ISSN: 2614-6754 (print)
ISSN: 2614-3097(online)

Halaman 34259-34270
Volume 8 Nomor 2 Tahun 2024

Introduction to Web Security: Detecting XSS with Dalfox and Paramspider

Mirza Maulana[1], Muhammad Luthfi Hermawan[2], Bagus Kurniawan[3], Wisnu Selaguna Ajinaya[4], Alif Naufal Teguh Putra[5], Rully Mujiastuti[6], Mirza Sutrisno[7], Rita Dewi Risanty[8], Popy Meilina[9], Sitti Nurbaya Ambo[10]
[1,2,3,4,5,6,7,8,9,10] Teknik Informatika, Universitas Muhammadiyah Jakarta
e-mail : luthfihrmwn26@gmail.com

Abstrak

Perkembangan teknologi selain menimbulkan dampak positif, juga menimbulkan dampak negatif. Kejahatan siber adalah salah satu ancaman yang menimbulkan banyak kerugian khususnya mengenai data diri seseorang. Untuk itu, perlu adanya pemahaman terkait keamanan siber oleh khalayak umum. Salah satu hal yang bisa dilakukan adalah dengan mengadakan webinar dan workshop mengenai keamanan siber. Penulis dan tim mengadakan kegiatan pengenalan mengenai keamanan siber dengan mengambil judul "Introduction To Web Security : Detecting XSS With Dalfox And Parampsider". Kegiatan ini dilaksanakan dengan metode pemaparan materi dengan Webinar dan dilanjutkan dengan Workshop. Dilakukan evaluasi kepuasan peserta melalui kuisioner yang menunjukkan respon positif terhadap pemateri dan materi yang disampaikan. Hasil dan pembahasan menunjukkan bahwa kegiatan berjalan sukses, dibuktikan dengan partisipasi dari 45 peserta dari berbagai instansi. Peserta juga mengisi Pre-Test dan Post-Test yang menunjukkan pemahaman yang baik terhadap materi. Feedback yang didapatkan dari peserta adalah 70,5% merasa puas dan 29,5% merasa sangat puas dengan kegiatan ini.

Kata kunci : *Keamanan Siber, Serangan Siber, Webinar, Workshop*

Abstract

The development of technology brings both positive and negative impacts, with cybercrime being a major threat that incurs significant losses, particularly in terms of personal data privacy. Hence, public understanding of cybersecurity is crucial. To address this, the author and team organized an introductory event on cybersecurity titled "Introduction to Web Security: Detecting XSS with Dalfox and Parampsider." The event was conducted through a webinar followed by a workshop. Participant satisfaction was evaluated via a questionnaire, which showed positive responses towards the presenters and the material provided. The results indicate that the event was successful, evidenced by the participation of 45 individuals from various institutions. Participants also completed Pre-Tests and Post-Tests, demonstrating good comprehension of the material. Feedback reveals that 70.5% of participants were satisfied and 29.5% were very satisfied with the event.

Keywords: *Cyber Security, Cyber Attack, Webinar, Workshop*

PENDAHULUAN

Kejahatan keamanan siber menjadi sebuah tantangan yang saat ini sedang dihadapi banyak pihak diseluruh dunia. Menurut Kapersky, di tahun 2024 Indonesia mengalami 5.863.955 serangan siber selama periode Januari hingga Maret. Metode serangan yang umumnya digunakan adalah dengan memberikan atau menanamkan *malware* tanpa *file*. Sebanyak 21,2% pengguna internet diserang oleh ancaman ini yang disebarkan melalui *website* selama periode Q1 2024. Hal ini membuat Indonesia berada di urutan ke 96 secara global dalam hal bahaya terkait penggunaan *website* (CNN Indonesia, 2024). Penelitian sebelumnya yang dilakukan oleh Rully Mujiastuti dan Ibnu Prasteyo tahun 2021 dengan judul "Membangun Sistem Keamanan Jaringan Berbasis VPN yang Terintegrasi dengan DNS Filtering PIHOLE" mengungkapkan bahwa salah satu serangan

yang bisa saja terjadi adalah *Man In The Middle* (MITM). MITM adalah sebuah serangan *cyber* yang terjadi ketika ada pihak ketiga yang mengambil informasi penting dari sebuah komunikasi yang dilakukan antara dua orang (Rully Mujiastuti, et al., 2021). Untuk mencegah hal ini terus terjadi, tentunya ada penanganan yang perlu ditingkatkan yaitu keamanan siber atau *cyber security*.

Cyber Security adalah sebuah kebijakan, prinsip perlindungan, strategi pengendalian informasi yang berisi ilmu teknologi untuk mengamankan organisasi atau dunia *online*, dengan kata lain *Cyber Security* adalah segala proses atau tindakan yang dilakukan untuk mempertahankan dan juga mengurangi masalah privasi (Indah, F et al., 2022). Menurut Pusiknas Polri pada tahun 2022, kejahatan siber di Indonesia meningkat berkali-kali lipat. Pada periode 1 Januari hingga 22 Desember 2022 telah terjadi 8831 tindakan kejahatan siber. Tentunya kemampuan dalam bidang *cyber security* menjadi sebuah kebutuhan yang paling penting untuk dipahami oleh khalayak umum untuk dapat mengamankan data dan sumber daya sebuah perusahaan atau bahkan sebuah negara.

