

Forum:[Hack Forums](#)

Thread: [How would I go about defacing this site?](#)

mdt3ch - May 31, 2015, 8:22 am

I have read about xss, rfi, fli, and sqli for website defacing.

However, I want to learn how to analyze a site and figure out the way to deface it

,case in point

sscrmn1.edu.ph

All the other tuts teach you how to search in Google dorks for sites. I want to pick the site and find angles to approach after analyzing how to deface it. Any help will be much appreciated.

Jason Stattham - May 31, 2015, 8:23 am

It's a .edu site, better keep off your hands before the feds knock at your door.

x4151rch - June 1, 2015, 6:57 am

Pinoy ka rin ba? Pm me, we will discuss things in private. :)

srory20wnu - June 1, 2015, 9:12 am

(Jun 1, 2015 06:57 AM)x4151rch Wrote: [\[CITE\]](#) Pinoy ka rin ba? Pm me, we will discuss things in private. :)

Yeah, get some uneducated kid arrested. Cool. ?

Abhax - June 1, 2015, 9:14 am

I wouldn't recommend defacing a .edu site, If you do you're going to have a bad time.

x4151rch - June 1, 2015, 9:11 pm

(Jun 1, 2015 09:12 AM)srory20wnu Wrote: [\[CITE\]](#) Yeah, get some uneducated kid arrested. Cool. ?
I'm also with you guys, I also don't recommend defacing (I have several shelled sites, on different servers, and none of them were defaced), especially on a .edu site ?. I just actually want to discuss some things with him as his target was the site of the school where I also attended ?

Gee4rce - June 2, 2015, 2:13 am

I could help OP out by linking him to what he is looking for, but i won't.

Reason: i don't like the idea of random defacements.

I wish OP no good luck with this, Bye.

R00t M4st3r - June 2, 2015, 2:02 pm

sscrmn1.edu.ph/?s=<try different xss vulnerability> Scan with acunetix for a list of known vulns.

D3xH3x - June 2, 2015, 2:11 pm

(Jun 2, 2015 02:13 AM)Gee4rce Wrote: [\[CITE\]](#) I could help OP out by linking him to what he is looking for, but i won't.

Reason: i don't like the idea of random defacements.

I wish OP no good luck with this, Bye.

Indeed. Why not try your new skills out on DVWA

WubCannon - June 2, 2015, 2:26 pm

(Jun 2, 2015 02:02 PM)R00t M4st3r Wrote: [\[CITE\]](#) sscrml.edu.ph/?s=<try different xss vulnerability>
Scan with acunetix for a list of known vulns.
wow, pls tech me ur ways mastur hecker

Th3PonyWizard - June 3, 2015, 12:52 am

(Jun 2, 2015 02:02 PM)R00t M4st3r Wrote: [\[CITE\]](#) sscrml.edu.ph/?s=<try different xss vulnerability>
Scan with acunetix for a list of known vulns.every time acunetix is recommended another kitten commits suicide

R00t M4st3r - June 3, 2015, 12:31 pm

(Jun 3, 2015 12:52 AM)Th3PonyWizard Wrote: [\[CITE\]](#) every time acunetix is recommended another kitten commits suicide

Although I agree sometimes Acunetix is not the best vulnerability scanner out there. However, it does pick up a good majority of corrupt code. You also have to worry about Acunetix reporting false positives. However, Acunetix is a fairly good web scanner out there to gather information on a target. They have default presets, you may need to enter your own code.

UnParad0x - June 3, 2015, 12:33 pm

.edu = jail time plus being monitored and logged for the rest of your life

R00t M4st3r - June 3, 2015, 12:35 pm

(May 31, 2015 08:22 AM)mdt3ch Wrote: [\[CITE\]](#) I have read about xss, rfi, fli, and sqli for website defacing.

However, I want to learn how to analyze a site and figure out the way to deface it

,case in point

sscrml.edu.ph

All the other tuts teach you how to search in Google dorks for sites. I want to pick the site and find angles to approach after analyzing how to deface it. Any help will be much appreciated.

