

LAMPIRAN

Lampiran 1 Surat Permohonan Data Tugas Akhir

**FAKULTAS TEKNIK**
ft.umm.ac.id | ftumm@umm.ac.id

Malang, 03 Januari 2024

UNIVERSITAS MUHAMMADIYAH MALANG
Nomor : E.S.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 SIM-PKN 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. Bencengan Sutani No.189 Malang, Jawa Timur
P : +62 341 551 140 (Hunting)
F : +62 341 582 980


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

CS Dipindai dengan CamScanner

Lampiran 2 Bukti Scanning Keseluruhan Kerentanan Sedang

Absence of Anti-CSRF Tokens

URL: <https://simpkn-informatika.umm.ac.id/pengumuman>

Risk: Medium

Confidence: Low

Parameter:

Attack:

Evidence: <form action="https://simpkn-informatika.umm.ac.id/pengumuman">

CWE ID: 352

WASC ID: 9

Source: Passive (10202 - Absence of Anti-CSRF Tokens)

Input Vector:

Description:

No Anti-CSRF tokens were found in a HTML submission form. A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form

Other Info:

No known Anti-CSRF token [anticrsrf, CSRFToken, _RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrfSecret, _csrf_magic, CSRF_token, csrf_token] was found in the following HTML form: [Form 1: "search"]

Solution:

Content Security Policy (CSP) Header Not Set

URL: <http://simpkn-informatika.umm.ac.id/>

Risk: Medium

Confidence: High

Parameter:

Attack:

Evidence:

CWE ID: 693

WASC ID: 15

Source: Passive (10038 - Content Security Policy (CSP) Header Not Set)

Alert Reference: 10038-1

Input Vector:

Description:

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers

Other Info:

HTTP to HTTPS Insecure Transition in Form Post

URL: <http://simpkn-informatika.umm.ac.id/>

Risk: Medium

Confidence: Medium

Parameter:

Attack:

Evidence: <https://simpkn-informatika.umm.ac.id/login>

CWE ID: 319

WASC ID: 15

Source: Passive (10041 - HTTP to HTTPS Insecure Transition in Form Post)

Input Vector:

Description:

This check looks for insecure HTTP pages that host HTTPS forms. The issue is that an insecure HTTP page can easily be hijacked through MITM and the secure HTTPS form can be replaced or spoofed.

Other Info:

The response to the following request over HTTP included an HTTPS form tag action attribute value:

<http://simpkn-informatika.umm.ac.id/The context was:>

Solution:

Hidden File Found

URL: <http://simpkn-informatika.umm.ac.id/hg>

Risk: Medium

Confidence: Low

Parameter:

Attack:

Evidence: HTTP/1.1 301 Moved Permanently

CWE ID: 538

WASC ID: 13

Source: Active (40035 - Hidden File Finder)

Input Vector:

Description:

A sensitive file was identified as accessible or available. This may leak administrative, configuration, or credential information which can be leveraged by a malicious individual to further attack the system or conduct social engineering efforts.

Other Info:

Solution:

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)
- Dynamic Content Control Directives (19)

Alerts 0 6 8 7 Main Proxy: localhost:8080

Current Scans 0 0 0 0 0 0 0 0 0 0

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:

History Search Alerts Output Spider

Alerts (21)