Salah satu cara yang dapat dilakukan adalah dengan mengedukasi khalayak umum akan pentingnya pemahaman keamanan siber. Seperti Pengabdian Kepada Masyarakat (PKM) dalam bidang *cyber security* yang dilakukan oleh Mochammad Machlul Alamin dkk, pada tahun 2023 yang mengangkat judul "Peningkatan Kualitas SDM Melalui Pelatihan *Cyber Security* Pada Anggota Polisi Daerah Jawa Timur". Pada kegiatan PKM tersebut, Mochammad Machlul Alamin dkk memberikan edukasi kepada para anggota Polisi daerah Jawa Timur mengenai dasar keamanan siber, ancaman keamanan siber, keamanan jaringan, keamanan sistem operasi, keamanan data, keamanan aplikasi serta kesadaran pengguna dalam keamanan jaringan. Hasil dari PKM tersebut menunjukkan peningkatan pemahaman anggota polri Jawa Timur mengenai *cyber security* dan juga merekomendasikan untuk dapat melanjutkan program pelatihan keamanan siber secara berkala. Maka dari itu, penulis dan tim mengadakan kegiatan *Webinar* dan *Workshop* ini sebagai salah satu bentuk keberlanjutan program pengabdian kepada masyarakat dalam bidang keamanan siber. Kemampuan dalam bidang *Cyber Security* sangat dibutuhkan saat ini karena perkembangan teknologi yang sangat pesat ditambah dengan adanya kejahatan *cyber* meningkat, bidang *Cyber Security* menjadi salah satu bidang yang dibutuhkan. Selain serangan siber MITM diatas, salah satu *cyber attack* yang sering terjadi adalah serangan *cyber Cross Site Scripting (XSS)*.

Cross Site Scripting (XSS)

XSS merupakan sebuah serangan dengan memanfaatkan kerentanan keamanan sebuah *website*. Penyerang akan menyisipkan sebuah skrip berbahaya ke dalam *website* untuk dapat mengambil alih *website* tersebut. Skrip yang disisipkan biasanya berupa skrip *JavaScript*, tetapi juga bisa berupa *HTML* atau bentuk lainnya yang dapat dieksekusi oleh *browser*. *XSS* ini dapat digunakan untuk mencuri informasi pengguna seperti *cookie* atau data sesi, serta untuk menjalankan sebuah operasi yang mengatasnamakan pengguna (Hakim A. S et al., 2020)*.* Terdapat beberapa jenis *XSS* antara lain :

1. *Presistent*
   Presistent merupakan serangan *XSS* yang berbentuk kode yang akan disimpan ke dalam penyimpanan database yang kemudian dapat dilihat oleh pengguna yang lain, misalnya pada kolom komentar sebuah *website*. Penyerang akan membuat komentar yang bisa dibaca orang lain namun komentar itu telah disusupi skrip. Ketika orang lain melihat komentar yang disusupi skrip itu, maka kode yang ada di dalamnya akan langsung di eksekusi. Jenis serangan ini sangat rentan karena penyerang dapat dengan mudah mencuri *cookies website* dan dapat melakukan modifikasi pada halaman *website.*
2. *Reflected XSS*
   Reflected XSS adalah sebuah serangan yang terjadi ketika skip berbahaya dikirimkan ke server melalui permintaan dan kemudian dikembalikan oleh server. Biasanya, penyerang mengirimkan email dengan *link* yang mengandung skrip berbahaya. Ketika pengguna mengklik link tersebut, dan skrip dikirimkan ke server, maka server akan mengembalikan skrip dalam halaman respon dan akan dijalankan di *browser* pengguna.

3. *DOM Based XSS*
   DOM Based XSS adalah sebuah serangan yang terjadi dimana ketika skrip berbahaya dimanipulasi dan dieksekusi di sisi klien yaitu dalam *Document Object Model* (*DOM*) halaman *website*.

Dalgi Form XSS (Dalfox)

Dalfox ini adalah sebuah alat keamanan yang digunakan khusus untuk mendeteksi kerentanan *XSS* dengan menganalisis parameter *website* (*Dalfox*, 2024). *Dalfox* ini dapat mendeteksi berbagai jenis *XSS* seperti *Presistence, Reflected XSS*, dan *DOM Based XSS*. *Dalfox* bekerja dengan cara menginisiasi dan mengumpulkan infromasi dasar dari *URL* target *website* seperti parameter, form, dan elemen input. Kemudian *Dalfox* akan menyuntikkan berbagai jenis *payload XSS* ke dalam parameter atau *URL* yang ditemukan dari sebuah *website*. Operasi ini memanfaatkan *fuzzy logic* untuk mencoba berbagai kombinasi *payload*. Kemudian *Dalfox* akan menganalisis respon dari server untuk mendeteksi tanda-tanda eksekusi *payload XSS*. Setelah mendeteksi potensi kerentanan, *Dalfox* melakukan validasi untuk memastikan bahwa temuan tersebut adalah kerentanan *XSS*.

