Penetration Testing Report

Keamanan Informasi e-Government
Teknologi Informasi dan Komunikasi
Dinas Komunikasi Informatika dan Persandian Aceh

2022

Detail Dokumen

Laporan PenTest	**:**	**https://kumkm.latih.id**			
Tanggal PenTest	:	24/05/2022, 12:41:19			
Instansi	:	E-Gov			
Klasifikasi	:	Publik	Internal	Rahasia	Sangat Rahasia

Penanggung Jawab PenTest

Nama	Jabatan	Instansi
Bustamam, S.Kom. MM	Kasi Keamanan Informasi E-government	Diskominfo&sandi Aceh

PetugasPenTest

Nama	Jabatan	Instansi
Elvisyahr, A.Md	Staf Seksi Keamanan Informasi E-government	Diskominfo&sandi Aceh
Fakhrurrazi, ST	Staf Seksi Keamanan Informasi E-government	Diskominfo&sandi Aceh
Muhammad Rizki Juanda, S.T	Pentester	Diskominfo&sandi Aceh

Penanggung Jawab Aplikasi

Nama	Jabatan	No. Telepon/Hp	Instansi
Muhammad Ichsan	-	085277931161	E-Gov
Yudi Kasmara, S.Kom, M.Cs	Kepala Bidang Layanan E-Government Sub Koordinator Pengembangan Aplikasi	085277823123	E-Gov

Server information

Website/Aplication information

Web frameworks

Laravel

Web servers

Nginx

Programming languages

PHP 7.4.24

CDN

Cloudflare

Unpkg

jsDelivr

cdnjs

JavaScript libraries

core-js 3.1.3

OWL Carousel

jQuery 3.6.0

DataTables 1.11.4

Reverse proxies

Nginx

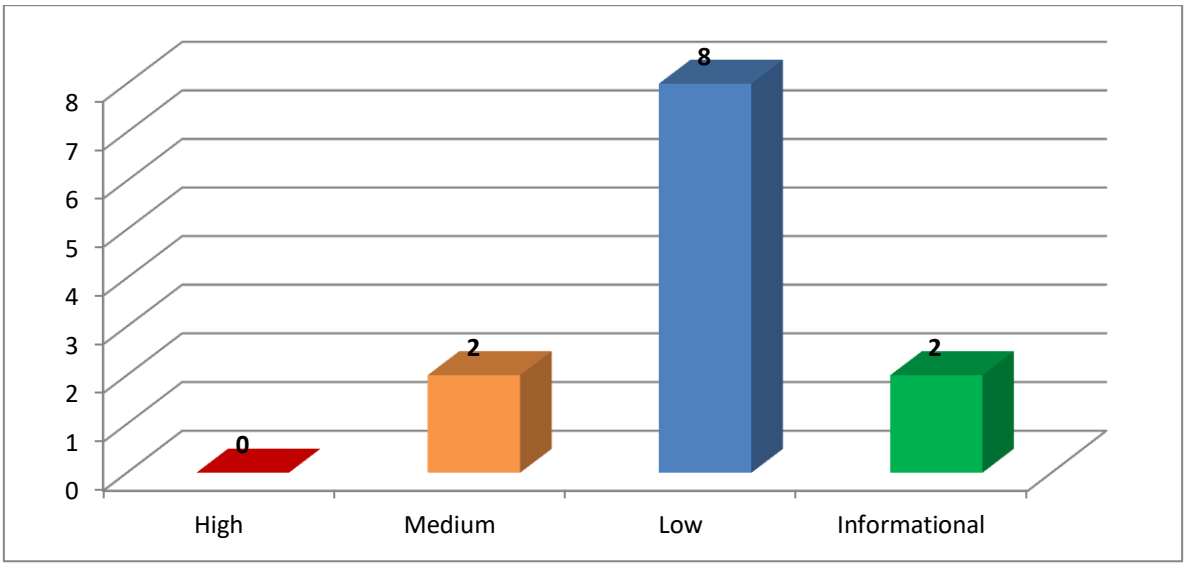
UI frameworks

Bootstrap

Ringkasan Grafik

Grafik Informasi Risiko

Total alerts found	12
High	0
Medium	2
Low	8
Informational	2



Alert group	Severity	Alert count
.htaccess file readable	Medium	1
Password field submitted using GET method	Medium	1
Possible sensitive files	Low	3
Possible sensitive directories	Low	2
Clickjacking: X-Frame-Options header missing	Low	1
Cookie(s) without HttpOnly flag set	Low	1
Cookie(s) without Secure flag set	Low	1

