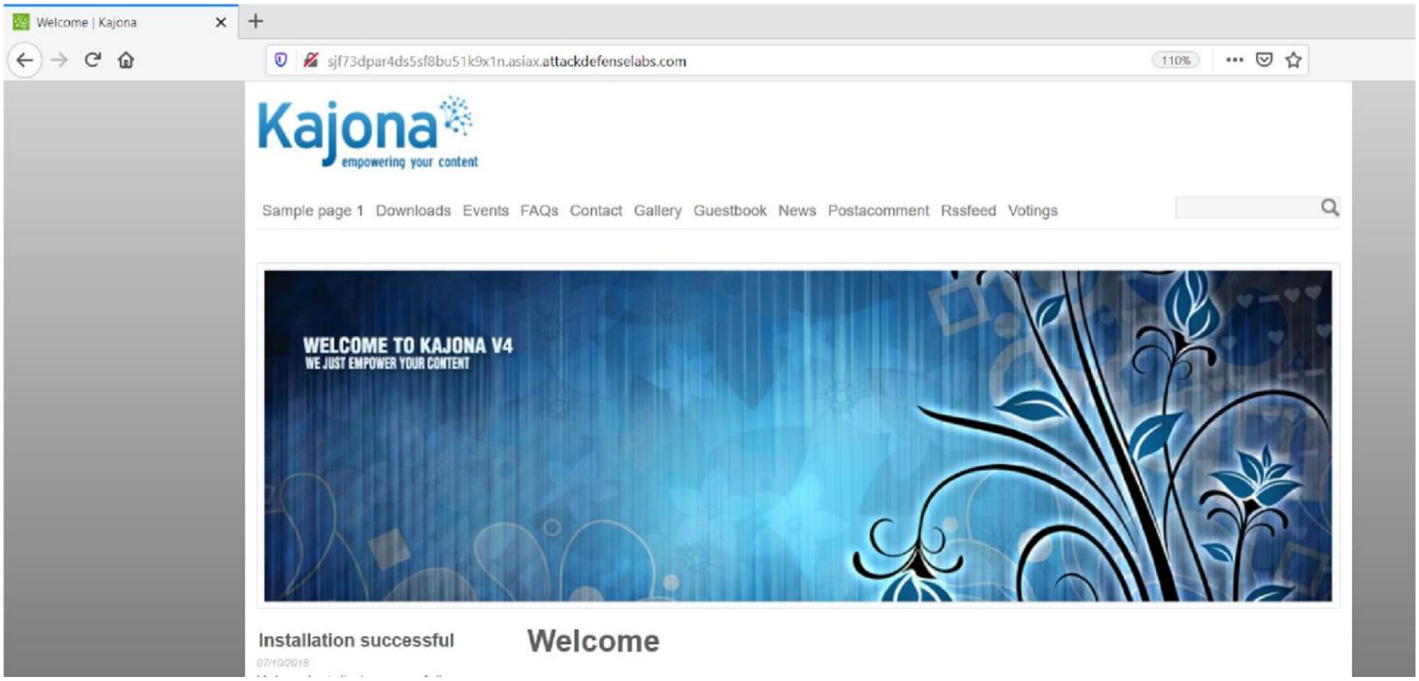
Name	Kajona
URL	https://www.attackdefense.com/challengedetails?cid=332
Type	Real World Webapps : Stored XSS

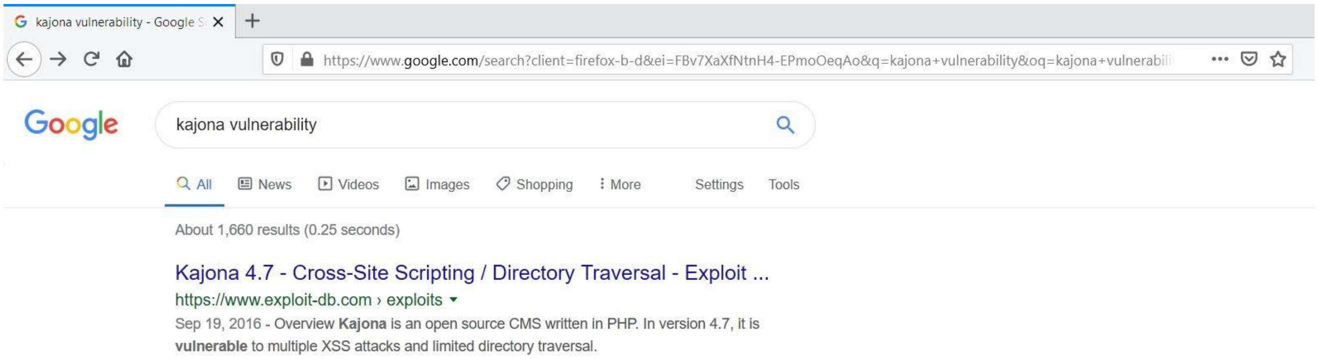
Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Solution:

