



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:** QUALSIASI COSA VERRÀ INSERITA VERRÀ AGGIUNTA ALLA PAGINA, POSSIAMO QUINDI INIETTARE UN TAG SCRIPT CON UN CODICE DI ALERT:  
`<SCRIPT>ALERT()</SCRIPT>`

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

The screenshot shows a browser window with the title "I am vulnerable". The URL bar contains "https://xss-game.appspot.com/level1/frame". The main content area displays the text "FourOrFour" in large purple letters. Below it is a search bar with the placeholder "Enter query here..." and a "Search" button. A message box on the right side of the page says "Congratulations, you executed an alert:" followed by "undefined". At the bottom, it says "You can now advance to the next level."

The screenshot shows a browser window with the title "I am vulnerable". The URL bar contains "https://xss-game.appspot.com/level1/frame?". The main content area displays the text "FourOrFour" in large purple letters. Below it is a search bar with the placeholder "<script>alert()</script>" and a "Search" button. In the top right corner of the browser window, there is a blue "OK" button and a cursor icon 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.

The screenshot shows a web browser window titled "I am vulnerable" with the URL <https://xss-game.appspot.com/level2/frame>. The page is titled "Madchattr" with the subtitle "Chatter from across the Web.". It features a user profile picture of an astronaut and a message from the user "You". The message content is: "Welcome! This is your personal stream. You can post anything you want here, especially **madness**.<img src='x' onerror='alert()'>". A green button at the bottom right says "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