Alerts summary

.htaccess file readable

Classification	
CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16

Affected items	Variation
Web Server	1

Password field submitted using GET method

Classification	
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200

Affected items	Variation
/login	1

Clickjacking: X-Frame-Options header missing

Classification	
	Base Score: 6.8 Access Vector: Network_accessible Access Complexity: Medium Authentication: None Confidentiality Impact: Partial

CVSS2	Integrity Impact: Partial Availability Impact: Partial Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-693

Affected items	Variation
Web Server	1

Cookie(s) without HttpOnly flag set

Classification	
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16

Affected items	Variation
Web Server	1

Cookie(s) without Secure flag set

Classification	
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16

Affected items	Variation
Web Server	1

Possible sensitive directories

Classification	
	Base Score: 5.0

CVSS2	Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200

Affected items	Variation
/assets/css/users	1
/assets/js/users	1

Possible sensitive files

Classification	
CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200

Affected items	Variation
/.htaccess	1
/storage/.gitignore	1
/web.config	1

Email address found

Classification	
CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200

Affected items	Variation
Web Server	1

Password type input with auto-complete enabled

Classification	
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200

Affected items	Variation
/login	1

Alerts details

.htaccess file readable

Severity	**Medium**
Reported by module	Scripting (htaccess_File_Readable.script)

Description

This directory contains an **.htaccess** file that is readable. This may indicate a server misconfiguration. htaccess files are designed to be parsed by web server and should not be directly accessible. These files could contain sensitive information that could help an attacker to conduct further attacks. It's recommended to restrict access to this file.

Impact

Possible sensitive information disclosure.

Recommendation

Restrict access to the .htaccess file by adjusting the web server configuration.