Step 1: Inspect the web application.


Welcome | Kajona
sjf73dpar4ds5sf8bu51k9x1n.asiax.attackdefenselabs.com
110%
Kajona
empowering your content
Sample page 1 Downloads Events FAQs Contact Gallery Guestbook News Postacomment Rssfeed Votings
WELCOME TO KAJONA V4
WE JUST EMPOWER YOUR CONTENT
Installation successful
07/10/2018
Welcome

Step 2: Search on google “kajona vulnerability” and look for publicly available exploits.



https://www.google.com/search?client=firefox-b-d&ei=FBv7XaXfNtnH4-EPmoOeqAo8&q=kajona+vulnerability&oq=kajona+vulnerabil

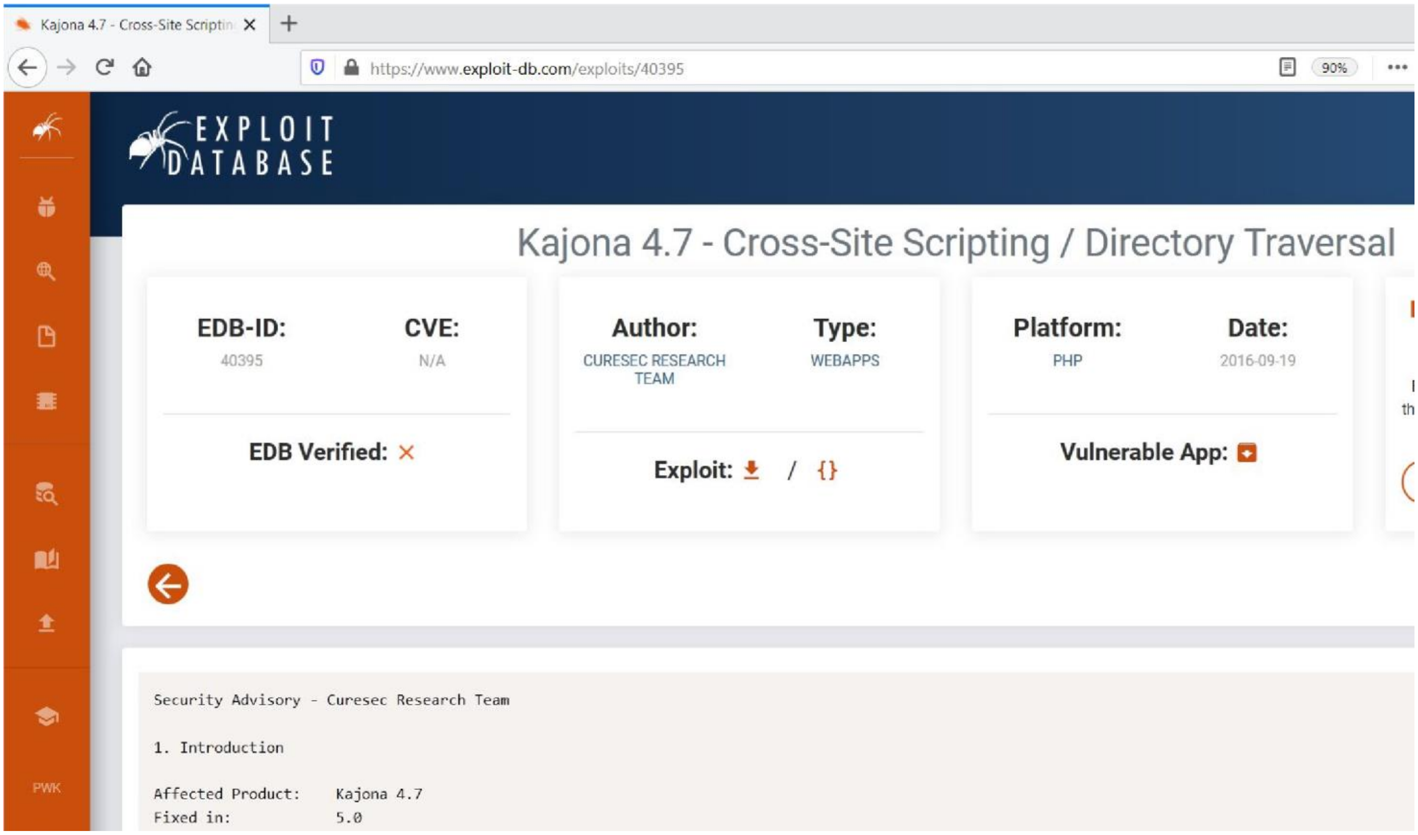
kajona vulnerability

About 1,660 results (0.25 seconds)

Kajona 4.7 - Cross-Site Scripting / Directory Traversal - Exploit ...
https://www.exploit-db.com › exploits
