

CYBEREAGLES

5375
BONUS

START

MENU

SIGN IN

XSS GAME



INTRODUZIONE



L'XSS GAME È UNA SERIE DI ESERCIZI INTERATTIVI PROGETTATI PER INSEGNARE LE BASI DELLE VULNERABILITÀ DI TIPO CROSS-SITE SCRIPTING (XSS) E COME SFRUTTARLE.



CONSAPEVOLEZZA



PREVENZIONE



EDUCAZIONE

AUMENTARE LA CONSAPEVOLEZZA TRA SVILUPPATORI E PROFESSIONISTI DELLA SICUREZZA CIRCA I RISCHI LEGATI AGLI XSS.

INSEGNARE LE MIGLIORI PRATICHE PER PREVENIRE GLI ATTACCHI XSS NELLE APPLICAZIONI WEB.

FORNIRE UNA PIATTAFORMA PRATICA PER APPRENDERE LA TEORIA E LA PRATICA DELLE VULNERABILITÀ XSS.

MENU

LIVELLO 1



HELLO, WORLD OF XSS

DESCRIZIONE DELLA MISSIONE

QUESTO LIVELLO DIMOSTRA UNA CAUSA COMUNE DI CROSS-SITE SCRIPTING IN CUI L'INPUT DELL'UTENTE VIENE INCLUSO DIRETTAMENTE NELLA PAGINA SENZA UN'ADEGUATA SEQUENZA DI ESCAPE.
INTERAGITE CON LA FINESTRA DELL'APPLICAZIONE VULNERABILE QUI SOTTO E TROVATE UN MODO PER FARLE ESEGUIRE UN CODICE JAVASCRIPT A VOSTRA SCELTA. È POSSIBILE ESEGUIRE AZIONI ALL'INTERNO DELLA FINESTRA VULNERABILE O MODIFICARE DIRETTAMENTE LA SUA BARRA DEGLI URL.

OBIETTIVO DELLA MISSIONE

INIETTARE UNO SCRIPT PER FAR APPARIRE UN AVVISO JAVASCRIPT (ALERT()) NEL RIQUADRO SOTTOSTANTE.
UNA VOLTA MOSTRATO L'AVVISO, SARETE IN GRADO DI PASSARE AL LIVELLO SUCCESSIVO.

VETTORE: <SCRIPT>ALERT()</SCRIPT>

N.B. OGNI LIVELLO HA UN CODICE SORGENTE DIVERSO DA ANALIZZARE

The screenshot shows a browser window titled "I am vulnerable". The URL bar contains "https://xss-game.appspot.com/level1/frame?<script>alert()</script>". The main content area displays the text "FourOrFour" and a search bar with "Enter query here...". A message box on the right says "Congratulations, you executed an alert:" followed by "undefined". Below it is the text "You can now advance to the next level."

The screenshot shows a browser window titled "I am vulnerable". The URL bar contains "https://xss-game.appspot.com/level1/frame?<script>alert()</script>". The main content area displays the text "FourOrFour" and a search bar with "<script>alert()</script>". A blue button labeled "OK" is visible on the right, and a cursor icon is shown pointing towards it.

MENU

LIVELLO 2

N.B. OGNI LIVELLO HA UN CODICE SORGENTE DIVERSO DA ANALIZZARE



PERSISTENCE IS KEY



DESCRIZIONE DELLA MISSIONE

LE APPLICAZIONI WEB SPESO CONSERVANO I DATI DEGLI UTENTI IN DATABASE LATO SERVER E, SEMPRE PIÙ SPESO, LATO CLIENT, PER POI MOSTRARLI AGLI UTENTI. INDIPENDENTEMENTE DALLA PROVENIENZA DI TALI DATI CONTROLLATI DALL'UTENTE, ESSI DEVONO ESSERE GESTITI CON ATTENZIONE.
QUESTO LIVELLO MOSTRA COME SIA FACILE INTRODURRE BUG XSS IN APPLICAZIONI COMPLESSE.

I am vulnerable

URL <https://xss-game.appspot.com/level2/frame>

Madchattr

Chatter from across the Web.

You

Fri Jul 12 2024 15:06:44 GMT+0200 (Central European Summer Time)

Welcome!

This is your personal stream. You can post anything you want here, especially **madness**.

Share status!