Try some of these tools:

mediafire.com/folder/yb3fy22w4dvrr/Security_Tools

Site Admin Login:

sscrml.edu.ph/wp-login.php?redirect_to=http%3A%2F%2Fsscrml.edu.ph%2Fwp-admin%2F&reauth=1

WubCannon - June 3, 2015, 1:18 pm

(Jun 3, 2015 12:31 PM)R00t M4st3r Wrote: [\[CITE\]](#) Although I agree sometimes Acunetix is not the best vulnerability scanner out there. However, it does pick up a good majority of corrupt code. You also have to worry about Acunetix reporting false positives. However, Acunetix is a fairly good web scanner out there to gather information on a target. They have default presets, you may need to enter your own code.

It also stands out like a clown in a synagogue in webserver logs. Its pretty much the best way to get the server admins attention aside from sending him an email saying "hai can i heck ur server pl0x"

R00t M4st3r - June 3, 2015, 3:52 pm

(Jun 3, 2015 01:18 PM)WubCannon Wrote: [\[CITE\]](#) It also stands out like a clown in a synagogue in webserver logs. Its pretty much the best way to get the server admins attention aside from sending

him an email saying "hai can i heck ur server pl0x"

There server also doesn't support proxy blocking. So, even though your basically knocking on the door, you can knock on the door, using different people.

s27.postimg.org/zfwd4l3jn/Untitled.png

sscrm.pinnacle.com.ph/sansebastian/students/index.php

Btw, it has a SQL injection vulnerability.

WubCannon - June 3, 2015, 6:08 pm

(Jun 3, 2015 03:52 PM)R00t M4st3r Wrote: [\[CITE\]](#) There server also doesn't support proxy blocking. So, even though your basically knocking on the door, you can knock on the door, using different people.

s27.postimg.org/zfwd4l3jn/Untitled.png

sscrm.pinnacle.com.ph/sansebastian/students/index.php

Btw, it has a SQL injection vulnerability.

its not all about bruting your way in. Most likely OP wants to change his grades or hack his school. As soon as an admin checks the logs they are going to know something is up.

ret20 - June 3, 2015, 6:24 pm

(Jun 3, 2015 12:33 PM)UnParad0x Wrote: [\[CITE\]](#) .edu = jail time plus being monitored and logged for the rest of your life

this is a bit of a ridiculous claim to make

ProblemSolva - June 4, 2015, 1:09 am

(Jun 3, 2015 03:52 PM)R00t M4st3r Wrote: [\[CITE\]](#) There server also doesn't support proxy blocking. So, even though your basically knocking on the door, you can knock on the door, using different people.

s27.postimg.org/zfwd4l3jn/Untitled.png

sscrm.pinnacle.com.ph/sansebastian/students/index.php

Btw, it has a SQL injection vulnerability.

Haha its funny that you found, this sql vuln through an xss injection happened to me, in alot of situations aswell.

Nice find :)

Rilit - June 4, 2015, 1:13 am

After few days you post a thread "What i do, Police took my PC". lol

R00t M4st3r - June 4, 2015, 12:45 pm

(Jun 4, 2015 01:13 AM)Rilit Wrote: [\[CITE\]](#) After few days you post a thread "What i do, Police took my PC". lol

Police actually need a warrant to take your belongings. Even if there on your person. Time they get the warrant. You can break your computer, reformat your hard drive. Encrypt your data. There's tools where they can go back and unscramble the reformatted data and see what you been doing. But who cares haha most of the time if you are smart about it you won't get caught.

WubCannon - June 4, 2015, 8:09 pm

(Jun 4, 2015 12:45 PM)R00t M4st3r Wrote: [\[CITE\]](#) Police actually need a warrant to take your belongings. Even if there on your person. Time they get the warrant. You can break your computer, reformat your hard drive. Encrypt your data. There's tools where they can go back and unscramble the reformatted data and see what you been doing. But who cares haha most of the time if you are smart about it you won't get caught.

> need a warrent
> noshit.jpg

> break RAM
> dissassemble hard drive + use magnets, hammer, flames as well as AES 256bit encryption.
> they can still go back and 'usncramble the data'
> unscramble

pls.