ParamSpider

ParamSpider adalah sebuah skrip berbahasa *python* yang digunakan untuk mencari parameter dari sebuah *website* yang tujuannya juga untuk mendeteksi adanya kerentanan *XSS* pada sebuah *website* (n00bie, 2020). *ParamSpider* bekerja dengan cara mengumpulkan parameter dari berbagai sumber seperti *URL, HTML*, dan *file JavaScript* kemudian mengelompokkan dan menyaring parameter yang diekstrak untuk menemukan parameter yang berpotensi dieksploitasi oleh penyerang. Hasilnya nanti dapat dijadikan untuk pengujian keamanan lebih lanjut oleh *developer* seperti memvalidasi setiap *input* dalam *website*, menggunakan *header* keamanan, dan lain sebagainya.

Pengenalan *cyber security* kepada khalayak umum harus banyak dilakukan. Kegiatan *Webinar* dan *workshop* " *Introduction to Web Security : Detecting XSS with Dalfox and ParamSpider* " merupakan bentuk kegiatan Kuliah Kerja Nyata sekaligus sebagai hasil diseminasi program Magang dan Studi Independen Bersertifikat yang bertujuan untuk memberikan ilmu, wawasan, dan pelatihan kepada peserta yaitu mahasiswa dan umum dengan memberikan pengetahuan dan melatih keterampilan peserta dalam memahami proses pendeteksian kerentanan dalam dunia *Cyber Security*.

METODE

Untuk merealisasikan kegiatan yang telah diuraikan diatas, maka penulis dan tim membuat langkah-langkah yang ditempuh guna melaksanakan kegiatan tersebut. Kegiatan ini dilakukan dengan dua tahapan yaitu Pendidikan Masyarakat berbentuk *Webinar* dan Pelatihan yang berbentuk *Workshop*. Untuk mengadakan *Webinar* dan *Workshop*, ada beberapa tahapan yang penulis dan tim lakukan.

1. Tahap 1 (Sosialisasi Kegiatan)
   Pada tahap ini, penulis dan tim melakukan sosialisasi di media sosial dengan membagikan *flyer* dan link pendaftaran pada *url* https://forms.gle/qH1vpvGGUvVd7Zhs5 mengenai kegiatan *Webinar* dan *Workshop*. Poster diposting pada media sosial instagram, linkedin, dan *broadcast message* grup WhatsApp.
2. Tahap 2 (Pembuatan Materi Kegiatan)
   Pada tahap ini, penulis dan tim membuat materi kegiatan untuk *Webinar* dan *Workshop* yang akan diadakan. Materi disajikan dalam bentu PPT dan akan dipresentasikan oleh para pemateri disaat kegiatan berlangsung.
3. Tahap 3 (Pengisian *Pre-Test* oleh peserta)
   Sebelum kegiatan dimulai, peserta diminta untuk mengisi *pre-test* pada *url* https://shorturl.at/t3Qlv yang berisi materi mengenai *Webinar* dan *Workshop*. Pembuatan *pre-test* bertujuan untuk mengetahui tingkat kepahaman peserta terhadap materi yang akan diberikan. Hasilnya nanti akan dibandingkan dengan *post-test* yang diberikan setelah kegiatan berlangsung.

4. Tahap 4 (Pendidikan Masyarakat melalui *Webinar*)
   Pada *Webinar* ini, penulis dan tim melakukan pemaparan materi dasar sehingga peserta dapat memahami dengan baik mengenai materi *Cyber Security* khususnya mendeteksi *XSS*. Keluaran dari tahapan ini adalah pengenalan materi mengenai *XSS*, *Dalfox, dan ParamSpider*. Materi *Webinar* dimulai dengan Pengertian *Cyber Security*, Ancaman dan Resiko dalam *Cyber Security, Blue Team* dan *Red Team* dalam *Cyber Security*, *Penetration Testing*, Pengenalan *XSS*, Dalfox dan juga ParamSpider.
5. Tahap 5 (Pelatihan melalui *Workshop*)
   Workshop ini merupakan implementasi dari materi pertama berupa pendeteksian *XSS* dengan menggunakan *Dalfox* dan *ParamSpider*. Para peserta sebelumnya dijelaskan secara singkat mekanisme pendeteksian kerentanan *XSS* ini. Para peserta melakukan pendeteksian kerentanan *XSS* pada beberapa *website* yang telah ditargetkan untuk dideteksi. Pendeteksian ini dilakukan dengan menggunakan *tools Virtual Machine* berupa *Virtual Box* yang telah di instal sistem operasi *Kali Linux*. Para peserta sebelumnya telah dihimbau untuk dapat menginstal *tools* tersebut sebelum kegiatan dimulai dan dapat mengikuti langkah-langkah yang dipaparkan ketika kegiatan berlangsung.
6. Tahap 6 (Pengisian *Feedback* dan *Post-Test* oleh peserta)
   Pada akhir kegiatan, peserta diminta untuk dapat mengisikan *feedback* untuk mengetahui seberapa puas mereka dengan pemaparan materi yang disampaikan oleh para pemateri dan juga peserta diminta untuk merngisi *Post-Test*. *Feedback* dan *Post-Test* peserta dapat diakses pada *url* https://shorturl.at/gcag0. Hasil dari *Post-Test* akan disandingkan dengan *Pre-Test* untuk melihat seberapa baik tingkat pemahaman peserta terhadap materi yang dibawakan.