Sep 19, 2016 - Overview **Kajona** is an open source CMS written in PHP. In version 4.7, it is **vulnerable** to multiple XSS attacks and limited directory traversal.

The exploit db link contains the payload required to exploit the vulnerability.

Exploit DB Link: https://www.exploit-db.com/exploits/40395



https://www.exploit-db.com/exploits/40395

Kajona 4.7 - Cross-Site Scripting / Directory Traversal

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
40395	N/A	CURESEC RESEARCH TEAM	WEBAPPS	PHP	2016-09-19

EDB Verified: ✗

Exploit: ⬇ / {}

Vulnerable App: ⬇

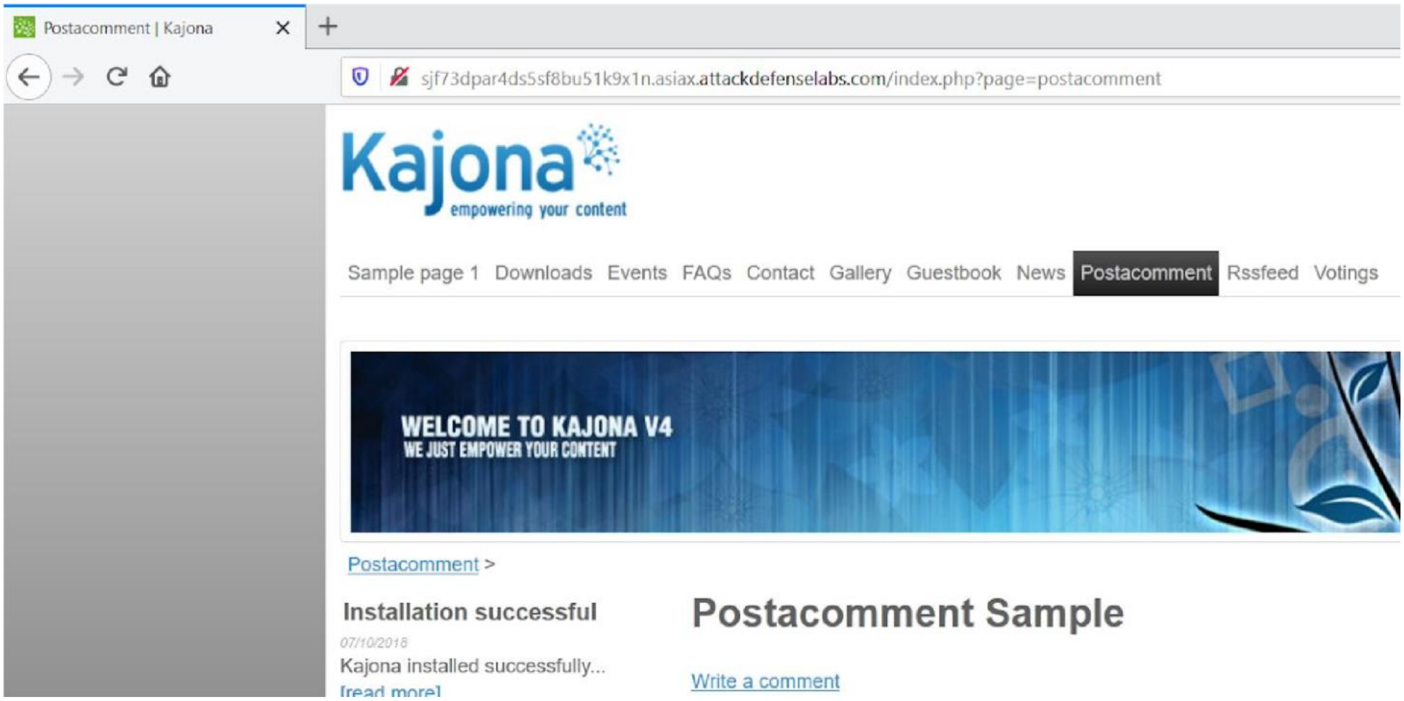
```
Security Advisory - Curesec Research Team

1. Introduction

Affected Product:    Kajona 4.7
Fixed in:            5.0
```

