

Quick Report

Acunetix Security Audit

2023-02-20

Scan of acunetix.eramba.org

Scan details




| | |
|--------------------|----------------------------------|
| Scan information | |
| Start time | 2023-01-16T13:05:21.166590+00:00 |
| Start url | https://acunetix.eramba.org/ |
| Host | acunetix.eramba.org |
| Scan time | 127 minutes, 7 seconds |
| Profile | Full Scan |
| Server information | Apache/2.4.52 (Ubuntu) |
| Responsive | True |
| Server OS | Unix |

Threat level

Acunetix Threat Level 1

One or more low-severity type vulnerabilities have been discovered by the scanner.

Alerts distribution

| | |
|---|----|
| Total alerts found | 16 |
|  High | 0 |
|  Medium | 0 |
|  Low | 5 |
|  Informational | 11 |

Alerts

Clickjacking: X-Frame-Options header

| | |
|---------------|------------|
| Affected item | Web Server |
|---------------|------------|

| | |
|--------------------|--|
| Affected parameter | |
|--------------------|--|

Request

```
GET /login?redirect=%2F HTTP/1.1
Host: acunetix.eramba.org
Pragma: no-cache
Cache-Control: no-cache
accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*
/*;q=0.8,application/signed-exchange;v=b3;q=0.9
accept-language: en-US
upgrade-insecure-requests: 1
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip,deflate,br
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/108.0.0.0 Safari/537.36
```

Cookies with missing, inconsistent or contradictory properties (verified)

| | |
|---------------|------------|
| Affected item | Web Server |
|---------------|------------|

| | |
|--------------------|--|
| Affected parameter | |
|--------------------|--|

Request

```
POST /login?redirect=%2F HTTP/1.1
Host: acunetix.eramba.org
Content-Length: 332
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
Origin: https://acunetix.eramba.org
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*
/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://acunetix.eramba.org/login?redirect=%2F
Accept-Encoding: gzip,deflate,br
Cookie: PHPSESSID=43hf4s6p43dvd7c28948cr4po1; translation=1;
csrfToken=J8%2FvGrjDpBNarVlvnC5qCTBlNzQ4ZDU3NzQ5NGY0NmY2MDRiYTc1YmM0MTEzNjllNmQxM2U0ZmU%
3D
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/108.0.0.0 Safari/537.36

_csrfToken=3%2BxTURxflRLHBnSEU%2FS0KSkT2Tmycr80MJzhvULERwEdHdSYwnv6SLmpBetyczFLXQdk7RXAI
Pn4I7xLpJwxCh2rLevP2t4gGXbuDYowigMHqNiJL3BxZyst4PqjTM8q2p002kFFCC5rY1XecPRGnA%3D%3D&logi
n=acunetix&password=alphanumeric1%21&_Token%5Bfields%5D=ad53d77407f5d9a95bcf91a827e1ecd9
9398659c%253A&_Token%5Bunlocked%5D=%257CmodalBreadcrumbs%257CmodalId
```

Cookies without HttpOnly flag set (verified)

| | |
|---|------------|
| Affected item | Web Server |
| Affected parameter | |
| Request | |
| <pre> POST /login?redirect=%2F HTTP/1.1 Host: acunetix.eramba.org Content-Length: 332 Pragma: no-cache Cache-Control: no-cache Upgrade-Insecure-Requests: 1 Origin: https://acunetix.eramba.org Content-Type: application/x-www-form-urlencoded Accept-Language: en-US Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,* /*;q=0.8,application/signed-exchange;v=b3;q=0.9 Sec-Fetch-Site: same-origin Sec-Fetch-Mode: navigate Sec-Fetch-User: ?1 Sec-Fetch-Dest: document Referer: https://acunetix.eramba.org/login?redirect=%2F Accept-Encoding: gzip,deflate,br Cookie: PHPSESSID=43hf4s6p43dvd7c28948cr4po1; translation=1; csrfToken=J8%2FvGrjDpBNarVlvnC5qCTBlNzQ4ZDU3NzQ5NGY0NmY2MDRiYTclYmM0MTEzNjllNmQxM2U0ZmU% 3D Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36 _csrfToken=3%2BxTURxf1RlHBnSEU%2FS0KSkT2Tmycr80MJzhvULERwEdHdSYwnv6SLmpBetyczFLXQdk7RXAI Pn4I7xLpJwxCh2rLevP2t4gGXbuDYowigMHqNiJL3BxZyst4PqjTM8q2p002kFFCC5rY1XecPRGnA%3D%3D&logi n=acunetix&password=alphanumeric1%21&_Token%5Bfields%5D=ad53d77407f5d9a95bcf91a827e1ecd9 9398659c%253A&_Token%5Bunlocked%5D=%257CmodalBreadcrumbs%257CmodalId </pre> | |

