Jurnal Infosecure Vol.1 No.1, April 2020
p-ISSN: 2087-1023
MTI-UNLA

PENETRATION TESTING WEBSITE KAMPUS POLITEKNIK AL ISLAM BERDASARKAN OWASP TOP 10

Salman Rashif Fadhilah

Program Studi Informatika, Fakultas Teknik, Universitas Langlangbuana

salmanrf5@gmail.com

Abstrak— Keamanan aplikasi merupakan hal yang penting mengingat ancaman serangan terhadap web sangat meningkat saat ini. Website menjadi salah satu aset penting yang berpotensi menjadi target serangan siber, yang dapat mengakibatkan kerugian data dan gangguan operasional. Dalam penelitian ini, serangkaian pengujian dilakukan untuk mengidentifikasi kerentanan yang ada.

Hasil dari proses penetration testing mengungkapkan beberapa titik lemah yang memerlukan perhatian lebih. Tujuan penelitian ini adalah untuk mencari celah kerentanan keamanan pada website Politeknik Al-Islam dan memberikan solusi untuk memberpaiki celah kerentanan mengacu pada metode Open Web Application Security Project (OWASP) Top 10 Tahun 2021.

Untuk pencarian informasi kerentanan tools yang digunakan adalah OWASPZap, WPSCAN, dan nessus essentials. Penelitian ini menghasilkan beberapa resiko keamanan seperti HSTS missing from HTTPS server, clickjacking, Content Security Policy (CSP) Header Not Set dan cross-domain misconfiguration dengan tingkatan resiko medium. Hasil penelitian celah kerentanan ini nantinya dapat membantu pengelola situs web mengidentifikasi ancaman keamanan yang mungkin terjadi, sehingga mereka dapat mengambil langkah-langkah untuk mencegah serangan dan mengurangi risiko serangan tersebut**.**

Kata kunci— penetration testing, keamanan website, OWASP Top 10, OWASPZap, WPSCAN, nessus essentials, HSTS missing from HTTPS server, clickjacking, (CSP) Header Not Set, cross-domain misconfiguration

I. PENDAHULUAN

Dalam era digital saat ini, keberadaan website menjadi sangat penting bagi berbagai organisasi, termasuk institusi pendidikan, perusahaan, dan lembaga pemerintah. *Website* tidak hanya berfungsi sebagai media informasi, tetapi juga sebagai platform interaksi dan transaksi. Namun, dengan meningkatnya ketergantungan terhadap teknologi informasi, risiko serangan siber juga meningkat. Sesuai data dari *The Open Web Application Security Project (OWASP)* di tahun 2017-2021, yang melakukan survei tentang ancaman yang sering terjadi pada aplikasi web diantaranya *SQL injection*, *cross-site scripting* serta *unrestricted file upload* ([1]).

Website menjadi alternatif bagi perusahaan untuk berhubungan dengan pelanggan dan menjual barang mereka orang-orang dapat dengan mudah dapat diakses kapan saja dan di mana saja. Sebuah laporan dari Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) menunjukkan bahwa jumlah pengguna internet di Indonesia meningkat menjadi 210.026.769 juta pada tahun 2021–2022. Tingkat penetrasi internet di Indonesia meningkat menjadi 77,02%. ([2])

Dengan terus bertambahnya pengguna internet dan pesatnya perkembangan teknologi, maka ada dampak yang pasti akan terjadi pada hal tersebut. Perlu diingat bahwa dengan adanya dampak positif, tentu tidak menutup kemungkinan dengan kemajuan teknologi dan semakin mudahnya mengakses internet tentunya ada hal yang harus diperhatikan dalam hal ini yaitu menyangkut terkait dari adanya ancaman atau serangan kejahatan yang dilakukan oleh pihak tidak bertanggung jawab. Ada banyak macam bentuk ancaman yang sering terjadi pada saat kita menggunakan akses internet salah satunya yaitu yang terjadi pada aplikasi *website*. ([3])

Bicara soal ancaman tentunya berkaitan akan adanya pelaku kejahatan. Didalam *cybercrime* pelaku kejahatan biasanya disebut *Hacker* sedangkan *Hacking* merupakan kejahatan yang telah ada sejak adanya perkembangan teknologi dan internet.

Hacking merupakan masalah yang signifikan dalam jaringan internet di seluruh dunia. *Hacking* adalah tindakan seorang hacker yang mencari kelemahan sistem. Di mana hasilnya dapat berupa program kecil yang dapat digunakan untuk masuk ke sistem atau memanfaatkannya untuk tujuan tertentu tanpa perlu menggunakan akun *user*. Namun, *hacker* adalah istilah yang digunakan untuk menggambarkan beberapa jenis kemampuan komputer. *Hacker* ialah suatu kegiatan yang dilakukan oleh seseorang dalam menguji sebuah sistem atau dapat juga mencari celah kemanan pada sistem seperti *bug*, bongkar pasang sistem dan juga mencari kelemahan suatu sistem. Perlu diketahui bahwa terdapat pengklasifikasian dan karakteristik pada *hacker* yaitu *black hacker*, *white hacker* dan *grey hacker*. Yang pertama ada *black hacker* merupakan salah satu jenis kategori *hacker* yang berbahaya dikarnakan tujuan dari si pelaku ialah melakukan hacking untuk mencuri data pribadi pengguna internet secara ilegal contohnya seperti pembobolan website, password, merusak dan mencuri informasi yang sensitif, nomor telepon, alamat email serta sering juga menginfeksi perangkat software menggunakan virus. ([3])

Berikutnya ada *White Hacker* yang merupakan kebalikan dari *Black Hacker*. *White Hacker* berfokus pada memperkuat

mekanisme yang biasa digunakan dalam hal ini merujuk orang untuk langkah sebuah keamanan. Dengan ini white hacker mempunyai fungsi untuk mencari celah keamanan dari sistem yang demikian celah tersebut dapat dilakukan sebuah analisis dan pengujian guna memastikan sistem dari yang mempunyai celah dapat dilakukan perbaikan serta pencegahan dari tindakan kejahatan. Kemudian yang terakhir ada *Grey Hacker* yang mana jenis hacer yang satu ini merupakan kombinasi jenis diantara *black hacker* dan *white hacker*. *Grey hacker* ini dapat menyesuaikan kondisi dalam hal menerapkan sebuah metode dalam melakukan aksinya, dan disatu sisi *grey hacker* ini tidak selalu melakukan *hacker* untuk kepentingan pribadi akan tetapi sering juga melakukan pelanggaran aturan dari perbuatannya dalam mengekploitasi kemanan dari suatu sistem, dikarenakan tujuan utama dari *grey hacker* ini ialah melakukan peretasan sistem yang digunakan untuk uji coba dalam mengukur tingkat kemampuan yang dimilikinya ([4]).

