LAMPIRAN

Lampiran 1 Surat Permohonan Data Tugas Akhir

FAKULTAS TEKNIK

ft.umm.ac.id | ftumm@umm.ac.id

UNIVERSITAS MUHAMMADIYAH MALANG

Malang, 03 Januari 2024

Nomor : E.5.d/ /FT-Inf/UMM/I/2024
Lampiran : -
Perihal : ***Permohonan Data Tugas Akhir (Skripsi)***

Kepada : **Yth. Kepala Website SIM-PKN-MBKM Informatika Universitas Muhammadiyah Malang Fakultas Teknik Program Studi Informatika Gedung Kuliah Bersama (GKB) III Jl. Raya Tlogomas No. 246 Telp (0341) 464318 Psw 247 Di Tempat**

Assalamualaikum Wr. Wb.

Dengan hormat, guna melengkapi dan menyelesaikan Tugas Akhir (Skripsi) sebagai syarat kelulusan bagi Mahasiswa Fakultas Teknik Universitas Muhammadiyah Malang sebagai berikut :

Nama	: Helmi Indra Perdhana
NIM/Prodi	: 202010370311484 / Informatika
Email	: helmiindra22@webmail.umm.ac.id
Telepon	: 085746303429

Dengan Judul Tugas Akhir **"Analisis Dan Mitigasi Celah Keamanan Website SIMPKN Informatika Menggunakan Metode Owasp Zed Attack Proxy (ZAP)".**

Maka dengan ini kami mohon Kepada Bapak/Ibu untuk dapat memberikan Ijin/Rekomendasi Kepada Mahasiswa tersebut untuk melakukan penelitian atau mendapatkan data penyusunan Tugas Akhir/Skripsi di **Website SIM-PKN-MBKM Informatika.**

Demikian surat permohonan ini. Atas perhatian dan bantuan Bapak/Ibu kami sampaikan terimakasih.

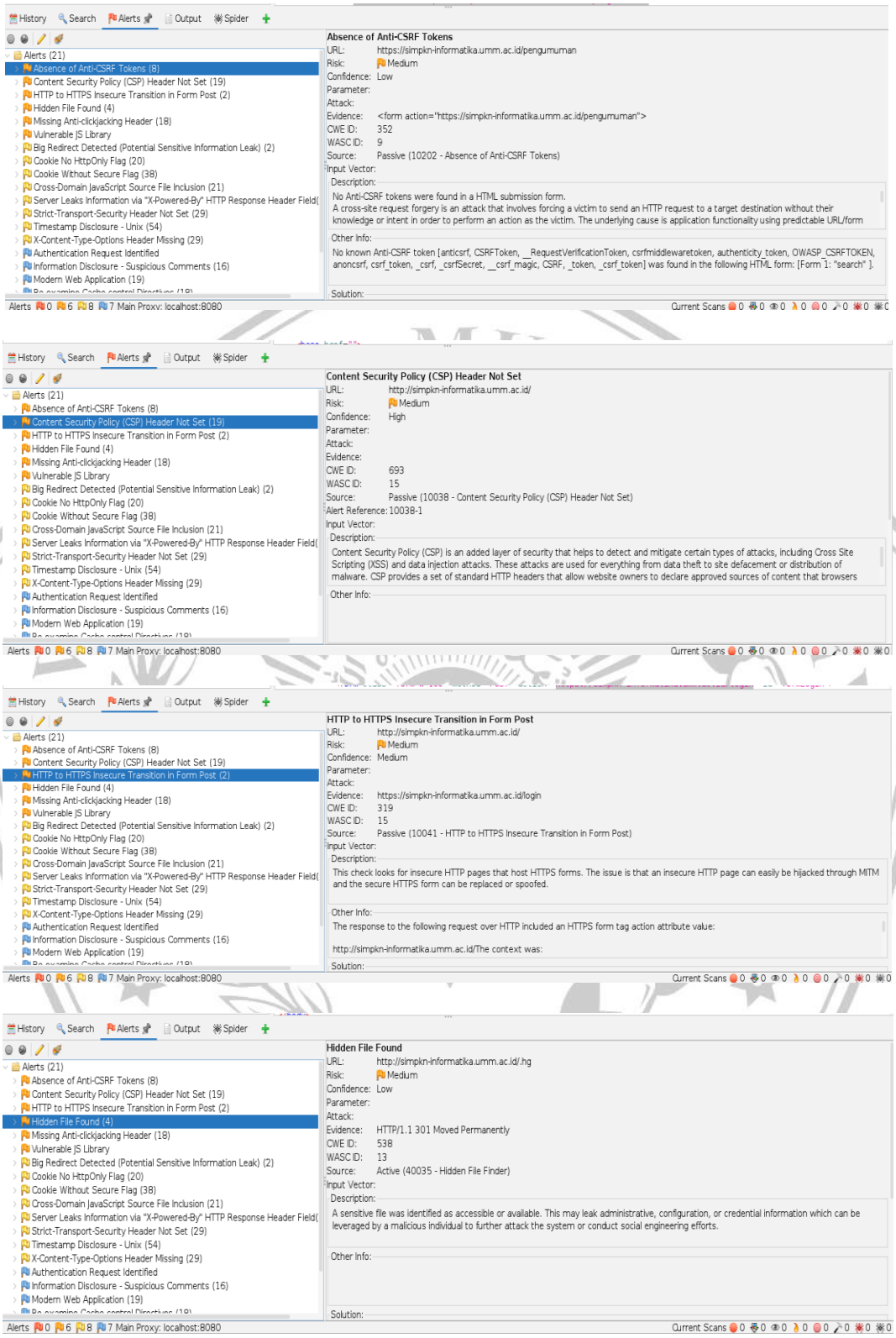
Wassalamualaikum Wr. Wb.

