DOI: https://doi.org/10.12962/j26139960.v7i6.624 | Naskah Masuk 29-05-2023; | Naskah Diulas 03-07-2023; | Naskah Diterima 06-07-2023

NASKAH ORISINAL

Pendampingan Analisis *Vulnerability* dan *Hardening* pada *Website* Pemerintah Kota Surabaya

Bambang Setiawan | Febriliyan Samopa | Izzat Aulia Akbar | Nisfu Asrul Sani | Bekti Cahyo Hidayanto | Yogantara S. Dharmawan*

Departemen Sistem Informasi, Institut Teknologi Sepuluh Nopember, Surabaya, Indonesia

Korespondensi

*Yogantara S. Dharmawan, Departemen Sistem Informasi, Institut Teknologi Sepuluh Nopember, Surabaya, Indonesia. Alamat e-mail: yogantara@its.ac.id

Alamat

Laboratorium Infrastruktur dan Keamanan Informasi, Departemen Sistem Informasi, Institut Teknologi Sepuluh Nopember, Surabaya, Indonesia

Abstrak

Keamanan siber penting karena digunakan untuk melindungi semua informasi/ data dari pencurian dan kerusakan. Termasuk data sensitif, informasi identitas pribadi, informasi pribadi, kekayaan intelektual, tidak terkecuali pada sistem informasi *website* pemerintahan. Tanpa keamanan siber, organisasi pemerintahan tidak dapat mempertahankan diri, menjadikannya target bagi penjahat dunia maya. Tes penetrasi adalah salah satu metode yang dapat mengetahui keamanan. Tes Penetrasi, dalam bahasa sehari-hari dikenal sebagai *penetration test*, *pentest* atau *ethical hack*, adalah serangan siber simulasi resmi pada sistem komputer, dilakukan untuk mengevaluasi keamanan sistem. Sedikit berbeda dengan penilaian kerentanan. Tes dilakukan untuk mengidentifikasi kelemahan (juga disebut sebagai kerentanan), termasuk potensi pihak yang tidak berwenang untuk mendapatkan akses ke fitur dan data sistem, serta kekuatan, memungkinkan penilaian risiko penuh untuk diselesaikan. Dengan dilakukannya tes penetrasi *website* di lingkungan pemerintahan Kota Surabaya diharapkan akan meningkatkan kualitas dan ketersediaan layanan kepada masyarakat.

Kata Kunci:

Ethical Hack, Keamanan Siber, Kerentanan *Website*, Tes Penetrasi

1 | PENDAHULUAN

1.1 | Latar Belakang

Pemerintah Kota Surabaya memiliki banyak departemen dan pelayanan yang dapat membantu masyarakat Surabaya untuk mendapatkan informasi dan kebutuhan yang berkaitan dengan berbagai hal selama tinggal di Kota Surabaya. Dalam pemberian pelayanan, diharapkan dapat memudahkan masyarakat dan meningkatkan efektifitas dari pelayanan tersebut. Sehingga dalam era teknologi yang semakin pesat ini, pelayanan di pemerintah kota Surabaya pun banyak berubah menjadi ber-*platform* digital.

Perubahan sistem pelayanan menjadi digital tentu saja dibarengi dengan tanggung jawab yang besar terhadap keamanan informasi yang ditransaksikan dari dan ke masyarakat. Terlebih data yang ditransaksikan tidak jarang merupakan data pribadi yang sensitif seperti nomor KTP, nomor telepon, alamat tempat tinggal, sampai dengan informasi penting lainnya[1].

Bahaya yang mengancam terhadap sistem digital adalah serangan siber[2] [3]. Serangan siber atau *cyber threat* merupakan kejadian yang mengganggu berjalannya sistem elektronik misalnya serangan virus, pencurian data, informasi pribadi, hak kekayaan intelektual perusahaan, *web defacement* dan gangguan akses terhadap layanan elektronik[4]. Dalam undang-undang Republik Indonesia, peraturan ini sudah tertuang dalam Undang-undang Informasi dan Transaksi Elektronik (UU ITE) dimana di dalam undang-undang tersebut terdapat beberapa jenis kejahatan siber dalam transaksi elektronik, yaitu:

- *Cyber-terrorism*

  Serangan elektronik melalui jaringan komputer terhadap infrastruktur kritis yang memiliki potensi dampak kritis terhadap kegiatan sosial dan ekonomi bangsa.

