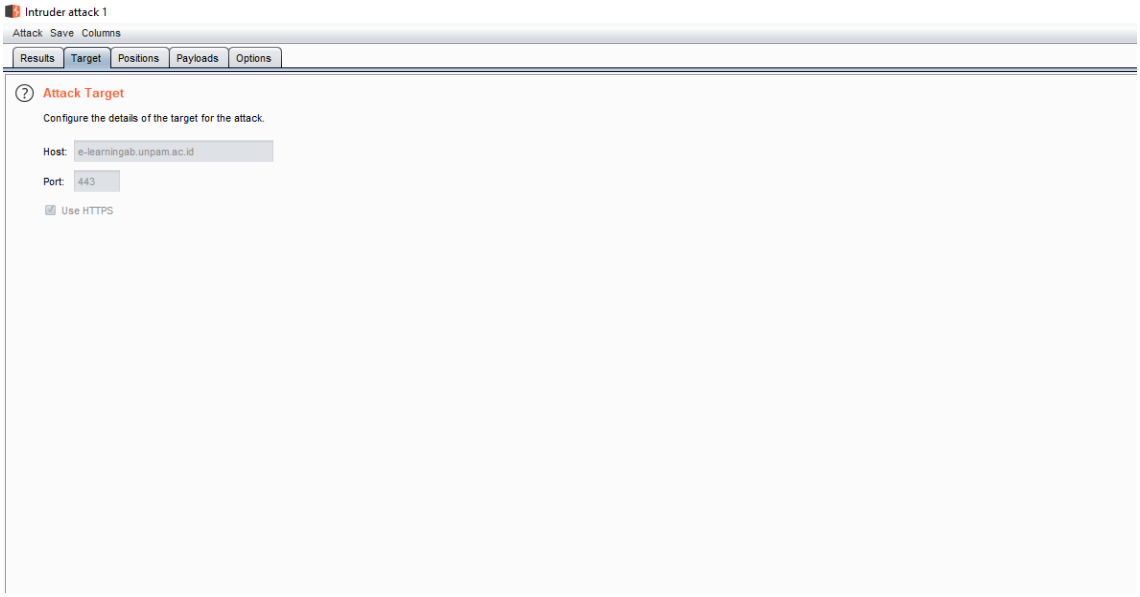
2. Data fuzzing atau payloads yang digunakan ada 2 jenis yaitu sql-fuzzing dan xss-fuzzing. Ini adalah common payloads. Datanya seperti berikut:

Tabel 1 Data fuzzing

No.	Sql-Fuzzing	Xss-Fuzzing
1	‘	<x onclick=alert(1)>click this!
2	‘’	<script>alert(1)//
3	#	<script>alert(1)<!–
4	--	<script>alert(1)</script>
5	0 or 1=1	<script src=javascript:alert(1)>
6	‘ or 0=0 --	<form><input formaction=javascript:alert(1) type=image src=SOURCE>
7	“ or 0=0 --	<script src="data:,alert(1)//
8	Or 0=0 --	"><script src=data:,alert(1)//
9	‘ or ‘1’=’1’--	<script/src="data:,eval (atob(location.hash.slice(1)))//#alert(1)
10	‘ or a=a--	<body onload=alert(1)>