OBIETTIVO DELLA MISSIONE

INIETTARE UNO SCRIPT PER FAR APPARIRE UN AVVISO() NEL CONTESTO DELL'APPLICAZIONE.
NOTA: L'APPLICAZIONE SALVA I POST, QUINDI SE SI INSERISCE DEL CODICE PER ESEGUIRE L'AVVISO, QUESTO LIVELLO SARÀ RISOLTO OGNI VOLTA CHE SI RICARICA L'APPLICAZIONE.

MENU

➤ LIVELLO 2



PERSISTENCE IS KEY

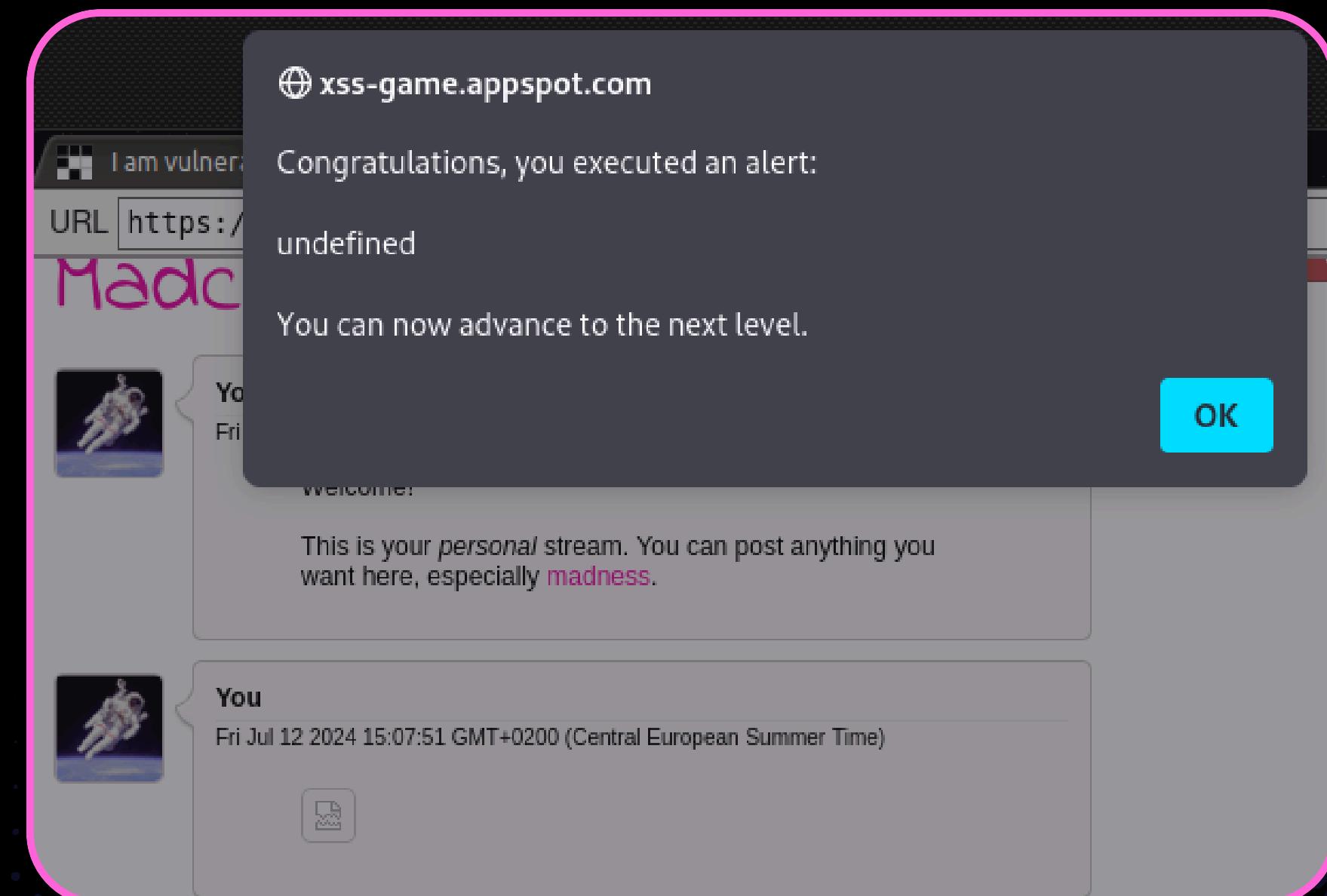


SOLUZIONE DELLA MISSIONE

LA VULNERABILITÀ DI QUESTA PAGINA È INCLUDERE HTML DIRETTAMENTE NELLA PAGINA. MA QUESTA VOLTA C'È UNA CONVALIDA CHE CI IMPEDISCE DI USARE LO SCRIPT TAG. PER BYPASSARLA POSSIAMO INSERIRE UN TAG IMMAGINE CON UN URL NON VALIDO E UN ATTRIBUTO ONERROR CHE ESEGUIRÀ UN AVVISO JAVASCRIPT.