- *Cyber-pornography*

  Penyebarluasan material yang berbau pornografi baik berupa tulisan, gambar maupun video. Bahkan ada undang-undang lain yang juga mengatur mengenai pornografi, yaitu Undang-Undang Nomor 44 Tahun 2008. Dalam undang-undang tersebut tertulis, bukan hanya yang menyebarluaskan melainkan sang pembuat material pornografi juga akan terjerat hukuman pidana.

- *Cyber-harassment*

  Pelecehan atau mengolok-olok seorang atau kelompok individu melalui e-mail, *website*, atau chat program.

- *Cyber-stalking*

  Kejahatan dengan melakukan penguntitan melalui penggunaan komputer dan internet.

- *Cyber-squatting*

  Diartikan sebagai mendapatkan, memperjualbelikan, atau menggunakan suatu nama domain dengan itikad tidak baik.

- *Hacking*

  Penggunaan keahlian programming dengan maksud yang bertentangan dengan hukum.

- *Carding*

  Melibatkan berbagai macam aktivitas yang berkaitan dengan kartu kredit. Carding muncul ketika seseorang yang bukan pemilik akun kartu kredit menggunakan kartu kredit tersebut secara melawan hukum.

- *Organized crime*

  Menggunakan internet untuk memfasilitasi kegiatan ilegal sekelompok individu (*smugling*, jual beli senjata, narkotika)

- *Academic cheating and scientific misconduct*

  Melakukan tindak pidana plagiarisme atau kegiatan keilmuan yang melawan hukum.

Oleh karena itu, perlu adanya penyelidikan mengenai kemungkinan adanya celah keamanan pada sistem pelayanan secara elektronik pada pemerintah khususnya Kota Surabaya untuk mengurangi potensi adanya kerugian di kemudian hari.

2 | SOLUSI PERMASALAHAN

Membantu pemerintah Kota Surabaya untuk melakukan pengecekan sistem pelayanan elektronik yang ada dalam salah biro atau pelayanan yang ada. Dalam hal ini pihak peneliti akan mendiskusikan masalah batasan sistem yang bisa dilakukan pengecekan

dan waktu pelaksanaan pengecekan sistem. Hal ini untuk mengurangi terjadinya penurunan performa pelayanan jika dilakukan pengecekan celah keamanan pada jam transaksi sibuk.

Tim peneliti juga akan mendiskusikan hal apa yang boleh disebarluaskan untuk keperluan publikasi kegiatan dan hal yang hanya boleh disampaikan secara internal terlebih mengenai celah keamanan yang ditemukan pada saat proses pengecekan.

2.1 | Tujuan dan Manfaat Kegiatan

Tujuan pelaksanaan kegiatan:

- Membantu pemerintah khususnya pemerintah kota Surabaya dalam menjaga data masyarakat kota Surabaya dengan mengurangi risiko serangan siber.
- Memberikan peringatan dini terhadap potensi serangan siber yang mungkin dapat terjadi kepada sistem pelayanan elektronik milik pemerintah Kota Surabaya.
- Memberikan saran atau masukan mengenai bagaimana cara memperbaiki celah keamanan yang ditemukan.

Manfaat pelaksanaan kegiatan:

- Terciptanya sistem pelayanan elektronik yang aman pada pemerintah Kota Surabaya
- Pengetahuan mengenai celah keamanan yang dapat muncul pada sistem pelayanan masyarakat

Sehingga dampak pelaksanaan kegiatan ini diharapkan Masyarakat Kota Surabaya akan merasa lebih aman dan puas dengan pelayanan pemerintah kota Surabaya.

3 | METODE KEGIATAN

Kegiatan pendampingan ini dilaksanakan selama kurun waktu 2 bulan secara bertahap. Daftar kegiatan yang dilakukan antara lain:

Gambar 1 Metode pelaksanaan Pelatihan Analisis *Vulnerability* dan *Hardening*.

1. Penyamaan persepsi

   Penyamaan persepsi dilakukan untuk memberikan penjelasan awal mengenai aktifitas pengabdian masyarakat ini. Dalam tahap ini tim peneliti juga akan menanyakan mengenai keadaan sistem, kendala yang sering terjadi pada sistem, atau rencana dari pihak instansi mengenai rencana mereka dalam hal keamanan informasi.

