

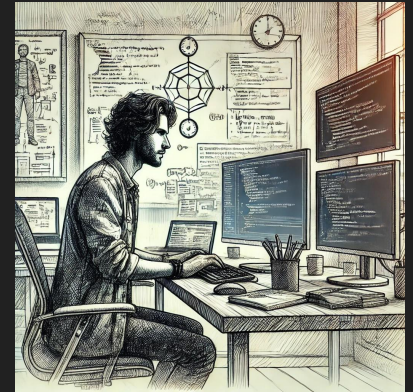
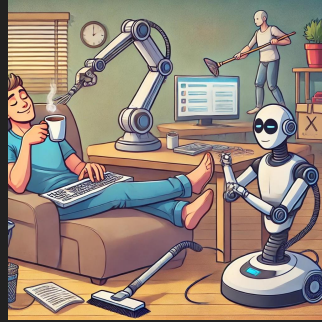


Hack.lu lightning talk

Cyrus - The story of no cloud

Cyrus stands for “Automated CYbeR secUrity teSting for Cyber Physical System”

Guessing this could be a CTF flag!



What we did ?

Scientific Paper

• Comparison of radiotherapy alone with radiotherapy plus hyperthermia in locally advanced pelvic tumours: a prospective randomised, multicentre trial

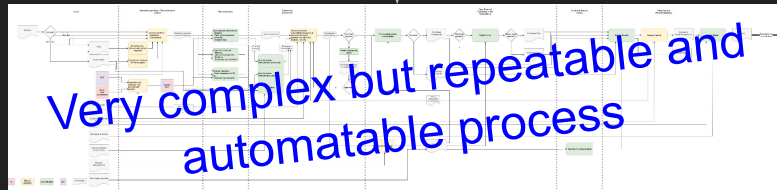
van der Lee J, Gonzalez Gonzalez D, van Nieuw GC, van Dijk JB, van Nieuw W, et al. *Radiotherapy plus Hyperthermia: Academic Medical Centre, Amsterdam, the Netherlands*

Background: Local-control rates after radiotherapy for locally advanced tumours of the bladder, cervix, and rectum are disappointing. We investigated the effect of adding hyperthermia to standard radiotherapy.

Methods: The study was a prospective, randomised, multicentre trial. 338 patients were enrolled from 1990 to 1998, in cancer centres in the Netherlands, who had bladder cancer stages T3, T4, N0, M0, cervical cancer stages IB, IIB, or II, or anal cancer stage M0-I were assessed. Patients were randomly assigned radiotherapy (median total dose 67 Gy) alone (n=164), or radiotherapy plus hyperthermia (n=182). Our primary endpoints were complete response and duration of local control. We did the analysis by intention to treat.


Findings: Complete response rates were 37% after radiotherapy and 53% after radiotherapy plus hyperthermia (p<0.001); the duration of local control was significantly longer with radiotherapy plus hyperthermia than with radiotherapy alone (p=0.04). Treatment effect did not differ significantly by tumour site, but the duration of hyperthermia seemed to be most important for cervical cancer, for which the complete-response rate with radiotherapy plus hyperthermia was 67% compared with 47% after radiotherapy alone (p=0.003). 3-year overall survival was 37% in the radiotherapy group and 31% in the radiotherapy plus hyperthermia group. For bladder cancer, an initial difference in local control disappeared during follow-up.

radiotherapy plus hyperthermia



That's not the end





Cyrus

Display menu

- Dashboard
 - Inputs
 - SUT
 - Add SUT
 - Add version
 - Asset
 - Add asset
 - Risk analysis
 - Add risk analysis
 - Add risk
 - Reconnaissance
 - Flow
 - Add flow
 - Flow execution
 - Test process
 - Vulnerability
 - Add vulnerability
 - Penetration tests
 - Test case
 - Add test case
 - Results
 - My account
 - Log out

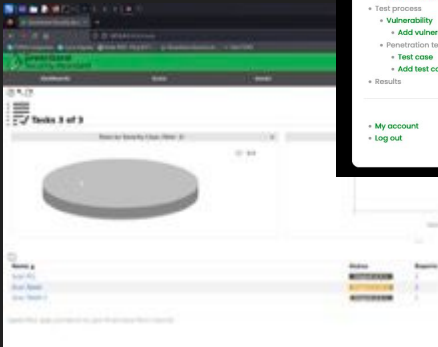
Welcome to the Crescendo project

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

SUT list

Demonstrator_4.0



Test Report Demonstrator_4.0

Vulnerability Name	Description	Asset Name	CVE	CWE	Test Name
Exploitable Service	Apache System-Package version 2.0.17 (http://www.apache.org/dist/httpd/httpd-2.0.17.tar.gz) has a remote denial of service (DoS) vulnerability.	Service Name	CVE-2017-15389	CWE-352	DoS

4.2 Tests result

This chapter present the results of the tests performed on the SUT. For each test, it provides the description of the test, the date when the test was executed, the results of the test and the global result. By convention, the test is passed if the vulnerability cannot be exploited as this is considered a positive result. A test with the error status means that the test had a problem in its execution.

Vulnerability Name	Description	Execution Date	Result	Comments
Dirve EDCU_SHELL	Save file to SUT, shell is active and use this path: /tmp/EDCU_SHELL	2019/4/08/13	PASSED	Folder not vulnerable to shell access.
Dirve DDI	Save file to SUT, shell is active and use this path: /tmp/DDI	2019/4/08/17	PASSED	Not vulnerable.
IPCLM DDoS	Send a DoS (IA) to the SUT path: /tmp/DoS	2019/4/08/17	ERROR	Not vulnerable. Need to find another way to do a DoS attack.
PLC DDoS	This security test send a DoS (IA) to the SUT path: /tmp/DoS	2019/4/08/16	PASSED	Not vulnerable to DoS attack.
IP passed password	Send a password to the SUT path: /tmp/passwd	2019/4/08/20	FAILED	Not vulnerable to DoS attack. The password is correct in the SUT. The password is 'admin'.
IP passed password	The test connect and login to the SUT path: /tmp/passwd	2019/4/08/20	FAILED	By using Cyber, we found on the SUT a vulnerability for password cracking. The test was successful. The password is 'admin'.

Want to know more?

Come speak with us

We are researchers from the CETIC, a research center in Belgium

Go on <https://www.cetic.be/Blog-en>

Stay tuned for the next steps...