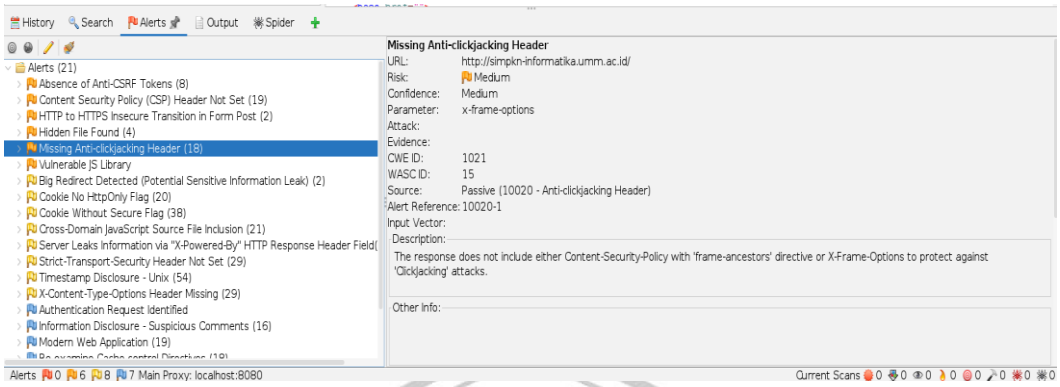
a.n. Dekan
Ketua Program Studi,

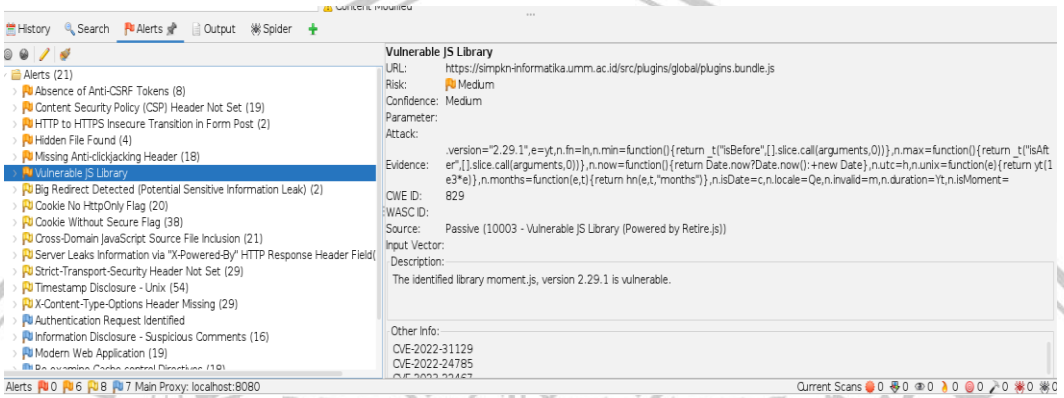
Ir. Galih Wasis Wicaksono, S.Kom., M.Cs.

Kampus I Jl. Bandung 1 Malang, Jawa Timur P. +62 341 551 253 (Hunting) F. +62 341 460 435
Kampus II Jl. Bendungan Sutami No.188 Malang, Jawa Timur P. +62 341 551 149 (Hunting) F. +62 341 582 060
Kampus III Jl. Raya Tlogomas No.246 Malang, Jawa Timur P. +62 341 464 318 (Hunting) F. +62 341 460 435 E. webmaster@umm.ac.id

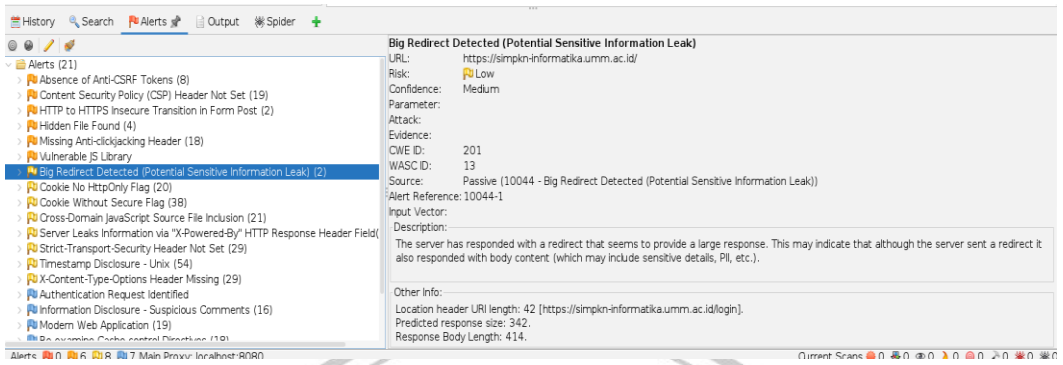
Lampiran 2 Bukti Scanning Keseluruhan Kerentanan Sedang

