

Forum:[Hack Forums](#)

Thread: [This site have sql or any vulnerability?](#)

laertisant - May 14, 2017, 5:10 am

Hey, need help!

I search site dark [-] net [.] news on WordPress 4.7.4, he is have oper directory, how i can hack this? need login pass admin or email on site

/wp-includes/
/wp-content/uploads/

Wingzor - May 14, 2017, 5:50 am

small hint -> Potential Unauthorized Password Reset (host header injection) vulnerability.

good luck !

1MKD - May 14, 2017, 6:02 am

You have a big chance, since it's linked in a shared hosting.

laertisant - May 14, 2017, 7:17 am

I'am read about this exploit for wp 4.7.4, but i can understand how doing this, what applications for this attack should I use?

Mohinder - May 14, 2017, 7:30 am

(May 14, 2017 07:17 AM)laertisant Wrote: [\[CITE\]](#) I'am read about this exploit for wp 4.7.4, but i can understand how doing this, what applications for this attack should I use?

If you don't understand how to do it this is probably nothing for you.

laertisant - May 14, 2017, 7:43 am

need manual video tutorial or example for this, how it's work

Rock™ - May 14, 2017, 9:30 am

(May 14, 2017 07:43 AM)laertisant Wrote: [\[CITE\]](#) need manual video tutorial or example for this, how it's work

Learn web headers and eventually you will figure out the lingo they are using

ubuntux92 - May 14, 2017, 12:17 pm

I get reference about host header attack from here

[www\[dot\]acunetix\[dot\]com/vulnerabilities/web/host-header-attack](http://www.dot.acunetix.com/vulnerabilities/web/host-header-attack)

Rel1k - May 14, 2017, 2:19 pm

(May 14, 2017 07:17 AM)laertisant Wrote: [\[CITE\]](#) I'am read about this exploit for wp 4.7.4, but i can understand how doing this, what applications for this attack should I use?

Before you want hacking the World maybe you must understand how web app work and you dont say what application but what i should do...

I dont read this WordPress vuln but if it is Host header injection learn CSRF ;) ill make a tutorial later ;)

Brill - May 14, 2017, 2:21 pm

(May 14, 2017 05:50 AM)Wingzor Wrote: [\[CITE\]](#) small hint -> Potential Unauthorized Password Reset (host header injection) vulnerability.

good luck !

pretty sure this was patched in the last update. wasn't it?

Rel1k - May 14, 2017, 2:37 pm

Go on exploit-db and you have all you need to exploit this vulnerability..
exploit-db.com/exploits/41963/

Thats all you need

laertisant - May 14, 2017, 2:41 pm

(May 14, 2017 12:17 PM)ubuntux92 Wrote: [\[CITE\]](#) I get reference about host header attack from here [www\[dot\]acunetix\[dot\]com/vulnerabilities/web/host-header-attack](http://www[dot]acunetix[dot]com/vulnerabilities/web/host-header-attack)
i found this [www \[.\] acunetix \[dot\] com/blog/articles/automated-detection-of-host-header-attacks/](http://www[.]acunetix[dot]com/blog/articles/automated-detection-of-host-header-attacks/)

but how to the create this http request...

(May 14, 2017 02:37 PM)Rel1k Wrote: [\[CITE\]](#) Go on exploit-db and you have all you need to exploit this vulnerability..
exploit-db.com/exploits/41963/

Thats all you need

yes, i read this) my problem is i dont know how to use it technically, I need examples, manuals, what applications are needed to attack...

Rel1k - May 14, 2017, 4:36 pm

WTF !!! If you dont have basics knowledge man...

If you dont know nothing about hacking, why you want to hack some site??

All you need is on that page ALL!!! You have a step by step...

And the 1 million dollars question is for staff, why i receive à friendly répondre about blackhat policy and After i read thread Like this ??

BigDap - May 14, 2017, 11:31 pm

Quote:Requests: 51

Avg. Response Time: 11,392ms

Locations: 78

Target Information

Address: dark-net.news

Server: Apache

Operating System: Unknown

Identified Technologies: PHP

Responsive: Yes

PHP Code

<?php

HTML form without CSRF protection

Quote:Vulnerability description

This alert may be a false positive, manual confirmation is required.

Cross-site request forgery, also known as a one-click attack or session riding and abbreviated as CSRF or XSRF, is a type of malicious exploit of a website whereby unauthorized commands are transmitted from a user that the website trusts.

Acunetix WVS found a HTML form with no apparent CSRF protection implemented. Consult details for more information about the affected HTML form.

Discovered by Crawler

The impact of this vulnerability

An attacker may force the users of a web application to execute actions of the attacker's choosing. A successful CSRF exploit can compromise end user data and operation in case of normal user. If the targeted end user is the administrator account, this can compromise the entire web application.

PHP Code

<?php

Classification

CWECWE-352

CVSS Base score: 4.3 — CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N

Attack Vector: Network

Attack Complexity: Low

Privileges Required: None

User Interaction: Required

Scope: Unchanged

Confidentiality: None

Integrity: Low

Availability: None

<https://cwe.mitre.org/data/definitions/352.html>

PHP Code

<?php

Clickjacking: X-Frame-Options header missing

Quote:Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.

The server didn't return an X-Frame-Options header which means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites.

Discovered by Scripting (Clickjacking_X_Frame_Options.script)

The impact of this vulnerability

The impact depends on the affected web application.

PHP Code
<?php
Classification

CWECWE-693

CVSS Base score: 6.8 — AV:N/AC:M/Au:N/C:P/I:P/A:P
Access Vector: Network
Access Complexity: Medium
Authentication: None
Confidentiality Impact: Partial
Integrity Impact: Partial
Availability Impact: Partial

<https://cwe.mitre.org/data/definitions/693.html>

PHP Code
<?php
Slow HTTP Denial of Service Attack

Quote:Vulnerability description

Your web server is vulnerable to Slow HTTP DoS (Denial of Service) attacks.

Slowloris and Slow HTTP POST DoS attacks rely on the fact that the HTTP protocol, by design, requires requests to be completely received by the server before they are processed. If an HTTP request is not complete, or if the transfer rate is very low, the server keeps its resources busy waiting for the rest of the data. If the server keeps too many resources busy, this creates a denial of service.

Discovered by Slow_HTTP_DOS

* The impact of this vulnerability

A single machine can take down another machine's web server with minimal bandwidth and side effects on unrelated services and ports.

PHP Code
<?php
Classification

CVSS Base score: 5.3 — CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None
Scope: Unchanged
Confidentiality: None
Integrity: None
Availability: Low

Quote:Discovered Hosts(15)

<https://cdn.bfm.ru/>
<https://cdn.securelist.ru/>
<http://cyberchimps.com/>
<http://gmpg.org/>
<https://img1.eadaily.com/>
<http://inosmi.ru/>
<https://pp.vk.me/>
<https://s.w.org/>
<http://s019.radikal.ru/>
<https://thumbs.dreamstime.com/>
<http://www.96studio.ru/>
<http://www.facebook.com/>
<http://www.google.com/>
<https://www.npu.gov.ua/>
<http://www.twitter.com/>

Hope this is some help.

Rel1k - May 15, 2017, 1:51 am

Lol he already has all this information... I say him without Saw anything that was à CSRF maybe and he gas the exploit for wp

laertisant - May 18, 2017, 11:00 am

sorry for nub... but need help

laertisant - June 5, 2017, 9:47 am

I'm read about this exploit for wp 4.7.4, but i can understand how doing this, what applications for this attack should I use?