HASIL DAN PEMBAHASAN

Kegiatan *Webinar* dan *Workshop* ini dilakukan oleh mahasiswa program studi Teknik Informatika Fakultas Teknik Universitas Muhammadiyah Jakarta. Hasilnya adalah kegiatan ini dilaksanakan secara daring melalui *Zoom Meeting Conference* dengan *link url* https://s.umj.ac.id/FTUMJ-02 pada Senin, 15 Juli 2024 pukul 10:00 – 12:00 WIB. Peserta yang hadir pada kegiatan ini berjumlah 45 orang dari berbagai instansi yang mayoritas diikuti oleh mahasiswa program studi Teknik Informatika Universitas Muhammadiyah Jakarta. Adapun kegiatan ini dilaksanakan secara daring melalui *Zoom Meeting Conference* dan terdapat sesi interaktif seperti *QnA* saat pelaksanaannya. Berikut ini merupakan susunan acara *Webinar* dan *workshop*:

Tabel 1. Susunan Acara

Waktu	Kegiatan	PIC
10.00 - 10.15	Kumpul Panitia dan Sebar Link Zoom dan Link VG (pre test)	Wisnu Selaguna Ajinaya
10.15 - 10.20	Pembukaan Oleh MC	Alif Naufal Teguh Putra
10.20 - 10.24	Indonesia Raya	Alif Naufal Teguh Putra
10.24 - 10.28	Mars Muhammadiyah	Alif Naufal Teguh Putra
10.28 - 10.30	Tilawah	Wisnu Selaguna Ajinaya
	Pembacaan CV Moderator	Alif Naufal Teguh Putra
	Pembacaan CV pemateri	Mirza Maulana
10.30 - 10.50	Webinar	Muhammad Luthfi Hermawan
10.50 - 11.00	Break (post test)	
	Pembacaan CV pemateri	Mirza Maulana
11.00 - 11.40	Workshop	Bagus Kurniawan
11.40 - 11.45	Tanya Jawab	Mirza Maulana
11.45 - 11.55	Quiz	Mirza Maulana
11.55 - 12.00	Foto Bersama, Link Presensi dan Feedback	Alif Naufal Teguh Putra
	Selesai	

Kemudian dilakukan tahapan pengabdian seperti yang sudah diuraikan diatas.

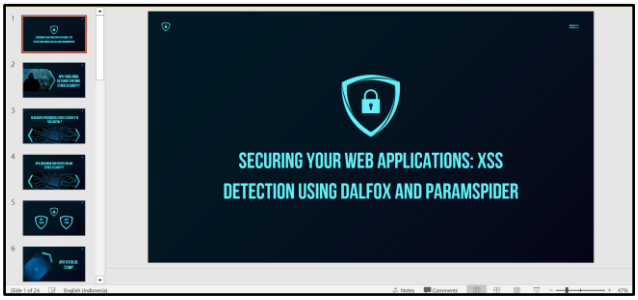
Tahapan 1 (Sosialisasi Kegiatan)

Pada tahap ini, penulis dan tim melakukan sosialisasi kepada khalayak umum melalui sosial media sekaligus untuk menjaring peserta yang berminat dengan membagikan *flyer* yang telah dibuat seperti pada gambar 1 berikut

Gambar 1. *Flyer* Kegiatan

Tahap 2 (Pembuatan Materi Kegiatan)

Pada tahap ini, pemateri menyusun materi yang akan dibawakan dalam format PPT. Materi disusun sedemikian rupa agar mudah dipahami oleh peserta. Pada materi ini, ada beberapa poin seperti *XSS*, *Dalfox, dan ParamSpider*. Materi *Webinar* dimulai dengan Pengertian *Cyber Security*, Ancaman dan Resiko dalam *Cyber Security, Blue Team* dan *Red Team* dalam *Cyber Security*, *Penetration Testing*, Pengenalan *XSS*, Dalfox dan juga ParamSpider. Materi kegiatan dapat dilihat pada gambar 2 dan 3 berikut.