Dari adanya pengklasifikasian jenis *hacker* tersebut, untuk dipenelitian ini penulis bertindak sebagai *white hacker* yaitu seseorang yang berfokus pada mekanisme keamanan sistem komputer.

OWASP TOP 10 menjadi rujukan mengenai keamanan sistem oleh banyak *cyber security expert*. Berikut beberapa penelitian yang menggunakan OWASP TOP 10 diantarannya pada penelitian pertama yang ditulis oleh pada penelitiannya melakukan pengujian pada website Universitas ARS menggunakan *Open Web Application Security Project* (*OWASP*), adapun pengujian ini menggunakan metode *penetration testing* dengan mengacu pada parameter *OWASP TOP 10* tahun 2017 dan adapun *tools* yang digunakan pada penelitian ini adalah *OWASP ZAP*, *uniscan* dan *nikto* menemukan bahwa *OWASP* versi 4 digunakan untuk pengujian penetrasi, dan alat pemindaian kelemahan *website* yang digunakan adalah *acunetix*. Objek yang diteliti adalah aplikasi berbasis *web*.

Untuk melakukan uji penetrasi, situs web dapat menggunakan tiga jenis uji kerentanan: uji *Black Box*, uji *White Box*, dan uji *Gray Box*. Menurut penjelasan ([5]) dalam bukunya yang berjudul *Etichal Hacking* and *Penetration Testing Guide* merinci bahwa pengujian penetrasi terbagi menjadi tiga bagian. Pengujian keamanan *Black Box* adalah pengujian yang dilakukan oleh orang yang tidak memiliki informasi apa pun tentang sistem operasi, versi *server*, atau jaringan yang ada di dalam sistem, sehingga orang yang melakukan pengujian harus mencari semua informasi yang dibutuhkan untuk melakukan pengujian. Pengujian Keamanan *white box* adalah pengujian yang dilakukan oleh orang yang tidak memiliki informasi apa pun tentang sistem operasi, versi *server*, atau jaringan yang ada di dalam sistem, dan yang ketiga ada *Gray Box Security Testing* yang merupakan gabungan dari kedua metode antara *Black Box Security Testing* dan *White Box Security Testing*. Metode ini menggunakan perspektif orang yang terlibat dalam sistem tetapi tidak dapat mengaksesnya secara langsung.

Penetration testing merupakan metode pengujian untuk mengidentifikasi celah keamanan dengan tujuan memperoleh akses ke suatu sistem atau situs *web*. Pengujian ini meniru teknik yang mungkin digunakan oleh pihak tak berwenang untuk menembus sistem keamanan dan mendapatkan akses tanpa izin ([6]). Proses pengujian dilakukan menggunakan metode *Penetration Testing Execution Standard* (*PTES*), yaitu panduan metodologis yang mencakup standar dan langkah-langkah penting dalam pelaksanaan uji penetrasi yang efektif ([7]). *PTES* dipilih karena tahapan-tahapannya dianggap lebih mudah dipahami, bahkan oleh pengguna yang bukan ahli dalam bidang keamanan system.

Vulnerability, juga dikenal sebagai kerentanan jaringan, adalah kelemahan program atau infrastruktur yang memungkinkan ekploitasi sistem. Kesalahan dalam desain, pembuatan, atau implementasi sistem dapat menyebabkan kelemahan ini. *Hacker* akan menggunakan kelemahan untuk masuk ke sistem ilegal. *Hacker* umumnya membuat eksploit yang disesuaikan dengan celah. Perangkat lunak komputer yang dikodekan dalam bahasa pemograman yang mendukung perangkat lunak berbasis web seperti *HTML*, *CSS*, *JavaScipt*, *Ruby*, *Python*, *PHP*, dan *Java* juga dapat mengalami kerentanan. ([8])

II. METODE

A. *Metode VAPT* (*Vulnerability Assessment and Penetration Testing*)

Vulnerability Assessment (VA) dan *Penetration Testing* (PT) adalah dua metode utama untuk mengevaluasi keamanan sistem informasi, dan keduanya saling melengkapi untuk memberikan gambaran keamanan sistem yang lengkap.

Proses menentukan, mengidentifikasi, mengklasifikasikan, dan memprioritaskan kerentanan dalam sistem komputer, aplikasi, dan infrastruktur jaringan dikenal sebagai *Vulnerability Assessment*. Tujuan dari *Vulnerability Assessment* adalah untuk menemukan kelemahan yang mungkin ada sebelum threat actor dapat memanfaatkannya. Ini mencakup pemindaian seluruh sistem secara manual dan otomatis untuk menemukan celah yang dapat menjadi sasaran empuk serangan siber.

Penetration testing, juga dikenal sebagai pentest, adalah sebuah teknik yang meniru serangan asli dalam upaya untuk mengidentifikasi cara untuk menghindari fitur keamanan aplikasi, sistem, atau jaringan. Pentest biasanya melibatkan serangan nyata pada sistem dan data, menggunakan alat dan teknik yang sama dengan yang digunakan oleh threat actor yang sebenarnya. Berbeda dengan *Vulnerability Assessment*, *pentest* bersifat aktif dan agresif, yang berarti penguji benar-benar mencoba memanfaatkan kelemahan. Tujuan dari penelitian ini adalah untuk menilai kapasitas pertahanan sistem terhadap serangan nyata. Ini menunjukkan seberapa jauh pelaku ancaman dapat memasuki jaringan, aplikasi, atau sistem keamanan.