2. Penentuan batasan sistem yang dicek

   Pada tahap ini, tim abmas dan pihak instansi terkait mendiskusikan batasan sistem apa saja yang boleh dilakukan pengecekan celah keamanan. Hal ini untuk menghindari sistem yang memang tidak boleh diakses oleh pihak luar instansi. Output dari tahap ini adalah didapatkannya list sistem yang boleh dilakukan pengecekan celah keamanan. Pada tahap ini juga didiskusikan apakah tim abmas diperbolehkan untuk mengecek *source code* sistem atau tidak. Hal ini akan menentukan teknik pengecekan celah apa yang akan dilakukan.

3. Penentuan data yang boleh dipublikasikan

   Pada tahap ini dilakukan diskusi mengenai data apa saja yang boleh dan tidak boleh untuk dipublikasikan. Walaupun tim abmas diberikan ijin untuk melakukan pengecekan celah keamanan, akan tetapi tidak semua informasi yang didapatkan dapat disebarluaskan untuk kepentingan publikasi kegiatan abmas dan hanya boleh untuk disampaikan secara internal terlebih mengenai celah keamanan yang ditemukan pada saat proses pengecekan.

4. Workshop Penggunaan Zap Owasp

   Tahapan ini dilakukan Bersama dengan tim Mitra untuk sharing mengenai penggunaan *tool* Zap Owasp (ZAP, 2023) dalam rangka analisis *vulnerability* dan *web hardening*. Kami membagikan modul dan juga slides mengenai tata cara pengecekan *vulnerability* berdasarkan batasan sistem yang telah disepakati sebelumnya

5. Pengecekan celah keamanan

   Tahap ini adalah tahap eksekusi dalam kegiatan pengabdian masyarakat dimana tim abmas akan melakukan pengecekan celah keamanan terhadap sistem yang telah ditentukan sebelumnya.

6. Sosialisasi Hasil dan Pendampingan *Web Hardening*

   Hasil dari eksekusi pengecekan dan analisis *vulnerability*, kami sosialisasi dalam bentuk FGD Bersama Mitra dan paparan kepada stakeholder mitra terkait. Informasi yang akan dilaporkan adalah nama celah keamanan, deskripsi celah keamanan, URL atau tempat celah keamanan berada, dan solusi yang dapat dilakukan oleh pihak instansi terkait untuk menutup celah Keamanan. Kami juga memberikan saran dan masukan untuk *web hardening* terhadap web Mitra sehingga dapat meminimalisir celah.

7. Pelaporan

   Pada tahap ini akan dilakukan pelaporan atas hasil aktifitas pengecekan celah keamanan pada sisten yang telah disepakati sebelumnya. Laporan yang telah kami susun kami paparkan kepada pimpinan Mitra dan juga penandaan secara simbolis bahwa kegiatan telah selesai.

3.1 | Tahap Teknis

Tahap teknis, tahap ini menggunakan tahapan umum yang sudah diimplementasikan dalam *penetration testing* [5]:

1. *Pre-engagement Interactions*

   Langkah ini sangat penting sebelum memulai, karena seharusnya kegiatan pentesting bukan mengenai berhasil diretas atau tidak, tetapi tentang mengidentifikasi resiko bisnis yang dapat diserang.

2. *Intelligence Gathering*

   Jika dalam pengembangan perangkat lunak dikenal dengan merumuskan dan mengetahui kebutuhan pengguna, dalam penetration tes dibutuhkan pengetahuan tentang sistem yang akan diretas. Rencana tindakan yang akan dilakukan sesuai dengan kesepakatan dari target.

3. *Threat Modeling*

Memodelkan proses bisnis dan ancaman, sehingga didapatkan gambaran dampak peretasan terhadap keberlangsungan proses bisnis.

4. *Vulnerability Analysis*

   Analisis Kerentanan dilihat dari temuan-temuan kerentanan dan diklasifikasikan terhadap jenis dan tingkat bahayanya.

5. *Exploitation*

   Kerentanan yang sudah ada dijadikan bahan untuk masuk dan melakukan eksploitasi lebih lanjut. Tahap ini akan mencoba semaksimal mungkin apa saja yang bisa dilakukan dan didapatkan dari sistem secara ilegal.

6. *Post Exploitation*

   Hasil tahap *exploitation* dikumpulkan dan dirangkum untuk selanjutnya akan dirangkum dalam laporan yang bersifat menyeluruh.

