



# Cyber-Lab.Tech

## Overview of Platform Exercises



</index.php/Tbilisi>



</OWASP-Tbilisi-Chapter>



</OWASP.Tbilisi>

# What is Cyber-Lab.Tech

CYBER-LAB  
T E C H

ჩვენ შესახებ

კონტაქტი

რეგისტრაცია



GEO | ENG



CYBER-LAB  
T E C H

კიბერ-ლაბორატორია

კიბერუსაფრთხოების საკითხებში რეალური დროის დისტანციურად მიღების საშუალება

შესასვლელად მიჰყავით ზგულის



CERT.GOV.GE



EaPConnect  
Eastern Partnership Connect

GRENA  
Georgia Research and Emergency Network  
for Incident Response and Analysis



CYBER-LAB  
T E C H

# Types of Exercises



- Log Analysis
- Malware Analysis
- Reverse Engineering
- PCAP Analysis
- Forensics
- Cyber Hygiene
- Cryptography
- Steganography
- Pentest
- Exploit Development
- Mix

# Exercise: “Stage 1”

LIVE

ამოცანა

0 ამოცანა



STAGE 1

10

პრიმინალურმა პოლიციამ აღმოაჩინა საეჭვო სერვერი, რომელიც ჰაკერების მიერ არის კონტროლირებადი და დაცულია პაროლით. თქვენი მიზანია გამოიხმოთ პაროლი.

STAGE1.ZIP

პასუხი

გაგზავნა

რამოდენიმე პასუხის შემთხვევაში პასუხები გამოყავით სპეისით

# Exercise: “Stage 1”



LIVE

# Exercise: “Stage1-JS”

LIVE

ამოცანა 0 ამოცანა

STAGE1-JS

10

კრიმინალურმა პოლიციამ აღმოაჩინა საეჭვო სერვერი, რომელიც ჰაკერების მიერ არის კონსოლირებადი და დაცულია პაროლით. თქვენი მიზანია გამოიხსნათ პაროლი.

STAGE-1-JS.ZIP

პასუხი

გამგზავნა

რამოდენიმე პასუხის შემთხვევაში პასუხები გამოყავით სპეისით

# Exercise: “Stage1-JS”

LIVE



# Exercise: “Stage2-JS”

LIVE

ამოცანა 0 ამოხსნა

STAGE2-JS

30

პრიმინალურმა პოლიციამ აღმოაჩინა საეჭვო სერვერი, რომელიც  
ჰაკერების მიერ არის კონფოლირებული და დაცულია პაროლით.  
თქვენი მიზანია გამოიხსნათ პაროლი.

STAGE-2-JS.ZIP

პასუხი

გამგზავნა

რამოდენიმე პასუხის შემთხვევაში პასუხები გამოყვებით სპეისით



# Exercise: “Stage2-JS”



LIVE

# Exercise: “Stage3-JS”

LIVE

ამოცანა 0 ამოხსნა

STAGE3-JS

10

კრიმინალურმა პოლიციამ აღმოაჩინა საეჭვო სერვერი, რომელიც ჰაკერების მიერ არის კონსოლირებადი და დაცულია პაროლით. თქვენი მიზანია გამოიხსნოთ პაროლი.

