Project WAS

2021

Report: deadline 15/10 at midnight

- Each report should be authored by 3 persons. Exchange of code/exploits among other groups would violate the rules for this project.
- Report should contain 17 pages in total to describe all the requested programs (without bonus programs).
- For the first page: Add your names, emails, and also a table with 16 rows and 6 columns summarizing the vulnerability you have succeed in finishing. Columns should be name : vulnerable code, **exploit**, defense code. Rows should have the name/kind of vulnerability.
- For the other 16 pages: each page should start by the title of the vulnerability (+OWASP link to its description) and contain 3 things: i) a program in php/html with the vulnerability ii) an exploit or "proof of vulnerability" in order to exploit the vulnerability when executing the program (please do try to run the program and exploit the vulnerability before sending the report) iii) a program where the vulnerability is absent due to a defense for example. You can, only if need be, add a small explanation if there anything special to configure before executing your program. Otherwise, no other text is needed for the page.
- Report should be sent by email to tamara.rezk@inria.fr. Subject of email should be

Report #YOURNAME# WAS-20. Email should be sent during Friday 15/10. If a report arrives later there will be a penality in the evaluation.

Report: example of first page with the summary that is requested – Don’t forget to add names of all people in the group in the first page.

ATTACK	LINK	Vulnerable program	Exploit	Defense	PAGE
XSS RULE 0	https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html	YES	YES (BUT IT DOESN’T WORK IN CERTAIN CASES)	NO	2
XSS RULE 1	….	NO	NO	YES	3
XML	https://cheatsheetseries.owasp.org/cheatsheets/XML_External_Entity_Prevention_Cheat_Sheet.html	YES	YES	NO	

Vulnerabilities for the project: implement one program attack, one defense (php+js), 32programs

- https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html (18 programs)
- https://cheatsheetseries.owasp.org/cheatsheets/DOM_based_XSS_Prevention_Cheat_Sheet.html (2 programs)
- https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html (6 programs)
- https://cheatsheetseries.owasp.org/cheatsheets/XML_External_Entity_Prevention_Cheat_Sheet.html (2 programs)
- https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html (2 programs)
- https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html (2 programs)

(see XXE post: https://portswigger.net/web-security/xxe)

Group grade of the 32programs

Each program receives 0.5 points if it is well done according to the owasp rule, if the exploit works, if the report is in the format and describes it as required.

Bonus could be granted if the programs are more elaborated but still follows the OWASP rules.

Bonus programs: If the 32 programs are all correct, the group has the opportunity to obtain 4 further points by studying 4 other cheetsheets and including correct triples (vulnerable program, exploit, protected program)

Individual grade: defense (virtual presentation)

- The presentation is individual
- Teacher chooses one of the pages from your report
- You present the vulnerable program, present the exploit and show its execution (attack), explain the defense, and show the defense code: if the 3 people from the group fail to explain one page of the report, there will be a penality on the group grade
- The presentation will be virtual on the week of 18/10 or later

Organize google document and write each group with an email next to it, and availability for the defense on the week of 18/10,19/10,20/10,21/10 18h or 19h (the whole group should be available for one hour for the defense): examples

Group 1 All dates and times are available.

John Doe john.doe@gmail.com

Anne Sokol anne.sokol@polytech.fr

Thibault Gregory gt@scx.ke

Group 2 18/10 18h and 20/10 19h

John1 Doe john.doe@gmail.com

Anne1 Sokol anne.sokol@polytech.fr

Thibault1 Gregory gt@scx.ke

Group 3 21/10 18h

John Doe john.doe@gmail.com

Anne Sokol anne.sokol@polytech.fr

Thibault Gregory gt@scx.ke

Group 4 No available on the proposed time

John1 Doe john.doe@gmail.com

Anne1 Sokol anne.sokol@polytech.fr

Thibault1 Gregory gt@scx.ke