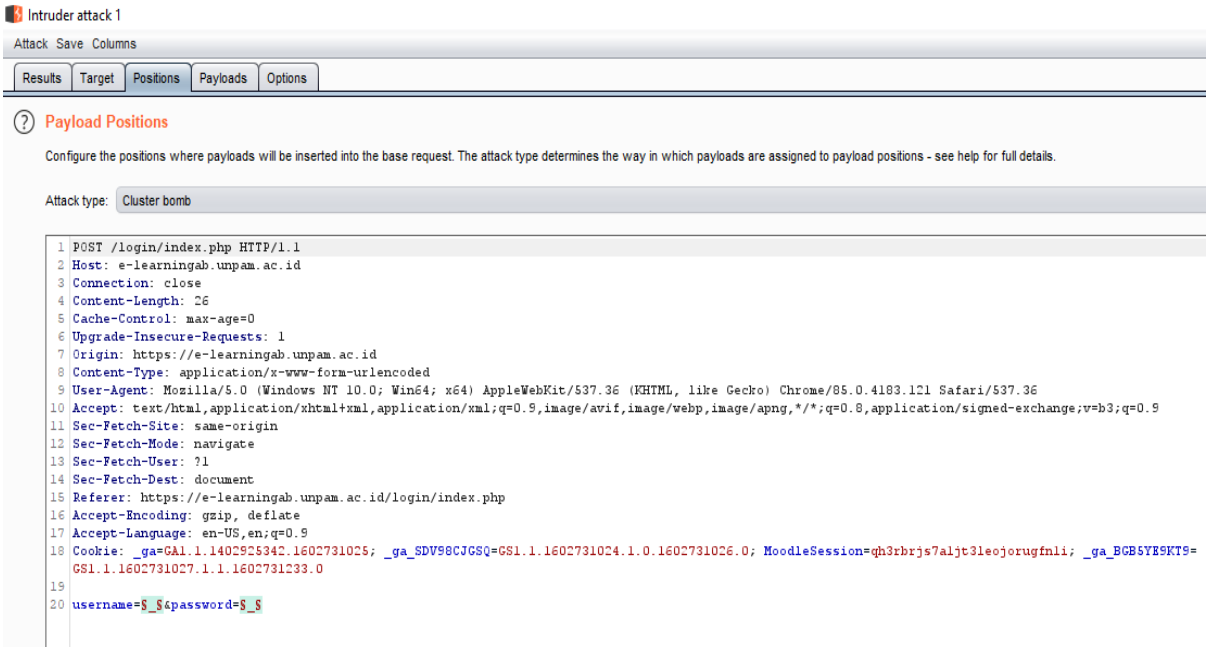
3. Melakukan fuzzing, kami menggunakan intruder yang ada pada burpsuite dengan port https (443). Ada 2 metode untuk melakukan fuzzing, yang pertaman untuk sql-fuzzing dan kedua untuk xss-fuzzing, yaitu:

- Sql-fuzzing
  Memasukkan data sql-fuzzing atau payloads secara bersama di form username dan password (cluster bomb) dan melakukan request ke server.



Gambar 3 Attack target pada Sql-fuzzing

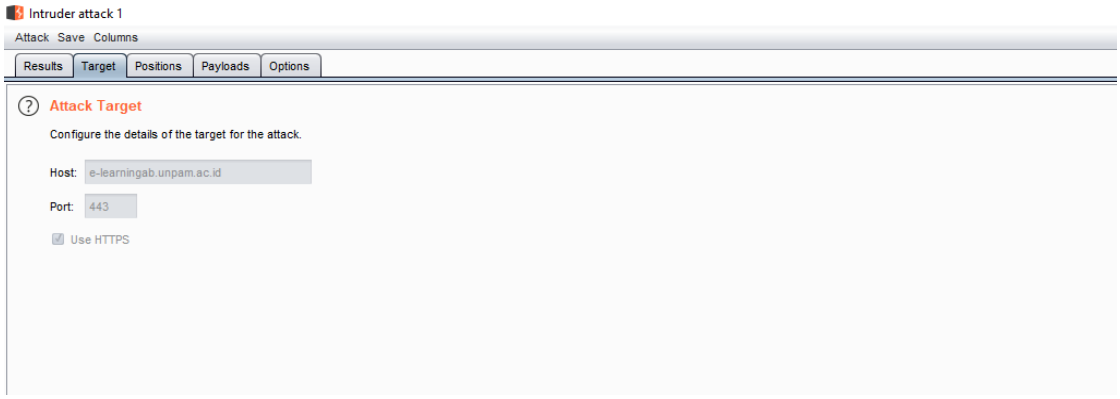
Dilakukan attack target yang ditunjukkan pada Gambar 3. Terlihat target host pada alamat ‘elearningab.unpam.ac.id, dengan menggunakan post 443 atau https.