Cookies without Secure flag set (verified)

| | |
|--------------------|------------|
| Affected item | Web Server |
| Affected parameter | |
| Request | |

```

POST /login?redirect=%2F HTTP/1.1
Host: acunetix.eramba.org
Content-Length: 332
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
Origin: https://acunetix.eramba.org
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-US
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*
/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://acunetix.eramba.org/login?redirect=%2F
Accept-Encoding: gzip,deflate,br
Cookie: PHPSESSID=43hf4s6p43dvd7c28948cr4po1; translation=1;
csrfToken=J8%2FvGrjDpBNarVlvnC5qCTBlNzQ4ZDU3NzQ5NGY0NmY2MDRiYTc1YmM0MTEzNjllNmQxM2U0ZmU%
3D
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/108.0.0.0 Safari/537.36

_csrfToken=3%2BxTURxflRLHBnSEU%2FS0KSkT2Tmycr80MJzhvULERwEdHdSYwnv6SLmpBetyczFLXQdk7RXAI
Pn4I7xLpJwxCh2rLevP2t4gGXbuDYoWigMHqNiJL3BxZyst4PqjTM8q2p002kFFCC5rY1XecPRGnA%3D%3D&logi
n=acunetix&password=alphanumeric1%21&_Token%5Bfields%5D=ad53d77407f5d9a95bcf91a827e1ecd9
9398659c%253A&_Token%5Bunlocked%5D=%257CmodalBreadcrumbs%257CmodalId

```

HTTP Strict Transport Security (HSTS) not implemented

| | |
|---|------------|
| Affected item | Web Server |
| Affected parameter | |
| Request | |
| <pre> GET /login?redirect=%2F HTTP/1.1 Host: acunetix.eramba.org Pragma: no-cache Cache-Control: no-cache accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,* /*;q=0.8,application/signed-exchange;v=b3;q=0.9 accept-language: en-US upgrade-insecure-requests: 1 Sec-Fetch-Site: none Sec-Fetch-Mode: navigate Sec-Fetch-User: ?1 Sec-Fetch-Dest: document Accept-Encoding: gzip,deflate,br Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36 </pre> | |

Content Security Policy (CSP) not implemented

| | |
|--------------------|------------|
| Affected item | Web Server |
| Affected parameter | |
| Request | |

```
GET /login?redirect=%2F HTTP/1.1
Host: acunetix.eramba.org
Pragma: no-cache
Cache-Control: no-cache
accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*
/*;q=0.8,application/signed-exchange;v=b3;q=0.9
accept-language: en-US
upgrade-insecure-requests: 1
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip,deflate,br
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/108.0.0.0 Safari/537.36
```

Outdated JavaScript libraries

| | |
|---|------------|
| Affected item | Web Server |
| Affected parameter | |
| Request | |
| <pre>GET /login?redirect=%2F HTTP/1.1 Host: acunetix.eramba.org Pragma: no-cache Cache-Control: no-cache accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,* /*;q=0.8,application/signed-exchange;v=b3;q=0.9 accept-language: en-US upgrade-insecure-requests: 1 Sec-Fetch-Site: none Sec-Fetch-Mode: navigate Sec-Fetch-User: ?1 Sec-Fetch-Dest: document Accept-Encoding: gzip,deflate,br Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36</pre> | |

Outdated JavaScript libraries

| | |
|--------------------|------------|
| Affected item | Web Server |
| Affected parameter | |
| Request | |

```

GET /limitless_theme/js/plugins/forms/validation/validate.min.js HTTP/1.1
Host: acunetix.eramba.org
Pragma: no-cache
Cache-Control: no-cache
accept: */*
accept-language: en-US
cookie: PHPSESSID=43hf4s6p43dvd7c28948cr4po1; translation=1;
csrfToken=J8%2FvGrjDpBNarVlvnC5qCTBlNzQ4ZDU3NzQ5NGY0NmY2MDRiYTc1YmM0MTEzNjllNmQxM2U0ZmU%
3D
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://acunetix.eramba.org/login?redirect=%2F
Accept-Encoding: gzip,deflate,br
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/108.0.0.0 Safari/537.36