Affected items

Web Server
Details
Request headers

```
GET /.htaccess HTTP/1.1
Cookie: XSRF-
TOKEN=eyJpdiI6Ikd3bEVGVEFsZ1NSSXI3TmtxblU5eXc9PSIsInZhbHVlIjoieGRkZ2dJZGoyVVV1N01Hb1orUngyQ3
hCOVRzT0ZlUndqWThlTjdycXpHNExVL1lYTGljSGZGVjRKd0ljU3A2QjRZbVMvYU1OTHZibk9DM3FNa0k1Y1NWWGsyTG
J5VWhyVmxCRXpmWWJUcmRzSjFjbW9vVXJpRW1wQTdsNVVQMkUiLCJtYWMiOiJlODI2ZGFjZGRkYWU5ZTg4MGZkYzZkNj
Y4OWZiOWVkMWFjYmE0ZjIyNGQ2ZDY5NThiNDkwZjg3NGE0OTkzZDY0IiwidGFnIjoiIn0%3D;
laravel_session=1UkuxvpDax86o2UJLJbc19ogXT3rWgJ44JxRETmN
Host: kumkm.latih.id
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

Password field submitted using GET method

Severity	**Medium**
Reported by module	Crawler

Description

This page contains a form with a password field. This form submits user data using the GET method, therefore the contents of the password field will appear in the URL.Sensitive information should not be passed via the URL. URLs could be logged or leaked via the Referer header.

Impact

Possible sensitive information disclosure.

Recommendation

The password field should be submitted through POST instead of GET.

Affected items

/login
Details
form name: "<unnamed>" form action: "javascript:void(0);" password input: "password"
Request headers
GET /login HTTP/1.1 Pragma: no-cache Cache-Control: no-cache Referer: https://kumkm.latih.id/ Cookie: XSRF-TOKEN=eyJpdiI6Ilh2N254UXJObkdPTDFXTXRIb2lkdUE9PSIsInZhbHVlIjoiY1dDaEo3UmZwQ0hGYk5nUlNLVHFuUlhrUS9OOTBVenhsbGkvcGdvUXE1RnRld2N2Uk5Rb3J2cTMzWkVVNTYySGJrZ0dDTTZtcnpIRm5LV2tpNGxISDY2b29hdzc4Wi9NUGlOOU51SzZQRFZXSGlQNDZlV09Ra0cyTThYdUhORUkiLCJtYWMiOiJhN2NjMTI2MGYxN2RhZTMyMzEzOThlMzM1NDllOWY5OTY2ZDlmZTc0YzRiYjBiZmI5MGRiZDAxODYwZDkxYzMxIiwidGFnIjoiIn0%3D; laravel_session=NkKgZX4jJgkzUFyxKjgtpMFxxeknvPneg7suCmg7 Host: kumkm.latih.id Connection: Keep-alive Accept-Encoding: gzip,deflate User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21 Accept: */*

Clickjacking: X-Frame-Options header missing

Severity	**Low**
Reported by module	Scripting (Clickjacking_X_Frame_Options.script)

Description

Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.

The server didn't return an **X-Frame-Options** header which means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites.

Impact

The impact depends on the affected web application.

Recommendation

Configure your web server to include an X-Frame-Options header. Consult Web references for more information about the possible values for this header.

References

The X-Frame-Options response header (https://developer.mozilla.org/en-US/docs/HTTP/X-Frame-Options)
Clickjacking (http://en.wikipedia.org/wiki/Clickjacking)
OWASP Clickjacking (https://www.owasp.org/index.php/Clickjacking)
Defending with Content Security Policy frame-ancestors directive (https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet#Defending_with_Content_Security_Policy_frame-ancestors_directive)
Frame Buster Buster (http://stackoverflow.com/questions/958997/frame-buster-buster-buster-code-needed)

Affected items

Web Server
Details

Request headers

```
GET / HTTP/1.1
Cookie: XSRF-
TOKEN=eyJpdiI6IkJ1SGNIMWpoYkxmQUN0R1JERElTNlE9PSIsInZhbHVlIjoiL0V5UTJUWkhkKzV4eWRYN0pISzNmTV
hzVCs1bndnQ0Z6L0NxNENoKzNpYk1PT1Qrd3NXNzViem5mYVJiVWVqQWVxTHc5ejBjN25kdDdiZkMyZ2cvWlFMTUFGcU
tYZitHQ0ZHaE9yK3liV0lEWC9PT3pWU29uRHBGNTFLbC9hU3UiLCJtYWMiOiI5OTgzZmJjNDQ4MjM1NTM4Y2I3NzE3ZD
MzOWY0OGRlMGVjZTRhODc3M2U3MDkwOTkyOTFkOTA5MDBiZjIzZDJkIiwidGFnIjoiIn0%3D;
laravel_session=NkKgZX4jJgkzUFyxKjgtpMFxxeknvPneg7suCmg7
Host: kumkm.latih.id
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

Cookie(s) without HttpOnly flag set

Severity	**Low**
Reported by module	Crawler

Description

This cookie does not have the HTTPOnly flag set. When a cookie is set with the HTTPOnly flag, it instructs the browser that the cookie can only be accessed by the server and not by client-side scripts. This is an important security protection for session cookies.

Impact

None

Recommendation

If possible, you should set the HTTPOnly flag for this cookie.

