

Forum:[Hack Forums](#)

Thread: [Need Explaining With Specific Exploit Terminology](#)

D0lche - August 3, 2022, 5:44 am

Hi,

I was looking at the Azorult 3.3.1 SQLi exploit and I would appreciate if someone can explain me what does guid mean in this content. Also it says that I can retrieve the guid and key from the sample but since I dont understand what guid is I dont know where to look (ex: Memory dump, Regkeys, strings etc...)

```
Code import requests
import argparse
import base64
```

```
# Azorult 3.3.1 C2 SQLi by prsecurity
# For research purposes only. Don't pwn what you don't own.
# change GUID and XOR key to specific beacon, can be extracted from a sample
```

```
guid =
"353E77DF-928B-4941-A631-512662F0785A3061-4E40-BBC2-3A27F641D32B-54FF-44D7-85F3-
D950F519F12F353E77DF-928B-4941-A631-512662F0785A3061-4E40-BBC2-3A27F641D32B-54F
F-44D7-85F3-D950F519F12F"
key = "\x03\x55\xae"
```

```
def get_args():
    parser = argparse.ArgumentParser(
        prog="azorult_splloit.py",
        formatter_class=lambda prog: argparse.HelpFormatter(prog, max_help_position=50),
        epilog= """
        This script will exploit the SQL vulnerability in Azorult 3.3.1 Dashboard.
        """)
    parser.add_argument("target", help="URL of index.php (ex: hxxp://target.com/index.php)")
    parser.add_argument("-n", "--id_record", default="1", help="id of record to dump")
    parser.add_argument("-p", "--proxy", default="hxxp://localhost:8080", help="Configure a proxy in
the format hxxp://127.0.0.1:8080/ (default = tor)")
    args = parser.parse_args()
    return args
```

Thanks

MoistBoi - August 3, 2022, 8:14 pm

(Aug 3, 2022 05:44 AM)D0lche Wrote: [\[CITE\]](#) Hi,

I was looking at the Azorult 3.3.1 SQLi exploit and I would appreciate if someone can explain me what does guid mean in this content. Also it says that I can retrieve the guid and key from the sample but since I dont understand what guid is I dont know where to look (ex: Memory dump, Regkeys, strings etc...)

```
Code import requests
import argparse
import base64
```

```
# Azorult 3.3.1 C2 SQLi by prsecurity
# For research purposes only. Don't pwn what you don't own.
# change GUID and XOR key to specific beacon, can be extracted from a sample
```

```
guid =
"353E77DF-928B-4941-A631-512662F0785A3061-4E40-BBC2-3A27F641D32B-54FF-44D7-85F3-
D950F519F12F353E77DF-928B-4941-A631-512662F0785A3061-4E40-BBC2-3A27F641D32B-54F
F-44D7-85F3-D950F519F12F"
key = "\x03\x55\xae"
```

```
def get_args():
    parser = argparse.ArgumentParser(
        prog="azorult_sploit.py",
        formatter_class=lambda prog: argparse.HelpFormatter(prog, max_help_position=50),
        epilog= """
        This script will exploit the SQL vulnerability in Azorult 3.3.1 Dashboard.
        """)
    parser.add_argument("target", help="URL of index.php (ex: hxxp://target.com/index.php)")
    parser.add_argument("-n", "--id_record", default="1", help="id of record to dump")
    parser.add_argument("-p", "--proxy", default="hxxp://localhost:8080", help="Configure a proxy in
the format hxxp://127.0.0.1:8080/ (default = tor)")
    args = parser.parse_args()
    return args
```

Thanks
I would also like to know.