Gambar 1 Metode VAPT

1. *Planning*
Pada tahap ini, saya melakukan perencaan seperti menentukan ruang lingkup penelitian, lalu mengidentifikasi target.
2. *Information Gathering*
Selanjutnya saya melakukan pencarian infromasi tentang *website* Politeknik Al-Islam dengan menggunakan *google hacking*.
3. *Vulnerability Scanning*
Setelah melakukan pencarian informasi tentang website Politeknik Al-Islam, saya melalakukan pemindaian pada website dengan tools seperti *OWASP ZAP*, *Nessus Essentials*, dan *WPScan*.
4. *Penetration Testing*
Setelah melakukan pemindaian, saya melakukan attacking terhadap website untuk menilai ketahanan sistem terhadap serangan.
5. *Reporting*
Langkah terakhir saya melakukan pelaporan dari semua riset seperti kerentanan yang teridentifikasi, potensi resiko, dan rekomendasi tindakan untuk memperkuat *website* Politeknik Al-Islam.

B. Langkah-Langkah Penetration Testing

1. Perencanaan (*planning*)
Pada tahap pertama, *pentester* harus merencanakan metode pengujian yang akan digunakan, sistem keamanan *server* yang digunakan, mengumpulkan data, dan mempersiapkan nama *domain server*. Tujuan dari tahap perencanaan adalah agar pentester mengetahui lingkungan sistem yang akan digunakan dan dapat menyesuaikan metode yang akan digunakan.
2. Pemindaian (*scanning*)
Setelah rencana selesai, langkah berikutnya adalah memindai kerentanan sistem keamanan. Pada tahap ini, alat tambahan biasanya membantu proses seperti pengelompokan layanan, *scanning port*, dan scanning kelemahan. Pada tahap ini, pentester akan melakukan dua metode pemindaian: analisis statis dan dinamis.
3. Mendapatkan akses (*gaining access*)
Pada tahap ketiga, *pentester* yang telah menemukan celah keamanan yang memungkinkan untuk disusupi akan mencoba memasuki sistem tersebut. *Pentester* akan bertindak seperti *hacker* dan mencoba mendapatkan akses penuh ke *server* tersebut.
4. Mempertahankan akses (*maintaining access*)
Pentester akan melihat apakah ada celah kerentanan yang bertahan atau permanen ketika mereka memiliki akses penuh. Jika celah tersebut dianggap permanen, itu akan berbahaya bagi pengguna karena *hacker* dapat masuk ke inti sistem.
5. Pelaporan hasil (*reporting*)
Hasil pindaian hingga pertahanan akses kemudian dilaporkan. Laporan tersebut mencakup informasi tentang penemuan celah yang rentan disusupi, solusi terbaik, dan rekomendasi sistem keamanan yang tepat.
6. Perbaikan (*remediation*)
Pada tahap terakhir, masalah atau kerentanan sistem keamanan akan diselesaikan dengan memperbaiki sistem. Jika masih ditemukan bahwa server memiliki kerentanan yang tinggi, server akan diuji ulang untuk memastikan bahwa keamanan jaringan telah ditingkatkan.

Gambar 2 Tahapan *Penetration Testing* sumber: [9]

III. HASIL DAN PEMBAHASAN

Pada implementasi *penetration testing website* Politeknik Al-Islam berdasarkan *OWASP TOP 10*, beberapa tahapan dan pengujian telah dilakukan untuk memastikan keamanan dan efisiensi sistem. Berikut ini adalah hasil utama dari implementasi tersebut:

A. Tahap Perencanaan (Planning)

Tahap planning meliputi alat pengujian, proses pengumpulan informasi, dan penentuan skala prioritas website target.

Alat yang digunakan dalam melakukan penelitian ini terdiri dari perangkat keras (*hardware*), perangkat lunak (*software*) dan tools lainnya.

TABEL I

Tabel I Tabel Perangkat Lunak (*software*)

Jenis *Software*	Spesifikasi
Operating System (OS)	*Windows* 11 dan *Kali linux* 2022.3
Application Software	*Oracle VM VirtualBox-amd64*

TABEL II

Tabel II Tabel Perangkat Keras (*Hardware*)

Komponen	Spesifikasi yang digunakan
Processor	12th Gen Intel(R) Core(TM) i5-12400F (12 CPUs), ~2.5GHz
RAM	8 GB
Storage Memory	1 TB

TABEL III

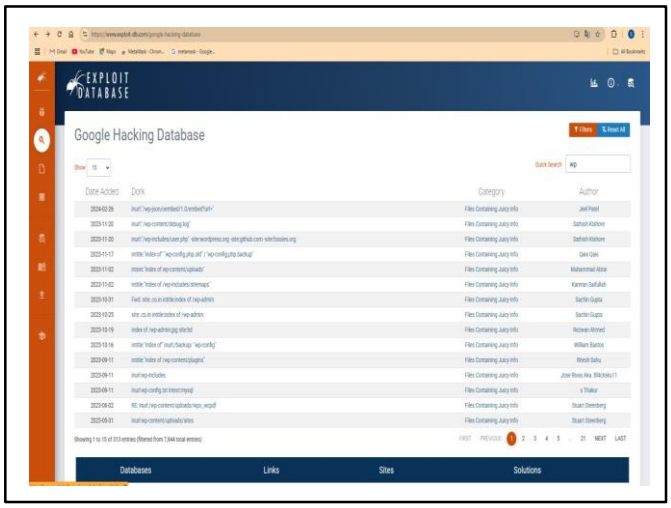
Tabel III Tabel *Tools*

Tahapan	*Tools*	Fungsi
Information Gathering	*Google Hacking*	Menemukan daftar celah yang tersedia dalam GHDB, lalu lanjut dicari dalam mesin pencari Google
Vulnerability Scanner	OWASP ZAP 2.12.0, *WPScan*, dan *Nessus essenials*	Mencari celah kerentanan yang terdapat pada website
Attacking	*Burp Suite, Sslstrip, HSTShijack, Pastebin, Bettercap, Arpsoof*	Menguji kerentanan website yang didapat pada proses sebelumnya.
Report	*Ms. Word*	Menulis dan melaporkan hasil pengujian

B. *Proses Pengumpulan Informasi*

Pada tahap ini ialah proses dalam melakukan pengumpulan informasi mengenai target dan pemindaian kerentanan. Proses ini dibagi menjadi yaitu *information gathering* dan *vulnerability Scanner*.