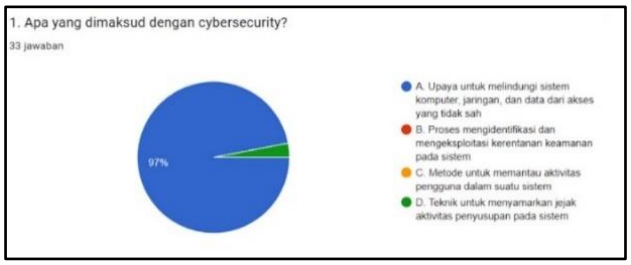


Gambar 2. Materi Kegiatan *Webinar*

Gambar 3. Materi Kegiatan *Workshop*

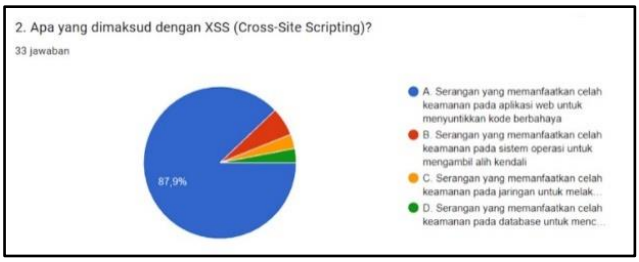
Tahap 3 (Pengisian *Pre-Test* Oleh Peserta)

Pada tahap ini, peserta diminta untuk mengerjakan *Pre-Test* yang diberikan oleh penulis dan tim. *Pre-Test* ini terdiri dari pertanyaan yang berisikan seputar *cyber security*, *XSS, Dalfox*, dan *ParamSpider*. Tujuan dari pengisian *Pre-Test* ini adalah untuk melihat sejauh mana pemahaman peserta sebelum penulis dan tim mengadakan kegiatan ini. Hasilnya adalah *Pre-Test* ini diisi oleh 33 peserta dengan pemahaman yang cukup.



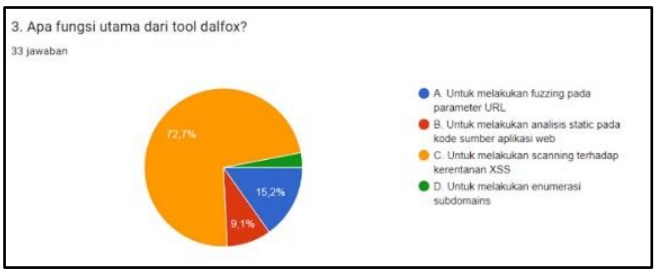
Gambar 4. *Pre-Test* Peserta Mengenai *Cyber Security*

Pada gambar 4 diatas dapat dilihat bahwa *pre-test* di isi oleh 33 peserta dengan persentase jawaban benar pada soal nomor 1 adalah 97%



Gambar 5. *Pre-Test* Peserta Mengenai *XSS*

Pada gambar 5 diatas terlihat hasil *pre-test* mengenai *XSS* adalah sebanyak 87,9% jawban benar yang di isi oleh 33 peserta.



Gambar 6. *Pre-Test* Peserta Mengenai *Dalfox*

Pada gambar 6 diatas, terlihat bahwa persentase peserta menjawab soal nomor 3 adalah 72,7% benar yang di isi oleh 33 peserta.

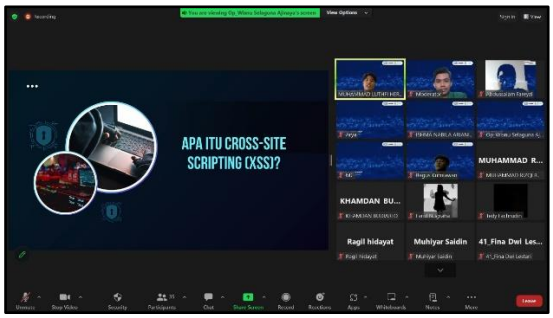
Gambar 7. *Pre-Test* Peserta Mengenai *ParamSpider*

Pada gambar 7 diatas terlihat bahwa, 60,6% dari 33 peserta menjawab benar pertanyaan *pre-test* tersebut.

Tahap 4 (Pendidikan Masyarakat Melalui *Webinar*)

Pada tahap ini, pemateri *Webinar* yang dibawakan oleh Muhammad Luthfi Hermawan, memaparkan materi yang telah dibuat sebelumnya pada tahap 3 diatas kepada peserta yakni

khalayak umum. Adapun pemaparan materi yang dipaparkan meliputi *XSS*, *Dalfox, dan ParamSpider*. Materi *Webinar* dimulai dengan Pengertian *Cyber Security*, Ancaman dan Resiko dalam *Cyber Security, Blue Team* dan *Red Team* dalam *Cyber Security*, *Penetration Testing*, Pengenalan *XSS*, Dalfox dan juga ParamSpider. Pada tahap ini, terdapat juga sesi interaktif kepada peserta seperti pertanyaan yang di berikan pemateri dan juga peserta melalui *chat zoom meeting conference*. Hasilnya adalah peserta jadi memahami secara mendalam mengenai *cyber security* khususnya pada webiste.



