

Forum:[Hack Forums](#)

Thread: [\[Stresser Owners\] Are you using a public source? READ THIS NOW](#)

0x - - August 7, 2014, 1:26 am

Fix your source and secure it!

Every Stresser that's been recently compromised, is because of the exact same vuln that is in the exact same file at the exact spot!

Now, I'm going to tell you how to fix these public known vulns because if not, the SST Section will be cleared out within days.

The most known vuln is in the ticket.php file that most users have including the old ass vDoS source.

Now, find the line that has the following (Or something familiar)

```
Code $SQLGetTickets = $odb -> execute("SELECT * FROM `tickets` WHERE `id` = $id");
```

If you have common sense, you'll see the issue.

You don't see it? You're going straight into a query with a un-sanitize variable.

The whole point of using PDO is to avoid sanitizing little stuff like this aka escaping strings like when you're using MySQL.

Now, I don't ever want you to use a query directly, especially if you're inserting data into that query.

Let's do it the proper way

```
Code $SQLGetTickets = $odb -> prepare("SELECT * FROM `tickets` WHERE `id` = :?") -> execute(array(":" => $id));
```

Every single booter who has been compromised, has been compromised because of this exact reason.

Now, I want you all to go into every single file you have and check if you're inserting data into a pdo query directly. If you are, FOR THE LOVE OF GOD GO PREPARE YOUR GOD DAMN PDO QUERY!!!

If you want to have that extra security, just bind it to the data type assigned to it.
With that being said, I'll let you go fix your stuff now.

Understalker - August 7, 2014, 1:27 am

I use PrettyBoot and never had a problem with my shit being compromised.

PrettyBoot is free and public and is one of the best sources imo.

.Matt - August 7, 2014, 1:28 am

Thanks for releasing this 0x68 - Lazerproducts.net is secured now

0x - - August 7, 2014, 1:28 am

(Aug 7, 2014 01:27 AM)Understalker Wrote: [\[CITE\]](#) I use PrettyBoot and never had a problem with my shit being compromised.

PrettyBoot is free and public and is one of the best sources imo.
imo prettyboot design is awful and overused

Happeh - August 7, 2014, 3:28 am

Nice of you to release this to all your competitors. If you hadn't I'm sure someone would of been exposed then tried to blame it on you.

Nob - August 7, 2014, 3:33 am

Variables are sanitized, sanitized and over-sanitized on my different sources.
No hack whatsoever. Except when one admin got compromised. But that was all.

0x - - August 7, 2014, 3:54 am

(Aug 7, 2014 03:33 AM)Urgo Wrote: [\[CITE\]](#) Variables are sanitized, sanitized and over-sanitized on my different sources.

No hack whatsoever. Except when one admin got compromised. But that was all.

That's why I've tripled the security to access our admin panel.

I'm also working on a customize encryption to store everything in our DB encrypted and decrypt it via well..I'm not sure yet. It's still work in progress but I'll figure something out. This is incase something do happen, our DB Data won't be readable.

SHADOW REALM - August 7, 2014, 5:42 am

(Aug 7, 2014 03:54 AM)0x68 Wrote: [\[CITE\]](#) That's why I've tripled the security to access our admin panel.

I'm also working on a customize encryption to store everything in our DB encrypted and decrypt it via well..I'm not sure yet. It's still work in progress but I'll figure something out. This is incase something do happen, our DB Data won't be readable.

"I'm also working on a customize encryption"

I would start with learning English