TYPO3 Core - Bug #91396

Story # 91384 (Closed): Backend login and referrer problems after recent TYPO3 9.5.17 and 10.4.2 security fixes

Allow SSO authentication handlers to pass SSRF referrer checks

2020-05-14 12:42 - Oliver Hader

Status:	Closed	**Start date:**	2020-05-14
Priority:	Should have	**Due date:**	
Assignee:	Oliver Hader	**% Done:**	100%
Category:	Security	**Estimated time:**	0.00 hour
Target version:	9.5.18 & 10.4.3		
TYPO3 Version:	9	**Complexity:**	
PHP Version:		**Is Regression:**	
Tags:		**Sprint Focus:**	

Description

Scenario

- https://sso.example.org/auth used to authenticate
- https://example.org/?eID=auth used for session transfer/activation (or similar technique, invoking a "callback")
  - request header Referer: https://sso.example.org/auth
  - response header Location: https://example.org/typo3/
- https://example.org/typo3/ as redirect
  - request header Referer: https://sso.example.org/auth (still the external SSO, since redirected via Location: headers)
  - response header Location: http://example/typo3/index.php?route=%2Fmain&token=1ed543d6ba3594722a69a1969abc15046631d7a5
- http://example/typo3/index.php?route=%2Fmain&token=1ed543d6ba3594722a69a1969abc15046631d7a5 checking the referrer
  - request header Referer: https://sso.example.org/auth (still the external SSO, since redirected via Location: headers)

Observation

- request is actually correct
- referrer is send - but with something "external" from /typo3/ (that the subject we want and must protect from being called **directly**)

Variations

- cross-site
  - Referer: https://sso.example.org/auth
  - expected Referer: https://example.org/typo3/.+
- same-site
  - Referer: https://example.org/?eID=auth
  - expected Referer: https://example.org/typo3/.+
- same-origin (the regular case)
  - Referer: https://example.org/typo3/index.php?route=%2Flogin
  - expected Referer: https://example.org/typo3/.+

Related issues:

Has duplicate TYPO3 Core - Bug #91414: After update from 9.5.16 to 9.5.17 I g...	**Closed**	**2020-05-15**

Associated revisions

Revision fbafe16c - 2020-05-18 10:09 - Oliver Hader

[BUGFIX] Allow multiple referrer types in backend main route

With TYPO3-CORE-SA-2020-006 (SSRF via XSS) a strict referrer handling
has been introduced to avoid the TYPO3 backend being called from other
non same-origin locations. In case a HTTP referrer header was empty
the system tried to refresh the view - otherwise the request was
denied completely.

It turned out that this scenario was probably too strict, disabling
feature `security.backend.enforceReferrer` was the only work-around
for site administrators.

This change adds new options for handling referrers in backend routes:

- refresh-empty (existed already): refresh in case referrer is empty
- refresh-same-site: refresh in case referrer is on same site, like `https://example.org/?eID=auth` calling `https://example.org/typo3/`
- refresh-always: refresh always in case there is not valid referrer

TYPO3's main backend route is using `refresh-always` now to be more relaxed on handling same-site and cross-site referrers as well.

The term "refreshing" relates to trigger a reload in the browser to get the referrer of the current location. This still block direct CSRF/SSRF requests since the refreshing HTML instructions are delivered back to the client. Besides that, cross-site requests are covered by the `same-site` cookie policy, and existing CSRF tokens.

Resolves: #91396
Releases: master, 9.5
Change-Id: Ib3756671fa60c6f41ba992d0e645f03da1730d19
Reviewed-on: https://review.typo3.org/c/Packages/TYPO3.CMS/+/64492
Tested-by: Susanne Moog <look@susi.dev>
Tested-by: TYPO3com <noreply@typo3.com>
Tested-by: Richard Haeser <richard@maxserv.com>
Reviewed-by: Susanne Moog <look@susi.dev>
Reviewed-by: Richard Haeser <richard@maxserv.com>

Revision 6d9e803c - 2020-05-18 14:34 - Oliver Hader

[BUGFIX] Allow multiple referrer types in backend main route

With TYPO3-CORE-SA-2020-006 (SSRF via XSS) a strict referrer handling has been introduced to avoid the TYPO3 backend being called from other non same-origin locations. In case a HTTP referrer header was empty the system tried to refresh the view - otherwise the request was denied completely.

It turned out that this scenario was probably too strict, disabling feature `security.backend.enforceReferrer` was the only work-around for site administrators.

This change adds new options for handling referrers in backend routes:

- refresh-empty (existed already): refresh in case referrer is empty
- refresh-same-site: refresh in case referrer is on same site, like `https://example.org/?eID=auth` calling `https://example.org/typo3/`
- refresh-always: refresh always in case there is not valid referrer

TYPO3's main backend route is using `refresh-always` now to be more relaxed on handling same-site and cross-site referrers as well.

The term "refreshing" relates to trigger a reload in the browser to get the referrer of the current location. This still block direct CSRF/SSRF requests since the refreshing HTML instructions are delivered back to the client. Besides that, cross-site requests are covered by the `same-site` cookie policy, and existing CSRF tokens.

Resolves: #91396
Releases: master, 9.5
Change-Id: Ib3756671fa60c6f41ba992d0e645f03da1730d19
Reviewed-on: https://review.typo3.org/c/Packages/TYPO3.CMS/+/64499
Tested-by: TYPO3com <noreply@typo3.com>
Tested-by: Oliver Hader <oliver.hader@typo3.org>
Reviewed-by: Oliver Hader <oliver.hader@typo3.org>

Revision 86b9b4a2 - 2020-05-18 23:59 - Oliver Hader

[BUGFIX] Allow referrer refresh in install tool

With TYPO3-CORE-SA-2020-006 (SSRF via XSS) a strict referrer handling has been introduced to avoid the install tool being called from other non same-origin locations. In case a HTTP referrer header was empty the system tried to refresh the view - otherwise the request was denied completely.