LA PAGINA TENTERÀ DI CARICARE L'IMMAGINE DALLA SORGENTE 'X' CHE FALLIRÀ E QUINDI ATTIVERÀ IL CODICE DELL'ATTRIBUTO ONERROR.



MENU

→ LIVELLO 3



THAT SINKING FEELING...

DESCRIZIONE DELLA MISSIONE

COME VISTO NEL LIVELLO 2, ALCUNE JS FUNCION COMUNI SONO DEI SINK SINK ESECUTIVI, QUINDI CAUSERANNO L'ESECUZIONE DA PARTE DEL BROWSER DI TUTTI GLI SCRIPT CHE APPAIONO NEL LORO INPUT. A VOLTE CIÒ È NASCOSTO DA API DI LIVELLO SUPERIORE CHE UTILIZZANO UNA DI QUESTE FUNZIONI. L'APPLICAZIONE DI QUESTO LIVELLO UTILIZZA UNO DI QUESTI SINK NASCOSTI.

OBIETTIVO DELLA MISSIONE

COME PRIMA, INIETTARE UNO SCRIPT PER FAR APPARIRE UN ALERT() JAVASCRIPT NELL'APPLICAZIONE. POICHÉ NON È POSSIBILE INSERIRE IL PAYLOAD DA NESSUNA PARTE, SI DOVRÀDOVRETE MODIFICARE MANUALMENTE L'INDIRIZZO NELLA BARRA DEGLI URL SOTTOSTANTE.

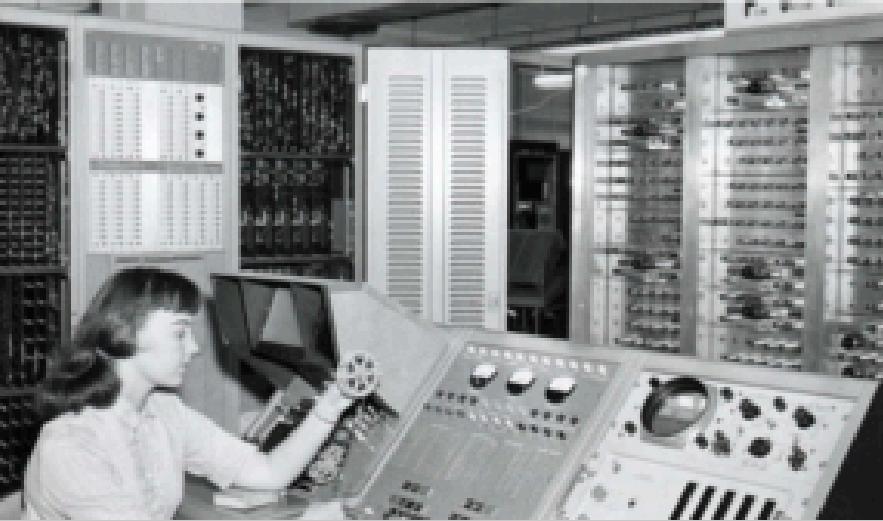
I am vulnerable

URL <https://xss-game.appspot.com/level3/frame#1> Go

 **clouiddly** Take a tour of our cloud data center.

Image 1 Image 2 Image 3

Image 1



N.B. OGNI LIVELLO HA UN CODICE SORGENTE DIVERSO DA ANALIZZARE

THAT SINKING FEELING...