STAGE-3-JS.ZIP

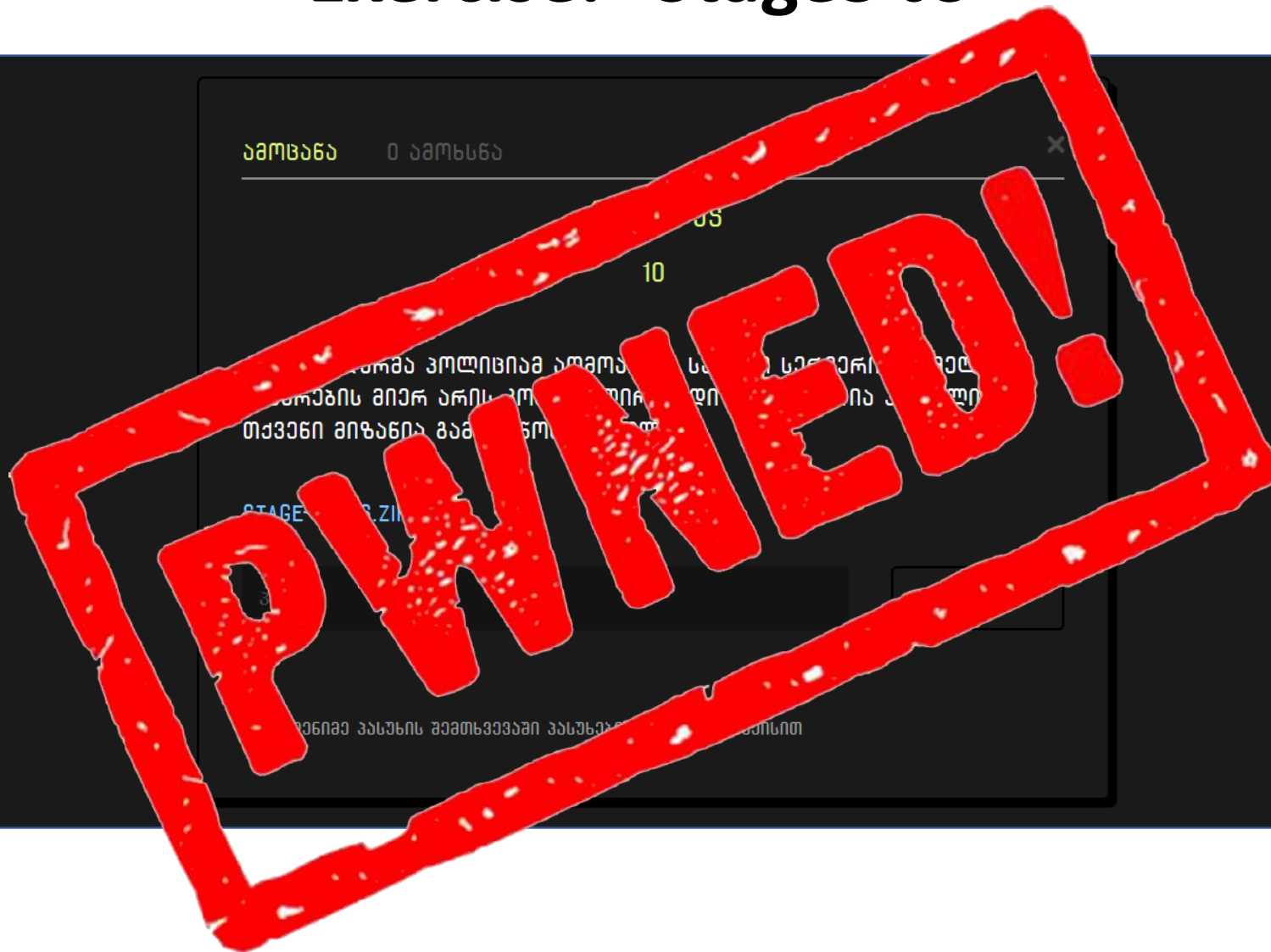
პასუხი

გამზავნა

რამოდენიმე პასუხის შემთხვევაში პასუხები გამოყვებით სპეცისით

# Exercise: “Stage3-JS”

LIVE



# Exercise: “Amadeus”

ამოცანა



AMADEUS

50

კომპანია “ალიგატორის” ვებგვერდი განხორციელდა შედევა, მაგრამ მისი ყველა დეტალი უცნობია. თქვენ გადმოგხვს სერვერის ე.წ. „ACCESS LOG“-ი შედევის მომენტში და უნდა გაიგოთ, თუ რა მოხდა შედევის დროს.

IACCESS.LOG

LIVE

- 1) რომელი IP მისამართი ჰქონდა შემტევს ?
- 2) რომელი სამი ხელსაწყო გამოიყენა შემტევმა ?
- 3) რომელი შეტევის მეთოდით მოახერხა მან სერვერზე შეღწევა ?
- 4) რა სახელის მქონე ე.წ. „პლაგინი“ ატვირთა შემტევმა ?
- 5) სერვერზე არსებული რომელი ფაილის შიგთავსი წაიკითხა მან ?

# Exercise: “Amadeus”

ამოცანა



AMADEUS

50

კომპანია “ალიგატორის” ვებგვერდი განხორციელდა შეტევა, მაგრამ მისი ყველა დეტალი უცნობია. თქვენ გადმოგხვს სერვერის ე.წ. „ACCESS LOG“-ი შეტევის მომენტში და უნდა გაიგოთ, თუ რა მოხდა შეტევის დროს.