```

Outdated JavaScript libraries

| | |
|--------------------|------------|
| Affected item | Web Server |
| Affected parameter | |

Request

```

GET /js/jquery-upgrade/jquery-ui-1.12.1.custom/jquery-ui.min.js HTTP/1.1
Host: acunetix.eramba.org
Pragma: no-cache
Cache-Control: no-cache
accept: */*
accept-language: en-US
cookie: translation=1;
csrfToken=J8%2FvGrjDpBNarVlvnC5qCTBlNzQ4ZDU3NzQ5NGY0NmY2MDRiYTc1YmM0MTEzNjllNmQxM2U0ZmU%
3D; PHPSESSID=12kr0tfcvgt5t51vibsm5jelsc
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://acunetix.eramba.org/dashboard
Accept-Encoding: gzip,deflate,br
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/108.0.0.0 Safari/537.36

```

Outdated JavaScript libraries

| | |
|--------------------|------------|
| Affected item | Web Server |
| Affected parameter | |

Request

```
GET /js/jquery-upgrade/jquery-ui-1.12.1.custom/jquery-ui.min.js HTTP/1.1
Host: acunetix.eramba.org
Pragma: no-cache
Cache-Control: no-cache
accept: */*
accept-language: en-US
cookie: translation=1;
csrfToken=J8%2FvGrjDpBNarVlvnC5qCTBlNzQ4ZDU3NzQ5NGY0NmY2MDRiYTc1YmM0MTEzNjllNmQxM2U0ZmU%
3D; PHPSESSID=12kr0tfcvgt5t51vibsm5je1sc
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://acunetix.eramba.org/dashboard
Accept-Encoding: gzip,deflate,br
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/108.0.0.0 Safari/537.36
```

Outdated JavaScript libraries

| | |
|---|------------|
| Affected item | Web Server |
| Affected parameter | |
| Request | |
| GET /js/jquery-upgrade/DataTables/ColReorder-1.5.2/js/dataTables.colReorder.min.js HTTP/1.1 Host: acunetix.eramba.org Pragma: no-cache Cache-Control: no-cache accept: */* accept-language: en-US cookie: translation=1; csrfToken=J8%2FvGrjDpBNarVlvnC5qCTBlNzQ4ZDU3NzQ5NGY0NmY2MDRiYTc1YmM0MTEzNjllNmQxM2U0ZmU% 3D; PHPSESSID=12kr0tfcvgt5t51vibsm5je1sc Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: script Referer: https://acunetix.eramba.org/dashboard Accept-Encoding: gzip,deflate,br Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36 | |

Outdated JavaScript libraries

| | |
|--------------------|------------|
| Affected item | Web Server |
| Affected parameter | |
| Request | |


```

GET /dashboard HTTP/1.1
Host: acunetix.eramba.org
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
Accept-Language: en-US
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*
/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
cookie: translation=1;
csrfToken=J8%2FvGrjDpBNarVlvnC5qCTBlNzQ4ZDU3NzQ5NGY0NmY2MDRiYTc1YmM0MTEzNjllNmQxM2U0ZmU%
3D; PHPSESSID=12kr0tfcvgt5t5lvibsm5jelsc
Referer: https://acunetix.eramba.org/login?redirect=%2F
Accept-Encoding: gzip,deflate,br
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/108.0.0.0 Safari/537.36

```

Outdated JavaScript libraries

| | |
|--------------------|------------|
| Affected item | Web Server |
| Affected parameter | |

Request

```

GET /limitless_theme/js/plugins/forms/selects/select2.min.js HTTP/1.1
Host: acunetix.eramba.org
Pragma: no-cache
Cache-Control: no-cache
accept: */*
accept-language: en-US
cookie: PHPSESSID=43hf4s6p43dvd7c28948cr4po1; translation=1;
csrfToken=J8%2FvGrjDpBNarVlvnC5qCTBlNzQ4ZDU3NzQ5NGY0NmY2MDRiYTc1YmM0MTEzNjllNmQxM2U0ZmU%
3D
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://acunetix.eramba.org/login?redirect=%2F
Accept-Encoding: gzip,deflate,br
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/108.0.0.0 Safari/537.36