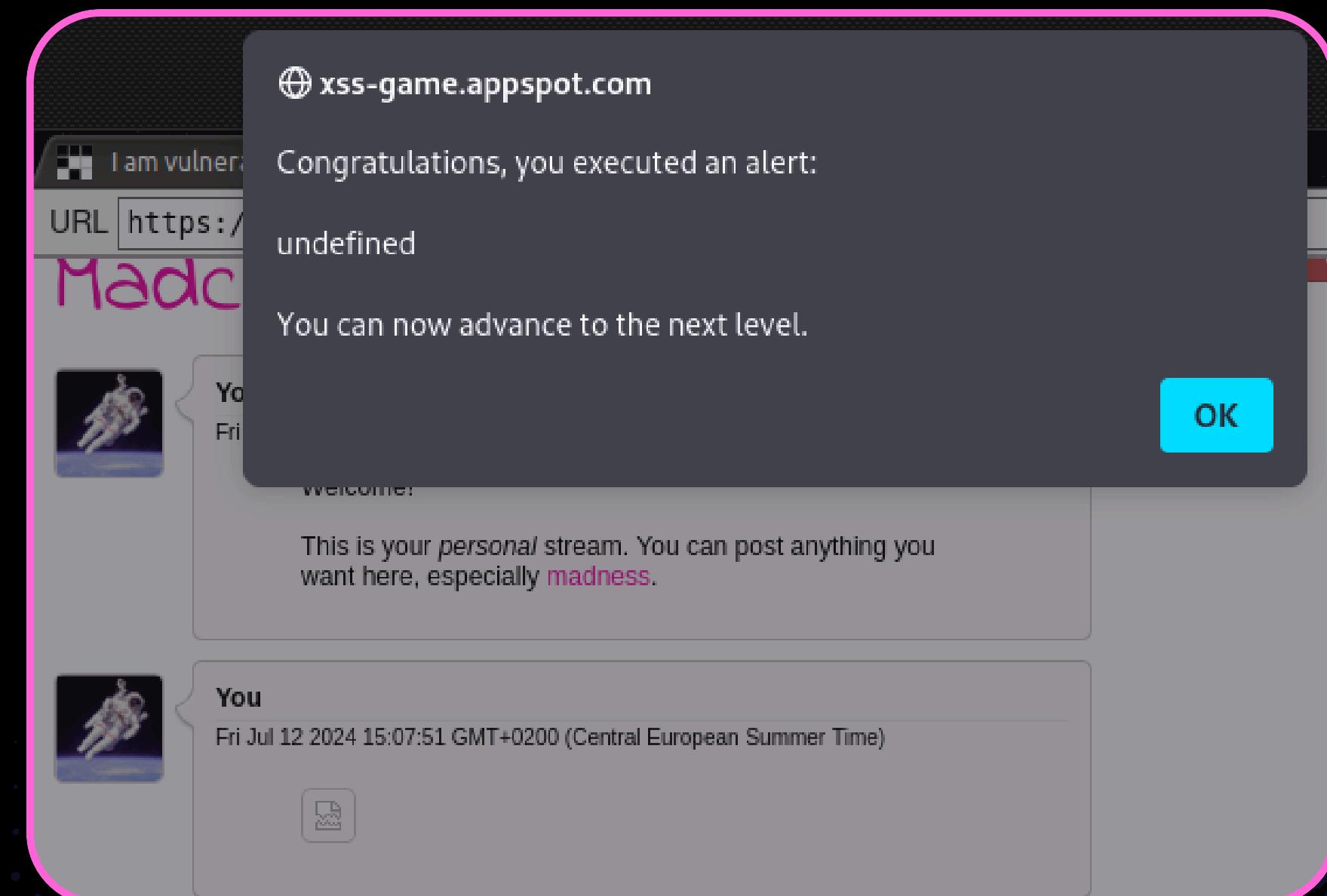
## SOLUZIONE DELLA MISSIONE

LA VULNERABILITÀ DI QUESTA LIVELLO È INCLUDERE HTML DIRETTAMENTE NELLA PAGINA; QUESTA VOLTA, PERÒ, 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:

```
<IMG SRC='X' ONERROR='ALERT()'>
```



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



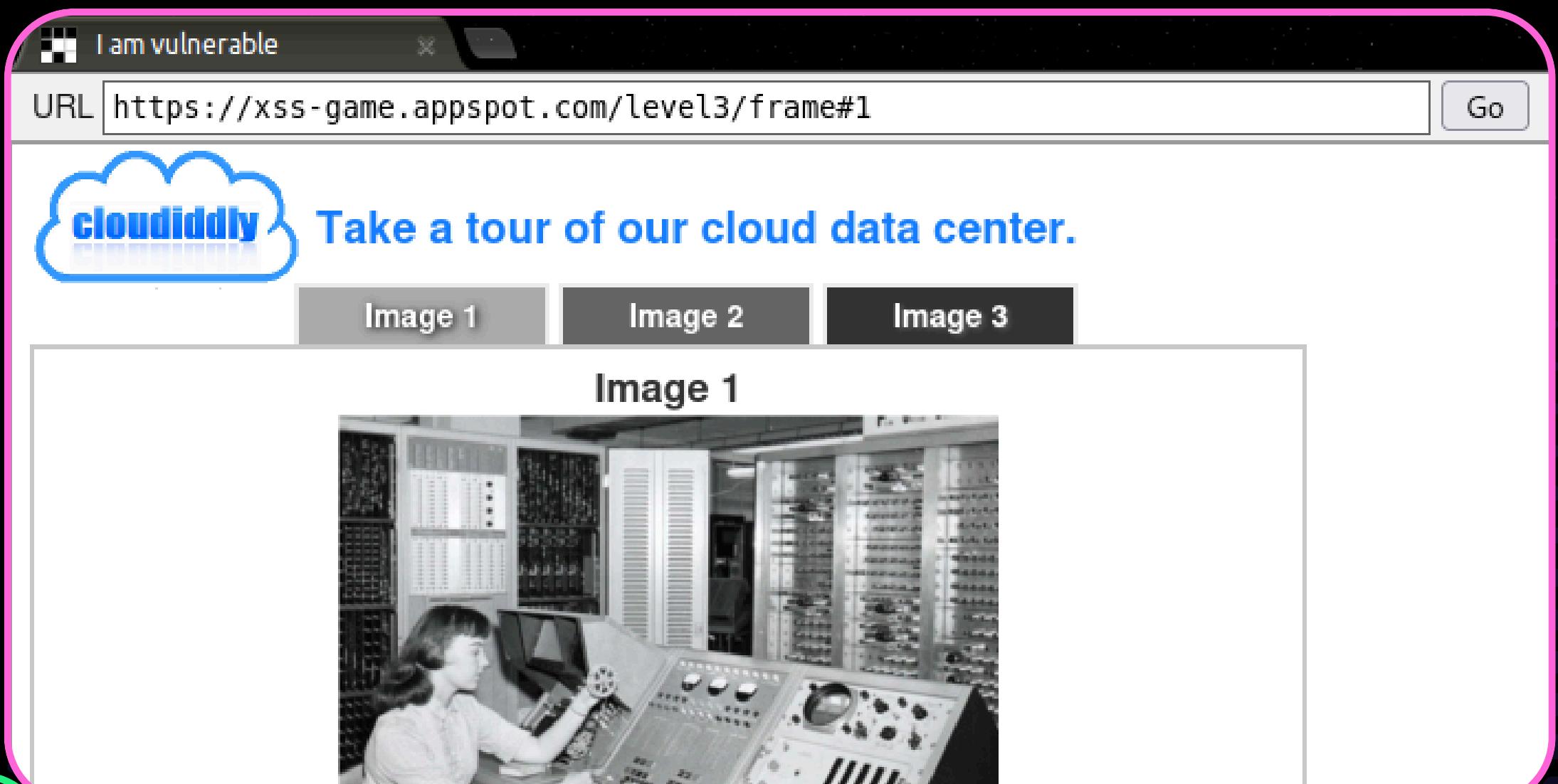
# THAT SINKING FEELING...

