



Fahmi Anwar
fahwar95@gmail.com
Magister Teknik Informatika, Universitas Ahmad Dahlan



Abdul Fadlil
fadlil@mti.uad.ac.id
Teknik Elektro, Universitas Ahmad Dahlan



Imam Riadi
imam.riadi@is.uad.ac.id
Sistem Informasi, Universitas Ahmad Dahlan

1. LATAR BELAKANG

Faktor keamanan sangatlah penting dikarenakan pada zaman yang semakin berkembang banyak sistem yang berbentuk digital. Ancaman serangan terhadap berbagai jenis sistem yang berbentuk digital atau server juga ikut berkembang maka diperlukan sebuah penanganan terhadap ancaman atau serangan pada server dengan celah fitur *file upload*. Salah satu teknik dalam menangani serangan atau eksploitasi *File Upload* adalah menerapkan teknik validasi yang tidak hanya mengecek MIME atau *File Extension* dan *File Size* tetapi memanfaatkan juga *Metadata* dan *Image Processing* sebagai penyaring *Image File* yang disisipi kode eksploitasi.

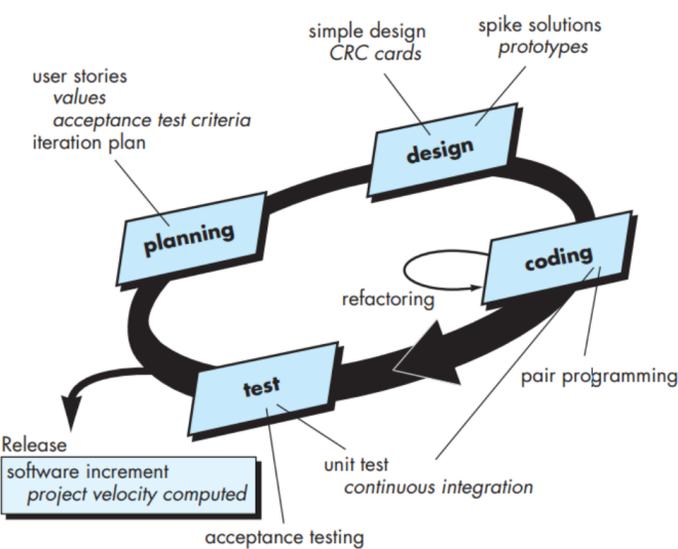
2. TUJUAN PENELITIAN

1. Teknik penyaringan dengan memvalidasi objek digital pada fitur File Upload menggunakan *image files* seperti JPEG, PNG dan SVG.
2. Menganalisa atau menghitung perbandingan kualitas citra sebelum dan sesudah diproses.

3. KAJIAN HASIL PENELITIAN TERDAHULU

NO	PENELITI	METODE/TOOLS	HASIL
1	(Li & Xue, 2011)	Web Application Security Testing	Jika kode lebih banyak disisi klien <i>front-end</i> dan banyak menggunakan aplikasi pihak ketiga maka penyerang akan lebih mudah
2	(Alanazi & Jones, 2016)	File System Metadata	Metadata dapat menghasilkan bukti yang tidak selalu mudah terlihat dan penyidik harus memastikan pengumpulan data tersebut dan validasinya
3	(Riadi & Aristianto, 2016)	Penetration Testing	Mengunggah <i>file</i> gambar dengan cara tidak dibatasi bisa digunakan untuk membuat penyerang mengambil informasi yang terkandung dalam suatu sistem.
4	(Jaiswal, Raj, & Singh, 2014)	Security testing of web applications	Penguji keamanan harus melacak semua masalah saat melakukan pengujian aplikasi web untuk keamanan.

4. METODOLOGI PENELITIAN



Metode penelitian yang digunakan merupakan Metode Eksperimental dan metode pengembangan adalah Extreme Programming (XP). XP adalah metode pengembangan software yang cepat, efisien, beresiko rendah, fleksibel, terprediksi, *scientific*, dan menyenangkan.

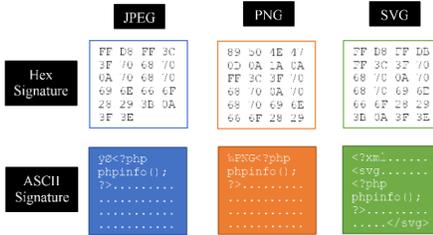
5. ALAT DAN BAHAN



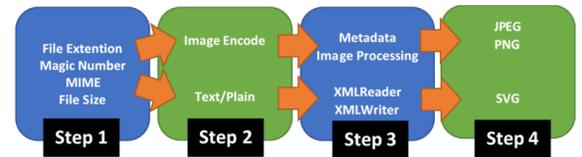
6. HASIL DAN PEMBAHASAN



6.1 Perencanaan



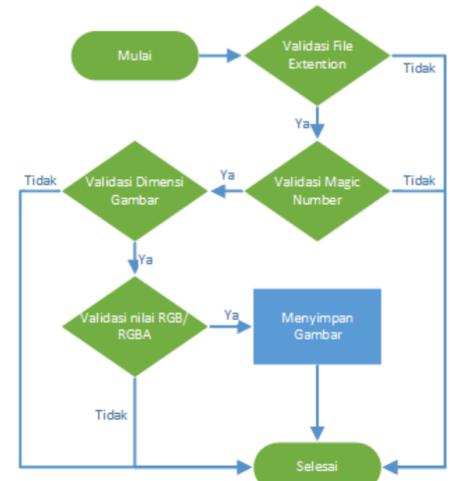
1. Membuat sampel Image File yang disisipi kode eksploitasi PHP untuk JPEG dan PNG atau XML untuk SVG.
2. Membuat teknik penyaringan untuk Image File bertipe JPEG, PNG dan SVG.