Affected items

Web Server
Details
Cookies found: • Name: XSRF-TOKEN, Domain: kumkm.latih.id
Request headers

```
GET / HTTP/1.1
Cookie: XSRF-
TOKEN=eyJpdiI6IkJ1SGNIMWpoYkxmQUN0R1JERElTNlE9PSIsInZhbHVlIjoiL0V5UTJUWkhkKzV4eWRYN0pISzNmTV
hzVCs1bndnQ0Z6L0NxNENoKzNpYk1PT1Qrd3NXNzViem5mYVJiVWVqQWVxTHc5ejBjN25kdDdiZkMyZ2cvWlFMTUFGcU
tYZitHQ0ZHaE9yK3liV0lEWC9PT3pWU29uRHBGNTFLbC9hU3UiLCJtYWMiOiI5OTgzZmJjNDQ4MjM1NTM4Y2I3NzE3ZD
MzOWY0OGRlMGVjZTRhODc3M2U3MDkwOTkyOTFkOTA5MDBiZjIzZDJkIiwidGFnIjoiIn0%3D;
laravel_session=NkKgZX4jJgkzUFyxKjgtpMFxxeknvPneg7suCmg7
Host: kumkm.latih.id
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

Cookie(s) without Secure flag set

Severity	**Low**
Reported by module	Crawler

Description

This cookie does not have the Secure flag set. When a cookie is set with the Secure flag, it instructs the browser that the cookie can only be accessed over secure SSL channels. This is an important security protection for session cookies.

Impact

None

Recommendation

If possible, you should set the Secure flag for this cookie.

Affected items

Web Server
Details
Cookies found: • Name: XSRF-TOKEN, Domain: kumkm.latih.id • Name: laravel_session, Domain: kumkm.latih.id
Request headers
GET / HTTP/1.1 Cookie: XSRF-TOKEN=eyJpdiI6IkJ1SGNIMWpoYkxmQUN0R1JERElTNlE9PSIsInZhbHVlIjoiL0V5UTJUWkhkKzV4eWRYN0pISzNmTVhzVCs1bndnQ0Z6L0NxNENoKzNpYk1PT1Qrd3NXNzViem5mYVJiVWVqQWVxTHc5ejBjN25kdDdiZkMyZ2cvWlFMTUFGcUtYZitHQ0ZHaE9yK3liV0lEWC9PT3pWU29uRHBGNTFLbC9hU3UiLCJtYWMiOiI5OTgzZmJjNDQ4MjM1NTM4Y2I3NzE3ZDMzOWY0OGRlMGVjZTRhODc3M2U3MDkwOTkyOTFkOTA5MDBiZjIzZDJkIiwidGFnIjoiIn0%3D; laravel_session=NkKgZX4jJgkzUFyxKjgtpMFxxeknvPneg7suCmg7 Host: kumkm.latih.id Connection: Keep-alive Accept-Encoding: gzip,deflate User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21 Accept: */*

Possible sensitive directories

Severity	**Low**
Reported by module	Scripting (Possible_Sensitive_Directories.script)

Description

A possible sensitive directory has been found. This directory is not directly linked from the website.This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

Impact

This directory may expose sensitive information that could help a malicious user to prepare more advanced attacks.

Recommendation

Restrict access to this directory or remove it from the website.

References

Web Server Security and Database Server Security (http://www.acunetix.com/websitesecurity/webserver-security/)

Affected items

/assets/css/users

Details

Request headers

```
GET /assets/css/users HTTP/1.1
Accept: acunetix/wvs
Range: bytes=0-99999
Cookie: XSRF-
TOKEN=eyJpdiI6Ikd3bEVGVEFsZ1NSSXI3TmtxblU5eXc9PSIsInZhbHVlIjoieGRkZ2dJZGoyVVV1N01Hb1orUngyQ3
hCOVRzT0ZlUndqWThlTjdycXpHNExVL1lYTGljSGZGVjRKd0ljU3A2QjRZbVMvYU1OTHZibk9DM3FNa0k1Y1NWWGsyTG
J5VWhyVmxCRXpmWWJUcmRzSjFjbW9vVXJpRW1wQTdsNVVQMkUiLCJtYWMiOiJlODI2ZGFjZGRkYWU5ZTg4MGZkYzZkNj
Y4OWZiOWVkMWFjYmE0ZjIyNGQ2ZDY5NThiNDkwZjg3NGE0OTkzZDY0IiwidGFnIjoiIn0%3D;
laravel_session=1UkuxvpDax86o2UJLJbc19ogXT3rWgJ44JxRETmN
Host: kumkm.latih.id
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
```

/assets/js/users

Details

Request headers