## 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.



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. INIETTANDO UN FRAMMENTO MALEVOLO CHE VERRÀ INSERITO NELLA PAGINA, SI ATTIVERÀ L'AVVISO.

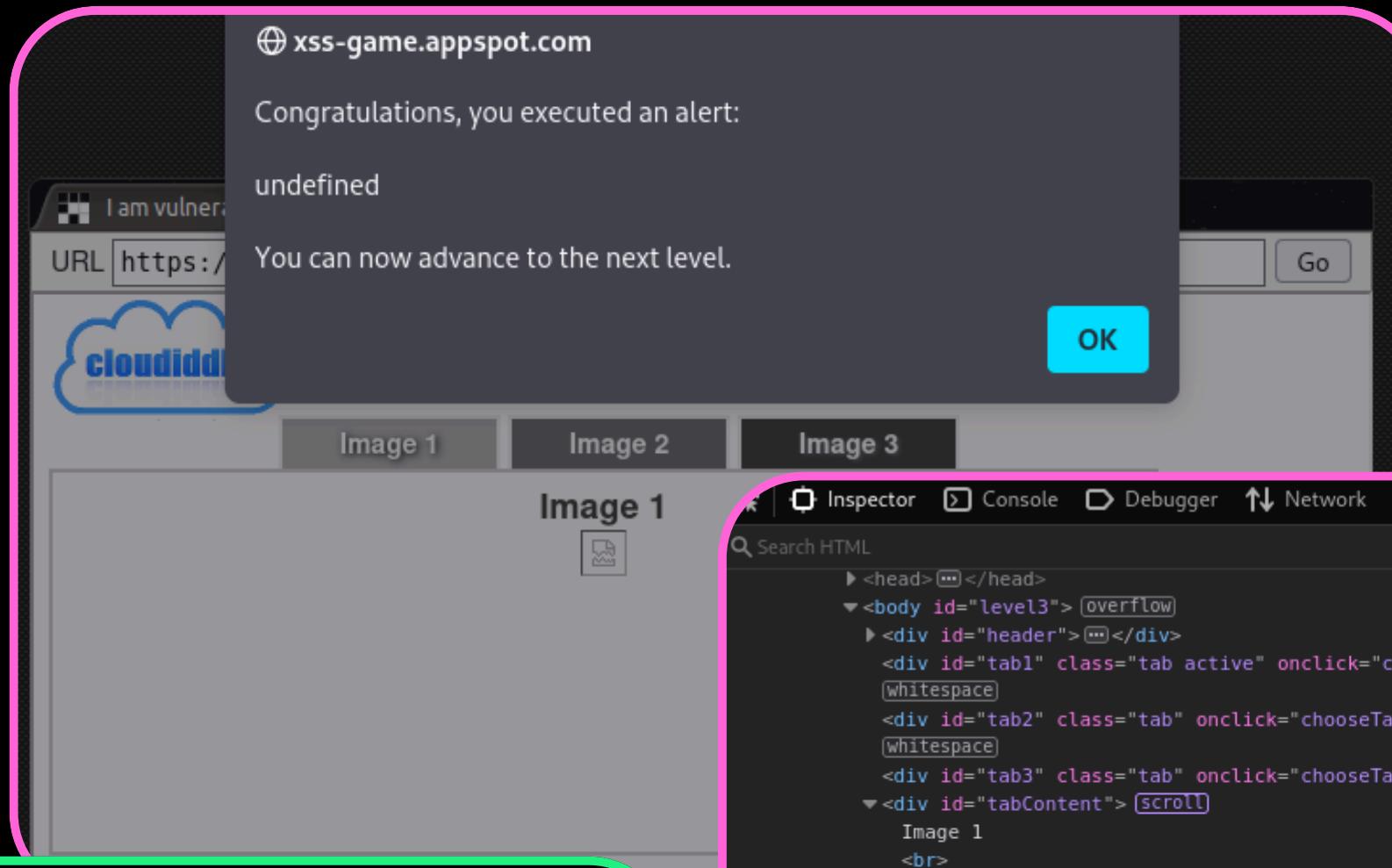
```
1' ONERROR='ALERT()//'
```

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 ANCHE OVIARE 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, RINOMINANDO '.JPG' CON DOPPIE BARRE CREANDO