Th3PonyWizard - June 5, 2015, 6:21 am

(Jun 4, 2015 08:09 PM)WubCannon Wrote: [\[CITE\]](#) > need a warrent
> noshit.jpg

> break RAM
> dissassemble hard drive + use magnets, hammer, flames as well as AES 256bit encryption.
> they can still go back and 'usncramble the data'
> unscramble

pls.RAM is a volatile storage unit. Completely erasing it is as simple as plugging it off.

WubCannon - June 5, 2015, 9:24 am

(Jun 5, 2015 06:21 AM)Th3PonyWizard Wrote: [\[CITE\]](#) RAM is a volatile storage unit. Completely erasing it is as simple as plugging it off.

Everyone knows you can perform coldboot attack on DRAM and SRAM. If the police are going to raid your house for a computer crime, they will either ensure the computer is kept on, or perform a rapid coldboot attack, with some RAM models being susseptible to this attack for upto several hours if the system is cooled, but even upto 2 minuites on DDR2

Paul Wilson - June 5, 2015, 5:22 pm

(Jun 4, 2015 12:45 PM)R00t M4st3r Wrote: [\[CITE\]](#) Police actually need a warrant to take your belongings. Even if there on your person. Time they get the warrant. You can break your computer, reformat your hard drive. Encrypt your data. There's tools where they can go back and unscramble the reformatted data and see what you been doing. But who cares haha most of the time if you are smart about it you won't get caught.

OK but even if you can remove the evidence, how do you know that the police are trying to get a warrant? They don't exactly send you a letter saying "We are trying to get a warrant to raid your place for computer related crimes so please be a good boy and dont destroy your evidence, thanks :)"

WubCannon - June 6, 2015, 11:24 am

(Jun 5, 2015 05:22 PM)MishaTheHoovy Wrote: [\[CITE\]](#) OK but even if you can remove the evidence, how do you know that the police are trying to get a warrant? They don't exactly send you a letter saying "We are trying to get a warrant to raid your place for computer related crimes so please be a good boy and dont destroy your evidence, thanks :)"

No, you just have to tighten your opsec. Using an os like tails, booted off a USB, in a cheap laptop with the harddrives taken out, and then attaching the USB to your person via string or cord, so that if the feds do bust in, all it takes is for you to walk away from that laptop, possibly break the RAM if needbe, and your in the clear. However, if they execute the warrant during the day, and you've left your computer in sleep mode or a similar state, all the encryption in the world can't help you, as it can be bypassed using certain methods

Th3PonyWizard - June 6, 2015, 11:37 am

(Jun 5, 2015 09:24 AM)WubCannon Wrote: [\[CITE\]](#) Everyone knows you can perform coldboot attack on DRAM and SRAM. If the police are going to raid your house for a computer crime, they will either ensure the computer is kept on, or perform a rapid coldboot attack, with some RAM models being susceptible to this attack for upto several hours if the system is cooled, but even upto 2 minutes on DDR2am going to ask for u to back dat up

[5:58:44 PM] Starfall: RAM is volatile, but it does have capacitance

[5:58:44 PM] Starfall: it will hold data for a few seconds when unpowered

[6:33:10 PM] Sonder: so few seconds

[6:33:14 PM] Sonder: ok

WubCannon - June 6, 2015, 1:41 pm

(Jun 6, 2015 11:37 AM)Th3PonyWizard Wrote: [\[CITE\]](#) am going to ask for u to back dat up

[5:58:44 PM] Starfall: RAM is volatile, but it does have capacitance

[5:58:44 PM] Starfall: it will hold data for a few seconds when unpowered

[6:33:10 PM] Sonder: so few seconds

[6:33:14 PM] Sonder: okLel, we can always rely on aurora. How is he? Haven't spoken to him for ages ?

The research paper was from Princeton, i cannot post links due to my account restrictions, feel free to pm me your Skype/email and I'll send you the link, however im sure results can be yeilded from a Google search of 'Princeton coldboot attack research paper'