```
GET /assets/js/users HTTP/1.1
Accept: acunetix/wvs
Range: bytes=0-99999
Cookie: XSRF-
TOKEN=eyJpdiI6Ikd3bEVGVEFsZ1NSSXI3TmtxblU5eXc9PSIsInZhbHVlIjoieGRkZ2dJZGoyVVV1N01Hb1orUngyQ3
hCOVRzT0ZlUndqWThlTjdycXpHNExVL1lYTGljSGZGVjRKd0ljU3A2QjRZbVMvYU1OTHZibk9DM3FNa0k1Y1NWWGsyTG
J5VWhyVmxCRXpmWWJUcmRzSjFjbW9vVXJpRW1wQTdsNVVQMkUiLCJtYWMiOiJlODI2ZGFjZGRkYWU5ZTg4MGZkYzZkNj
Y4OWZiOWVkMWFjYmE0ZjIyNGQ2ZDY5NThiNDkwZjg3NGE0OTkzZDY0IiwidGFnIjoiIn0%3D;
laravel_session=1UkuxvpDax86o2UJLJbc19ogXT3rWgJ44JxRETmN
Host: kumkm.latih.id
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
```

Possible sensitive files

Severity	**Low**
Reported by module	Scripting (Possible_Sensitive_Files.script)

Description

A possible sensitive file has been found. This file is not directly linked from the website. This check looks for common sensitive resources like password files, configuration files, log files, include files, statistics data, database dumps. Each one of these files could help an attacker to learn more about his target.

Impact

This file may expose sensitive information that could help a malicious user to prepare more advanced attacks.

Recommendation

Restrict access to this file or remove it from the website.

References

Web Server Security and Database Server Security (http://www.acunetix.com/websitesecurity/webserver-security/)

Affected items

/.htaccess

Details

Request headers

```
GET /.htaccess HTTP/1.1
Accept: acunetix/wvs
Cookie: XSRF-
TOKEN=eyJpdiI6Ikd3bEVGVEFsZ1NSSXI3TmtxblU5eXc9PSIsInZhbHVlIjoieGRkZ2dJZGoyVVV1N01Hb1orUngyQ3
hCOVRzT0ZlUndqWThlTjdycXpHNExVL1lYTGljSGZGVjRKd0ljU3A2QjRZbVMvYU1OTHZibk9DM3FNa0k1Y1NWWGsyTG
J5VWhyVmxCRXpmWWJUcmRzSjFjbW9vVXJpRW1wQTdsNVVQMkUiLCJtYWMiOiJlODI2ZGFjZGRkYWU5ZTg4MGZkYzZkNj
Y4OWZiOWVkMWFjYmE0ZjIyNGQ2ZDY5NThiNDkwZjg3NGE0OTkzZDY0IiwidGFnIjoiIn0%3D;
laravel_session=1UkuxvpDax86o2UJLJbc19ogXT3rWgJ44JxRETmN
Host: kumkm.latih.id
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
```

/web.config

Details

Request headers

```
GET /web.config HTTP/1.1
Accept: acunetix/wvs
Cookie: XSRF-
TOKEN=eyJpdiI6Ikd3bEVGVEFsZ1NSSXI3TmtxblU5eXc9PSIsInZhbHVlIjoieGRkZ2dJZGoyVVV1N01Hb1orUngyQ3
hCOVRzT0ZlUndqWThlTjdycXpHNExVL1lYTGljSGZGVjRKd0ljU3A2QjRZbVMvYU1OTHZibk9DM3FNa0k1Y1NWWGsyTG
J5VWhyVmxCRXpmWWJUcmRzSjFjbW9vVXJpRW1wQTdsNVVQMkUiLCJtYWMiOiJlODI2ZGFjZGRkYWU5ZTg4MGZkYzZkNj
Y4OWZiOWVkMWFjYmE0ZjIyNGQ2ZDY5NThiNDkwZjg3NGE0OTkzZDY0IiwidGFnIjoiIn0%3D;
laravel_session=1UkuxvpDax86o2UJLJbc19ogXT3rWgJ44JxRETmN
Host: kumkm.latih.id
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
```

/storage/.gitignore

Details

Request headers