7. *Reporting*

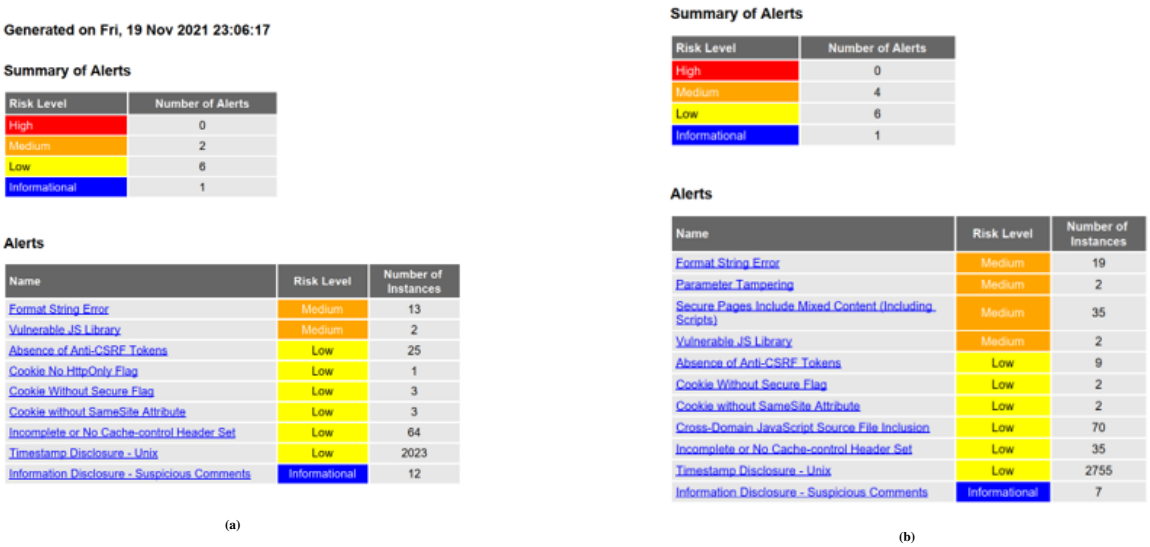
   Mengidentifikasi dan mendokumentasikan hasil. Hal terpenting dalam tahap ini adalah memberikan gambaran umum hingga rinci status sistem berdasarkan jenis dan tingkat kerentangan sistem terhadap serangan. Dari hasil ini pemangku kepentingan juga diberi gambaran bagaimana memprioritaskan dan menerapkan tindakan korektif untuk kerentanan yang diketahui yang dilaporkan.

4 | HASIL DAN DISKUSI

4.1 | Pelaksanaan Kegiatan

Pelaksanaan kegiatan telah dilakukan sesuai urutan pada metode pelaksanaan. Tabel 1 menunjukkan detil dari pelaksanaan kegiatan yang dilakukan.

Tools yang digunakan dalam analisis kerentanan adalah Zap Owasp[6] dan NetSparker[7]. Hasil analisis *vulnerability* dari 2 *tools* tersebut terhadap 2 *website* salah satu OPD di Pemerintah Kota Surabaya dijelaskan pada Gambar (2) dan (3).



Generated on Fri, 19 Nov 2021 23:06:17

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	2
Low	6
Informational	1

Alerts

Name	Risk Level	Number of Instances
Format String Error	Medium	13
Vulnerable JS Library	Medium	2
Absence of Anti-CSRF Tokens	Low	25
Cookie No HttpOnly Flag	Low	1
Cookie Without Secure Flag	Low	3
Cookie without SameSite Attribute	Low	3
Incomplete or No Cache-control Header Set	Low	64
Timestamp Disclosure - Unix	Low	2023
Information Disclosure - Suspicious Comments	Informational	12

(a)