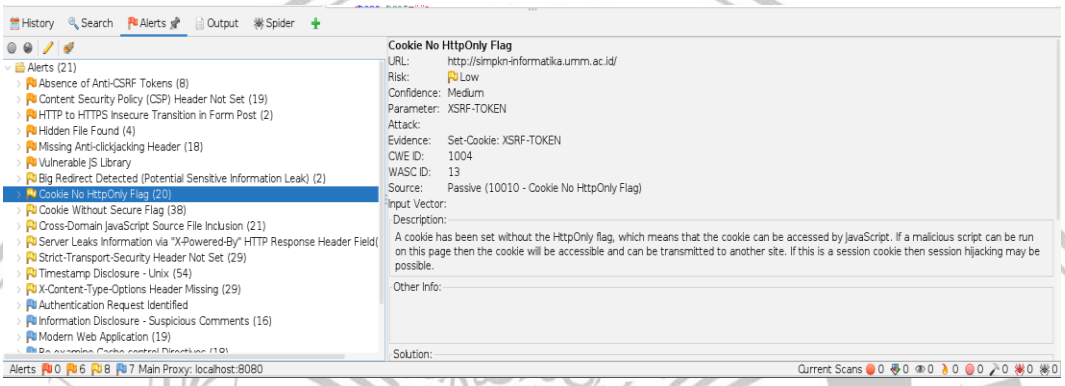


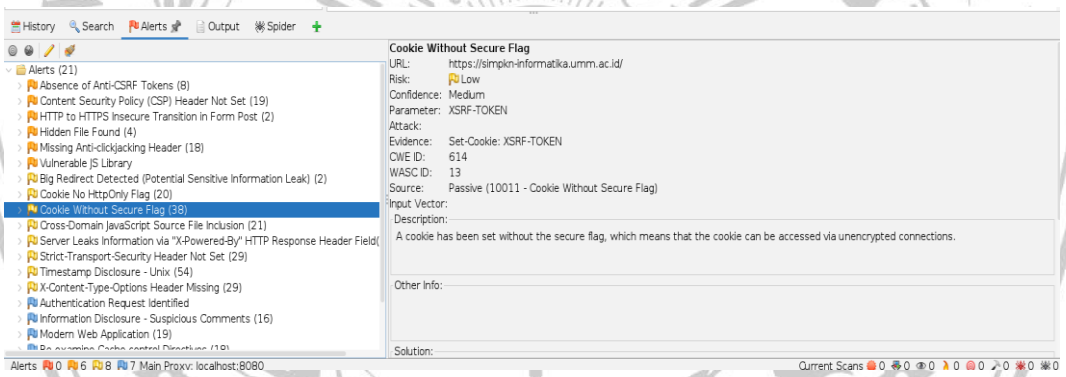

History
Search
Alerts
Output
Spider
Alerts (21)
Absence of Anti-CSRF Tokens (8)
Content Security Policy (CSP) Header Not Set (19)
HTTP to HTTPS Insecure Transition in Form Post (2)
Hidden File Found (4)
Missing Anti-clickjacking Header (18)
Vulnerable JS Library
Big Redirect Detected (Potential Sensitive Information Leak) (2)
Cookie No HttpOnly Flag (20)
Cookie Without Secure Flag (38)
Cross-Domain JavaScript Source File Inclusion (21)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(
Strict-Transport-Security Header Not Set (29)
Timestamp Disclosure - Unix (54)
X-Content-Type-Options Header Missing (29)
Authentication Request Identified
Information Disclosure - Suspicious Comments (16)
Modern Web Application (19)
Missing Anti-clickjacking Header
URL: http://simpkn-informatika.umm.ac.id/
Risk: Medium
Confidence: Medium
Parameter: x-frame-options
Attack:
Evidence:
CWE ID: 1021
WASC ID: 15
Source: Passive (10020 - Anti-clickjacking Header)
Alert Reference: 10020-1
Input Vector:
Description:
The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'Clickjacking' attacks.
Other Info:
Alerts 0 6 8 7 Main Proxy: localhost:8080
Current Scans 0 0 0 0 0 0 0 0