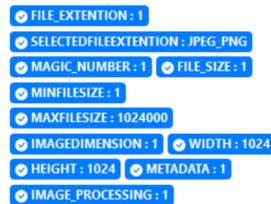
6.2 Perancangan



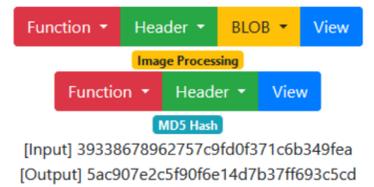
1. Membuat alur proses penyaringan dengan menggunakan File Extension, Magic Number, Metadata, Image Dimension, File Size dan Image Processing.
2. Merancang sebuah basis data untuk menampung informasi Image File yang diunggah, seperti File name, File Blob, File Size, Mime Type dan Hash MD5.



6.3 Pengkodean



Pengkodean atau Coding berisi tahapan dalam membuat sebuah sistem dengan menggunakan pemrograman PHP sebagai *backend* serta HTML, CSS dan JS sebagai *frontend*.



6.4 Pengujian

Pengujian pada penelitian ini menggunakan sampel gambar yang disisipi kode eksploitasi *server side script* kemudian di unggah sesuai dengan skenario uji yang telah ditentukan serta menghitung perbandingan kualitas citra antara gambar sebelum dan sesudah proses validasi *Image Processing* dengan hanya mengambil warna setiap *pixels*.

TEKNIK PENYARINGAN							HASIL	
NO.	FILE EXTENTION	MAGIC NUMBER	METADATA	IMAGE DIMENSION	FILE SIZE	IMAGE PROCESSING	HASIL YANG DIHARAPKAN	HASIL
1	✓						Hanya JPG, PNG dan SVG	[V] Berhasil [] Tidak Berhasil
2	✓	✓					Hanya JPG, PNG yang memiliki Magic Number Generic	[V] Berhasil [] Tidak Berhasil
3	✓	✓	✓				Hanya JPG, PNG yang memiliki Magic Number Generic yang memiliki Metadata	[V] Berhasil [] Tidak Berhasil
4	✓	✓	✓	✓			Hanya JPG, PNG yang memiliki Magic Number Generic juga memiliki Dimensi	[V] Berhasil [] Tidak Berhasil
5	✓	✓	✓	✓	✓		Hanya JPG, PNG yang memiliki Magic Number Generic juga dimensi serta memiliki ukuran file tertentu	[V] Berhasil [] Tidak Berhasil
6	✓	✓	✓	✓	✓	✓	Hanya JPG, PNG yang memiliki Magic Number Generic juga dimensi serta ukuran file tertentu dan dapat diambil warnanya	[V] Berhasil [] Tidak Berhasil

Perbandingan berdasarkan Kualitas Citra						
No.	Tipe Gambar	Resolusi (Pixel)	MSE	RMSE	PSNR	SSIM
1	JPEG	64x64	28,9729	5,19354	33,8215	0,975821
2		128x128	29,1645	5,40041	33,4823	0,977447
3		256x256	26,2135	5,11992	33,9455	0,979167
4		512x512	19,0711	4,36705	35,3270	0,982509
5		1024x1024	11,3565	3,36995	37,5783	0,984272
6	PNG	64x64	0,00545	0,07384	70,7649	0,999996
7		128x128	0,00240	0,04899	74,3274	0,999997
8		256x256	0,00050	0,02243	81,1105	1,000000
9		512x512	0,00027	0,01649	83,7833	1,000000
10		1024x1024	0,00038	0,01965	82,2623	1,000000

Perbandingan berdasarkan Dimensi dan Ukuran Berkas					
No.	Tipe Gambar	Resolusi Awal (Pixel)	Ukuran Awal (KB)	Resolusi Akhir (Pixel)	Ukuran Akhir (KB)
1	JPEG	64x64	16,60	64x64	5,59
2		128x128	38,10	128x128	19,70
3		256x256	106,00	256x256	71,40
4		512x512	302,00	512x512	255,00
5		1024x1024	973,00	1024x1024	914,00
6	PNG	64x64	5,00	64x64	16,10
7		128x128	9,06	128x128	64,30
8		256x256	16,60	256x256	256,00
9		512x512	32,10	512x512	1024,00
10		1024x1024	66,20	1024x1024	409,00

7. KESIMPULAN

Validasi gambar JPEG dan PNG memanfaatkan metadata dan *image processing* pada fitur file upload dengan keberhasilan menyaring kode eksploitasi sebesar 100% dari 12 skenario sedangkan SVG memanfaatkan XMLReader dan DOMDocument dengan keberhasilan menyaring kode eksploitasi sebesar 66,67% dari 3 skenario. Skenario uji berdasarkan jenis eksploitasi yang disisipi dengan keberhasilan sebesar 87,5% dari 8 jenis eksploitasi. Kualitas citra pada JPEG menghasilkan nilai PSNR diatas 33dB, SSIM diatas 0,97 dan RMSE diatas 3,3 dan dibawah 5,4. Kualitas citra pada PNG menghasilkan PSNR diatas 70dB, SSIM diatas 0,99 dan RMSE diatas 0,01 dan dibawah 0,07. SVG berbentuk XML format atau rumus sehingga tidak bisa dihitung kualitas citranya.

