

Forum:[Hack Forums](#)

Thread: [Mossad Challenge 2018](#)

sean.svg - April 18, 2018, 10:20 am

www dot r-u-ready dot xyz

Good luck ?

sorry guys i can't post url :(
dot = .

adv-it - April 18, 2018, 11:56 am

It's 16 lines of "morse code" in each column, two columns of code with 17 symbols.
Not sure if it's morse code.

-Elusive- - April 18, 2018, 12:15 pm

It's brainfuck but I don't want to spend the time to type it out.

<https://copy.sh/brainfuck/>

adv-it - April 18, 2018, 1:14 pm

First Column say: xor-with-key

Second Column store decimal list [122, 179, 92, 83, 85, 89, 3, 90, 65, 3, 6, 1]

Key probably: Israel-is-70, as decimal list [73, 115, 114, 97, 101, 108, 45, 105, 115, 45, 55, 48]

XOR Second Column to Key, results in ASCII: 3_2_5.32.11 where _ is unprintable symbol.

So probably IP address of challenge is: 3x.2x5.32.11 I scanned all possible X and only 34.215.32.11 replied, which is wrong address.

I resolved it, recorder how to find solution , look on my Youtube channel look for: ADV-IT

After finding correct IP address you will see this:

Challenge #1

Welcome back Agent C!

Your help is needed once again to solve an urgent matter.

Our digital forensics division is trying to track the source of a phishing attack on one of our government officials.

We have found an email which seems to be related to this attempt and points to a news blog.

We require your skills to track the source of this sophisticated attack.

The following link leads to the news blog.

Good luck!,
M.]

* This challenge relies on browser cookies and javascript. Please make sure scripting and cookies are enabled in your browser before you begin.

sean.svg - April 19, 2018, 1:01 am

(Apr 18, 2018 01:14 PM)adv-it Wrote: [\[CITE\]](#) First Column say: xor-with-key
Second Column store decimal list [122, 179, 92, 83, 85, 89, 3, 90, 65, 3, 6, 1]
Key probably: Israel-is-70, as decimal list [73, 115, 114, 97, 101, 108, 45, 105, 115, 45, 55, 48]
XOR Second Column to Key, results in ASCII: 3_2_5.32.11 where _ is unprintable symbol.
So probably IP address of challenge is: 3x.2x5.32.11 I scanned all possible X and only
34.215.32.11 replied, which is wrong address.
I resolved it, recorder how to find solution , look on my Youtube channel look for: ADV-IT

After finding correct IP address you will see this:

Challenge #1

Welcome back Agent C!

Your help is needed once again to solve an urgent matter.

Our digital forensics division is trying to track the source of a phishing attack on one of our government officials.

We have found an email which seems to be related to this attempt and points to a news blog.

We require your skills to track the source of this sophisticated attack.

The following link leads to the news blog.

Good luck!,
M.]

* This challenge relies on browser cookies and javascript. Please make sure scripting and cookies are enabled in your browser before you begin.

This is 35.205.32.11 and no 34.215.32.11

adv-it - April 19, 2018, 9:08 am

(Apr 19, 2018 01:01 AM)sean.svg Wrote: [\[CITE\]](#) This is 35.205.32.11 and no 34.215.32.11
I know...

I have posted Video recording of Entry Challenge Solution on youtube, but cannot add link here.
Look for ADV-IT Channel in YouTube, video called Mossad Challenge 2018 - Entry Solution

adv-it - April 20, 2018, 10:22 am

For Challenge#1,

User Anonymous message include script [authstealer_exploit.js]

UserDEP-ricate has clue like Hash [48614861486121]

And TECH topic has clue regarding type of Attack "pass-through"

Also Uploading image while registration can manage something in Cookies.

By the way I able to register as Anonymous user, looks like registration is Phishing kind.

ThomasGB - April 20, 2018, 10:35 am

(Apr 18, 2018 01:14 PM)adv-it Wrote: [\[CITE\]](#) First Column say: xor-with-key

Second Column store decimal list [122, 179, 92, 83, 85, 89, 3, 90, 65, 3, 6, 1]

Key probably: Israel-is-70, as decimal list [73, 115, 114, 97, 101, 108, 45, 105, 115, 45, 55, 48]

XOR Second Column to Key, results in ASCII: 3_2_5.32.11 where _ is unprintable symbol.

So probably IP address of challenge is: 3x.2x5.32.11 I scanned all possible X and only
34.215.32.11 replied, which is wrong address.

I resolved it, recorder how to find solution , look on my Youtube channel look for: ADV-IT

After finding correct IP address you will see this:

Challenge #1

Welcome back Agent C!

Your help is needed once again to solve an urgent matter.

Our digital forensics division is trying to track the source of a phishing attack on one of our government officials.

We have found an email which seems to be related to this attempt and points to a news blog. We require your skills to track the source of this sophisticated attack.

The following link leads to the news blog.

Good luck!,
M.]

* This challenge relies on browser cookies and javascript. Please make sure scripting and cookies are enabled in your browser before you begin.

Nice job , I didn't knew brain fuck lang before

mapux - April 20, 2018, 2:33 pm

(Apr 20, 2018 10:22 AM)adv-it Wrote: [\[CITE\]](#) For Challenge#1,

User Anonymous message include script [authstealer_exploit.js]

UserDEP-ricate has clue like Hash [48614861486121]

And TECH topic has clue regarding type of Attack "pass-through"

Also Uploading image while registration can manage something in Cookies.