```
GET /storage/.gitignore HTTP/1.1
Accept: acunetix/wvs
Cookie: XSRF-
TOKEN=eyJpdiI6Ikd3bEVGVEFsZ1NSSXI3TmtxblU5eXc9PSIsInZhbHVlIjoieGRkZ2dJZGoyVVV1N01Hb1orUngyQ3
hCOVRzT0ZlUndqWThlTjdycXpHNExVL1lYTGljSGZGVjRKd0ljU3A2QjRZbVMvYU1OTHZibk9DM3FNa0k1Y1NWWGsyTG
J5VWhyVmxCRXpmWWJUcmRzSjFjbW9vVXJpRW1wQTdsNVVQMkUiLCJtYWMiOiJlODI2ZGFjZGRkYWU5ZTg4MGZkYzZkNj
Y4OWZiOWVkMWFjYmE0ZjIyNGQ2ZDY5NThiNDkwZjg3NGE0OTkzZDY0IiwidGFnIjoiIn0%3D;
laravel_session=1UkuxvpDax86o2UJLJbc19ogXT3rWgJ44JxRETmN
Host: kumkm.latih.id
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
```

Email address found

Severity	**Informational**
Reported by module	Scanner

Description

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

Impact

Email addresses posted on Web sites may attract spam.

Recommendation

Check references for details on how to solve this problem.

References

Anti-spam techniques (https://en.wikipedia.org/wiki/Anti-spam_techniques)

Affected items

Web Server
Details
List of all email addresses found on this host. • **feather-icons@4.28.0** / • **ionicons@5.5.2** /
Request headers

Password type input with auto-complete enabled

Severity	**Informational**
Reported by module	Crawler

Description

When a new name and password is entered in a form and the form is submitted, the browser asks if the password should be saved.Thereafter when the form is displayed, the name and password are filled in automatically or are completed as the name is entered. An attacker with local access could obtain the cleartext password from the browser cache.

Impact

Possible sensitive information disclosure.

Recommendation

The password auto-complete should be disabled in sensitive applications.
To disable auto-complete, you may use a code similar to:

```
<INPUT TYPE="password" AUTOCOMPLETE="off">
```

Affected items

/login
Details
Password type input(s): **password** from form with ID **form** with action **javascript:void(0);** have autocomplete enabled.
Request headers

```
GET /login HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: https://kumkm.latih.id/
Cookie: XSRF-
TOKEN=eyJpdiI6Ilh2N254UXJObkdPTDFXTXRIb2lkdUE9PSIsInZhbHVlIjoiY1dDaEo3UmZwQ0hGYk5nUlNLVHFuUl
hrUS9OOTBVenhsbGkvcGdvUXE1RnRld2N2Uk5Rb3J2cTMzWkVVNTYySGJrZ0dDTTZtcnpIRm5LV2tpNGxISDY2b29hdz
```

```
c4Wi9NUGlOOU51SzZQRFZXSGlQNDZlV09Ra0cyTThYdUhORUkiLCJtYWMiOiJhN2NjMTI2MGYxN2RhZTMyMzEzOThlMz
M1NDllOWY5OTY2ZDlmZTc0YzRiYjBiZmI5MGRiZDAxODYwZDkxYzMxIiwidGFnIjoiIn0%3D;
laravel_session=NkKgZX4jJgkzUFyxKjgtpMFxxeknvPneg7suCmg7
Host: kumkm.latih.id
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

