mozilla

) web vulnerability report (

Version 2.0

Info

Researcher's Name	Jose Carlos Exposito Bueno
Researcher's Site	https://www.0xlabs.com/
Publicly acknowledged	YES
Report Date	20 January 2015

INDEX

ID	Severity	Description	Via	Domain
001	CRITICAL	Cross Site Scripting	Arbitrarily supplied URL	qsurvey.mozilla.com

) HIGH (	Cross Site Scripting Reflected [via `Arbitrary supplied URL`]	**001**

Description

Cross-Site Scripting (also known as XSS) is one of the most common application-layer web attacks. XSS vulnerabilities target scripts embedded in a page that are executed on the client-side (in the user's web browser) rather than on the server-side. XSS in itself is a threat that is brought about by the internet security weaknesses of client-side scripting languages, such as HTML and JavaScript.

The concept of XSS is to manipulate client-side scripts of a web application to execute in the manner desired by the malicious user. Such a manipulation can embed a script in a page that can be executed every time the page is loaded, or whenever an associated event is performed.

XSS is the most common security vulnerability in software today. This should not be the case as XSS is easy to find and easy to fix. XSS vulnerabilities can have consequences such as tampering and sensitive data theft.

The name of an arbitrarily supplied URL parameter is vulnerable to Cross Site Scripting attacks.

Affected Domain:
qsurvey.mozilla.com

Annexed Files

Http Request File	`http_request.txt`
Http Response File	`http_response.txt`
Burp Repeater File	`burp_repeater.dmp`

Impact

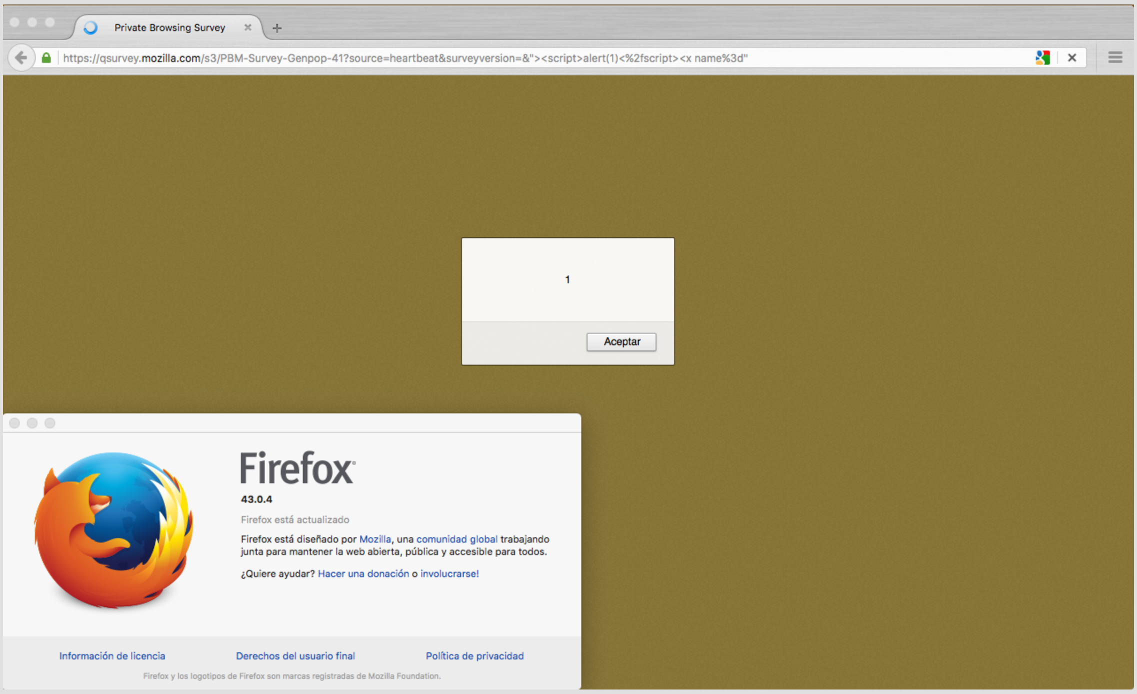
When attackers succeed in exploiting XSS vulnerabilities, they can gain access to account credentials. They can also spread web worms or access the user's computer and view the user's browser history or control the browser remotely. After gaining control to the victim's system, attackers can also analyze and use other intranet applications.

By exploiting XSS vulnerabilities, an attacker can perform malicious actions, such as:
- Hijack an account.
- Spread web worms.
- Access browser history and clipboard contents.
- Control the browser remotely.
- Scan and exploit intranet appliances and applications.
- Phishing attacks (Open Redirects via XSS)

POC

https://qsurvey.mozilla.com/s3/PBM-Survey-Genpop-41?source=heartbeat&surveyversion=&*%22%3e%3c%73%63%72%69%70%74%3e%61%6c%65%72%74%28%31%29%3c%2f%73%63%72%69%70%74%3e%3c%78%20%6e%61%6d%65%3d%22*

Evidence



https://qsurvey.mozilla.com/s3/PBM-Survey-Genpop-41?source=heartbeat&surveyversion=&"><script>alert(1)<%2fscript><x name%3d"

1

43.0.4

Firefox está actualizado

Firefox está diseñado por Mozilla, una comunidad global trabajando junta para mantener la web abierta, pública y accesible para todos.

¿Quiere ayudar? Hacer una donación o involucrarse!

Firefox y los logotipos de Firefox son marcas registradas de Mozilla Foundation.

References

- https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)
- https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet
- https://www.owasp.org/index.php/Testing_for_Reflected_Cross_site_scripting_(OWASP-DV-001)