By the way I able to register as Anonymous user, looks like registration is Phishing kind.

48614861486121 in hex => HaHaHa!

adv-it - April 20, 2018, 10:57 pm

As I see secret function is on Register page: h t t

p://35_205_32_11/testProfilePng?u=JSONCODEFROMYOURPNGFILE

When you upload PNG file, system creating "JSONCODE", this code tested by testProfilePng function.

For example:

h t t p://35_205_32_11/testProfilePng?u=aHR0cDovL2FzdGFob3YubmV0L2F0aGxldGUucG5n

Result:

```
{
  "err": "200",
  "png": "4e78646f12204d78b9efc6dd2081140a",
  "session": "Cookie saved: False"
}
```

Secret is here 100%, we need to provide some PNG file to generate correct JSON code for this Function, function will return key.

karkamel - April 21, 2018, 3:57 am

(Apr 20, 2018 10:57 PM)adv-it Wrote: [\[CITE\]](#) As I see secret function is on Register page: h t t

p://35_205_32_11/testProfilePng?u=JSONCODEFROMYOURPNGFILE

When you upload PNG file, system creating "JSONCODE", this code tested by testProfilePng function.

For example:

h t t p://35_205_32_11/testProfilePng?u=aHR0cDovL2FzdGFob3YubmV0L2F0aGxldGUucG5n

Result:

```
{
  "err": "200",
  "png": "4e78646f12204d78b9efc6dd2081140a",
  "session": "Cookie saved: False"
}
```

Secret is here 100%, we need to provide some PNG file to generate correct JSON code for this Function, function will return key.

you need to ssrf with that code file from the server. it's pretty simple.

adv-it - April 21, 2018, 12:22 pm

(Apr 21, 2018 03:57 AM)karkamel Wrote: [\[CITE\]](#) you need to ssrf with that code file from the server. it's pretty simple.

I'am able to download login.php and register.php sources code.

In login.php you can see than Admin user not using password, it using localhost ip

```
define("ADMIN_USER_NAME", "admin");
if ($remote_ip == "127.0.0.1" && $user == ADMIN_USER_NAME)
{
// local admin requires no validation
// generate session ID
$adminSession = create_session($user, null);
Challenge #2
Well done Agent!
```

Thanks to your efforts, our team has managed to locate and detain one of the hackers responsible. She was not cooperative, but we were able to extract a snippet of an application from her phone. We suspect it is used for gathering intelligence from their victims.

Your next mission is to locate the files the team stole following their successful phishing attack.

We executed the parts we extracted in a sandbox and managed to capture its initial communication with a c&c server. The following pcap file contains the captured data.

Needless to say, the information that was stolen is very valuable to us, so please do your best to retrieve it before it leaks...

Good luck!,
M.

karkamel - April 22, 2018, 5:01 am

(Apr 21, 2018 12:22 PM)adv-it Wrote: [\[CITE\]](#) I'am able to download login.php and register.php sources code.

In login.php you can see than Admin user not using password, it using localhost ip

```
define("ADMIN_USER_NAME", "admin");
if ($remote_ip == "127.0.0.1" && $user == ADMIN_USER_NAME)
{
// local admin requires no validation
// generate session ID
$adminSession = create_session($user, null);
Challenge #2
Well done Agent!
```

Thanks to your efforts, our team has managed to locate and detain one of the hackers responsible. She was not cooperative, but we were able to extract a snippet of an application from her phone. We suspect it is used for gathering intelligence from their victims. Your next mission is to locate the files the team stole following their successful phishing attack.

We executed the parts we extracted in a sandbox and managed to capture its initial communication with a c&c server. The following pcap file contains the captured data.

Needless to say, the information that was stolen is very valuable to us, so please do your best to retrieve it before it leaks...

Good luck!,
M.

you can actually download more files than these 2 you did.
for the pcap you can use wireshark.
btw if you want my mail is: f34flk34klfm@gmail.com

SI0thmachine - April 22, 2018, 7:32 am

(Apr 21, 2018 12:22 PM)adv-it Wrote: [\[CITE\]](#) I'am able to download login.php and register.php sources code.

In login.php you can see than Admin user not using password, it using localhost ip

```
define("ADMIN_USER_NAME", "admin");
if ($remote_ip == "127.0.0.1" && $user == ADMIN_USER_NAME)
{
// local admin requires no validation
// generate session ID
$adminSession = create_session($user, null);
Challenge #2
Well done Agent!
```

Thanks to your efforts, our team has managed to locate and detain one of the hackers responsible. She was not cooperative, but we were able to extract a snippet of an application from her phone. We suspect it is used for gathering intelligence from their victims. Your next mission is to locate the files the team stole following their successful phishing attack.

We executed the parts we extracted in a sandbox and managed to capture its initial communication with a c&c server. The following pcap file contains the captured data.

Needless to say, the information that was stolen is very valuable to us, so please do your best to retrieve it before it leaks...

Good luck!,
M.

I downloaded a bunch of files from the server as well as the login but can't seem to find any way to login as admin. How do you get the admin cookie? Where are they stored?

HFDone - April 22, 2018, 7:53 am

you run it on localhost and you get the cookie

SI0thmachine - April 22, 2018, 8:04 am

(Apr 22, 2018 07:53 AM)HFDone Wrote: [\[CITE\]](#) you run it on localhost and you get the cookie

How would I go about doing that?

Sorry for the ignorance just trying to learn hehe