# CSE 406
## COMPUTER SECURITY SESSIONAL
## OFFLINE REPORT
## CROSS SITE SCRIPTING

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

BANGLADESH UNIVERSITY OF

ENGINEERING AND TECHNOLOGY

LAB SUBSECTION: A2

SUBMITTED BY: 1905041

*SUBMITTED ON: 13/02/2024*

# Contents

# 1 Task 1: Adding User as Samy's Friend

## 1.1 Method

For this task, first the request for adding a user as a friend was examined. The URL (`http://www.seed-server.com/action/friends/add?friend=59`), the request type (GET) and the query parameters (`friend`, `__elgg_token`, `__elgg_ts`) was noted. A script was written that gets these values from the `elgg.session.user` and the `elgg.security.token` objects, creates proper URL for adding a friend and sends a `XMLHttpRequest` to add the user as a friend of Samy. Samy's userid was hardcoded to ensure the script does not affect Samy himself. The script was added in the *Brief Description* field of Samy's user profile so that it does not show in user preview.

## 1.2 Screenshots

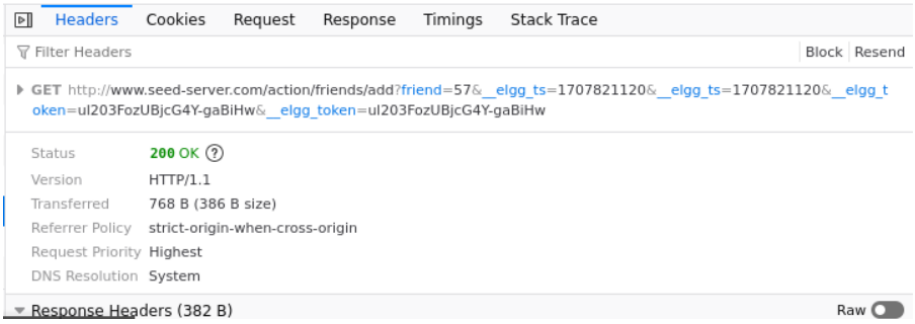


Figure 1: Task 1: Request Body


Figure 2: Task 1: `elgg.session.user` object


Figure 3: Task 1: `elgg.security.token` object


Figure 4: Task 1: Adding Script

# 2 Task 2: Editing User's Profile

## 2.1 Method

For this task, first the request for adding a user as a friend was inspected. The URL (`http://www.seed-server.com/action/profile/edit`), the request type (POST) and the query parameters was noted. A script was written that gets some of these values from the `elgg.session.user` and the `elgg.security.token` objects, sets other query parameters to random string, creates proper URL for editing a profile and sends a `XMLHttpRequest` to edit the user's profile. Samy's userid was hardcoded to ensure the script does not affect Samy himself. URL encoding was used to escape special characters in the URL. The script was added in the *Brief Description* field of Samy's user profile so that it does not show in user preview.

## 2.2 Screenshots

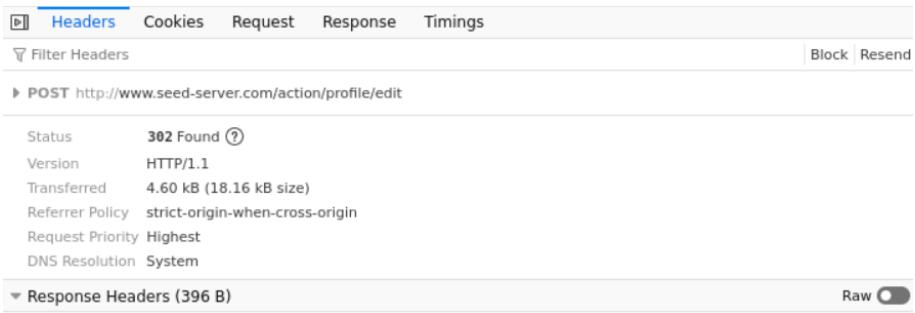


Figure 5: Task 2: Request Header

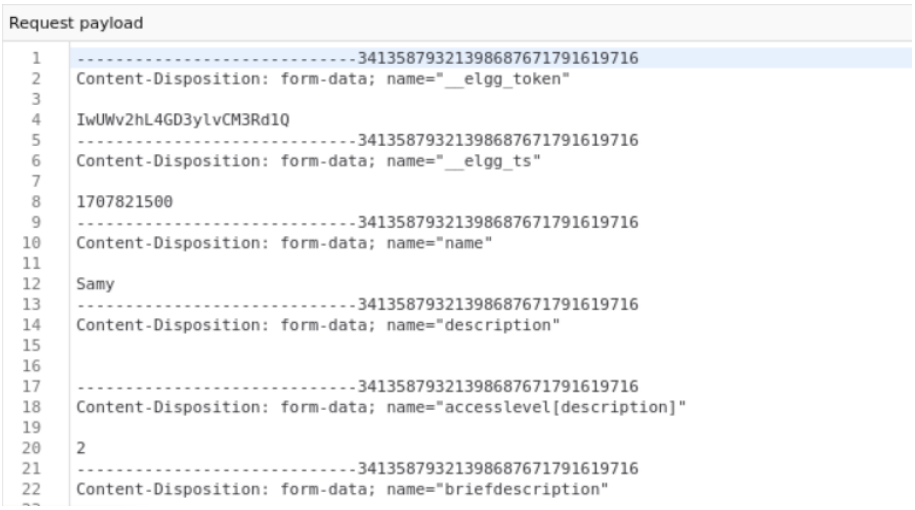


Figure 6: Task 2: Request Body


Figure 7: Task 2: URL encoded parameters, the script is dense due to character size limitations in input fields.