SOLUZIONE DELLA MISSIONE

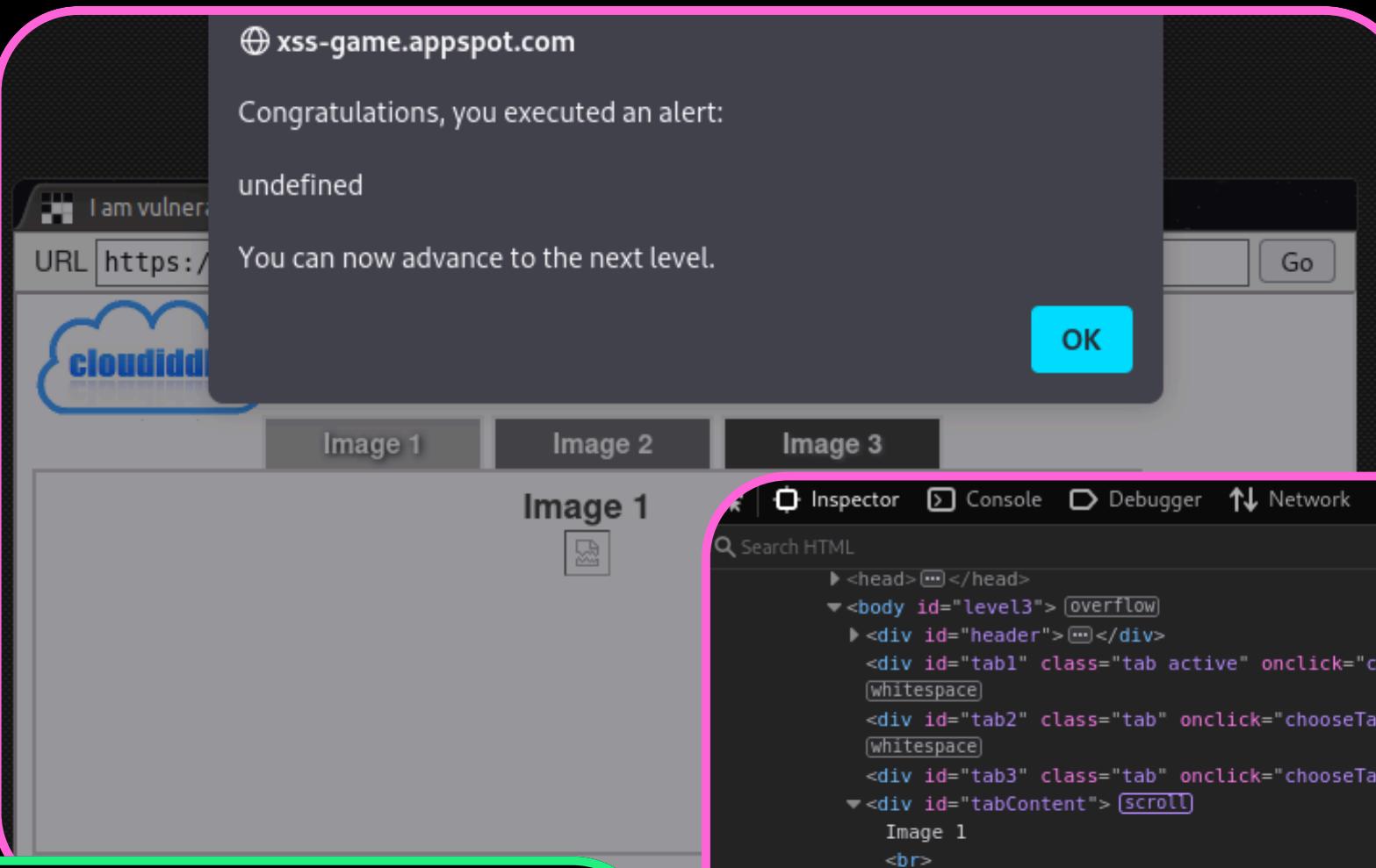
L'APPLICAZIONE SCEGLIE LA SCHEDA IMMAGINE IN BASE AL PRIMO FRAMMENTO DELL'URL (L'HASH DOPO L'URL). PASSANDO UN FRAMMENTO MALEVOLO CHE VERRÀ INSERITO NELLA PAGINA, SI ATTIVERÀ L'AVVISO.

```
1' ONERROR='ALERT()//'
```

IL CODICE SORGENTE DELLA PAGINA MOSTRA CHE OTTIENE IL FRAMMENTO URL E LO PASSA ALLA FUNZIONE CHOOSETAB. QUESTA FUNZIONE AGGIUNGE QUINDI IL TESTO DEL FRAMMENTO ALLA SORGENTE DEL TAG IMMAGINE E CARICA IL NUOVO TAG NELLA PAGINA.