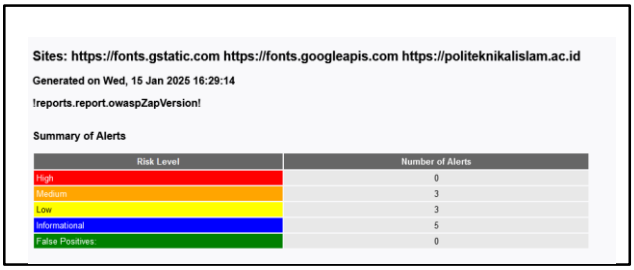
Pada tahap *information gathering* dilakukan penambahan informasi tentang daftar celah yang tersedia dalam Google *database* (GHDB), kemudian dilanjutkan menggunakan *search engine* google ([10])



Gambar 3 Daftar *Dork Wordpress* Dalam *Google Hacking*

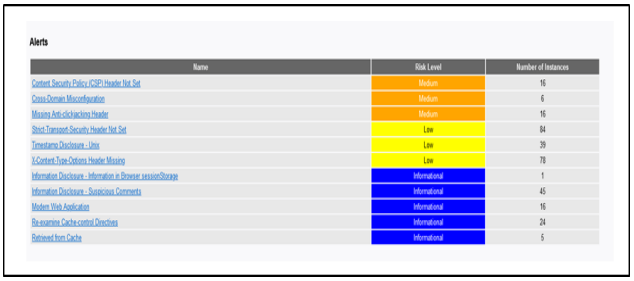
C. *Vulnerability Scan*

Tahap ini dilakukan dengan cara mencari celah keamanan menggunakan tools seperti WPScan, OWASP ZAP, dan Nessus Essentials.



Gambar 4 Gambar Hasil Scanning Dengan OWASP ZAP

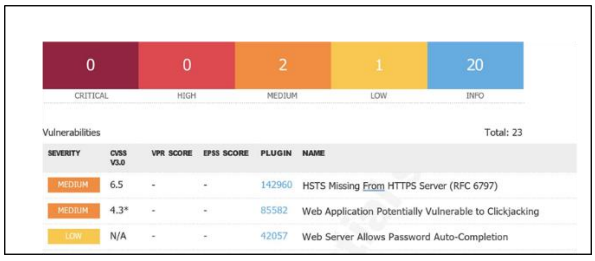
Berdasarkan hasil scan yang dilakukan menggunakan OWASP ZAP bahwa di website Politeknik Al-Islam dapat ditemukan hasil 3 alert medium, dan 3 alert low.



Gambar 5 Gambar Hasil Keseluruhan *Scanner* Dengan *OWASP ZAP*

Gambar 6 Gambar Hasil *Scanning* Dengan *WPS SCAN*

Dari hasil scanning menggunakan *WPScan* menunjukan bahwa website Politeknik Al-Islam yang bekerja sama dengan keamanan Sinatra bahwa keamanan Sinatra pernah memiliki kerentanan *Stored Cross-Site Scripting* dimana pengguna yang terautentikasi dapat menyisipkan kode *JavaScript* berbahaya yang disimpan didalam situs tersebut.



Gambar 7 Gambar hasil *scanning* dengan *Nessus Essentials*

Selanjutnya dari hasil *scanning* menggunakan *Nessus Essentials* menunjukan bahwa *website* Politeknik Al-Islam memiliki kerentanan seperti *HSTS Missing From HTTPS Server* menunjukan bahwa situs web tidak menggunakan *HSTS*, lalu ada *Web Application Potentially Vulnerable to Clickjacking* yaitu *web* yang rentan terhadap serangan *clickjacking*, *clickjacking* adalah serangan dimana pengguna mengklik halaman *web* yang tidak terlihat yang dapat pengguna mengunduh *malware*, dan mengunjungi situs yang bahaya.

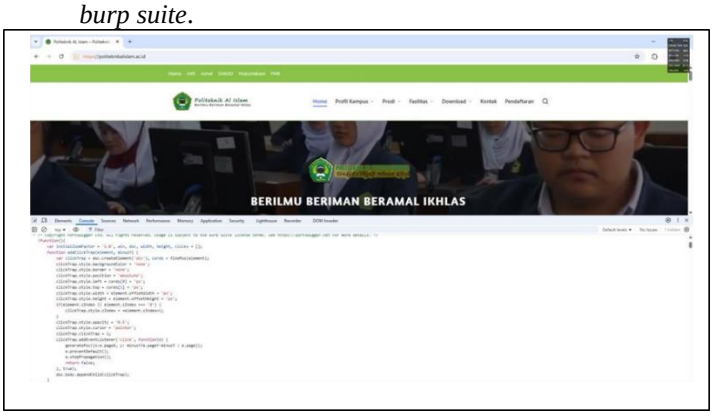
D. Tahap Attacking

1. *Clickjacking*

   Clickjacking disini saya akan menggunakan aplikasi *burp suite* dimana kita membuat *html* seolah-olah *website* tersebut *website* yang asli.

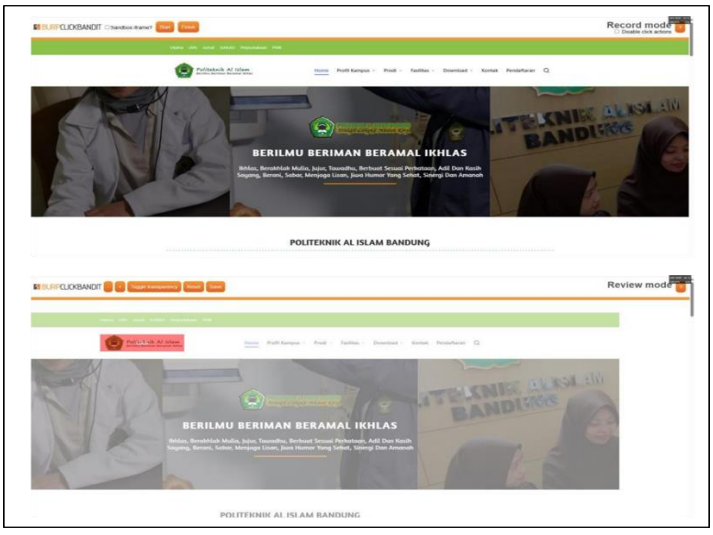
Gambar 8 Gambar Salinan *Script* Dari *Burp Suite*

Pertama-tama saya akan menyalin *script* dari aplikasi *burp suite*.