Step 3: Navigate to the vulnerable page.

URL: http://sjf73dpar4ds5sf8bu51k9x1n.asiax.attackdefenselabs.com/index.php?page=postacomment



sjf73dpar4ds5sf8bu51k9x1n.asiax.attackdefenselabs.com/index.php?page=postacomment

Postacomment >

Installation successful

07/10/2018

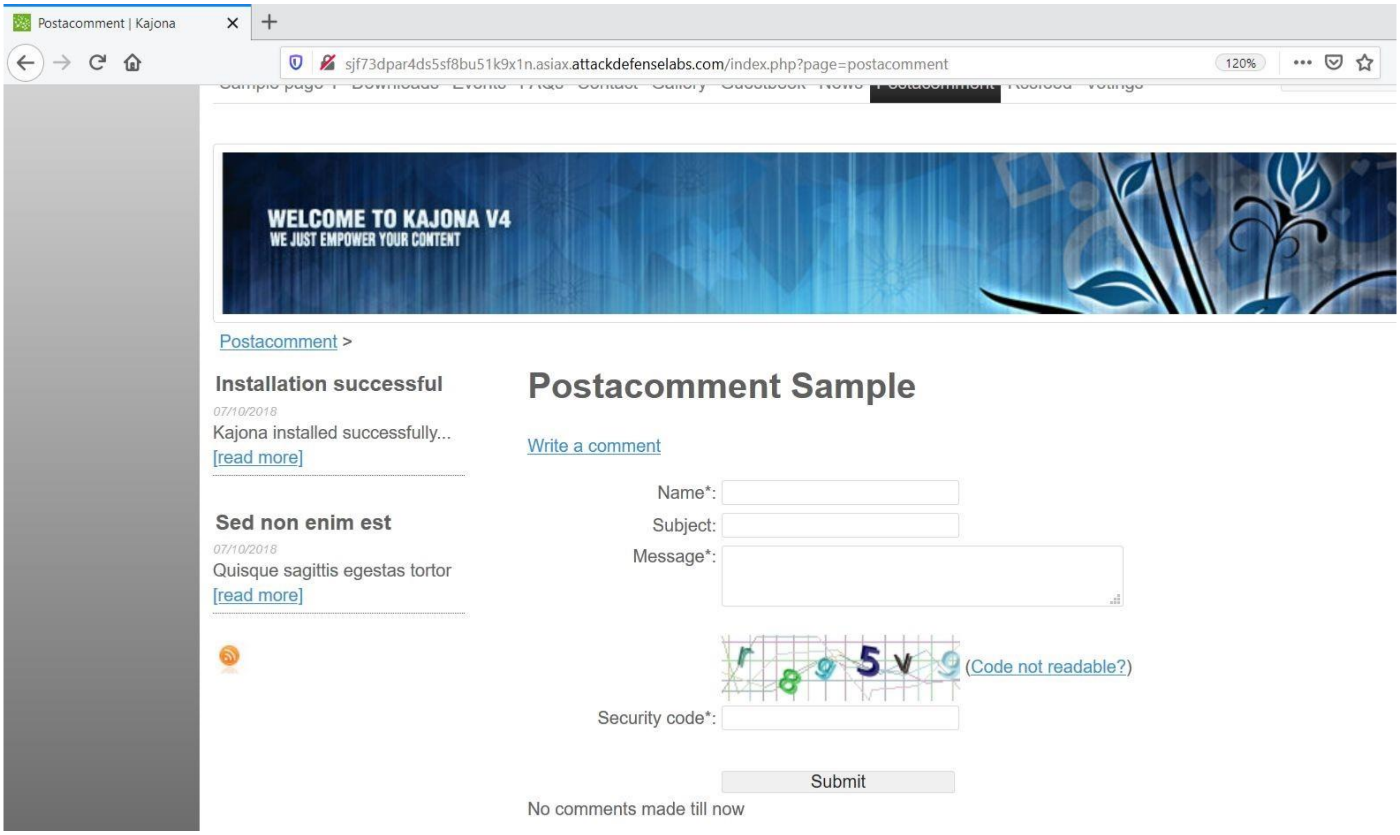
Kajona installed successfully...