POSSIAMO OVVIARE AL PROBLEMA CHIUDENDO L'ATTRIBUTO SRC CON UN SINGOLO APICE, E POI AGGIUNGENDO UN ATTRIBUTO ONERROR CON UNA FUNZIONE DI AVVISO COME NEL LIVELLO PRECEDENTE, RINOMINANDOLO '.JPG' CON DOPPIE BARRE CREANDO

```
<IMG SRC=' /STATIC/LEVEL3/CLOUD1' ONERROR='ALERT()//.JPG' />
```



MENU

➤ LIVELLO 4

CONTEXT MATTERS

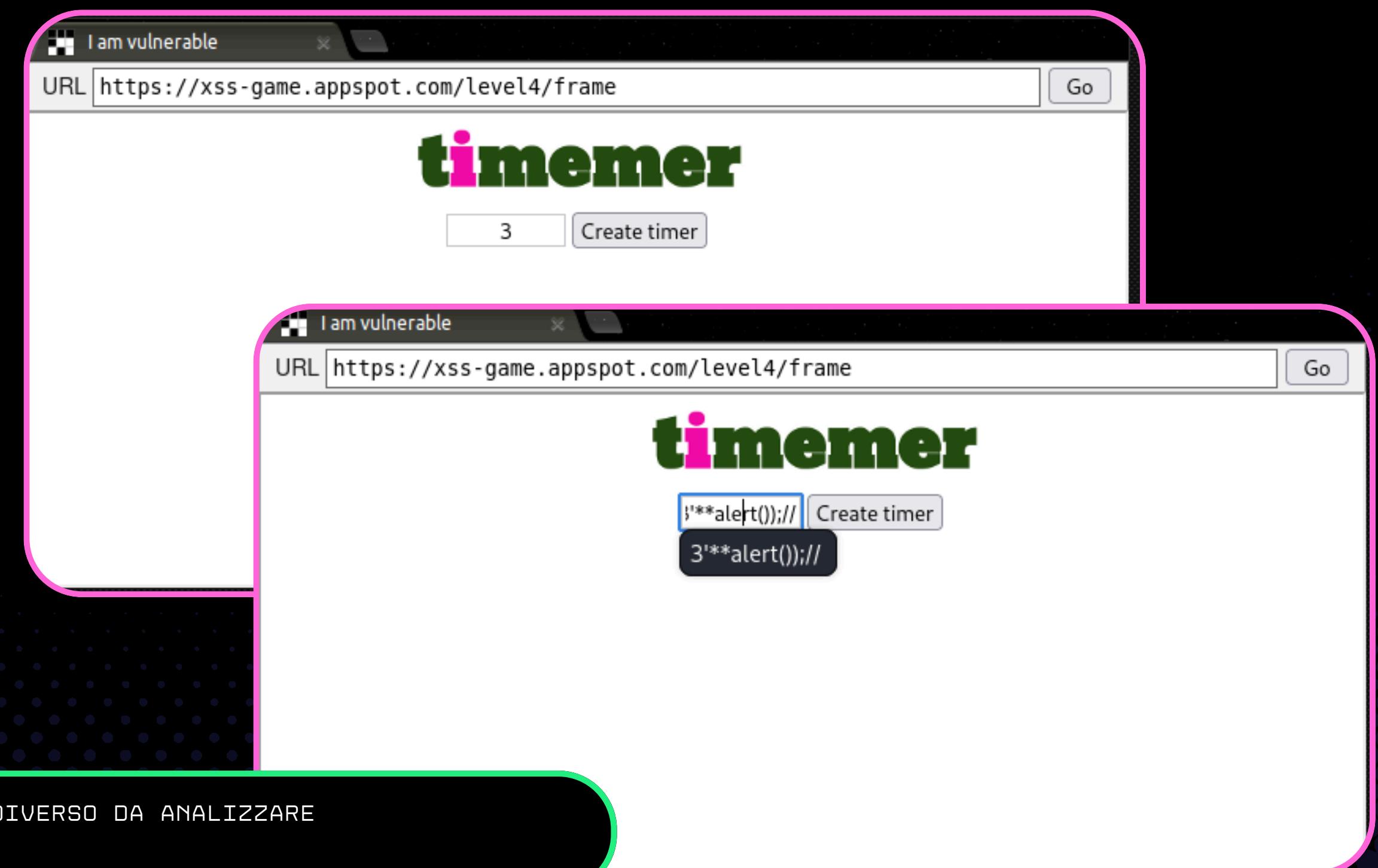
DESCRIZIONE DELLA MISSIONE

OGNI BIT DI DATI FORNITI DALL'UTENTE DEVE ESSERE CORRETTAMENTE GESTITO IN BASE AL CONTESTO DELLA PAGINA IN CUI APPARIRÀ. QUESTO LIVELLO MOSTRA IL MOTIVO.