Gambar 9 Gambar Salinan *Script* Ke *Console Website* Politeknik Al-Islam

Lalu salin *script* tersebut di console website Politeknik Al-Islam.

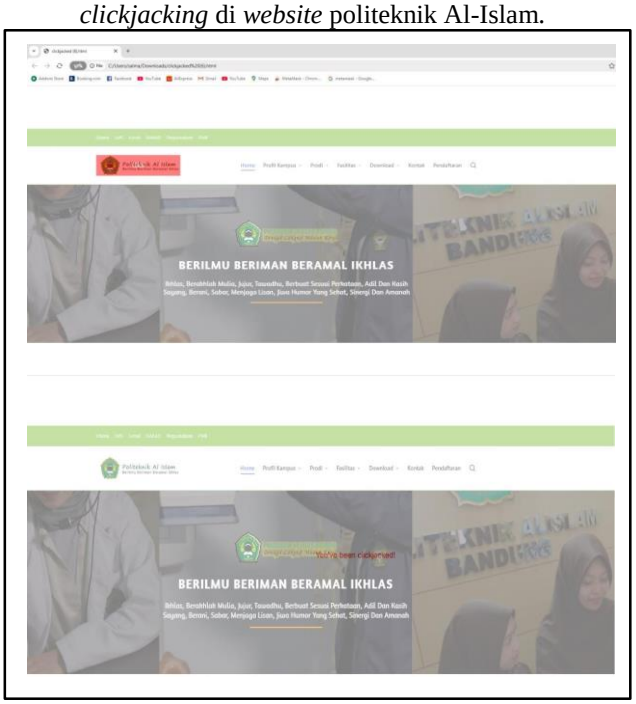


Gambar 10 Gambar Peletakan *Clickjacking* Pada Website

Selanjutnya meletakan *clickjacking* tersebut di *website* tersebut.

Gambar 11 Gambar *HTML* Dari *Website*

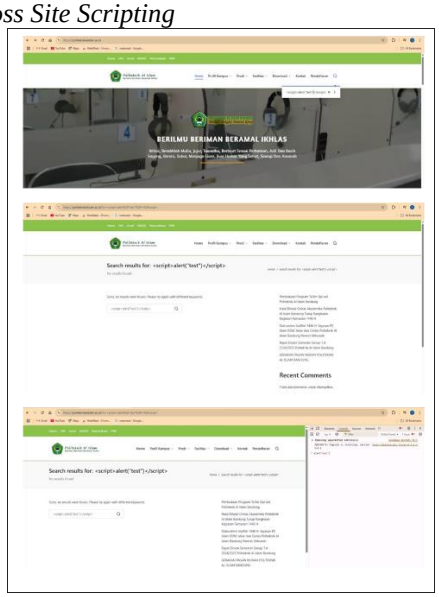
Dan setelahnya saya mendownload *HTML* yang ada *clickjacking* di *website* politeknik Al-Islam.

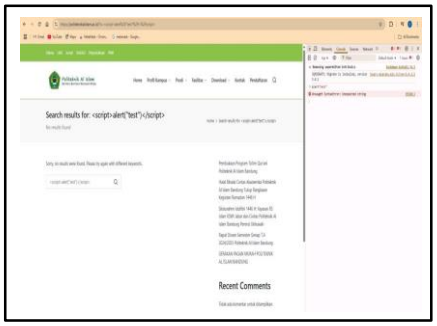


Gambar 12 Gambar *HTML* Yang Telah Dimasukan *clickjacking*

Selanjutnya ketika mengklik bagian yang dimasukan clickjacking maka akan muncul tulisan “You’ve been clickjacked!” yang membutikan bahwa website tersebut rentan terhadap serangan clickjacking.

2. *Cross Site Scripting*





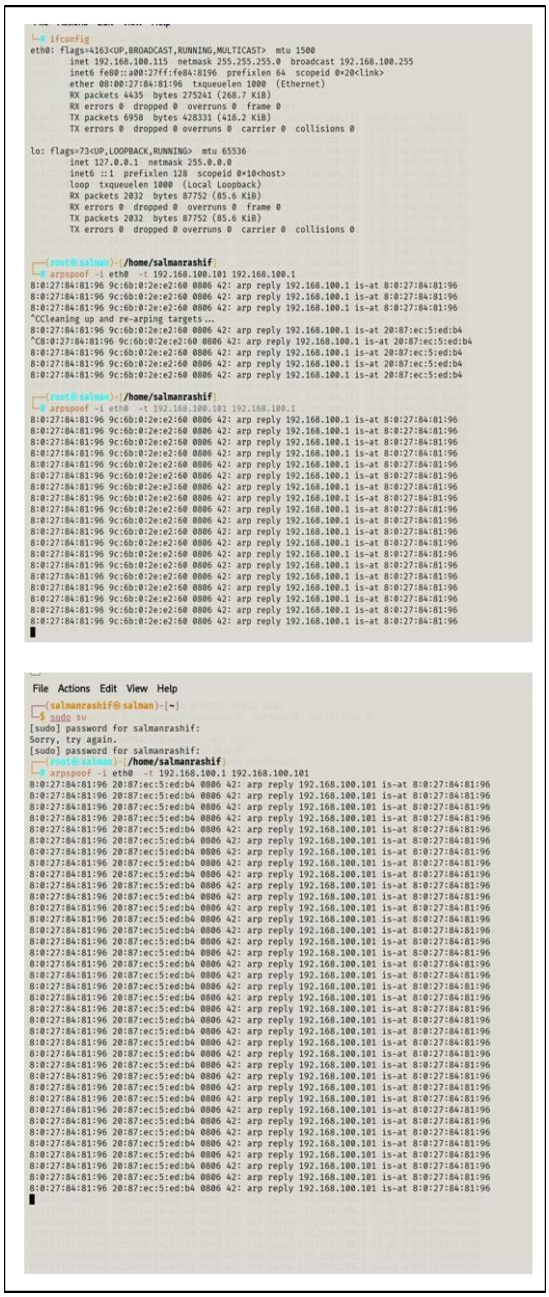
Gambar 13 Gambar Hasil Percobaan *Cross Site Scripting*

Pada percobaan ini saya memasukan script pada pencarian dan pada *console website* namun yang dihasilkan adalah *false positive* atau *website* tidak dapat di*attack* oleh serangan *cross site scripting*.