Changes of issue #91396 using refresh-always are applied as well.

Resolves: #91433
Related: #91396
Releases: master, 9.5
Change-Id: I2a570da4f2a933e709d653b54f1d53d5055ef3f7
Reviewed-on: https://review.typo3.org/c/Packages/TYPO3.CMS/+/64519
Tested-by: TYPO3com <noreply@typo3.com>
Tested-by: Oliver Hader <oliver.hader@typo3.org>
Reviewed-by: Oliver Hader <oliver.hader@typo3.org>

Revision 8a137310 - 2020-05-19 00:00 - Oliver Hader

[BUGFIX] Allow referrer refresh in install tool

With TYPO3-CORE-SA-2020-006 (SSRF via XSS) a strict referrer handling
has been introduced to avoid the install tool being called from other
non same-origin locations. In case a HTTP referrer header was empty
the system tried to refresh the view - otherwise the request was
denied completely.

Changes of issue #91396 using refresh-always are applied as well.

Resolves: #91433
Related: #91396
Releases: master, 9.5
Change-Id: I2a570da4f2a933e709d653b54f1d53d5055ef3f7
Reviewed-on: https://review.typo3.org/c/Packages/TYPO3.CMS/+/64518
Tested-by: TYPO3com <noreply@typo3.com>
Tested-by: Oliver Hader <oliver.hader@typo3.org>
Reviewed-by: Oliver Hader <oliver.hader@typo3.org>

History

#1 - 2020-05-14 12:52 - Oliver Hader

- Description updated

#2 - 2020-05-14 13:00 - Oliver Hader

- Status changed from New to Accepted

- Target version set to 9.5.18 & 10.4.3

#3 - 2020-05-14 13:58 - Richard Haeser

We have exactly this scenario with the OpenID extension: friendsoftypo3/openid

#4 - 2020-05-14 17:04 - Gerrit Code Review

- Status changed from Accepted to Under Review

Patch set 1 for branch **master** of project **Packages/TYPO3.CMS** has been pushed to the review server.
It is available at https://review.typo3.org/c/Packages/TYPO3.CMS/+/64492

#5 - 2020-05-14 17:25 - Gerrit Code Review

Patch set 2 for branch **master** of project **Packages/TYPO3.CMS** has been pushed to the review server.
It is available at https://review.typo3.org/c/Packages/TYPO3.CMS/+/64492

#6 - 2020-05-15 12:03 - David Rellstab

Tested and verified the patch with our sso setup on TYPO3 9.5.17.

Patch resolves the issue for our use case.

#7 - 2020-05-15 15:39 - Gerrit Code Review

Patch set 3 for branch **master** of project **Packages/TYPO3.CMS** has been pushed to the review server.
It is available at https://review.typo3.org/c/Packages/TYPO3.CMS/+/64492

#8 - 2020-05-15 16:16 - Richard Haeser

- Has duplicate Bug #91414: After update from 9.5.16 to 9.5.17 I get an error 'Missing referrer for /main' in /typo3 added

#9 - 2020-05-15 16:16 - Richard Haeser

- Has duplicate Bug #91415: After Update from 9.5.14 to 9.5.17 - backend and installer login are not working added

#10 - 2020-05-15 16:16 - Richard Haeser

- Has duplicate deleted (Bug #91415: After Update from 9.5.14 to 9.5.17 - backend and installer login are not working)

#11 - 2020-05-15 21:26 - Gerrit Code Review

Patch set 1 for branch **9.5** of project **Packages/TYPO3.CMS** has been pushed to the review server.
It is available at https://review.typo3.org/c/Packages/TYPO3.CMS/+/64499

#12 - 2020-05-15 21:27 - Gerrit Code Review

Patch set 2 for branch **9.5** of project **Packages/TYPO3.CMS** has been pushed to the review server.
It is available at https://review.typo3.org/c/Packages/TYPO3.CMS/+/64499

#13 - 2020-05-16 10:10 - Gerrit Code Review

Patch set 3 for branch **9.5** of project **Packages/TYPO3.CMS** has been pushed to the review server.
It is available at https://review.typo3.org/c/Packages/TYPO3.CMS/+/64499

#14 - 2020-05-18 10:09 - Gerrit Code Review

Patch set 4 for branch **9.5** of project **Packages/TYPO3.CMS** has been pushed to the review server.
It is available at https://review.typo3.org/c/Packages/TYPO3.CMS/+/64499

#15 - 2020-05-18 10:30 - Oliver Hader

- Status changed from Under Review to Resolved

- % Done changed from 0 to 100

Applied in changeset fbafe16c48fa47fd8d5d4d66436700b8d85d1bfa.

#16 - 2020-05-18 10:52 - Gerrit Code Review

- Status changed from Resolved to Under Review

Patch set 5 for branch **9.5** of project **Packages/TYPO3.CMS** has been pushed to the review server.
It is available at https://review.typo3.org/c/Packages/TYPO3.CMS/+/64499

#17 - 2020-05-18 15:00 - Oliver Hader

- Status changed from Under Review to Resolved

Applied in changeset 6d9e803c039257392a7b4ae487be33b93fea42af.

#18 - 2020-05-19 15:46 - Benni Mack

- Status changed from Resolved to Closed