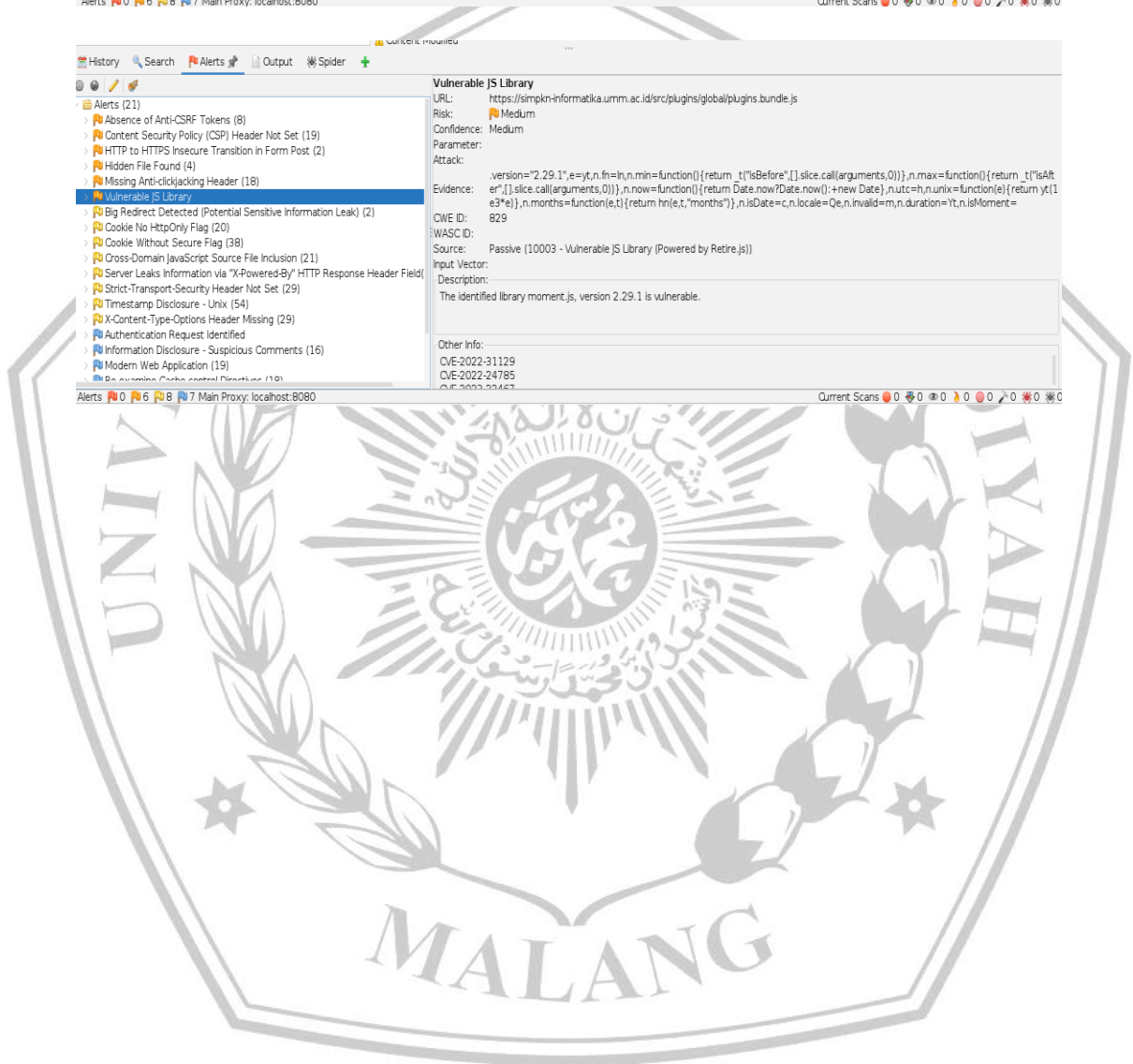
- Absence of Anti-CSRF Tokens (8)
- Content Security Policy (CSP) Header Not Set (19)
- HTTP to HTTPS Insecure Transition in Form Post (2)
- Hidden File Found (4)
- Missing Anti-clickjacking Header (18)
- Vulnerable JS Library**
- Big Redirect Detected (Potential Sensitive Information Leak) (2)
- Cookie 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)
- Dynamic Content Control Directives (19)

Alerts 0 6 8 7 Main Proxy: localhost:8080

Current Scans 0 0 0 0 0 0 0 0 0 0

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=y,n.fn=b,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=h,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=lt,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
 CVE-2022-32423