3. *Sslstripping* dan *Man In the Middle attack*

Gambar 14 Gambar Pencarian *Ip Address*

Pada *sslstripping* dan *man in the middle attack* pertama-tama saya melakukan pencarian *Ip target* di *kali linux* yang dimana saya menggunakan *ip target* saya yang ada di *windows* yaitu dengan *ip* 192.168.100.101.

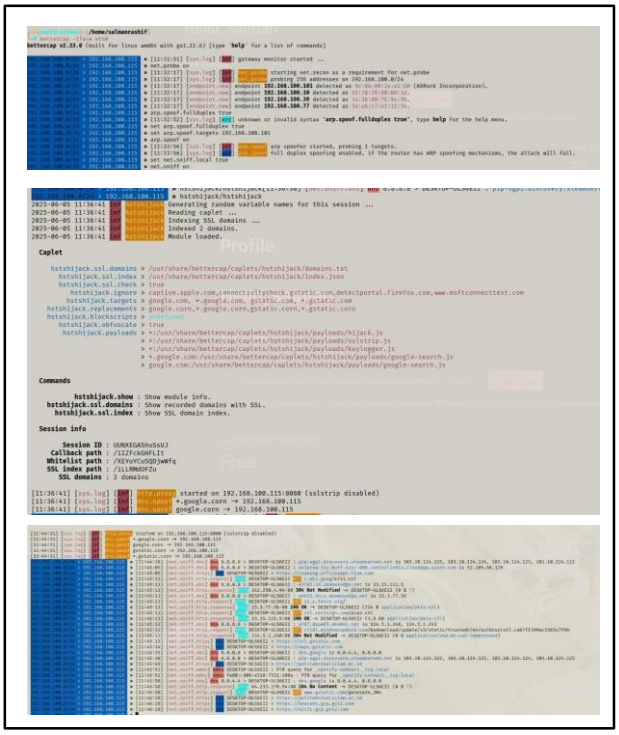


Gambar 15 Gambar *Arpsoof Ip*

Selanjutnya saya melakukan *arspoof* pada *ip kali linux* dengan *ip target* begitupun sebaliknya agar *ip* tersamarkan.

Gambar 16 Gambar Percobaan *Sslstriping*

Langkah berikutnya saya melakukan *sslstrip* dengan menambahkan kode diatas untuk membuka *HTTPS* ke *HTTP* namun hasil yang didapat adalah *false positive* dimana website Politeknik Al-Islam tidak dapat di*attack* oleh *sslstrip*.



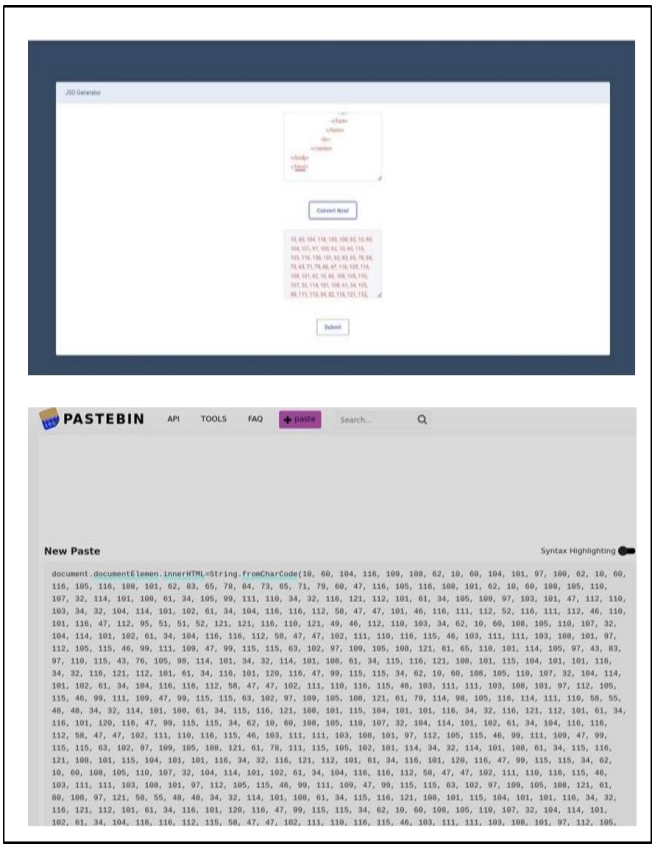
Gambar 17 Gambar *HSTS Hijack*

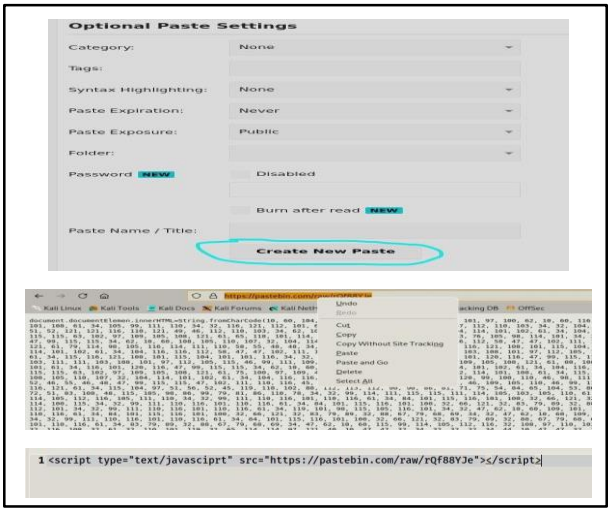
Di gambar diatas saya melakukan *HSTS hijack* agar bisa melakukan perubahan *website* dari *HTTPS* menjadi *HTTP* menggunakan bettercap namun hasilnya tetap *false positive* dimana *website* Politeknik Al-Islam tidak dapat diattack oleh *HSTS Hijack*.