OBIETTIVO DELLA MISSIONE

INIETTARE UNO SCRIPT PER FAR APPARIRE UN AVVISO JAVASCRIPT () NELL'APPLICAZIONE.

N.B. OGNI LIVELLO HA UN CODICE SORGENTE DIVERSO DA ANALIZZARE



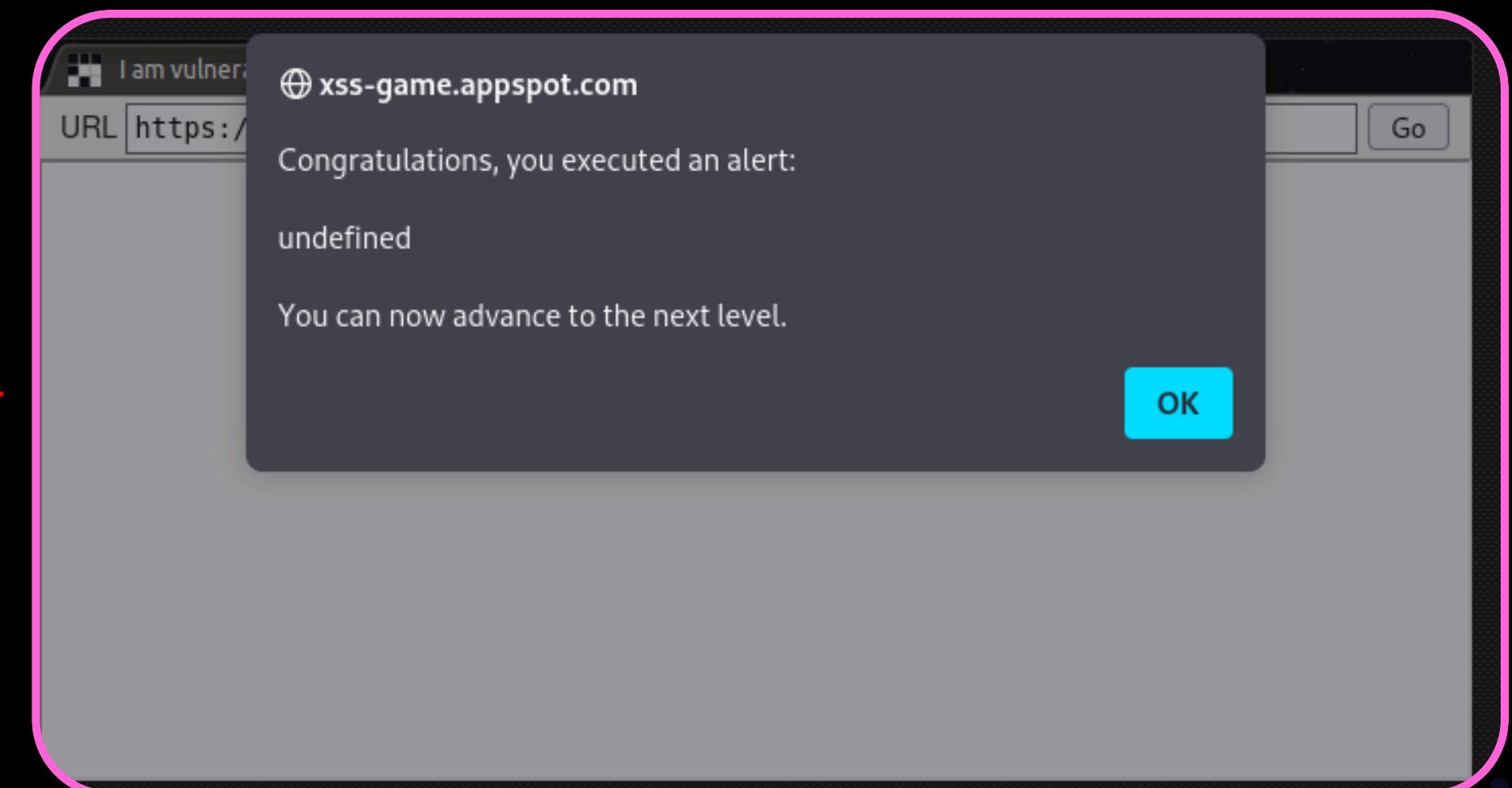
MENU

➤ LIVELLO 4

CONTEXT MATTERS

SOLUZIONE DELLA MISSIONE

LA PAGINA DELL'INDICE MOSTRA UN MODULO IN CUI VIENE PASSATO UN NUMERO ALLA PAGINA DEL TIMER LA CUI FUNZIONE È SEMPLICEMENTE CONTARE IL NUMERO CHE ABBIAMO PASSATO IN SECONDI E POI REINDIRIZZARCI ALL'INIZIO. POSSIAMO INGANNARE LA SUA FUNZIONE TIMER PER ESEGUIRE CODICE ARBITRARIO, POICHÉ VIENE AGGIUNTO DIRETTAMENTE ALLA PAGINA. IL VALORE CHE ABBIAMO PASSATO DALLA PAGINA DELL'INDICE VIENE AGGIUNTO DIRETTAMENTE AL PARAMETRO DELLA FUNZIONE NEL TIMER.



```
<IMG SRC="/STATIC/LOADING.GIF" ONLOAD="STARTTIMER('{{ TIMER }}');;" />
```

QUINDI POSSIAMO MANIPOLARE IL CODICE JAVASCRIPT ESEGUITO QUI. SE PASSIAMO IL SEGUENTE PARAMETRO

```
3***ALERT();//
```

JAVASCRIPT TENTERÀ DI VALUTARE 3ALERT() PRIMA DI CHIAMARE LA FUNZIONE STARTTIMER. INOLTRE, PER VALUTARE IL RISULTATO DI 3ALERT() DEVE OTTENERE IL VALORE RESTITUITO DALLA FUNZIONE ALERT(), CHE FARÀ ESEGUIRE AL BROWSER LA FUNZIONE DI AVVISO.

MENU

► LIVELLO 5

N.B. OGNI LIVELLO HA UN CODICE SORGENTE DIVERSO DA ANALIZZARE



BREAKING PROTOCOL



DESCRIZIONE DELLA MISSIONE

IL CROSS-SITE SCRIPTING NON RIGUARDA SOLO L'ESCAPE CORRETTO DEI DATI. A VOLTE, GLI AGGRESSORI POSSONO FARE COSE BRUTTE ANCHE SENZA INIETTARE NUOVI ELEMENTI NELLA DOM.