Gambar 8. Pemaparan Materi *Webinar*

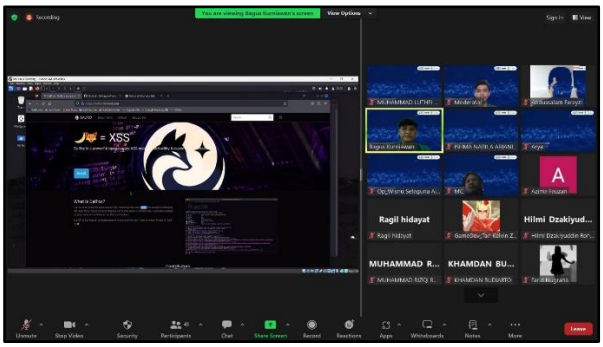
Pada gambar 8 diatas, permateri menjelaskan mengenai *XSS*. Pengenalan ini bertujuan agar peserta dapat memahami terlebih dahulu mengenai kerentanan *XSS* yang ada pada *website*.

Gambar 9. Pemaparan Materi *Webinar*

Pada gambar 9 diatas, pemateri mejelaskan mengenai alat pendeteksi kerentanan *XSS* yaitu *Dalfox* dan *ParamSpider*.

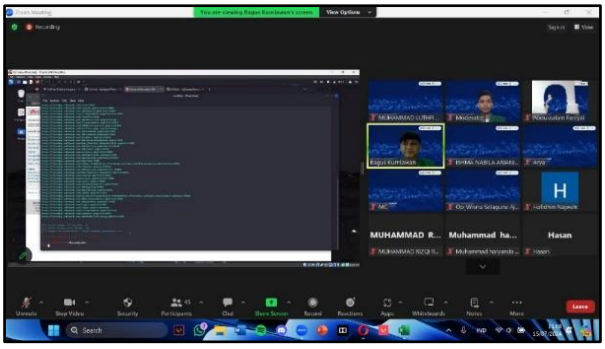
Tahap 5 (Pelatihan Melalui *Workshop*)

Pada tahap ini, pemateri *Workshop* yaitu Bagus Kurniawan memberikan implementasi langsung dari materi *Webinar* yang sebelumnya telah dibawakan. Pada implementasi *Workshop* ini, pemateri menggunakan *tools Virtual Machine* berupa *Virtual Box* yang telah di instal sistem operasi *Kali Linux*. Para peserta sebelumnya telah diimbau untuk dapat menginstal *tools* tersebut sebelum kegiatan dimulai. Pemateri menjelaskan tahapan penggunaan *Dalfox* dan *ParamSpider* untuk mendeteksi kerentanan *XSS* pada beberapa *website* yang dijadikan target. Hasilnya, pemateri menunjukkan adanya beberapa *website* yang memiliki kerentanan *XSS*. Dengan implementasi ini, diharapkan peserta jadi lebih memahami bagaimana mendeteksi kerentanan *XSS* pada *website*. Peserta dapat lebih berhati-hati dalam memberikan data pribadi mereka pada *website* tersebut.



Gambar 10. Pemaparan Materi Workshop

Pada gambar 10 diatas, pemater menjelaskan langkah-langkah yang perlu dilakukan dalam proses penginstalan *Dalfox* sebagai alat untuk mendeteksi kerentanan *XSS.*



Gambar 11. Pemaparan Materi *Workshop*

Pada gambar 11 diatas, didapatkan hasil dari pendeteksian beberapa *website* yang dijadikan target untuk mendeteksi kerentanan *XSS*. Pada proses ini memakan waktu yang cukup lama karena proses pendeteksian dilakukan satu per satu.

Tahap 6 (Pengisian *Feedback* dan *Post-Test* Oleh Peserta)

Pada tahap ini, peserta diminta untuk mengisi presensi kehadiran, *feedback* dan *Post-Test* yang ada dalam satu *form* yang sama yang disebar melalui *Google Form*. Untuk *feeedback*, dalam mengukur jawaban peserta, digunakan skala *likert*. Skala *likert* adalah skala yang terdiri dari beberapa pilihan jawaban yang mendefinisikan kesetujuan peserta terhadap pernyataan atau *steatment* yang ada dengan pilihan jawaban yang telah disesuaikan. Pada kuisioner ini digunakan 4 penilaian skor dengan ketentuan sebagai berikut : (4) Sangat Setuju, (3) Setuju, (2) Kurang Setuju, (1) Tidak Setuju. Pertanyaan kuisioner yang diajukan adalah sebagai berikut:

1. Apakah materi *Webinar* dan *Workshop* yang diberikan dapat mudah dipahami?
2. Apakah narasumber *Webinar* memberikan materi *Webinar* sesuai dengan bidang keilmuannya?
3. Apakah narasumber *Workshop* memberikan materi *Workshop* sesuai dengan bidang keilmuannya?
4. Apakah narasumber *Webinar* mampu menjelaskan materi dengan baik?
5. Apakah narasumber *Workshop* mampu menjelaskan materi dengan baik?
6. Apakah kualitas layanan online selama *Workshop* (suara maupun gambar) berkualitas baik?
7. Apakah layanan administrasi *online* yang diberikan mudah digunakan?
8. Seberapa puas anda dengan kegiatan ini?

