

PROJECT : 8

DATE : 23-10-2021

TOPIC : Session Hijacking.

1. In firefox browser, add the extension cookie quick manager.

The screenshot shows the Firefox Add-ons Manager interface. The title bar says "Search results for 'cookie quick manager'" - Add-ons for Firefox (en-US) - Mozilla Firefox. Below the title bar, there's a navigation bar with "Add-ons Manager" and a search bar containing "cookie quick manager". The main content area displays a message "13 results found for 'cookie quick manager'" and a search results panel. On the left of the results panel is a "Filter results" sidebar with "Sort by" set to "Relevance" and "Add-on Type" dropdown. The results panel shows one item: "Cookie Quick Manager" (Recommended), which has 53,409 users. The description for the addon states: "An addon to manage cookies (view, search, create, edit, remove, backup, restore, protect from deletion and much more). Firefox 57+ is supported."

2. Goto testphp.vulnweb.com website and click on any tab except signup/login.

The screenshot shows a Firefox window titled "you cart - Mozilla Firefox". The address bar shows the URL "testphp.vulnweb.com/cart.php". The page content is from the "Acunetix acuart" website, specifically the "TEST and Demonstration site for Acunetix Web Vulnerability Scanner". The page shows a sidebar with links like "home", "categories", "artists", "disclaimer", "your cart", "guestbook", and "AJAX Demo". The main content area displays an "Error" message: "You are not logged on. To log on please visit our login page". On the right side of the page, there are several icons, including a blue gear icon with the number "5" and a small cookie icon. The status bar at the bottom of the Firefox window shows "Cookie Quick Manager" as an active extension.

3. Click on cookie quick manager extension, and click on search for cookies.

you cart - Mozilla Firefox

you cart | Cookie Quick Manager | +

testphp.vulnweb.com/cart.php

acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art go

Browse categories

Browse artists

Your cart

Signup

Your profile

Our guestbook

AJAX Demo

Links

Security art

PHP

moz-extension://9616858b-85dc-47e4-8700-17c409fcaa80/menu.html#

4. Click on pen icon in bottom right and put the credentials in the boxes. Uncheck any checkboxes.

Cookie Quick Manager - Mozilla Firefox

vulnweb.com

Domains (0)

No cookies in this tab.

Cookies

No cookies in this tab.

Details

Domain: testphp.vulnweb.com

First-Party:

Name: login

Value: test/test

URL: B64

Path:

5. Set up burpsuite, and configure firefox to burpsuite. Here the extension foxyproxy is used.

you cart - Mozilla Firefox

• you cart +

testphp.vulnweb.com/cart.php

acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art go

Browse categories

Browse artists

Your cart

Signup

Your profile

Our guestbook

AJAX Demo

Links

Security art

PHP scanner

PHP vuln help

Error

You are not logged on. To log on please visit our [login page](#)

testphp.vulnweb.com

6. Intercept request in burpsuite and add the cookie “login=test/test”.

Burp Suite Community Edition v2021.5-7586 (Early Adopter) - Temporary Project

Burp Project Intruder Repeater Window Help

Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options

Intercept HTTP history WebSockets history Options

Request to http://testphp.vulnweb.com:80 [18.192.172.30]

Forward Drop Intercept is on Action Open Browser

Pretty Raw \n Actions ▾

1 GET /cart.php HTTP/1.1
2 Host: testphp.vulnweb.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://testphp.vulnweb.com/
8 cookie: login=test/test
9 DNT: 1
10 Connection: close
11 Upgrade-Insecure-Requests: 1
12 Cache-Control: max-age=0
13
14

INSPECTOR

Search... 0 matches

7. Forward the request and observe that you're logged in.

you cart - Mozilla Firefox

you cart + testphp.vulnweb.com/cart.php

Acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo Logout test

search art go

Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Logout
Links
Security art
DHD scanner

Product id	Title	Artist	Category	Price	
3	The universe	r4w8173	Posters	\$986	delete
1	The shore	r4w8173	Posters	\$986	delete
1	The shore	r4w8173	Posters	\$986	delete
1	The shore	r4w8173	Posters	\$986	delete

Total: \$3944

place a command for these items