OBIETTIVO DELLA MISSIONE

INIETTARE UNO SCRIPT PER FAR APPARIRE UN ALERT() NEL CONTESTO DELL'APPLICAZIONE.

SOLUZIONE DELLA MISSIONE

QUERY USATA: [HTTPS://XSS-GAME.APPSPOT.COM/LEVEL5/FRAME/SIGNUP?NEXT=JAVASCRIPT:ALERT\(1\)](https://xss-game.appspot.com/level5/frame/signup?next=javascript:alert()1)

VETTORE: JAVASCRIPT:ALERT(1)

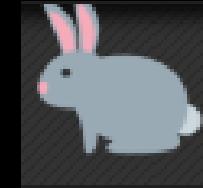
QUESTO LIVELLO ILLUSTRA COME I PROTOCOLLI URL POSSANO ESSERE SFRUTTATI. PASSANDO **JAVASCRIPT:** COME VALORE PER IL PARAMETRO NEXT, IL BROWSER INTERPRETA IL CONTENUTO COME CODICE JAVASCRIPT DA ESEGUIRE, MOSTRANDO L'ALERT.

The screenshot shows three browser windows illustrating the exploit:

- Top Window:** Shows the URL <https://xss-game.appspot.com/level5/frame>. The page displays "Welcome! Today we are announcing the much anticipated Groovy Reader 2.0". Below it is a sign-up form with fields for "Enter email:" and "Next >".
- Middle Window:** Shows the URL <https://xss-game.appspot.com/>. It displays a success message: "Congratulations, you executed an alert: undefined". It also says "You can now advance to the next level." and has an "OK" button.
- Bottom Window:** Shows the URL [https://xss-game.appspot.com/level5/frame/signup?next=javascript:alert\(\)1](https://xss-game.appspot.com/level5/frame/signup?next=javascript:alert()1). The Groovy Reader 2.0 sign-up page is shown again, but an alert box is visible in the bottom right corner of the browser window, indicating the exploit was successful.



