

Forum:[Hack Forums](#)

Thread: [Vulnerability, Web application analysis Crew](#)

KillerSavage - May 12, 2017, 3:55 pm

I find my self enjoying how the Internet works and how vulnerabilities work. I my self is a start at this but I have a few knowledge in some aspects of vulnerabilities and web app analysis.

My all in one KIT is Kali linux.

Spoiler ([Click to View](#))

XSS

Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-supplied code into a user's browser instance. A browser instance can be a standard web browser client, or a browser object embedded in a software product such as the browser within WinAmp, an RSS reader, or an email client. The code itself is usually written in HTML/JavaScript, but may also extend to VBScript, ActiveX, Java, Flash, or any other browser-supported technology.

When an attacker gets a user's browser to execute his/her code, the code will run within the security context (or zone) of the hosting web site. With this level of privilege, the code has the ability to read, modify and transmit any sensitive data accessible by the browser. A Cross-site Scripted user could have his/her account hijacked (cookie theft), their browser redirected to another location, or possibly shown fraudulent content delivered by the web site they are visiting. Cross-site Scripting attacks essentially compromise the trust relationship between a user and the web site. Applications utilizing browser object instances which load content from the file system may execute code under the local machine zone allowing for system compromise.

There are three types of Cross-site Scripting attacks: non-persistent, persistent and DOM-based. Non-persistent attacks and DOM-based attacks require a user to either visit a specially crafted link laced with malicious code, or visit a malicious web page containing a web form, which when posted to the vulnerable site, will mount the attack. Using a malicious form will oftentimes take place when the vulnerable resource only accepts HTTP POST requests. In such a case, the form can be submitted automatically, without the victim's knowledge (e.g. by using JavaScript). Upon clicking on the malicious link or submitting the malicious form, the XSS payload will get echoed back and will get interpreted by the user's browser and execute. Another technique to send almost arbitrary requests (GET and POST) is by using an embedded client, such as Adobe Flash.

Persistent attacks occur when the malicious code is submitted to a web site where it's stored for a period of time. Examples of an attacker's favorite targets often include message board posts, web mail messages, and web chat software. The unsuspecting user is not required to interact with any additional site/link (e.g. an attacker site or a malicious link sent via email), just simply view the web page containing the code.[]

SQL INJECT

SQL Injection is a code injection technique, used to attack data-driven applications, in which nefarious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker).

And many more to this.

I will be using discord as the main chat because I am booting Kali from a flash drive.

Code Age:

Any experience with Vulnerability and Web application analysis:

Rate your self out of 10:

PS: We are doing this for good and we can report this to site owners and simply make some profit or something beneficial.

LMK guys

McDolands - May 12, 2017, 5:00 pm

Age: 13

Any experience with Vulnerability and Web application analysis: All of it

Rate your self out of 10: 10

KillerSavage - May 12, 2017, 5:39 pm

(May 12, 2017 05:00 PM)McDolands Wrote: [\[CITE\]](#) Age: 13

Any experience with Vulnerability and Web application analysis: All of it

Rate your self out of 10: 10

NA bro am actually serious about this group.

Psynsay - May 13, 2017, 2:32 am

I attempted to form a group like this a while back, i was in a couple too..

That being said my knowledge needs a refresher, but i would be willing to join.

I dont understand why people treat groups so non-seriously.

Age: Can be discussed later, not a kid though.

Any experience with Vulnerability and Web application analysis: Vulnerability meaning only web API, or ?, in case you mean besides web API, then a strong yes, otherwise a weak yes.

Rate your self out of 10: 7, i knew people who were 10's and they do not exist on any forum I know of.

Rock™ - May 13, 2017, 2:59 am

Age: 14

Any experience with Vulnerability and Web application analysis: I was the first person to hack the Nintendo switch web based. I have a fair knowledge about autoexecute exe and any downloaded file In JavaScript.

Rate your self out of 10: 8

Faith Connors - May 13, 2017, 8:18 pm

>screenshot with terminal

>no neofetch

>not even screenfetch

>base kali de and theme

This is a weird looking desktop thread?

Brill - May 13, 2017, 8:24 pm

why did you just copy paste from this

<http://projects.webappsec.org/w/page/13246920/Cross%20Site%20Scripting>

rofl

(May 13, 2017 02:59 AM)Rock™ Wrote: [\[CITE\]](#) Age: 14

I have a fair knowledge about autoexecute exe and any downloaded file In JavaScript.

Rate your self out of 10: 8

what

gitclone - May 14, 2017, 1:05 am

(May 13, 2017 08:18 PM)Faith Connors Wrote: [\[CITE\]](#) >screenshot with terminal

>no neofetch

>not even screenfetch

>base kali de and theme

This is a weird looking desktop thread?

Just what I thought.

Haven't even changed name.

And what's there on background?

Automated tool! (Doesn't surprise)

Ninja - May 14, 2017, 8:30 am

Why is age relevant? I met 12 year olds that acted more mature and knew more than 18 year olds and vice versa.

ConfusionG - May 14, 2017, 9:52 am

Age: 15

Any experience with Vulnerability and Web application analysis: i think enough

Rate your self out of 10: 6,5