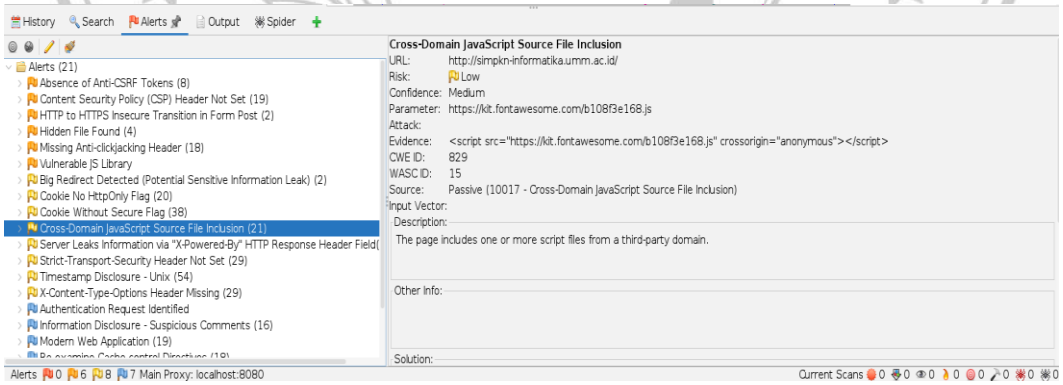

History
Search
Alerts
Output
Spider
Alerts (21)
Absence of Anti-CSRF Tokens (8)
Content Security Policy (CSP) Header Not Set (19)
HTTP to HTTPS Insecure Transition in Form Post (2)
Hidden File Found (4)
Missing Anti-clickjacking Header (18)
Vulnerable JS Library
Big Redirect Detected (Potential Sensitive Information Leak) (2)
Cookie No HttpOnly Flag (20)
Cookie Without Secure Flag (38)
Cross-Domain JavaScript Source File Inclusion (21)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(
Strict-Transport-Security Header Not Set (29)
Timestamp Disclosure - Unix (54)
X-Content-Type-Options Header Missing (29)
Authentication Request Identified
Information Disclosure - Suspicious Comments (16)
Modern Web Application (19)
Vulnerable JS Library
URL: https://simpkn-informatika.umm.ac.id/src/plugins/global/plugins.bundle.js
Risk: Medium
Confidence: Medium
Parameter:
Attack:
Evidence: .version="2.29.1",e=yt,n.fn=ln,n.min=function(){return _t("isBefore",[].slice.call(arguments,0))},n.max=function(){return _t("isAfter",[].slice.call(arguments,0))},n.now=function(){return Date.now?Date.now():+new Date},n.utc=hn,n.unix=function(e){return yt(1e3*e)},n.months=function(e,t){return hn(e,t,"months")},n.isDate=c,n.locale=Qe,n.invalid=m,n.duration=Yt,n.isMoment=
CWE ID: 829
WASC ID:
Source: Passive (10003 - Vulnerable JS Library (Powered by Retire.js))
Input Vector:
Description:
The identified library moment.js, version 2.29.1 is vulnerable.
Other Info:
CVE-2022-31129
CVE-2022-24785
Alerts 0 6 8 7 Main Proxy: localhost:8080
Current Scans 0 0 0 0 0 0 0 0

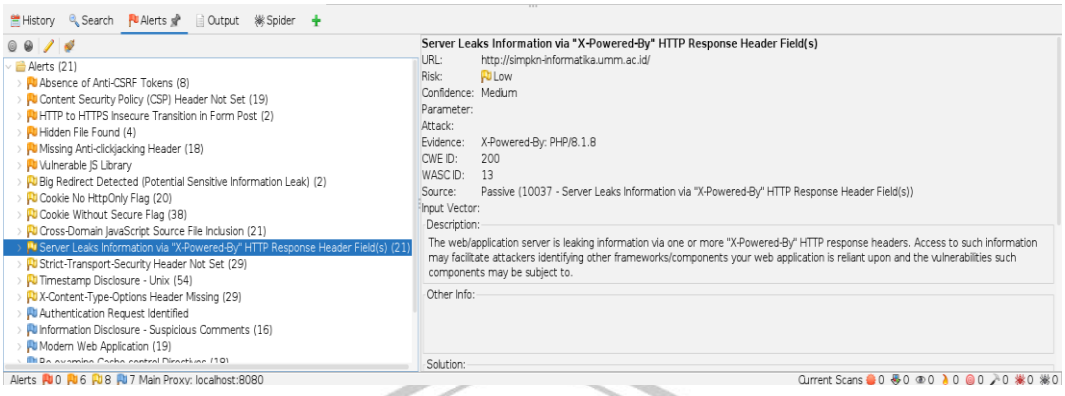
Lampiran 3 Bukti Scanning Keseluruhan Kerentanan Rendah