FOLLOW THE



DESCRIZIONE DELLA MISSIONE

LE APPLICAZIONI WEB COMPLESSE A VOLTE HANNO LA CAPACITÀ DI CARICARE DINAMICAMENTE LIBRERIE JAVASCRIPT IN BASE AI VALORI DEI PARAMETRI DELL'URL O ALLA PARTE LOCATION.HASH. CIÒ È MOLTO DELICATO PERCHÈ CONSENTE ALL'INPUT DELL'UTENTE DI INFLUENZARE L'URL QUANDO SI CARICANO SCRIPT O ALTRI TIPI DI DATI POTENZIALMENTE PERICOLOSI, COME XMLHTTPREQUEST, CHE SPESSO PORTA GRAVI VULNERABILITÀ.



OBIETTIVO DELLA MISSIONE

TROVA UN MODO PER FAR SÌ CHE L'APPLICAZIONE RICHIEDA UN FILE ESTERNO CHE CAUSI L'ESECUZIONE DI UN ALERT () .

The screenshot displays three browser windows from a game titled "I am vulnerable". The top window shows a "GLOVE GADGETS" page with a Rubik's cube icon. The middle window shows the same page with an alert box: "Congratulations, you executed an alert: xss". The bottom window shows a confirmation message: "You can now advance to the next level." Below the browser windows, a status message reads: "Loaded gadget from data:text/plain,alert('xss')".



SOLUZIONE DELLA MISSIONE

LA PAGINA AGGIUNGE UN TAG SCRIPT CON L'ATTRIBUTO SRC CHE PUNTA AL VALORE DEL PRIMO FRAMMENTO DELL'URL. MA, PRIMA DI FARLO, VERIFICA SE IL FRAMMENTO INIZIA CON LE PAROLE 'HTTP' O 'HTTPS', PER IMPEDIRCI DI CARICARE FILE ESTERNI.

POSSIAMO BYPASSARE QUESTA VALIDAZIONE OMETTENDO IL PROTOCOLLO 'HTTP', SOSTITUENDO L'URL CON:

HTTPS://XSS-GAME.APPSPOT.COM/LEVEL6/FRAME#DATA:TEXT/PLAIN,ALERT('XSS')

N.B. OGNI LIVELLO HA UN CODICE SORGENTE DIVERSO DA ANALIZZARE



SIGN IN



RICERCA XSS AUTOMATIZZATA

QUESTO GIOCHINO È UN OTTIMO MODO PER ENTRARE NEL MONDO DELLE VULNERABILITÀ CROSS-SITE SCRIPTING. MENTRE STRUMENTI AUTOMATICI COME XSSER POSSONO VELOCIZZARE LA RICERCA DI QUESTE VULNERABILITÀ, È FONDAMENTALE EVITARNE L'USO NELLA FASE DI APPRENDIMENTO. XSSER È UN TOOL OPEN-SOURCE CHE AUTOMATIZZA L'INDIVIDUAZIONE DI XSS, UTILIZZANDO VARIE TECNICHE DI INIEZIONE PER TESTARE LE APPLICAZIONI WEB. TUTTAVIA, FARE TROPPO AFFIDAMENTO SU STRUMENTI AUTOMATICI PUÒ FARTI PERDERE DI VISTA I DETTAGLI E LE TECNICHE FONDAMENTALI.

```
#xsser --help
Usage:

xsser [OPTIONS] [--all <url> | -u <url> | -i <file> | -d <dork> (options)|-l ] [-g
|get> | -p <post> | -c <crawl> (options)]
[Request(s)] [Checker(s)] [Vector(s)] [Anti-antiXSS/IDS] [Bypasser(s)] [Techniqu
e(s)] [Final Injection(s)] [Reporting] {Miscellaneous}

Cross Site "Scripter" is an automatic -framework- to detect, exploit and
report XSS vulnerabilities in web-based applications.

Options:
--version          show program's version number and exit
-h, --help         show this help message and exit
-s, --statistics   show advanced statistics output results
-v, --verbose       active verbose mode output results
--gtk              launch XSSer GTK Interface
--wizard           start Wizard Helper!

*Special Features*:
You can set Vector(s) and Bypasser(s) to build complex scripts for XSS
code embedded. XST allows you to discover if target is vulnerable to
'Cross Site Tracing' [CAPEC-1071]
```

CYBEREAGLES



VICTORIA BRAILE



NOEMI DE MARTINO



MATTEO BELTRAMI MARZOLINI

MENU

FLAVIO SCOGNAMIGLIO

SARAH ORTIZ



CRISTIAN BONALDI