[read more]

Postacomment Sample

Write a comment

Step 4: Click on “Write a Comment”.



Installation successful
07/10/2018
Kajona installed successfully...
[read more]

Sed non enim est
07/10/2018
Quisque sagittis egestas tortor
[read more]

Postacomment Sample

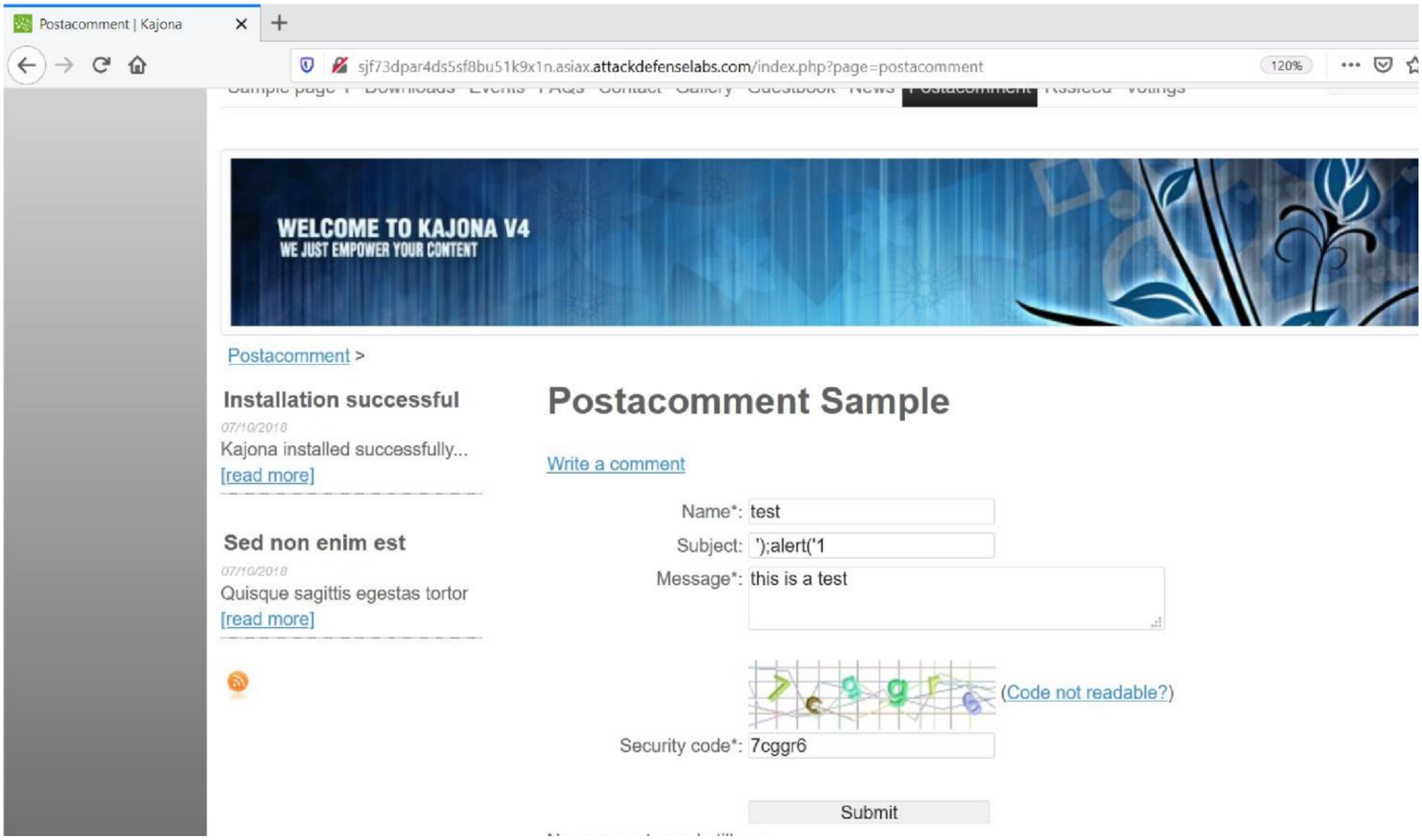