4. *Deface Website*

Gambar 18 Gambar Pembuatan *HTML* Untuk *Deface Website*

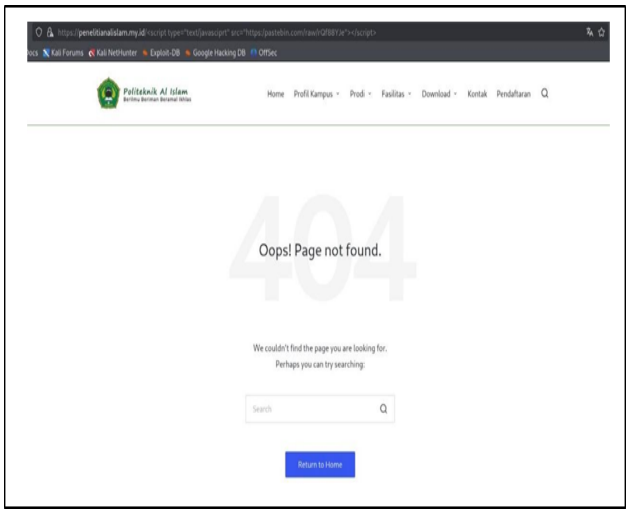
Untuk melakukan *deface website* pertama-tama saya membuat *HTML* untuk dimasukan kedalam *website target*.





Gambar 19 Gambar Pengubahan *HTML* Menjadi *Source*

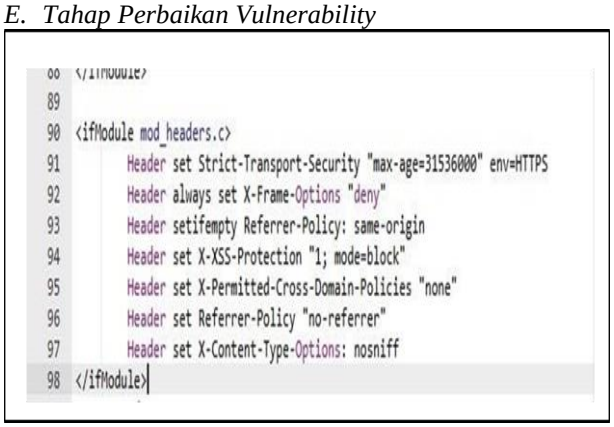
Setelah membuat *HTML* lalu *HTML* tersebut di *convert* menjadi kode dan diubah menjadi *source* agar bisa dimasukan kedalam *script*.



Gambar 20 Gambar *Attacking CSRF* pada *website*

Lalu masukan *script* tersebut pada alamat *website*, namun hasilnya *false positive* dimana *website* tersebut tidak dapat di *deface*.

E. Tahap Perbaikan Vulnerability

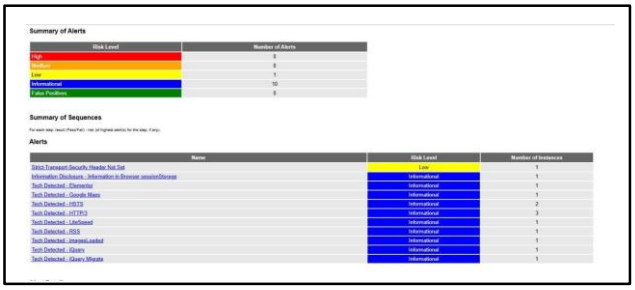


```
89
90  <ifModule mod_headers.c>
91      Header set Strict-Transport-Security "max-age=31536000" env=HTTPS
92      Header always set X-Frame-Options "deny"
93      Header setifempty Referrer-Policy: same-origin
94      Header set X-XSS-Protection "1; mode=block"
95      Header set X-Permitted-Cross-Domain-Policies "none"
96      Header set Referrer-Policy "no-referrer"
97      Header set X-Content-Type-Options: nosniff
98  </ifModule>
```

Gambar 21 Gambar Pembuatan *Header* Pada *Website*

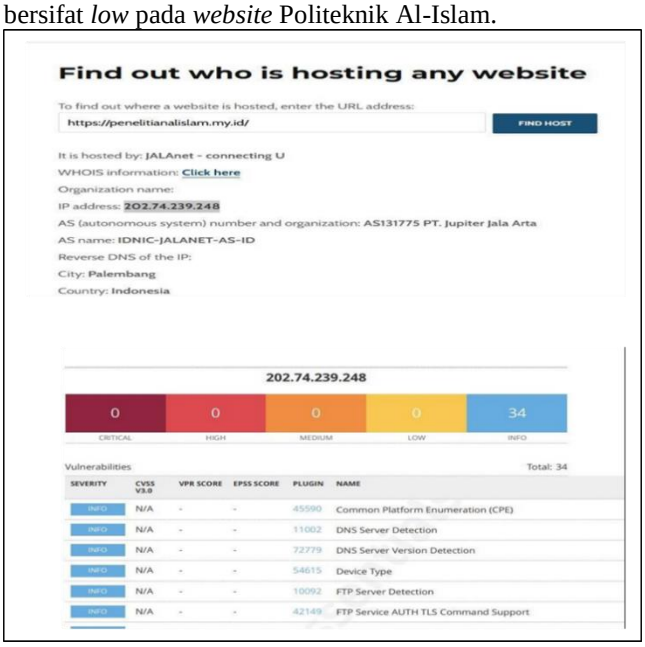
Untuk mencegah *clickjacking* saya menambahkan *.htacces* dengan header set x- frame options agar website mencegah *frame* didalamnya.
Setelah itu ada *header-header* lain yang berfungsi:

1. Header set Strict-Transport-Security "max-age=31536000" env=HTTPS berfungsi untuk mengaktifkan HSTS.
2. Header setifempty Referrer-Policy: same-origin berfungsi untuk mengatur Referrer-Policy hanya jika belum diatur.
3. Header set X-XSS-Protection "1; mode=block" berfungsi untuk mengaktifkan proteksi Cross-Site Scripting di browser.
4. Header set X-Permitted-Cross-Domain-Policies "none" berfungsi untuk mencegah Flash atau PDF dari melakukan permintaan lintas domain.
5. Header set Referrer-Policy "no-referrer" berfungsi untuk menetapkan kebijakan referer untuk tidak mengirimkan header Referer sama sekali.
6. Header set X-Content-Type-Options: nosniff berfungsi untuk melindungi dari serangan sniffing.