```

Outdated JavaScript libraries

| | |
|--------------------|------------|
| Affected item | Web Server |
| Affected parameter | |

Request

```

GET /js/jquery-upgrade/DataTables/Buttons-1.6.1/js/dataTables.buttons.min.js HTTP/1.1
Host: acunetix.eramba.org
Pragma: no-cache
Cache-Control: no-cache
accept: */*
accept-language: en-US
cookie: translation=1;
csrfToken=J8%2FvGrjDpBNarVlvnC5qCTBlNzQ4ZDU3NzQ5NGY0NmY2MDRiYTc1YmM0MTEzNjllNmQxM2U0ZmU%
3D; PHPSESSID=12kr0tfcvgt5t51vibsm5je1sc
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://acunetix.eramba.org/dashboard
Accept-Encoding: gzip,deflate,br
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/108.0.0.0 Safari/537.36

```

Outdated JavaScript libraries

| | |
|--|------------|
| Affected item | Web Server |
| Affected parameter | |
| Request | |
| <pre> GET /js/jquery-upgrade/DataTables/datatables.min.js HTTP/1.1 Host: acunetix.eramba.org Pragma: no-cache Cache-Control: no-cache accept: */* accept-language: en-US cookie: translation=1; csrfToken=J8%2FvGrjDpBNarVlvnC5qCTBlNzQ4ZDU3NzQ5NGY0NmY2MDRiYTc1YmM0MTEzNjllNmQxM2U0ZmU% 3D; PHPSESSID=12kr0tfcvgt5t51vibsm5je1sc Sec-Fetch-Site: same-origin Sec-Fetch-Mode: no-cors Sec-Fetch-Dest: script Referer: https://acunetix.eramba.org/dashboard Accept-Encoding: gzip,deflate,br Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36 </pre> | |

Permissions-Policy header not implemented

| | |
|--------------------|------------|
| Affected item | Web Server |
| Affected parameter | |
| Request | |

```
POST /login?redirect=%2F HTTP/1.1
Host: acunetix.eramba.org
Content-Length: 756
accept: */*
accept-language: en-US
content-type: multipart/form-data; boundary=----WebKitFormBoundaryEEf95DZz4BhVlkTE
cookie: translation=1;
csrfToken=J8%2FvGrjDpBNarVlvnC5qCTBlNzQ4ZDU3NzQ5NGY0NmY2MDRiYTc1YmM0MTEzNjllNmQxM2U0ZmU%
3D; PHPSESSID=12kr0tfcvgt5t51vibsm5je1sc; PHPSESSID=43hf4s6p43dvd7c28948cr4po1;
translation=1;
csrfToken=J8%2FvGrjDpBNarVlvnC5qCTBlNzQ4ZDU3NzQ5NGY0NmY2MDRiYTc1YmM0MTEzNjllNmQxM2U0ZmU%
3D
origin: https://acunetix.eramba.org
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://acunetix.eramba.org/login?redirect=%2F
Accept-Encoding: gzip,deflate,br
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/108.0.0.0 Safari/537.36

-----WebKitFormBoundaryEEf95DZz4BhVlkTE
Content-Disposition: form-data; name="_csrfToken"

3+xtURxfLrLHbnSEU/S0KSKt2Tmycr80MJzhvULERwEdHdSYwnv6SLmpBetyczFLXQdk7RXAIPn4I7xLpJwxCh2r
LevP2t4gGXbuDYoWigMHqNiJL3BxZyst4PqjTM8q2p002kFFCC5rY1XecPRGnA==
-----WebKitFormBoundaryEEf95DZz4BhVlkTE
Content-Disposition: form-data; name="login"

-----WebKitFormBoundaryEEf95DZz4BhVlkTE
Content-Disposition: form-data; name="password"

-----WebKitFormBoundaryEEf95DZz4BhVlkTE
Content-Disposition: form-data; name="_Token[fields]"

ad53d77407f5d9a95bcf91a827e1ecd99398659c%3A
-----WebKitFormBoundaryEEf95DZz4BhVlkTE
Content-Disposition: form-data; name="_Token[unlocked]"

%7CmodalBreadcrumbs%7CmodalId
-----WebKitFormBoundaryEEf95DZz4BhVlkTE--
```