No comments made till now

Step 5: Inject the payload in Subject field and fill any data in Name and Message textbox.

Name: test

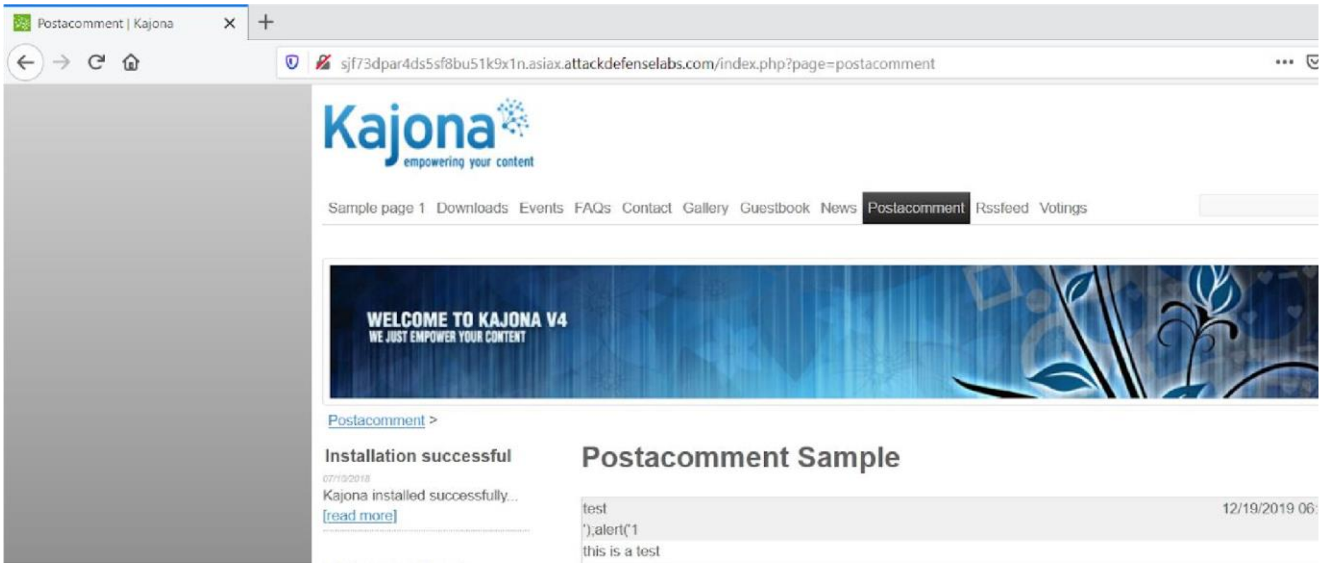
Payload: ');alert('1

Message: this is a test



Name*: test
Subject: ');alert('1
Message*: this is a test
Security code*: 7cggr6

Click on Submit button.