IACCESS.LOG

LIVE

1) ~~რომელი IP მისამართი ჰქონდა შემტევს?~~

2) რომელი სამი ხელსაწყო გამოიყენა შემტევმა?

3) რომელი შეტევის მეთოდით მოახერხა მან სერვერზე შეღწევა?

4) რა სახელის მქონე ე.წ. „პლაგინი“ ატვირთა შემტევმა?

5) სერვერზე არსებული რომელი ფაილის შიგთავსი წაიკითხა მან?

# Exercise: “Amadeus”

ამოცანა



AMADEUS

50

კომპანია “ალიგატორის” ვებგვერდი განხორციელდა შეიქმნა, მაგრამ მისი ყველა დეტალი უცნობია. თქვენ გადმოგხვს სერვერის ე.წ. „ACCESS LOG“-ი შეიქმნის მომენტში და უნდა გაიგოთ, თუ რა მოხდა შეიქმნის დროს.

IACCESS.LOG

LIVE

1) ~~რომელი IP მისამართი ჰქონდა შემტევს?~~

2) ~~რომელი სამი ხელსაწყო გამოიყენა შემტევმა?~~

3) რომელი შეტევის მეთოდით მოახერხა მან სერვერზე შეღწევა ?

4) რა სახელის მქონე ე.წ. „პლაგინი“ ატვირთა შემტევმა ?

5) სერვერზე არსებული რომელი ფაილის შიგთავსი წაიკითხა მან ?

# Exercise: “Amadeus”

ამოცანა



AMADEUS

50

კომპანია “ალიგატორის” ვებგვერდი განხორციელდა შედევა, მაგრამ მისი ყველა დეტალი უცნობია. თქვენ გადმოგხვს სერვერის ე.წ. „ACCESS LOG“-ი შედევის მომენტში და უნდა გაიგოთ, თუ რა მოხდა შედევის დროს.

IACCESS.LOG

LIVE

- ~~1) რომელი IP მისამართი ჰქონდა შემტევს?~~
- ~~2) რომელი სამი ხელსაწყო გამოიყენა შემტევმა?~~
- ~~3) რომელი შეტევის მეთოდით მოახერხა მან სერვერზე შეღწევა?~~
- 4) რა სახელის მქონე ე.წ. „პლაგინი“ ატვირთა შემტევმა ?
- 5) სერვერზე არსებული რომელი ფაილის შიგთავსი წაიკითხა მან ?

# Exercise: “Amadeus”

ამოცანა



AMADEUS

50

კომპანია “ალიგატორის” ვებგვერდი განხორციელდა შეთქვა, მაგრამ მისი ყველა დეტალი უცნობია. თქვენ გადმოგხვს სერვერის ე.წ. „ACCESS LOG“-ი შეთქვის მომენტში და უნდა გაიგოთ, თუ რა მოხდა შეთქვის დროს.

IACCESS.LOG

LIVE

1) ~~რომელი IP მისამართი ჰქონდა შემტევს?~~

2) ~~რომელი სამი ხელსაწყო გამოიყენა შემტევმა?~~

3) ~~რომელი შეტევის მეთოდით მოახერხა მან სერვერზე შეღწევა?~~

4) ~~რა სახელის მქონე ე.წ. „პლაგინი“ ატვირთა შემტევმა?~~

5) სერვერზე არსებული რომელი ფაილის შიგთავსი წაიკითხა მან ?



# Exercise: "Amadeus"

ამოცანა

AMADEUS

50

კომპანია "ალიგატორის" ვებგვერდიდან აღმოჩენილი შეტევების შესახებ ინფორმაცია მოცემულია ქვემოთ. თქვენს მიერ მოხდეს სერვერის ატეხვა. „ACCESS LOG“-ი შეტევების მომენტის დაზუსტება და გავიგოთ თუ რა დროს შეტევის დროს.

IACCESS.LOG

LIVE

**PWNED!**

## **What's Next :**

- HackLab
- Virtual Machines
- Penetration Testing
- Exploit Development

# Questions ?

Thank you.



/index.php/Tbilisi



/OWASP-Tbilisi-Chapter



/OWASP.Tbilisi