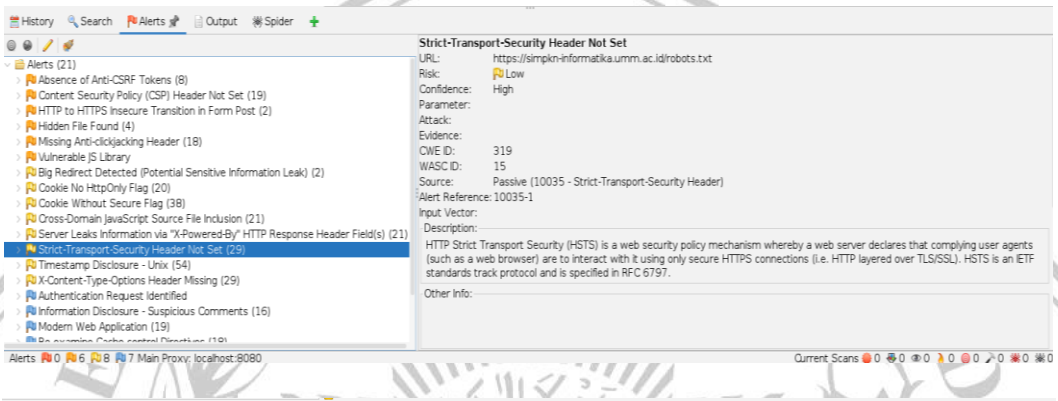


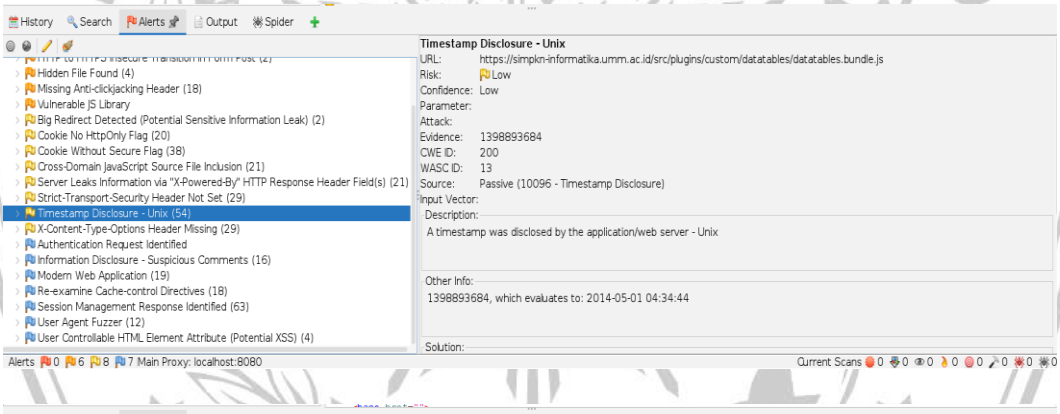


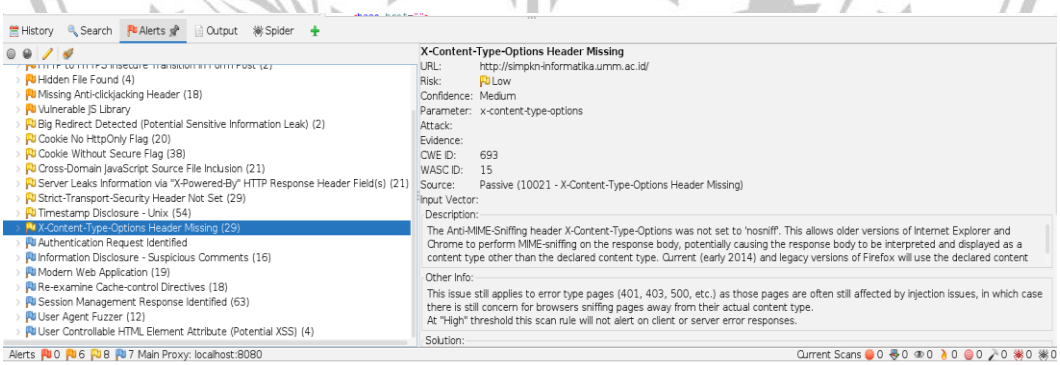





History
Search
Alerts
Output
Spider
Alerts (21)
Absence of Anti-CSRF Tokens (8)
Content Security Policy (CSP) Header Not Set (19)
HTTP to HTTPS Insecure Transition in Form Post (2)
Hidden File Found (4)
Missing Anti-clickjacking Header (18)
Vulnerable JS Library
Big Redirect Detected (Potential Sensitive Information Leak) (2)
Cookie No HttpOnly Flag (20)
Cookie Without Secure Flag (38)
Cross-Domain JavaScript Source File Inclusion (21)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) (21)
Strict-Transport-Security Header Not Set (29)
Timestamp Disclosure - Unix (54)
X-Content-Type-Options Header Missing (29)
Authentication Request Identified
Information Disclosure - Suspicious Comments (16)
Modern Web Application (19)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
URL: http://simpkn-informatika.umm.ac.id/
Risk: Low
Confidence: Medium
Parameter:
Attack:
Evidence: X-Powered-By: PHP/8.1.8
CWE ID: 200
WASC ID: 13
Source: Passive (10037 - Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s))
Input Vector:
Description:
The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.
Other Info:
Solution:
Alerts 0 6 8 7 Main Proxy: localhost:8080
Current Scans