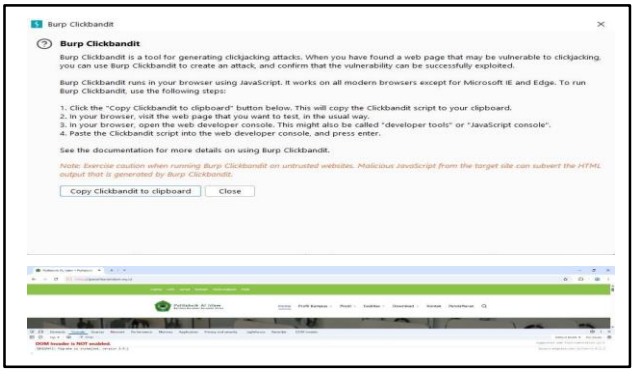
Gambar 22 Gambar Scanning Owasp Zap Setelah Dilakukan Perbaikan

Setelah dilakukan perbaikan hanya ada satu kerentanan yang bersifat *low* pada *website* Politeknik Al-Islam.



Gambar 23 Gambar *Scanning Nessus Essentials* Setelah Dilakukan Perbaikan

Setelah dilakukan perbaikan pada scanning *Nessus Essentials* tidak ada kerentanan pada website Politeknik Al-Islam.



Gambar 24 Gambar Pengujian ulang *Clickjacking*

Setelah diuji ulang hasilnya kerentanan *Clickjacking* bisa diblokir dan situs aman dari kerentanan *Clickjacking*.

TABEL IV

Tabel IV Tabel *Resume*

NO	Temuan	*Severity*	Hasil *Attack*	Kesimpulan
1	*Clickjacking*	*Medium*	Berhasil	Ditanggulangi dengan menambahkan header di *.htacces*
2	*Cross site scripting*	*Hight*	Gagal	*False Positive*
3	*Sslstripping dan Man In the Middle attack*	*Medium*	Gagal	*False Positive*
4	*Device Website*	*Medium*	Gagal	*False Positive*

IV. SIMPULAN

Kesimpulan yang dapat diambil dari penetration testing website Politeknik Al- Islam yang berdasarkan OWASP TOP 10 dengan metode *VAPT* (*Vulnerability Assessment and Penetration Testing*) adalah sebagai berikut:

1. *Website* Politeknik Al-Islam saat dilakukan *penetration testing* oleh aplikasi *OWASPZap*, *Nessus Essentials*, dan *WPScan* terdapat beberapa kerentanan seperti *clickjacking*, *HSTS Missing*, *Cross-Domain Misconfiguration*, dan *Cross-Domain Misconfiguration*.
2. Saat dilakukan *attacking* hanya kerentanan *clickjacking* yang berhasil menembus keamanan website Politeknik Al-Islam dengan menggunakan aplikasi burp suite dan Kerentanan pada website Politeknik Al-Islam dapat ditangani dengan menambah beberapa *header* di *.htacces website* tersebut.

REFERENSI

[1] OWASP Top Ten | OWASP Foundation. Retrieved May 19, 2023, from https://owasp.org/www-project-top-ten/

[2] Agustantia. (2022). Penetration Testing Menggunakan Owasp Top 10 Pada Domain ps://jurnal.poltekst paul.ac.id/index.php/jelekn/article/download/455/328

[3] Yusuf DM. (2022). Analisis Kejahatan Hacking Sebagai Bentuk Cyber Crime Dalam Sistem Hukum yang berlaku di Indonesia. Pendidikan Dan Konseling, 4(6), 3029–3034

[4] Peter, A. (2023). The Basics of Hacking and Penetration Testing. Cybersecurity and Identity Access Management, 21–46. https://doi.org/10.1007/978-981-19- 2658-7_2 Baloch, R. (2017). Ethical Hacking and Penetration Testing Guide. In Ethical Hacking and Penetration Testing Guide. https://doi.org/10.4324/9781315145891

[5] Baloch, R. (2017). Ethical Hacking and Penetration Testing Guide. In Ethical Hacking and Penetration Testing Guide. https://doi.org/10.4324/9781315145891

[6] Rosaliah. (2021), "Pengujian Celah Keamanan Website Menggunakan Teknik Penetration Testing dan Metode OWASP TOP 10 pada Website SIM xxx," conference.upnvj.ac.id

[7] Utoro. (2020), "Analisis Keamanan Website E-Learning SMKN 1 Cibatu Menggunakan Metode Penetration Testing Execution Standard," vol. 6, no. 2, pp. 169–178, 2020

[8] Ghozali, B., Kusrini, K., & Sudarmawan, S. (2019). Mendeteksi Kerentanan Keamanan Aplikasi Website Menggunakan Metode Owasp Untuk Penilaian Risk Rating. Creative Information Technology Journal, 4(4), 264. https://doi.org/10.24076/citec.2017v4i4.119

[9] Septian Bagus. (2024). Apa Itu Penetration Testing? Jenis, Fungsi dan Tahapannya. https://digitalsolusigrup.co.id/apa-itu-penetration-testing/

[10] Inggih Pangestu. (2022). Mengenal Apa itu Google Dork: Pengertian, Fungsi dan Cara Menggunakannya idmetafora. https://idmetafora.com/news/read/2015/Mengenal-Apa-itu-Google-