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	4
Low	6
Informational	1

Alerts

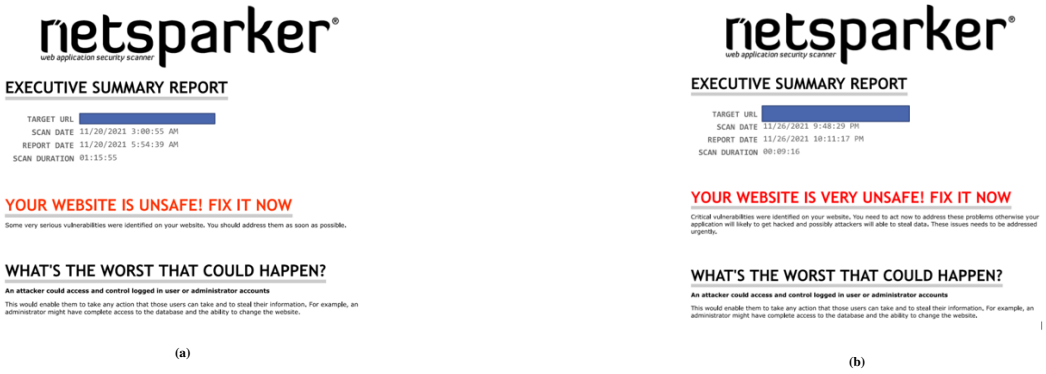
Name	Risk Level	Number of Instances
Format String Error	Medium	19
Parameter Tampering	Medium	2
Secure Pages Include Mixed Content (Including Scripts)	Medium	35
Vulnerable JS Library	Medium	2
Absence of Anti-CSRF Tokens	Low	9
Cookie Without Secure Flag	Low	2
Cookie without SameSite Attribute	Low	2
Cross-Domain JavaScript Source File Inclusion	Low	70
Incomplete or No Cache-control Header Set	Low	35
Timestamp Disclosure - Unix	Low	2755
Information Disclosure - Suspicious Comments	Informational	7

(b)

Gambar 2 Hasil analisis dengan Zap Owasp (a) Website 1; (b) Website 2 OPD Pemkot Surabaya.

Tabel 1 Pelaksanaan Kegiatan

No	Tanggal	Kegiatan	Presentase Kegiatan
1	01 September 2021	Pre-engagement Interactions	5%
2	04 September 2021	Mengidentifikasi resiko bisnis yang dapat diserang	6%
3	05 September 2021	*Intelligence Gathering*	5%
4	07 September 2021	Rencana tindakan yang akan dilakukan sesuai dengan kesepakatan dari target	6%
5	10 September 2021	*Threat Modeling*	6%
6	12 September 2021	Memodelkan proses bisnis dan ancaman, sehingga didapatkan gambaran dampak peretasan terhadap keberlangsungan proses bisnis	8%
7	16 September 2021	*Vulnerability Analysis*	9%
8	24 September 2021	Analisis Kerentanan dilihat dari temuan-temuan kerentanan dan diklasifikasikan terhadap jenis dan tingkat bahayanya	5%
9	26 September 2021	*Exploitation*	9%
10	29 September 2021	Kerentanan yang sudah ada dijadikan bahan untuk masuk dan melakukan eksploitasi lebih lanjut	5%
11	03 Oktober 2021	*Post Exploitation*	5%
12	12 Oktober 2021	Hasil tahap *exploitation* dikumpulkan dan dirangkum untuk selanjutnya akan dirangkum dalam laporan yang bersifat menyeluruh	6%
13	30 Oktober 2021	Reporting	7%
14	05 November 2021	Mengidentifikasi dan mendokumentasikan hasil	5%
15	09 November 2021	Gambaran umum hingga rinci status sistem berdasarkan jenis dan tingkat kerentangan sistem terhadap serangan	5%
16	14 November 2021	Memberikan rekomendasi prioritas dan penerapan tindakan korektif untuk kerentanan yang diketahui yang dilaporkan	6%
17	10 Desember 2021	Diseminasi akhir	2%
			100%



Gambar 3 Hasil analisis dengan Netsparker (a) Website 1; (b) Website 2, OPD Pemkot Surabaya.

4.2 | Hasil dan Manfaat yang dirasakan Masyarakat

Pada temuan celah keamanan yang didapat dalam pelaksanaan aktifitas pengecekan celah keamanaan akan diberikan saran mengenai Langkah yang dapat diambil oleh pihak terkait[8] untuk menutup celah keamaan yang didapat. Solusi yang diberikan akan spesifik terhadap permasalah celah keamanan yang didapat.