Gambar 4 Payload Positions pada Sql-fuzzing

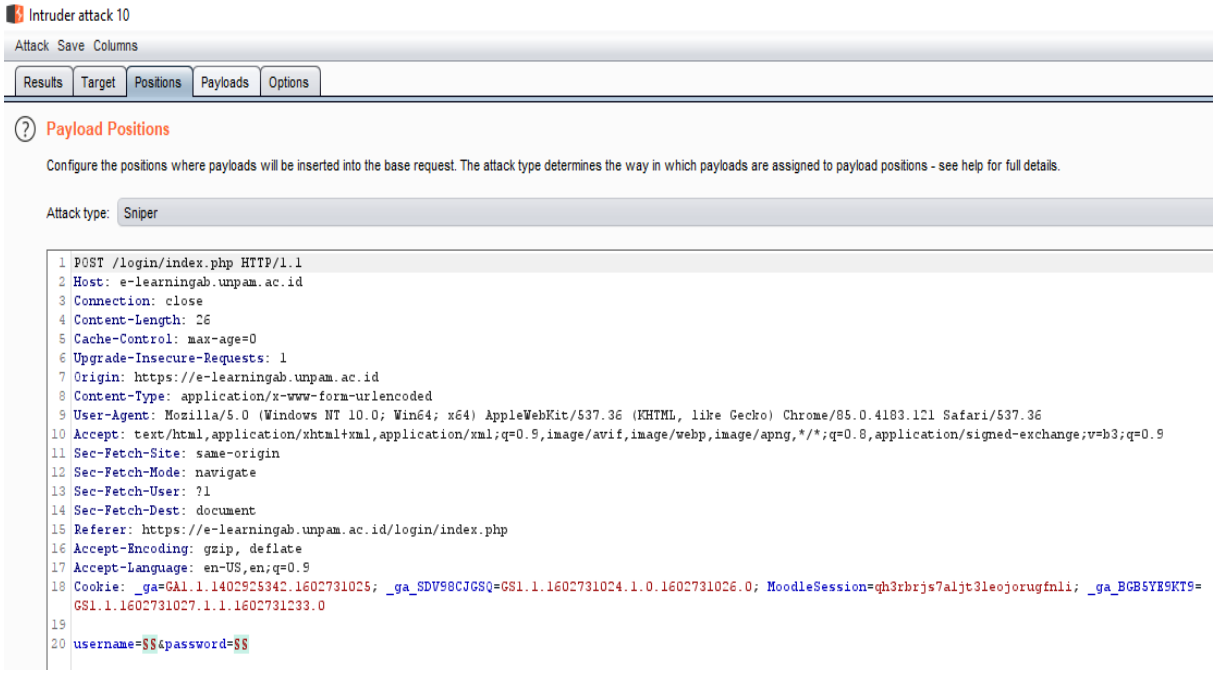
Potition adalah tempat mengatur data fuzzing yang akan dimasukan. Terlihat pada parameter ‘username’ dan ‘password’ ditambahkan sintaks untuk memasukan data fuzzing.

- Xss-fuzzing
  Memasukan data xss-fuzzing atau payloads secara bergantian untuk masukan username dan dilanjutkan password (sniper) lalu request ke server.



Gambar 5 Attack target pada xss-fuzzing

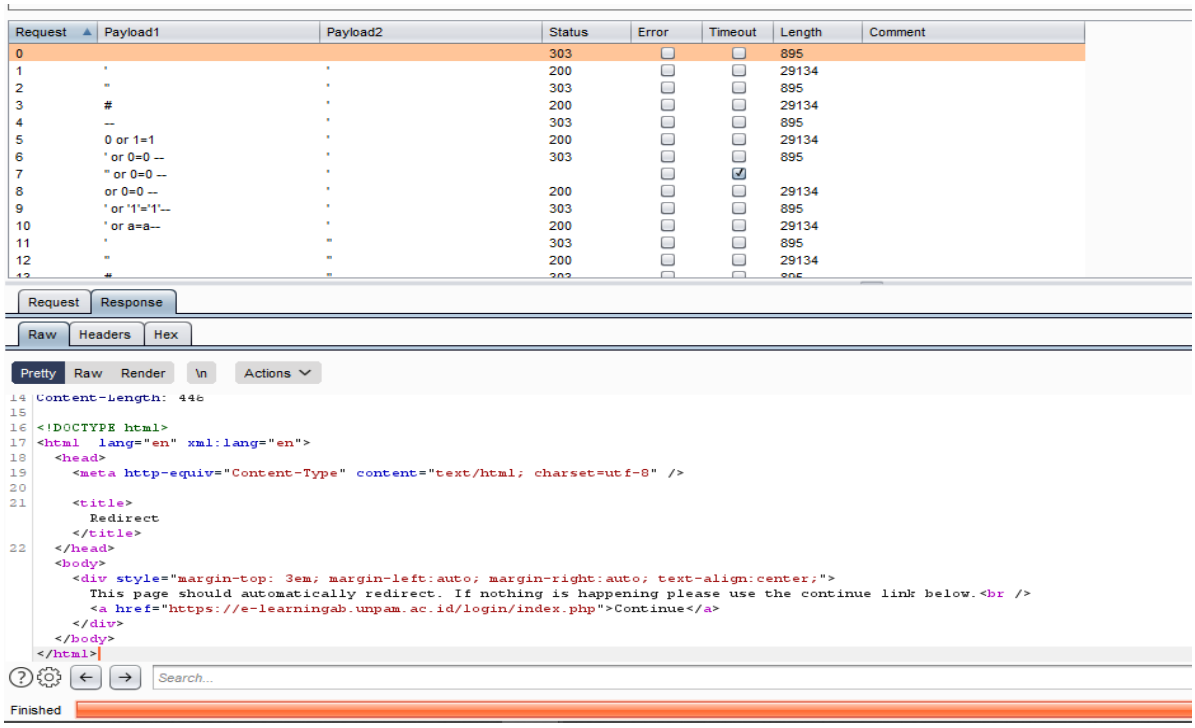
Dilakukan attack target yang ditunjukkan pada Gambar 5. Terlihat target host pada alamat ‘elearningab.unpam.ac.id, dengan menggunakan post 443 atau https.