Lampiran 3 Bukti Scanning Keseluruhan Kerentanan Rendah

Big Redirect Detected (Potential Sensitive Information Leak)

URL: <https://simpkn-informatika.umm.ac.id/>
Risk: Low
Confidence: Medium
Parameter:
Attack:
Evidence:
CVE ID: 201
WASC ID: 13
Source: Passive (10044 - Big Redirect Detected (Potential Sensitive Information Leak))
Alert Reference: 10044-1
Input Vector:
Description:
The server has responded with a redirect that seems to provide a large response. This may indicate that although the server sent a redirect it also responded with body content. (which may include sensitive details, PII, etc.).
Other Info:
Location header URI length: 42 [<https://simpkn-informatika.umm.ac.id/login>].
Predicted response size: 342.
Response Body Length: 414.

Cookie No HttpOnly Flag

URL: <http://simpkn-informatika.umm.ac.id/>
Risk: Low
Confidence: Medium
Parameter: XSRF-TOKEN
Attack:
Evidence: Set-Cookie: XSRF-TOKEN
CVE ID: 1004
WASC ID: 13
Source: Passive (10010 - Cookie No HttpOnly Flag)
Input Vector:
Description:
A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
Other Info:
Solution:

Cookie Without Secure Flag

URL: <https://simpkn-informatika.umm.ac.id/>
Risk: Low
Confidence: Medium
Parameter: XSRF-TOKEN
Attack:
Evidence: Set-Cookie: XSRF-TOKEN
CVE ID: 614
WASC ID: 13
Source: Passive (10011 - Cookie Without Secure Flag)
Input Vector:
Description:
A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
Other Info:
Solution:

Cross-Domain JavaScript Source File Inclusion

URL: <http://simpkn-informatika.umm.ac.id/>
Risk: Low
Confidence: Medium
Parameter: <https://kit.fontawesome.com/b108f3e168.js>
Attack:
Evidence: `<script src="https://kit.fontawesome.com/b108f3e168.js" crossorigin="anonymous"></script>`
CVE ID: 829
WASC ID: 15
Source: Passive (10017 - Cross-Domain JavaScript Source File Inclusion)
Input Vector:
Description:
The page includes one or more script files from a third-party domain.
Other Info:
Solution:

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)
- Re-examine Cache-control Directives (18)

Alerts: 0 0 6 8 7 Main Proxy: localhost:8080 Current Scans: 0 0 0 0 0 0 0 0 0 0 0 0

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:

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)
- Re-examine Cache-control Directives (18)

Alerts: 0 0 6 8 7 Main Proxy: localhost:8080 Current Scans: 0 0 0 0 0 0 0 0 0 0 0 0

Strict-Transport-Security Header Not Set

URL: https://simpkn-informatika.umm.ac.id/robots.txt
 Risk: Low
 Confidence: High
 Parameter:
 Attack:
 Evidence: 319
 CWE ID: 15
 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:
 Solution:

History Search Alerts Output Spider +

Alerts (21)

- 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)
- Re-examine Cache-control Directives (18)
- Session Management Response Identified (63)
- User Agent Fuzzer (12)
- User Controllable HTML Element Attribute (Potential XSS) (4)

Alerts: 0 0 6 8 7 Main Proxy: localhost:8080 Current Scans: 0 0 0 0 0 0 0 0 0 0 0 0

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:

History Search Alerts Output Spider +

Alerts (21)

- 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)
- Re-examine Cache-control Directives (18)
- Session Management Response Identified (63)
- User Agent Fuzzer (12)
- User Controllable HTML Element Attribute (Potential XSS) (4)

Alerts: 0 0 6 8 7 Main Proxy: localhost:8080 Current Scans: 0 0 0 0 0 0 0 0 0 0 0 0