Adapun *post-test* yang diberikan adalah soal yang serupa dengan *pre-test* yang mana hasilnya dapat dijadikan perbandingan pemahaman para peserta sebelum dan sesudah mengikuti kegiatan *Webinar* dan *Workshop* ini. Berikut ini merupakan hasil dari *feedback* dan *post-test* yang diisi oleh peserta.

Pada setiap sesi *Webinar* dan *workshop*, para peserta sangat antusias dengan pemaparan yang disampaikan oleh para pemateri. Hal itu terlihat dari *form* kuisioner *feedback* yang telah diberikan pada akhir sesi acara kepada para peserta. Dalam *form* kuisioner *feedback* tersebut, terlihat jawaban dari pernyataan yang diberikan kepada para peserta rata-rata menyatakan puas terhadap pemaparan materi.

Gambar 12. Tingkat Pemahaman Peserta Terhadap Materi yang Dipaparkan

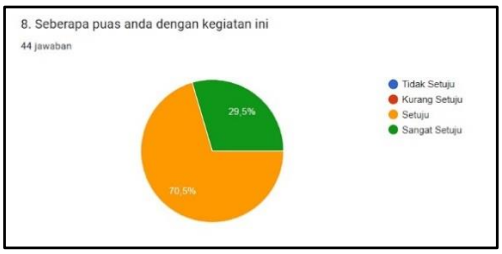
Pada gambar 12 diatas, terlihat bahwa *feedback* yang diberikan oleh peserta menyatakan setuju dengan persentase 75% dan 27% menyatakan sangat setuju. Pada pernyataan selanjutnya, hasil *feedback* juga menunjukkan angka yang positif seperti pada gambar dibawah ini:

Gambar 13. Tingkat Penilaian Pemaparan Materi *Webinar*

Pada gambar 13 diatas, terlihat bahwa 70,5% peserta menyatakan setuju bahwa pemateri *Webinar* menyampaikan materi dengan baik dan 27,3% peserta menyatakan sangat setuju terhadap pernyataan tersebut.

Gambar 14. Tingkat Penilaian Pemaparan Materi *Workshop*

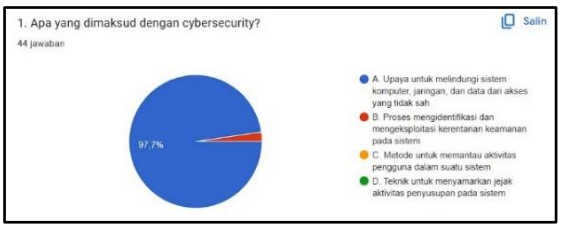
Pada gambar 14 diatas, sebanyak 68,2% peserta *workshop* menyatakan setuju bahwa pemateri memaparkan materi *workshop* dengan baik. Sementara itu 27,3% peserta menyatakan sangat setuju dengan pernyataan tersebut.



Gambar 15. Tingkat Kepuasan Terhadap Pelaksanaan Kegiatan

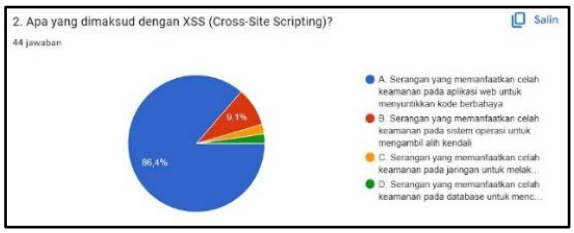
Pada gambar 15 diatas, terlihat baha sebanyak 70,5 % peserta merasa setuju dengan kegiatan ini dan sebanyak 29,5% peserta merasa sangat setuju bahwa mereka puas dengan kegiatan ini. Berdasarkan pertanyaan yang di sampaikan kepada para peserta lalu peserta mengisi kuisonser terlihat bahwa peserta mendapatkan pemahaman mengenai materi baru sesuai dengan tema kegiatan. Respon peserta yang menyatakan puas atas materi yang disampaikan menandakan bahwa penyampaian materi oleh pemateri cukup baik dan mudah di pahami sehingga mereka dapat mempelajari serta memahami ilmu baru. Dengan kata lain kegiatan ini berjalan dengan baik dan dapat di pahami oleh masyarakat umum.

Selain kuisioner *feedback*, para peserta juga diminta untuk mengisi *post-test* yang diberikan ketika kegiatan sudah berakhir dengan tujuan mengetahui peningkatan pemahaman peserta setelah mengikuti kegiatan ini. Berikut ini merupakan beberapa hasil pengisisan *post-test* dari peserta:



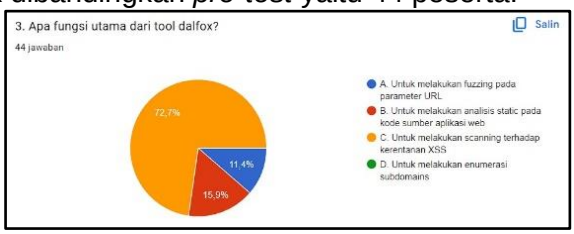
Gambar 16. *Post-Test* Peserta Mengenai *CyberSecurity*

Pada gambar 16 diatas terlihat hasil *post-test* peserta pada soal nomor 1 adalah sebesar 97,7% yang diisi oleh 44 peserta. Secara persentase terjadi peningkatan kecil yang mana ini berarti peserta dapat memahami mengenai *Cyber Security*.