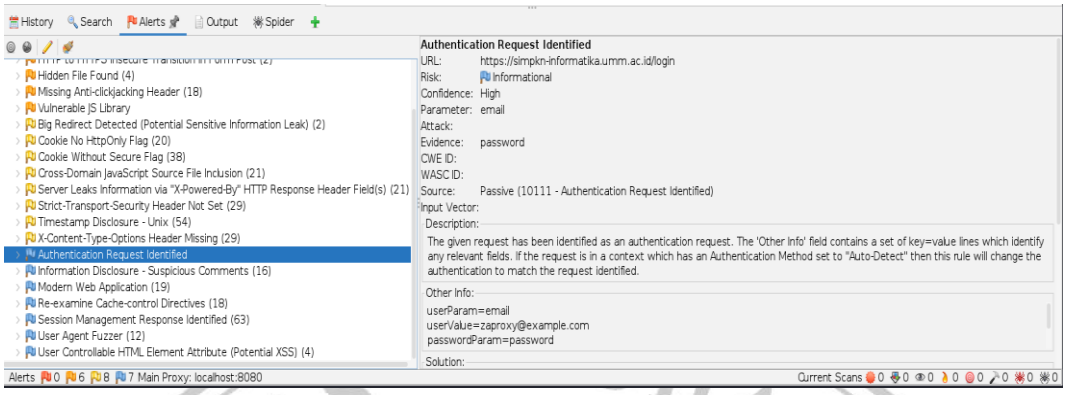

History
Search
Alerts
Output
Spider
Alerts (21)
Absence of Anti-CSRF Tokens (8)
Content Security Policy (CSP) Header Not Set (19)
HTTP to HTTPS Insecure Transition in Form Post (2)
Hidden File Found (4)
Missing Anti-clickjacking Header (18)
Vulnerable JS Library
Big Redirect Detected (Potential Sensitive Information Leak) (2)
Cookie No HttpOnly Flag (20)
Cookie Without Secure Flag (38)
Cross-Domain JavaScript Source File Inclusion (21)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) (21)
Strict-Transport-Security Header Not Set (29)
Timestamp Disclosure - Unix (54)
X-Content-Type-Options Header Missing (29)
Authentication Request Identified
Information Disclosure - Suspicious Comments (16)
Modern Web Application (19)
Strict-Transport-Security Header Not Set
URL: https://simpkn-informatika.umm.ac.id/robots.txt
Risk: Low
Confidence: High
Parameter:
Attack:
Evidence:
CWE ID: 319
WASC ID: 15
Source: Passive (10035 - Strict-Transport-Security Header)
Alert Reference: 10035-1
Input Vector:
Description:
HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
Other Info:
Alerts 0 6 8 7 Main Proxy: localhost:8080
Current Scans

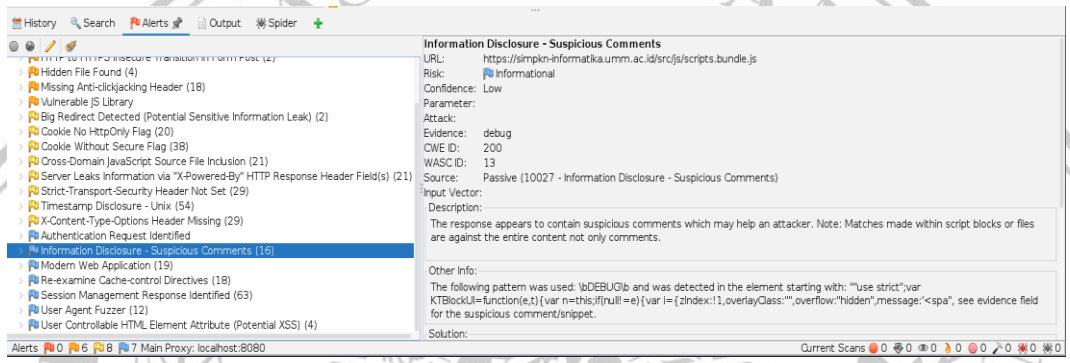

History
Search
Alerts
Output
Spider
Hidden File Found (4)
Missing Anti-clickjacking Header (18)
Vulnerable JS Library
Big Redirect Detected (Potential Sensitive Information Leak) (2)
Cookie No HttpOnly Flag (20)
Cookie Without Secure Flag (38)
Cross-Domain JavaScript Source File Inclusion (21)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) (21)
Strict-Transport-Security Header Not Set (29)
Timestamp Disclosure - Unix (54)
X-Content-Type-Options Header Missing (29)
Authentication Request Identified
Information Disclosure - Suspicious Comments (16)
Modern Web Application (19)
Re-examine Cache-control Directives (18)
Session Management Response Identified (63)
User Agent Fuzzer (12)
User Controllable HTML Element Attribute (Potential XSS) (4)
Timestamp Disclosure - Unix
URL: https://simpkn-informatika.umm.ac.id/src/plugins/custom/datatables/datatables.bundle.js
Risk: Low
Confidence: Low
Parameter:
Attack:
Evidence: 1398893684
CWE ID: 200
WASC ID: 13
Source: Passive (10096 - Timestamp Disclosure)
Input Vector:
Description:
A timestamp was disclosed by the application/web server - Unix
Other Info:
1398893684, which evaluates to: 2014-05-01 04:34:44
Solution:
Alerts 0 6 8 7 Main Proxy: localhost:8080
Current Scans