Dari celah keamanan pada Bab 1, maka solusi yang dapat diberikan untuk masing-masing celah keamanan adalah:

- *Vulnerable JS Library*
  - Critical : Medium
  - Description : Ditemukan Library Javascript yang memiliki kelemahan
  - URL : *https://XYZ/js/jquery.js*
  - Solution : Melakukan *update* terhadap *library* javascript
- *Custom 404 page identified*
  - Critical : Medium
  - Description : Ditemukan halaman *custom* untuk mengelabuhi pengakses jika *directory* tersebut tidak *exist*. Pada umumnya jika suatu *directory* tersebut tidak *exist*, maka akan mengeluarkan pesan *error 404*. Tetapi pada kasus ini halaman terlihat putih dan memiliki *header* halaman yang berbeda. Hal ini menandakan sebenarnya halaman tersebut ada/ *exist* hanya ditutupi supaya terlihat tidak ada.
  - URL : *https://XYZ/pdfdoc/*
  - Solution : Sebaiknya diberikan dibatasi aksesnya secara permanen dengan memberikan konfigurasi pada *.htaccess*
- *Possibility of SQL Injection*
  - Critical : High
  - Description : Ditemukan kemungkinan adanya celah *SQL Injection* yang dapat menyerang database
  - URL : *https://XYZ/t_detail.php*, *https://XYZ/t_prokum.php*
  - Solution : Diberikan *filter* untuk setiap parameter yang ada di dalam *website*
- *Cookie not marked as Secure*
  - Critical : Low
  - Description : Metode OPTIONS terindentifikasi aktif pada *HTTP Request Method*. Pada kondisi umum seharusnya hanya metode GET, HEAD dan POST saja yang aktif. Metode OPTIONS akan memudahkan orang umum dapat melakukan *request* untuk mendapatkan list metode HTTP apa saja yang aktif. Sehingga akan memberikan informasi tambahan untuk memudahkan aktifitas peretasan.
  - URL : *https://XYZ/images/*
  - Solution : Menonaktifkan metode OPTIONS dengan merubah *setting* pada file konfigurasi *Apache Web Server*(*httpd.conf*)
- *Cookie not marked as HttpOnly*
  - Critical : Low
  - Description : *Cookie* tidak di *set* dengan *flag* HttpOnly
  - URL : *https://XYZ/index.php*

- Solution : Memberikan *flag* HttpOnly pada *Cookie*
- Pada bahasa pemrograman PHP, dapat menggunakan perintah berikut: *setcookie (string $name [, string $value [, int $expire= 0 [, string $path [, string $domain [, bool $secure= false [, bool $httponly= false]]]]]])*

- *OPTIONS Method Enabled*
  - Critical : Low
  - Description : Metode OPTIONS terindentifikasi aktif pada *HTTP Request Method*. Pada kondisi umum seharusnya hanya metode GET, HEAD dan POST saja yang aktif. Metode OPTIONS akan memudahkan orang umum dapat melakukan *request* untuk mendapatkan list metode HTTP apa saja yang aktif. Sehingga akan memberikan informasi tambahan untuk memudahkan aktifitas peretasan.
  - URL : *https://XYZ/images/*
  - Solution : Menonaktifkan metode OPTIONS dengan merubah *setting* pada *file* konfigurasi Apache Web Server (*httpd.conf*)
- *Possibility of Cross-site Request Forgery*
  - Critical : Low / Medium
  - Description : Tidak adanya Anti-CSRF yang terpasang pada *website* target. CSRF adalah serangan yang memanfaatkan sebuah *website* beserta otentikasinya untuk menyerang *website* lain. Walaupun celah ini terindentifikasi sebagai celah yang memiliki kategori *Low*, akan tetapi salah satu *tools* kami mengidentifikasinya sebagai kategori *Medium*. Hal ini dikarenakan CSRF dapat digunakan untuk kegiatan modifikasi konten hingga menghapus data jika celah keamanan CSRF ini berhasil dilakukan.
  - URL : *https://XYZ/index.php*
  - Solution : Disarankan untuk membuat atau memasang anti-CSRF. Contohnya dengan OWASP CSRFGuard.
- *Apache Webserver Confirmed*
  - Critical : Low
  - Description : Diketahui *webserver* yang digunakan oleh *website* JDIH adalah Apache. Apache merupakan *webserver* yang dikeluarkan oleh perusahaan pengembang yang bernama Apache Software Foundation. Dengan mengetahui jenis *webserver* yang digunakan dapat menjadi informasi yang penting untuk mencari kelemahan spesifik pada suatu *webserver*.
  - URL : *https://XYZ/index.php*
  - Solution : Menyembunyikan informasi *webserver* bisa menjadi solusi terbaik untuk mengurasi resiko peretasan di masa mendatang

Berikut dokumentasi kegiatan dari abmas;

Gambar 4 Dokumentasi kegiatan.