X-Content-Type-Options Header Missing

URL: http://simpkn-informatika.umm.ac.id/
 Risk: Low
 Confidence: Medium
 Parameter: x-content-type-options
 Attack:
 Evidence: 693
 CWE ID: 15
 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 type.
 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:

Lampiran 4 Bukti Scanning Keseluruhan Kerentanan Tidak Berdampak (Informatif)

This screenshot shows the Nessus interface with the 'Authentication Request Identified' rule selected in the left sidebar. The main pane displays the following details:

- URL:** https://simprk-informatika.umm.ac.id/login
- Risk:** Informational
- Confidence:** High
- Parameter:** email
- Attack:** Evidence: password
- CWE ID:** WASC ID:
- Source:** Passive (10111 - Authentication Request Identified)
- Input Vector:** Description: The given request has been identified as an authentication request. The 'Other Info' field contains a set of key=value lines which identify any relevant fields. If the request is in a context which has an Authentication Method set to "Auto-Detect" then this rule will change the authentication to match the request identified.
- Other Info:** userParam=email, userValue=zaproxy@example.com, passwordParam=password
- Solution:**

This screenshot shows the Nessus interface with the 'Information Disclosure - Suspicious Comments' rule selected. The main pane displays the following details:

- URL:** https://simprk-informatika.umm.ac.id/src/js/scripts.bundle.js
- Risk:** Informational
- Confidence:** Low
- Parameter:** Evidence: debug
- Attack:** CWE ID: 200
- Source:** Passive (10027 - Information Disclosure - Suspicious Comments)
- Input Vector:** Description: The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
- Other Info:** The following pattern was used: \bDEBUG\b and was detected in the element starting with: "Use strict";var KBlockUI=function(e,t){var n=this;if(n===e){var i=zindex;!1,overlayClass:"",overflow:"hidden",message:"<spa", see evidence field for the suspicious comment/snippet.
- Solution:**

This screenshot shows the Nessus interface with the 'Modern Web Application' rule selected. The main pane displays the following details:

- URL:** http://simprk-informatika.umm.ac.id/
- Risk:** Informational
- Confidence:** Medium
- Parameter:** Evidence:
- Attack:** CWE ID: WASC ID: 13
- Source:** Passive (10109 - Modern Web Application)
- Input Vector:** Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
- Other Info:** Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
- Solution:**

This screenshot shows the Nessus interface with the 'Re-examine Cache-control Directives' rule selected. The main pane displays the following details:

- URL:** https://simprk-informatika.umm.ac.id/robots.txt
- Risk:** Informational
- Confidence:** Low
- Parameter:** cache-control
- Attack:** Evidence: CWE ID: 525
- Source:** Passive (10015 - Re-examine Cache-control Directives)
- Input Vector:** Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
- Other Info:**
- Solution:**

History Search Alerts Output Spider

- HTTP 401 Unauthorized (17)
- 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: eyJpdjRjR4WFp0YTR0QWR6Y1hJRlYTHvafE9F5slszbHwJj0b2c5cm9a50v6VfHjamNkcVlaEhZwkoYSHQ3dHFY3B1eG5P5l9hWkQv6EaP4Q0v3v3h0z2D02vWj0Y0R5d1N4QFwZnSURa21ndWJTaycxcm15YUfFmH5Zj3NzZURC9HahaKQJ9QR25xcmLR5WRTWFPWBNvL4VzklQYWMQ0ISNzZjNGFmMz0GQ2NzE4NWwMGE3ODdhOWYwWZzZjNmNzk1MGVjMjQ0MTRjMExmMmQ2Ng4ZTU1YTk4MmEwIiwidGFmJ0ln093D

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 0

History Search Alerts Output Spider

- HTTP 401 Unauthorized (17)
- 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 0

History Search Alerts Output Spider

- HTTP 401 Unauthorized (17)
- 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 0



Lampiran 5 Bukti Uji Coba Pentesting Hasil Scanning Kerentanan