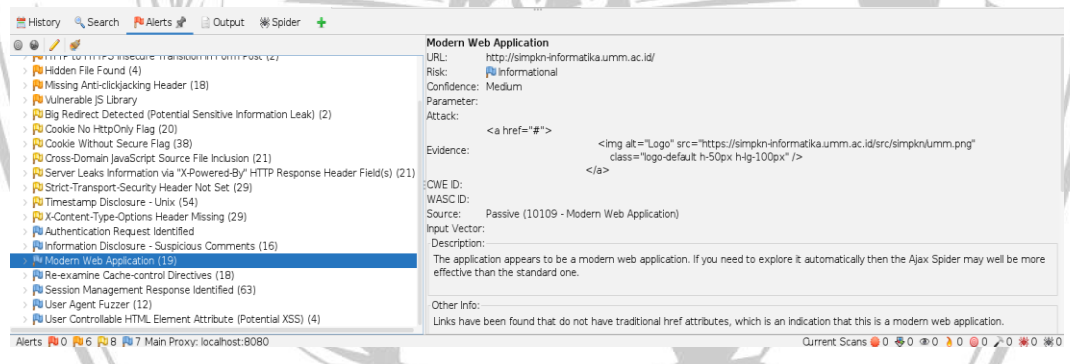

History
Search
Alerts
Output
Spider
Hidden File Found (4)
Missing Anti-clickjacking Header (18)
Vulnerable JS Library
Big Redirect Detected (Potential Sensitive Information Leak) (2)
Cookie No HttpOnly Flag (20)
Cookie Without Secure Flag (38)
Cross-Domain JavaScript Source File Inclusion (21)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) (21)
Strict-Transport-Security Header Not Set (29)
Timestamp Disclosure - Unix (54)
X-Content-Type-Options Header Missing (29)
Authentication Request Identified
Information Disclosure - Suspicious Comments (16)
Modern Web Application (19)
Re-examine Cache-control Directives (18)
Session Management Response Identified (63)
User Agent Fuzzer (12)
User Controllable HTML Element Attribute (Potential XSS) (4)
X-Content-Type-Options Header Missing
URL: http://simpkn-informatika.umm.ac.id/
Risk: Low
Confidence: Medium
Parameter: x-content-type-options
Attack:
Evidence:
CWE ID: 693
WASC ID: 15
Source: Passive (10021 - X-Content-Type-Options Header Missing)
Input Vector:
Description:
The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content
Other Info:
This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type.
At "High" threshold this scan rule will not alert on client or server error responses.
Solution:
Alerts 0 6 8 7 Main Proxy: localhost:8080
Current Scans

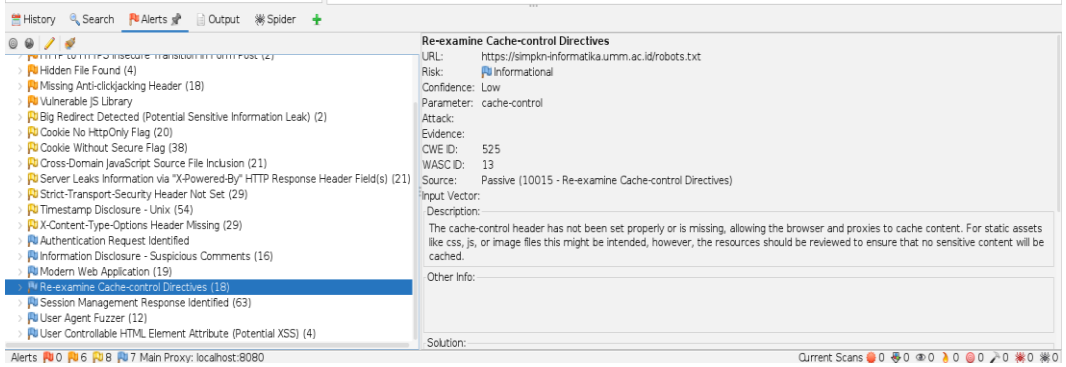
Lampiran 4 Bukti Scanning Keseluruhan Kerentanan

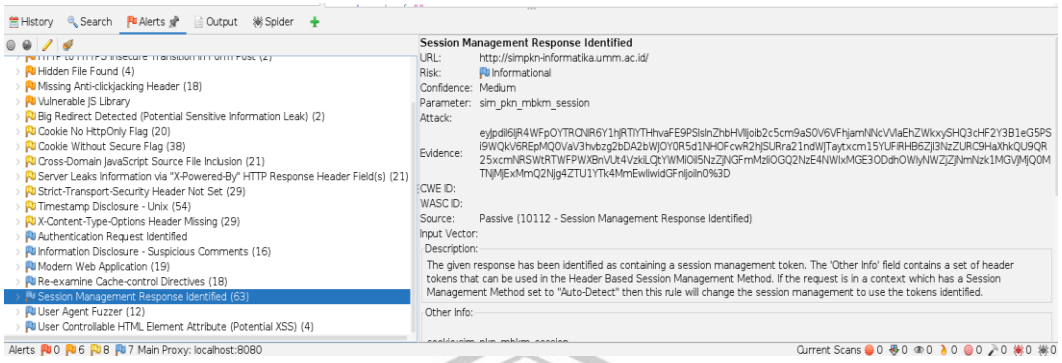
Tidak Berdampak (Informatif)