# 3 Task 3: Posting On the Wire as User

## 3.1 Method

For this task, first the request for posting on the wire was examined. The URL (`http://www.seed-server.com/action/thewire/add`), the request type (POST), the query parameters (`body`, `__elgg_token`, `__elgg_ts`) was noted. A script was written that gets these values from the `elgg.session.user` and the `elgg.security.token` objects, creates proper URL for posting on the wire and sends a `XMLHttpRequest` to post on the wire. Samy's userid was hardcoded to ensure the script does not affect Samy himself. URL encoding was used to escape special characters in the URL. The script was added in the *Brief Description* field of Samy's user profile so that it does not show in user preview.

### 3.2 Screenshots

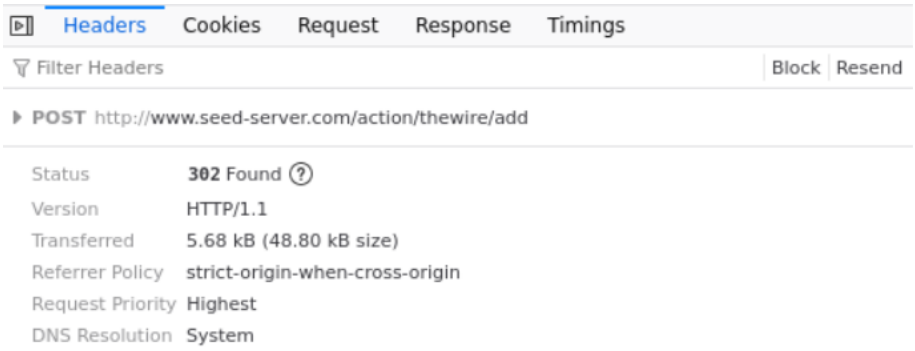


Figure 8: Task 3: Request Header

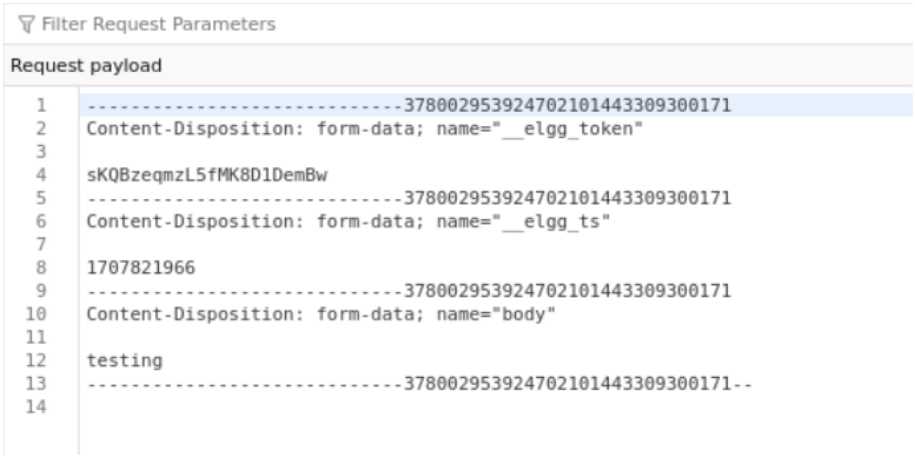


Figure 9: Task 3: Request Body

## 4 Task 4: Self Propagating XSS Worm

### 4.1 Method

For this task, code for task 1, 2 and 3 were combined. The script read it's own code using DOM and it's script id.
The URL (`http://www.seed-server.com/action/friends/add?friend=59`), with request type (GET) and query parameters (`friend`, `__elgg_token`, `__elgg_ts`) was used to add Samy as a friend. `__elgg_token`, `__elgg_ts` values were accessed from the `elgg.session.user` and the `elgg.security.token` objects. The URL(`http://www.seed-server.com/action/profile/edit`) with request type(POST) and proper query parameters was used to add the worm in victim user's profile. The URL (`http://www.seed-server.com/action/thewire/add`),

the request type (POST), the query parameters (`body`, `__elgg_token`, `__elgg_ts`) was used to post the user's profile link on the wire. Samy's userid was hard-coded to ensure the script does not affect Samy himself.

## 4.2 Screenshots


Figure 10: Task 4: Getting User URL


Figure 11: Task 4: Script id to access selfcode, the script is dense due to character size limitations in input fields