Gambar 6 Payload Positions pada pada xss-fuzzing

Potition adalah tempat mengatur data fuzzing yang akan dimasukan. Terlihat pada parameter ‘username’ dan ‘password’ ditambahkan sintaks untuk memasukan data fuzzing. Namun kali ini menggunakan tipe sniper.

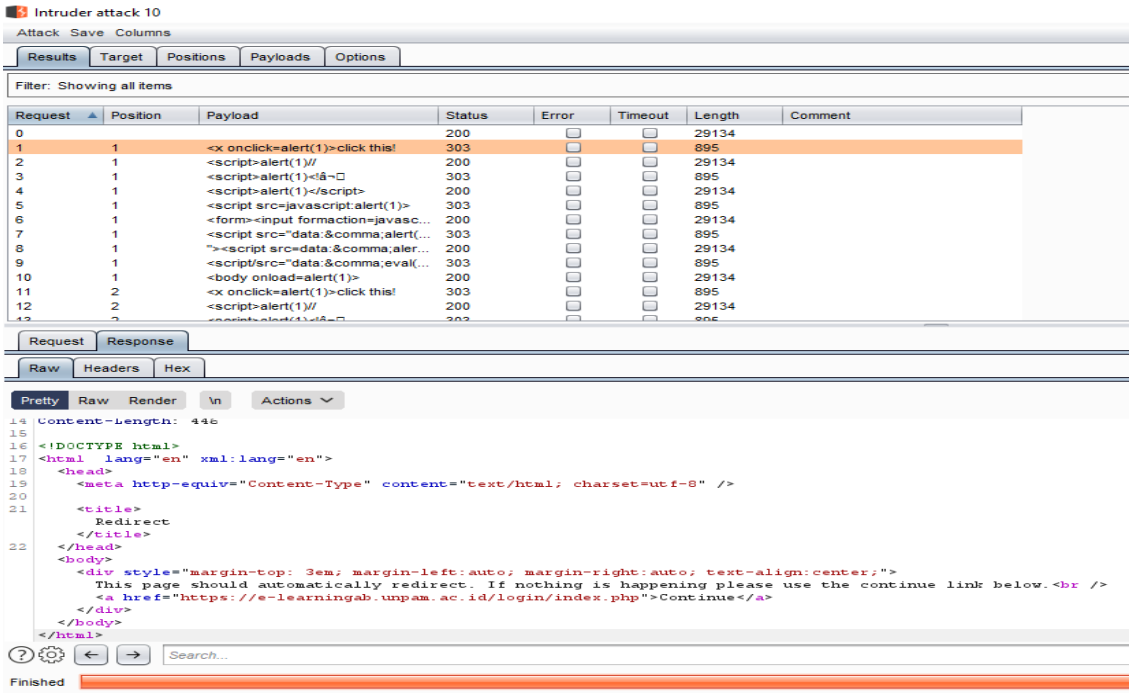
4. Mengamati respon yang dikembalikan oleh server.
   - Sql-fuzzing = terdapat status code 200 dan 303 bergantian secara continue dan ada satu request yang time out.



Gambar 7 Respon dari Server pada sql-fuzzing

Gambar 7 menunjukkan respon yang dikembalikan oleh server terhadap data sql-fuzzing yang dikirimkan.

- Xss-fuzzing = respon code dari server adalah 200 dan 303 bergantian secara continue.



Gambar 8 Respon dari Server pada xss-fuzzing

Sama seperti pada sql-fuzzing, respon yang dikembalikan oleh server berupa status kode, panjangnya data, dan ada koneksi time out.