Gambar 17. *Post-Test* Peserta Mengenai *XSS*

Pada gambar 17 terlihat terjadi penurunan persentase ke 86,4% namun, *post-test* ini diikuti oleh peserta yang lebih banyak dibandingkan *pre-test* yaitu 44 peserta.



Gambar 18. *Post-Test* Peserta Mengenai Dalfox

Pada gambar 18 diatas terlihat bahwa 44 peserta menjawab benar dengan persentase yang serupa dengan *pre-test*.

Gambar 19. *Post-Test* Peserta Mengenai ParamSpider

Pada gambar 19 diatas terlihat bahwa *post-test* mengalami peningkatan yaitu sebanyak 65,9% dari 44 peserta menjawab benar pertanyaan tersebut. Pada *post-test* terdapat beberapa soal yang mengalami penurunan persentase jawaban benar namun peserta yang mengisi jauh lebih banyak dibandingkan *pre-test.* Namun pemahaman secara umum mengenai *cyber security, XSS, Dalofx,* dan *ParamSpider* mengalami peningkatan persentase.

Setelah semua kegiatan sudah dilakukan, peserta yang telah mengikuti kegiatan *Webinar* dan *Workshop* akan mendapatkan sertifikat yang telah disahkan oleh Ketua Program Studi Teknik Informatika UMJ.

SIMPULAN

Berdasarkan hasil kegiatan *Webinar* dan *workshop* "*Introduction to Web Security : Detecting XSS with Dalfox and ParamSpider*" yang berlangsung pada tanggal 15 Juli 2024 melalui konferensi *Zoom* dari pukul 10.00 - 12.00 WIB, dapat disimpulkan bahwa kegiatan tersebut berlangsung dengan lancar dan sukses. Acara ini menarik perhatian 45 peserta dari berbagai instansi yang hadir untuk mempelajari dasar-dasar *Cyber Security. Feedback* yang diberikan oleh peserta menunjukkan bahwa mereka puas dengan materi yang disampaikan dan mampu memahaminya dengan mudah sehingga dapat meningkatkan kemampuan mereka di bidang tersebut berdasarkan hasil *post-test*. Kepuasan peserta serta respon positif terhadap pemateri dan materi yang disampaikan menunjukkan bahwa kegiatan ini telah sukses dilaksanakan.

UCAPAN TERIMA KASIH

Penulis dan tim mengucapkan terima kasih kepada Program Studi Teknik Informatika Fakultas Teknik Universitas Muhammadiyah Jakarta yang telah memberikan dukungan serta memfasilitasi kegiatan *Webinar* dan *Workshop* "*Introduction to Web Security : Detecting XSS with Dalfox and ParamSpider*" serta kepada rekan-rekan panitia dan penyelenggara yang telah bekerja sama dalam merencanakan dan melaksanan kegiatan ini dengan baik. Dan tentunya, terima kasih kepada para peserta yang telah berpatisipasi dan berkontribusi dalam memberikan *feedback* dalam kegiatan ini.

DAFTAR PUSTAKA

DalFox. (n.d.). Retrieved from https://dalfox.hahwul.com/

Hakim, A. S., Cahyanto, T. A., & Azizah, H. n.d. "Serangan Cross-Site Scripting (Xss) Berdasarkan Base Metric CVSS V.2."

Indah, F., Sidabutar, A., & Annisa, N. 2022. "Peran *Cyber Security* Terhadap Keamanan Data Penduduk Negara Indonesia (Studi Kasus: Hacker Bjorka)." 1(1).

Machlul, M. 2024. "Peningkatan Kualitas SDM Melalui Pelatihan *Cyber Security* Pada Anggota Polisi Daerah Jawa Timur." *Parta: Jurnal Pengabdian Kepada Masyarakat* 4(2):150–55. doi: 10.38043/parta.v4i2.4655.

Mujiastuti, R., & Prasetyo, I. n.d. "Membangun Sistem Keamanan Jaringan Berbasis VPN yang Terintegrasi dengan DNS Filtering PIHOLE."

N00bie. (2021, December 15). Install and Use ParamSpider (a parameter miner) - n00bie - Medium. *Medium*. Retrieved from https://n00bie.medium.com

Suroto, S., & Asman, A. n.d. "Ancaman Terhadap Keamanan Informasi Oleh Serangan Cross-Site Scripting (Xss) Dan Metode Pencegahannya." 11.

Tim. (2024, June 3). Indonesia Digempur 6 Juta Ancaman Siber di Awal 2024, Cek Modusnya. *Teknologi*. Retrieved from https://www.cnnindonesia.com