Scanned items (coverage report)

https://kumkm.latih.id/
https://kumkm.latih.id/.htaccess
https://kumkm.latih.id/assets
https://kumkm.latih.id/assets/css
https://kumkm.latih.id/assets/css/apps
https://kumkm.latih.id/assets/css/authentication
https://kumkm.latih.id/assets/css/authentication/form-2.css
https://kumkm.latih.id/assets/css/custom.css
https://kumkm.latih.id/assets/css/elements
https://kumkm.latih.id/assets/css/elements/alert.css
https://kumkm.latih.id/assets/css/forms
https://kumkm.latih.id/assets/css/forms/switches.css
https://kumkm.latih.id/assets/css/main.css
https://kumkm.latih.id/assets/css/plugins.css
https://kumkm.latih.id/assets/css/structure.css
https://kumkm.latih.id/assets/css/users
https://kumkm.latih.id/assets/data
https://kumkm.latih.id/assets/images
https://kumkm.latih.id/assets/img
https://kumkm.latih.id/assets/js
https://kumkm.latih.id/assets/js/apps
https://kumkm.latih.id/assets/js/authentication
https://kumkm.latih.id/assets/js/authentication/form-2.js
https://kumkm.latih.id/assets/js/forms
https://kumkm.latih.id/assets/js/libs
https://kumkm.latih.id/assets/js/libs/jquery-3.1.1.min.js
https://kumkm.latih.id/assets/js/sweetalert.min.js
https://kumkm.latih.id/assets/js/users
https://kumkm.latih.id/bootstrap
https://kumkm.latih.id/bootstrap/css
https://kumkm.latih.id/bootstrap/css/bootstrap.min.css
https://kumkm.latih.id/bootstrap/js
https://kumkm.latih.id/bootstrap/js/bootstrap.min.js
https://kumkm.latih.id/bootstrap/js/popper.min.js
https://kumkm.latih.id/favicon.ico
https://kumkm.latih.id/forgot-password
https://kumkm.latih.id/index.php
https://kumkm.latih.id/index.php/assets
https://kumkm.latih.id/index.php/assets/images
https://kumkm.latih.id/index.php/forgot-password
https://kumkm.latih.id/index.php/login
https://kumkm.latih.id/index.php/storage
https://kumkm.latih.id/index.php/storage/produk
https://kumkm.latih.id/landing
https://kumkm.latih.id/landing/custom
https://kumkm.latih.id/landing/custom/base.js
https://kumkm.latih.id/landing/custom/custom.min.css
https://kumkm.latih.id/landing/dist
https://kumkm.latih.id/landing/dist/css
https://kumkm.latih.id/landing/dist/css/bootstrap.min.css
https://kumkm.latih.id/landing/dist/images
https://kumkm.latih.id/landing/dist/js
https://kumkm.latih.id/landing/dist/js/bootstrap.bundle.min.js
https://kumkm.latih.id/landing/plugin
https://kumkm.latih.id/landing/plugin/owlcarousel
https://kumkm.latih.id/landing/plugin/owlcarousel/dist
https://kumkm.latih.id/landing/plugin/owlcarousel/dist/assets
https://kumkm.latih.id/landing/plugin/owlcarousel/dist/assets/owl.carousel.min.css
https://kumkm.latih.id/landing/plugin/owlcarousel/dist/assets/owl.theme.default.min.css
https://kumkm.latih.id/landing/plugin/owlcarousel/dist/owl.carousel.min.js
https://kumkm.latih.id/login
https://kumkm.latih.id/news
https://kumkm.latih.id/plugins
https://kumkm.latih.id/plugins/highlight
https://kumkm.latih.id/plugins/highlight/styles
https://kumkm.latih.id/plugins/highlight/styles/monokai-sublime.css
https://kumkm.latih.id/plugins/perfect-scrollbar

https://kumkm.latih.id/plugins/perfect-scrollbar/perfect-scrollbar.css
https://kumkm.latih.id/robots.txt
https://kumkm.latih.id/storage
https://kumkm.latih.id/storage/.gitignore
https://kumkm.latih.id/storage/img
https://kumkm.latih.id/storage/produk
https://kumkm.latih.id/web.config