5 | KESIMPULAN DAN SARAN

Pengabdian masyarakat ini telah membantu salah satu departemen dalam Pemerintah Kota Surabaya untuk mengurangi potensi tindak kejahatan siber yang dapat terjadi pada sistem. Hal ini dibuktikan dengan berhasilnya menemukan banyak celah keamanan dengan rincian sebagai berikut:

- 1 celah keamanan dengan dampak kerentanan tinggi / *high*
- 1 celah keamanan dengan dampak kerentanan *medium*
- 2 celah keamanan dengan dampak kerentanan *low* (*important*)
- 3 celah keamanan dengan dampak kerentanan *low*

Dengan ditemukannya celah keamanan tersebut dapat menjadikan bahan evaluasi terhadap departemen terkait dan dapat dilakukan perbaikan sebelum hal yang tidak diinginkan terjadi. Dalam pelayanan berbasis online, hal yang paling krusial adalah data. Jika data sampai bocor, apalagi menyangkut data yang sensitif, maka kerugian yang ditimbulkan akan sangat besar. Kerugian bukan hanya untuk departemen yang terkait, tetapi juga untuk setiap individu pengguna yang datanya bocor. Hasil temuan tersebut kami sosialisasikan dan kami melakukan pendampingan dalam melakukan *web hardening*. Saran dan Masukan perbaikan celah *website* telah kami paparkan untuk kemudian dilakukan penguatan/ penutupan celah tersebut. Hasil tersebut telah kami paparkan kepada pimpinan Mitra dan mendapatkan apresiasi dari pimpinan Departemen tersebut.

Saran dari kegiatan ini adalah dilakukannya proses pengecekan kelemahan sistem pada departemen lain di lingkungan Pemerintah Kota Surabaya. Hal ini dikarenakan hampir semua layanan yang ada didalam pemerintah Kota Surabaya sudah bermigrasi ke dalam online atau elektronik. Sehingga dengan melakukan kegiatan pengecekan, maka dapat peringatan dini terhadap potensi serangan siber yang mungkin dapat terjadi kepada sistem pelayanan elektronik milik pemerintah kota Surabaya.

6 | UCAPAN TERIMA KASIH

Pengabdian masyarakat ini didukung oleh DRPM ITS, Departemen Sistem Informasi ITS serta Mitra yakni salah satu Organisasi Perangkat Daerah Pemerintah Kota Surabaya.

Referensi

1. Badan Siber dan Sandi Negara, Rekap Serangan Siber (Januari – April 2020); 2020. https://bssn.go.id/rekap-serangan-siber-januari-april-2020/.
2. Darmaningrat EWT, Ali AHN, Herdiyanti A, Subriadi AP, Muqtadiroh FA, Astuti HM, et al. Sosialisasi Bahaya dan Upaya Pencegahan Social Engineering untuk Meningkatkan Kesadaran Masyarakat tentang Keamanan Informasi. Sewagati 2022;6(2):159–168.
3. Noer LR, Handiwibowo GA, Syairudin B. Analisis Loyalitas Pengguna Electronic Wallet Terhadap Kemanan Transaksi. Sewagati 2020;4(2):88–94.
4. Office of Chief Information Officer U S Department of the Interior, Penetration Testing; 2021. https://www.doi.gov/ocio/customers/penetration-testing.
5. Funk M, Web Application Penetration Testing Checklist (* New* Updated 2019); 2019. https://cybersguards.com/web-application-penetration-testing-checklist-updated-2019/.
6. OWASP, Penetration Testing Methodologies; 2021. https://owasp.org/www-project-web-security-testing-guide/latest/3-The_OWASP_Testing_Framework/1-Penetration_Testing_Methodologies.
7. Invicti Security Corp, Enterprise Web Application Security Best Practices: How to Build a Successful AppSec Program;. https://www.invicti.com/white-papers/enterprise-web-security-best-practices-whitepaper/, diakses Maret 2022.

8. Setiyawan W, Churniawan E, Faried F. Information Technology Regulatory Efforts in Dealing With Cyber Attack To Preserve State. Jurnal USM 2020;3(2):275–295.

Cara mengutip artikel ini: Setiawan, B., Samopa, F., Akbar, I.A., Sani, N.A., Hidayanto, B.C., Dharmawan, Y.S., (2023), Pendampingan Analisis *Vulnerability* dan *Hardening* pada *Website* Pemerintah Kota Surabaya, *Sewagati*, *7(6):897–906*, https://doi.org/10.12962/j26139960.v7i6.624.