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

E SOSTITUENDOLO POI NEL SOURCE CODE



MENU

➤ LIVELLO 4

# CONTEXT MATTERS

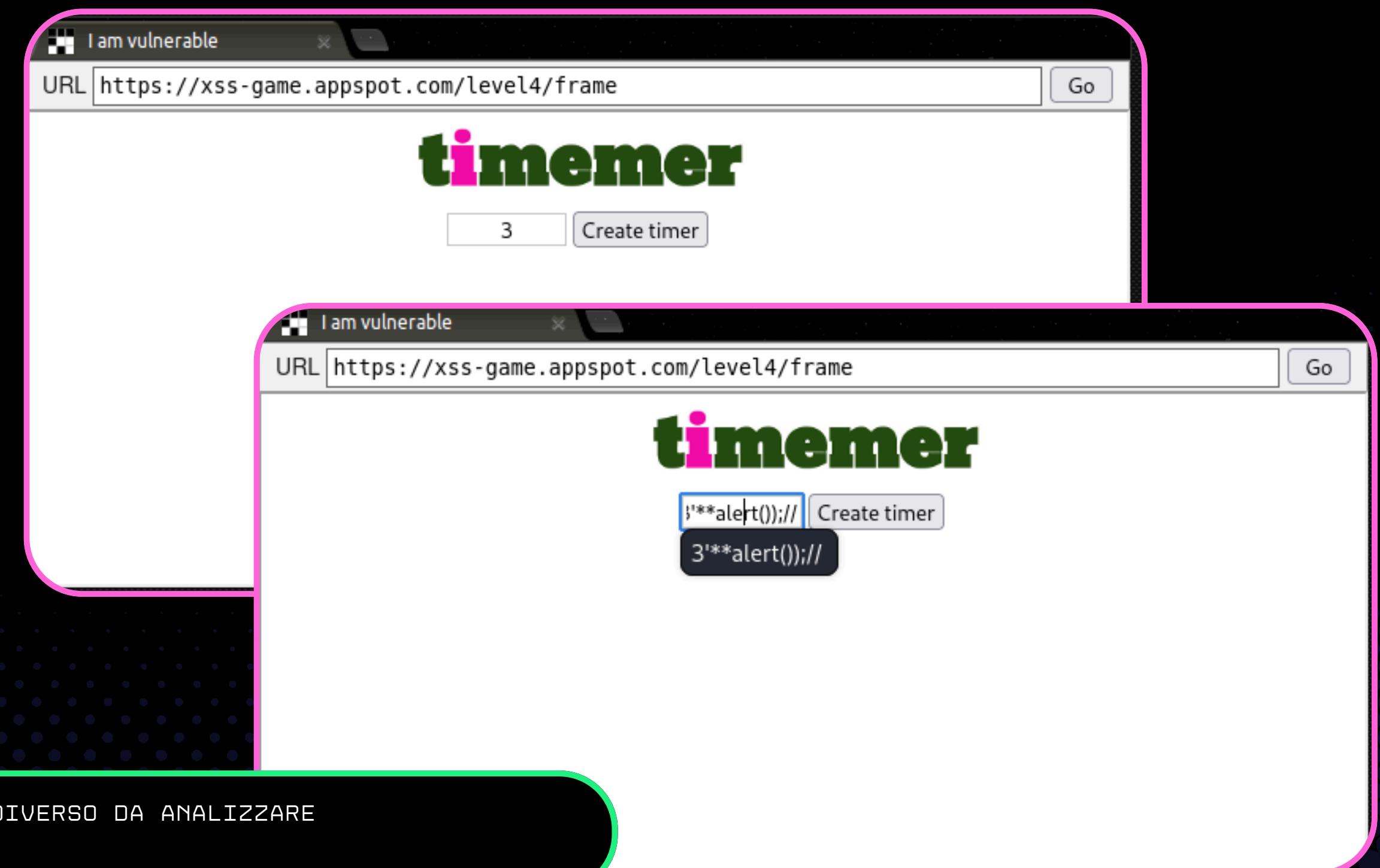
## DESCRIZIONE DELLA MISSIONE

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



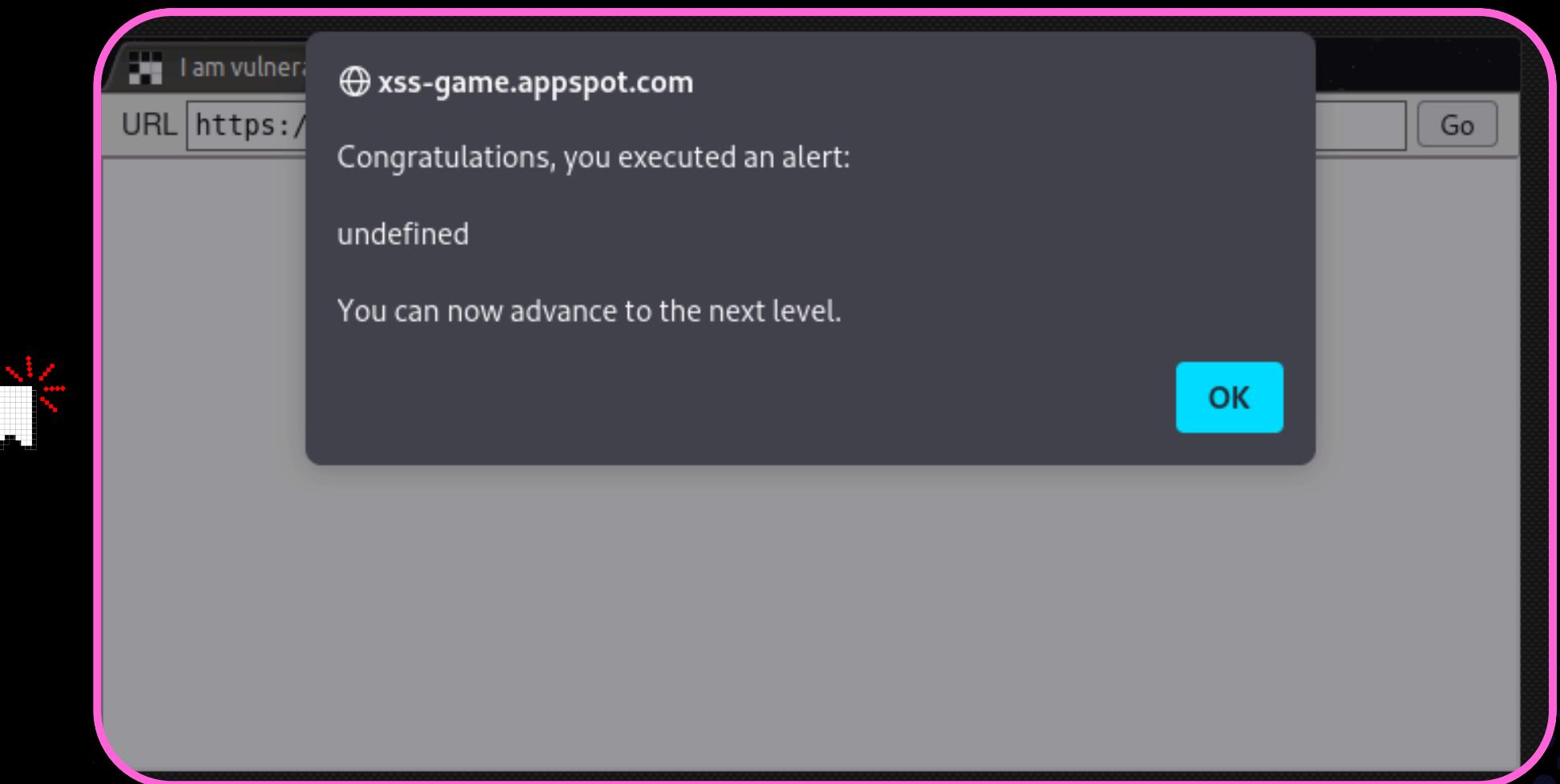
MENU

LIVELLO 4

# CONTEXT MATTERS

## SOLUZIONE DELLA MISSIONE

LA PAGINA DELL'INDICE MOSTRA FORM IN CUI VIENE CHIESTO DI INSERIRE UN NUMERO PER FAR PARTIRE UN TIMER. L'INPUT VIENE INSERITO DIRETTAMENTE ALLA PAGINA, SENZA SANITIZZAZIONE.



SE INSERIAMO QINDI IL SEGUENTE ALERT:

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

JAVASCRIPT TENTERÀ DI VALUTARE 3ALERT() 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)`

QUESTO LIVELLO ILLUSTRA COME I PROTOCOLLI URL POSSANO ESSERE SFRUTTATI. PASSANDO **JAVASCRIPT**.

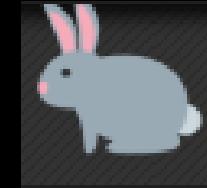
IL PARAMETRO NEXT, VIENE UTILIZZATO DIRETTAMENTE COME VALORE PER L'ATTRIBUTO HREF, SENZA SANITIZZAZIONE.

IL BROWSER INTERPRETA QUINDI IL CONTENUTO COME CODICE JAVASCRIPT DA ESEGUIRE, MOSTRANDO L'ALERT.

The screenshots illustrate the execution of a JavaScript alert on the Groovy Reader 2.0 sign-up page. In the first screenshot, the URL is `https://xss-game.appspot.com/level5/frame`. In the second screenshot, after entering the URL with the parameter `?NEXT=JAVASCRIPT:ALERT(1)`, an alert box appears with the message "Congratulations, you executed an alert: undefined". In the third screenshot, the URL is `https://xss-game.appspot.com/level5/frame/signup?next=javascript:alert()`, and another alert box appears with the message "undefined".



# 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. The top window shows a page titled 'GLOVE GADGETS' 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 success message: 'You can now advance to the next level.' with an 'OK' button. The URL in all windows is 'https://xss-game.appspot.com/level6/frame#static/gadget.js'.



## 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