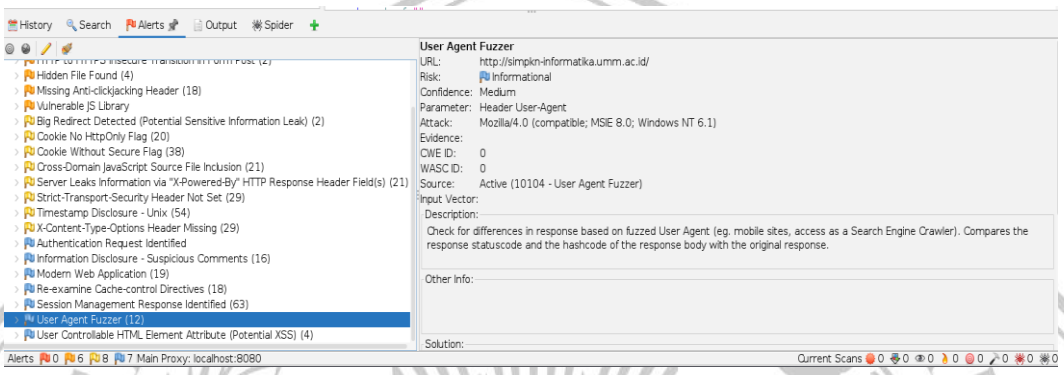


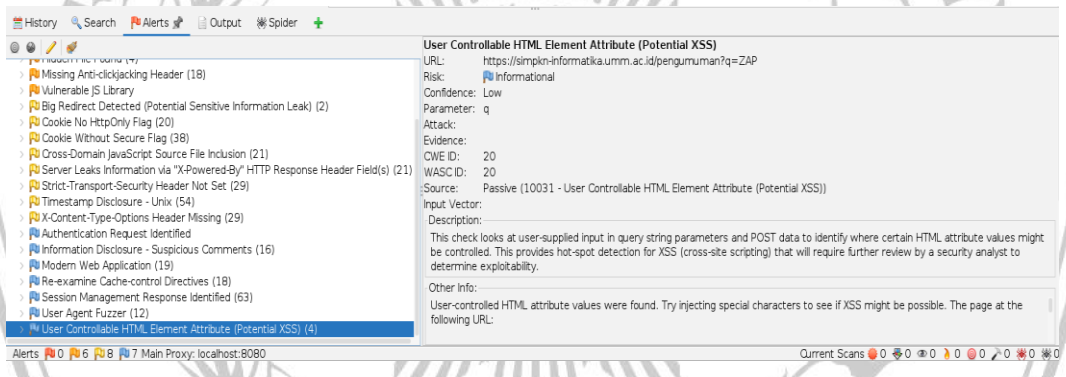







History
Search
Alerts
Output
Spider
Hidden File Found (4)
Missing Anti-clickjacking Header (18)
Vulnerable JS Library
Big Redirect Detected (Potential Sensitive Information Leak) (2)
Cookie No HttpOnly Flag (20)
Cookie Without Secure Flag (38)
Cross-Domain JavaScript Source File Inclusion (21)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) (21)
Strict-Transport-Security Header Not Set (29)
Timestamp Disclosure - Unix (54)
X-Content-Type-Options Header Missing (29)
Authentication Request Identified
Information Disclosure - Suspicious Comments (16)
Modern Web Application (19)
Re-examine Cache-control Directives (18)
Session Management Response Identified (63)
User Agent Fuzzer (12)
User Controllable HTML Element Attribute (Potential XSS) (4)
Session Management Response Identified
URL: http://simpkn-informatika.umm.ac.id/
Risk: Informational
Confidence: Medium
Parameter: sim_pkn_mbkm_session
Attack:
Evidence:
CWE ID:
WASC ID:
Source: Passive (10112 - Session Management Response Identified)
Input Vector:
Description:
The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
Other Info:
Alerts 0 6 8 7 Main Proxy: localhost:8080
Current Scans 0 0 0 0 0 0 0 0 0


History
Search
Alerts
Output
Spider
Hidden File Found (4)
Missing Anti-clickjacking Header (18)
Vulnerable JS Library
Big Redirect Detected (Potential Sensitive Information Leak) (2)
Cookie No HttpOnly Flag (20)
Cookie Without Secure Flag (38)
Cross-Domain JavaScript Source File Inclusion (21)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) (21)
Strict-Transport-Security Header Not Set (29)
Timestamp Disclosure - Unix (54)
X-Content-Type-Options Header Missing (29)
Authentication Request Identified
Information Disclosure - Suspicious Comments (16)
Modern Web Application (19)
Re-examine Cache-control Directives (18)
Session Management Response Identified (63)
User Agent Fuzzer (12)
User Controllable HTML Element Attribute (Potential XSS) (4)
User Agent Fuzzer
URL: http://simpkn-informatika.umm.ac.id/
Risk: Informational
Confidence: Medium
Parameter: Header User-Agent
Attack: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence:
CWE ID: 0
WASC ID: 0
Source: Active (10104 - User Agent Fuzzer)
Input Vector:
Description:
Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.
Other Info:
Solution:
Alerts 0 6 8 7 Main Proxy: localhost:8080
Current Scans 0 0 0 0 0 0 0 0 0


History
Search
Alerts
Output
Spider
Missing Anti-clickjacking Header (18)
Vulnerable JS Library
Big Redirect Detected (Potential Sensitive Information Leak) (2)
Cookie No HttpOnly Flag (20)
Cookie Without Secure Flag (38)
Cross-Domain JavaScript Source File Inclusion (21)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) (21)
Strict-Transport-Security Header Not Set (29)
Timestamp Disclosure - Unix (54)
X-Content-Type-Options Header Missing (29)
Authentication Request Identified
Information Disclosure - Suspicious Comments (16)
Modern Web Application (19)
Re-examine Cache-control Directives (18)
Session Management Response Identified (63)
User Agent Fuzzer (12)
User Controllable HTML Element Attribute (Potential XSS) (4)
User Controllable HTML Element Attribute (Potential XSS)
URL: https://simpkn-informatika.umm.ac.id/pengumuman?q=ZAP
Risk: Informational
Confidence: Low
Parameter: q
Attack:
Evidence:
CWE ID: 20
WASC ID: 20
Source: Passive (10031 - User Controllable HTML Element Attribute (Potential XSS))
Input Vector:
Description:
This check looks at user-supplied input in query string parameters and POST data to identify where certain HTML attribute values might be controlled. This provides hot-spot detection for XSS (cross-site scripting) that will require further review by a security analyst to determine exploitability.
Other Info:
User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:
Alerts 0 6 8 7 Main Proxy: localhost:8080
Current Scans 0 0 0 0 0 0 0 0 0

Lampiran 5 Bukti Uji Coba Pentesting Hasil Scanning Kerentanan