5. Evaluasi hasil pengamatan
   Evaluasi hasil pengujian yang dilakukan adalah:
   - Respon code yang dikembalikan server adalah 200 dan 303 dan 1 timeout.
   - Respon 200 artinya server menerima request dan mengembalikan respon normal
   - Respon 303 artinya server menerima request dan mengembalikan sebuah request GET baru ke URI yang diberikan.
   - 1 request timeout ada 2 kemungkinan, yang pertama jaringan terputus. dan yang kedua server down karena terlalu banyak request.
   - Website telah memiliki kemampuan untuk eror handling, menagani berbagai data yang tidak normal dan script.

4 Kesimpulan

Fuzzing yang kami lakukan merupakan salah satu cara menguji kerentanan aplikasi web untuk input validation yaitu SQL-injection dan XSS (cross site scripting). Hasil dari penelitian ini tentunya belum bisa merepresentasikan bahwa suatu web dikatakan rentan atau memiliki kerentanan secara keseleuruhan, karena pengujian ini masih terbatas.

Form yang diuji hanya form login, dan data yang digunakan hanya 10 data yang paling sering digunakan untuk mengetes suatu form masukan. Masih banyak metode yang perlu dilakukan dan form yang perlu diuji untuk mengetahui kerentanan website secara keseluruhan.

Dari hasil pengujian yang dilakukan pada website e-learning Universitas Pamulang pada form login, kami tidak menemukan kerentanan yang dimaksud yaitu SQL-ijection dan XSS. Namun tidak menutup kemugkinan website e-learning Universitas Pamulang memiliki kerentanan pada input validation. maka perlu pengujian lebih lanjut dalam scope yang lebih luas.

Referensi

Afandi, T. A., Iswahyudi, C., & Rachmawati, Y. (2019). Aplikasi Pendeteksi Celah Keamanan Aplikasi Web Dengan Penetration Testing Menggunakan Metode Input Validation Testing. *jurnal SCRIPT, 7*, 132-141.

Andria. (2020). Analisis Celah Keamanan Website Menggunakan Tools WEBPWN3R di Kali Linux. *Generation jurnal, 4*, 69-76.

Gultom, L. M., & Harahap, M. (2015). Analisis Celah Keamanan Website Instansi Pemerintahan Di Sumatera Utara. *Jurnal Teknovasi, 2*, 1-7.

Guntoro, Costaner, L., & Mustawati. (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, 5*, 45-55.

Nurudin, M., Jayanti, W., Saputro, R. D., Saputra, M. P., & Yulianti, Y. (2019). Pengujian Black Box pada Aplikasi Penjualan Berbasis Web Menggunakan Teknik Boundary Value Analysis. *Jurnal Informatika Universitas Pamulang, 4*(4), 143-148.

Riadi, I., Yudhana, A., & Wahyu, Y. (2020). Analisis Keamanan Website Open Journal System menggunakan Metode vulnerability Assessment. *Jurnal Teknologi Informasi dan Ilmu Komputer, 7*, 863-860.

Sanjaya, A. S., Sasmita, A., & Arsa, S. (2020). Evaluasi Keamanan Website Lembaga X Melalui Penetration Testing Menggunakan Framework ISSAF. *jurnal ilmiah merpati, 8*, 113-124.

Shaleh, I. A., Prayogi, J., Pirdaus, P., Syawal, R., & Saifudin, A. (2021). Pengujian Black Box pada Sistem Informasi Penjualan Buku Berbasis Web dengan Teknik Equivalent Partitions. *Jurnal Teknologi Sistem Informasi dan Aplikasi, 4*(1), 38-45. doi:10.32493/jtsi.v4i1.8960

Susanto, J., Biqirrosyad, B., Junaidi, M. M., Sudrajat, Y., & Desyani, T. (2021). Pengujian Black Box pada Aplikasi Desktop Penjualan Elektronik Menggunakan Metode Equivalence Partitioning. *Jurnal Teknologi Sistem Informasi dan Aplikasi, 4*(1), 38-45. doi:10.32493/jtsi.v4i1.8960

Wahyudi, W. (2019). Analisa Pengujian Kerentanan terhadap Web Server SIMAK. *Jurnal Teknologi Informasi, 5*(1), 6-13. doi:10.52643/jti.v5i1.321

Wahyuningrum, T., & Januarita, D. D. (2015). Implementasi dan Pengujian Web E-commerce untuk Produk Unggulan Desa. *Jurnal Komputer Terapan, 1*, 57-66.

Wicaksono, B., Kusumaningsih, Y. R., & Iswahyudi, c. (2020). Pengujian Celah Keamanan Aplikasi Berbasis Web Menggunakan Teknik Penetration Testing dan Dast(Dynamic Application Security Testing). *jurnal jarkom, 8*, 1-9.