Автор:
07.10.14 10:25 -

В [выпусках](#) 4.0.14, 4.2.10, 4.4.5 и 4.5.5 [BugZilla](#) системы для ведения базы данных о устранена опасная [уязвимость](#) [CVE-2014-1572](#)

Проблемы вызвана непониманием особенности разбора повторяющихся параметров в URL - в сл

Например, в случае запроса "index.cgi?realname=JRandomUser&realname=login_name&realname=a

Используя данный метод [сможет](#) [злоумыш](#) создать аккаунты с доступом к закрытым областям BugZilla проек

Вектором атаки может [широко](#) использоваться для доступа к закрытым ... исправлений безопасно

1. [Главная ссылка к новости (http://krebsonsecurity.com/2014/10/bugzi...)](#)
2. [OpenNews: Проект Mozilla объявил о возможной утечке 97 тысяч аккаунтов тестового сервера Bugzilla](#)
3. [OpenNews: Релиз свободной системы отслеживания ошибок Bugzilla 4.0](#)

Тип: Проблемы безопасности
Ключевые слова: [bugzilla](#) , ([найти похожие документы](#))

[1.1](#) , [Гость](#) , 13:50, 07/10/2014 [[ответить](#)] [[смотреть все](#)
[+](#)
[–](#)
:-D красиво!

1.2 , онаним , 14:25, 07/10/2014 [ответить] [смотреть все] [к модератору] + / –
fail. Удивительно, как можно делать столь сильные предположения о типе переменной в динам

1.3 , Аноним , 15:13, 07/10/2014 [ответить] [смотреть все] [к модератору] –1 + / –
http bloodhound apache org ...
весь текст скрыт
[
показать
]

1.4
,
Аноним
, 16:23, 07/10/2014 [
ответить
] [
смотреть все
] [
к модератору
]
–1
+
/
–
В BugZilla устранена опасная уязвимость, позволяющая повысит.....
весь текст скрыт
[
показать
]

2.14
анонимес
^
ответить
смотреть все
к модератору
+
–
знакомые буквы увидел?

1.5 , vitalif , 16:24, 07/10/2014 [ответить] [смотреть все] [к модератору] + / – Я всегда охреневал от людей, которые вообще CGI.pm используют. Его достаточно один раз открыть, чтобы понять, что его писал героиновый наркоман. Эталонный кусок

перл-говнокода.

И Bugzilla сама тоже хороша, я её форк пилю уже лет 5, планомерно говнокод (и CGI.pm тоже, ага) оттуда выкашивая. Хочу допилить и потом опубликовать где-нибудь с намёком на то, что "эй смотрите мазильщики, я тут ваш говнокод немного в чувство привёл"...

2.7 , vitalif , 16:59, 07/10/2014 [^] [ответить] [смотреть все] [к модератору] + / –

Так НЕ надо писать... Надо писать %hash = (key => scalar $cgi->param('key'));

Иначе если передать несколько значений key, то у тебя весь хеш "поедет" - контекст списочный, cgi->param вернёт список всех значений, и часть из них станет ключами, т.к. "=>" - синоним запятой.

А ещё лучше ВООБЩЕ НЕ ЮЗАТЬ $cgi->param - даже если используется CGI.pm, то просто стырить себе куда-нибудь все параметры в виде хеша и хавать их оттуда. Причём $cgi->Vars возвращает криво tie'енный хеш, так что нужно просто в цикле вытаскивать все параметры.

Ну или вообще юзать какой-нибудь PCGI.pm.

3.8 , PavelR , 17:03, 07/10/2014 [^] [ответить смотреть все к модератору + –

Эмм, я как раз и имел ввиду, что так писать не надо, и если так написать - то именно так и схва

В чем кривизна $cgi->Vars(), если это можно в двух словах описать?

4.9 , vitalif , 17:09, 07/10/2014 [^] [ответить смотреть все к модератору +

–
Если у какого-то ключа несколько значений, то в $cgi->Vars значением этого ключа будут прост

5.10 , PavelR , 17:44, 07/10/2014 [^] [ответить смотреть все к модератору + –

ух-ты, прикольно. Спасибо за разъяснение.)

3.13 , vitalif , 19:50, 07/10/2014 [^] [ответить] [смотреть все] [к модератору] + / – А, кстати нет, с PCGI та же хрень - он вообще не умеет хеш значений вернуть...

1.11 , Аноним , 18:20, 07/10/2014 [ответить] [смотреть все] [к модератору] + / – с ам повысил свои привилегии, потом сам же и пофиксил с новыми привилегиями ...
весь текст скрыт
[
показать
]

Ваш комментарий

Read more http://www.opennet.ru/opennews/art.shtml?num=40766