Postacomment | Kajona
sjf73dpar4ds5sf8bu51k9x1n.asiax.attackdefenselabs.com/index.php?page=postacomment
Kajona
empowering your content
Sample page 1 Downloads Events FAQs Contact Gallery Guestbook News Postacomment Rssfeed Votings
WELCOME TO KAJONA V4
WE JUST EMPOWER YOUR CONTENT
Postacomment >
Installation successful
07/10/2018
Kajona installed successfully...
[read more]
Postacomment Sample

test 12/19/2019 06:
');alert('1
this is a test

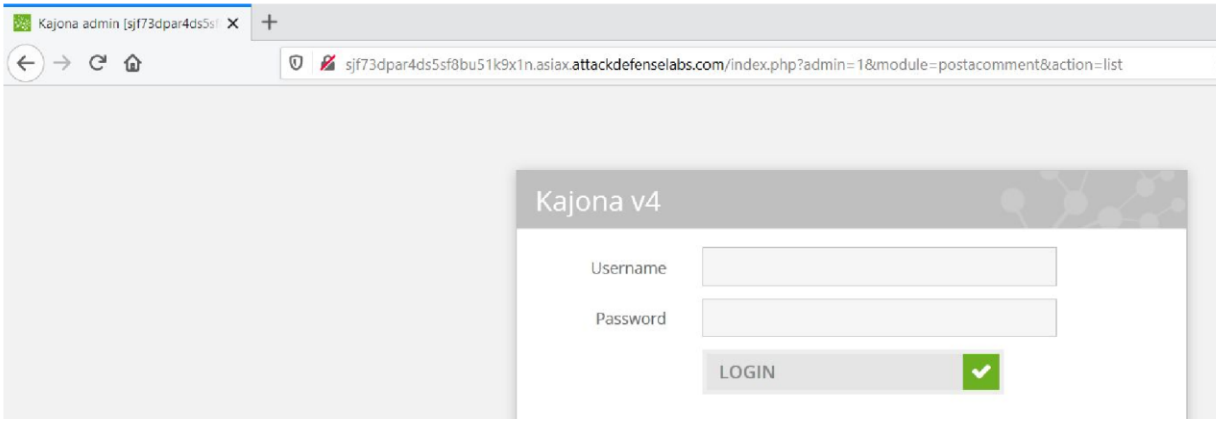
Step 6: The user has to authenticate in order to exploit the vulnerability. The login credentials are provided in the challenge description. Navigate to the URL provided at exploit db page.

URL:
http://sjf73dpar4ds5sf8bu51k9x1n.asiax.attackdefenselabs.com/index.php?admin=1&module=postacomment&action=list

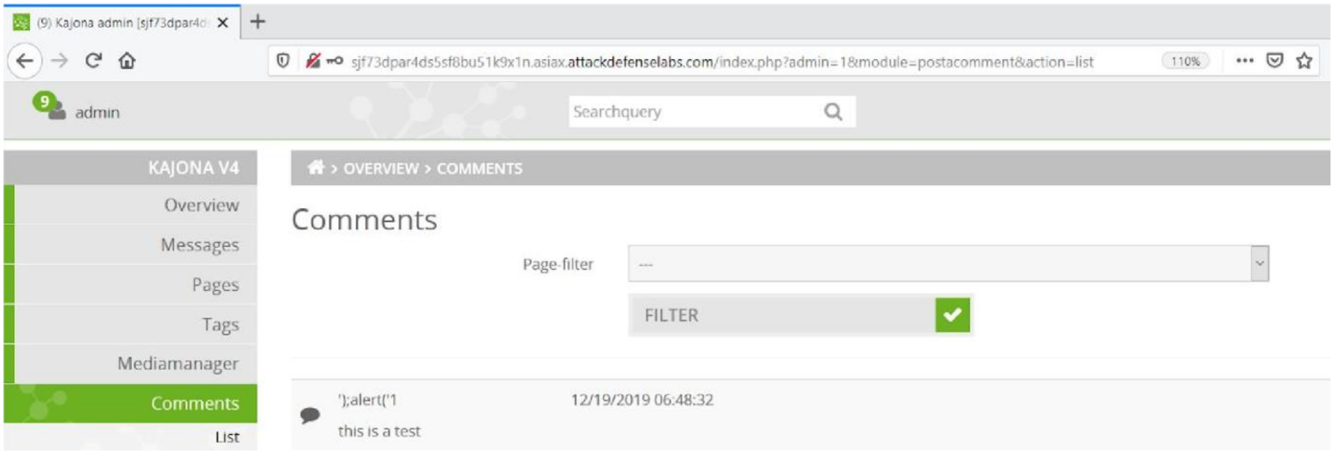
Credentials:

- **Username:** admin
- **Password:** password

Login Page


Kajona admin [sjf73dpar4ds5s
sjf73dpar4ds5sf8bu51k9x1n.asiax.attackdefenselabs.com/index.php?admin=1&module=postacomment&action=list
Kajona v4
Username
Password
LOGIN

Admin Dashboard

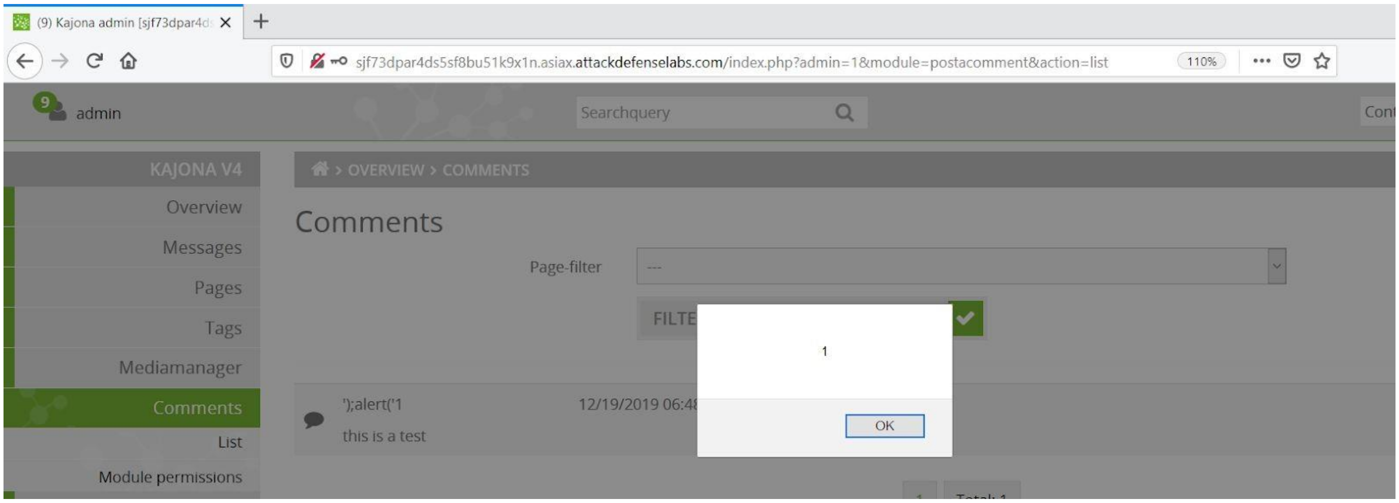

(9) Kajona admin [sjf73dpar4d
sjf73dpar4ds5sf8bu51k9x1n.asiax.attackdefenselabs.com/index.php?admin=1&module=postacomment&action=list
110%
9
admin
Searchquery
KAJONA V4
Overview
Messages
Pages
Tags
Mediamanager
Comments
List
OVERVIEW > COMMENTS
Comments
Page-filter

FILTER

');alert('1 12/19/2019 06:48:32

this is a test

Step 7: Click on Edit tags button located at the right option bar of the comment.



sjf73dpar4ds5sf8bu51k9x1n.asiax.attackdefenselabs.com/index.php?admin=1&module=postacomment&action=list

1

');alert('1 12/19/2019 06:4

this is a test

The XSS payload triggered successfully.

References:

1. Kajona (https://www.kajona.de /)
2. Kajona 4.7 - Cross-Site Scripting / Directory Traversal (https://www.exploit-db.com/exploits/40395)