OWASP AppSec EU Belfast

8th to 12th of May 2017

Waterfront Conference Center

WEBGOAT

Become a CtF Star

Housekeeping Note

- **Download ZAP Now**
- https://github.com/zaproxy/zaproxy/wiki/Downloads

WebGoat - Core Team

Bruce Mayhew (Sonatype) - The Goat Herder

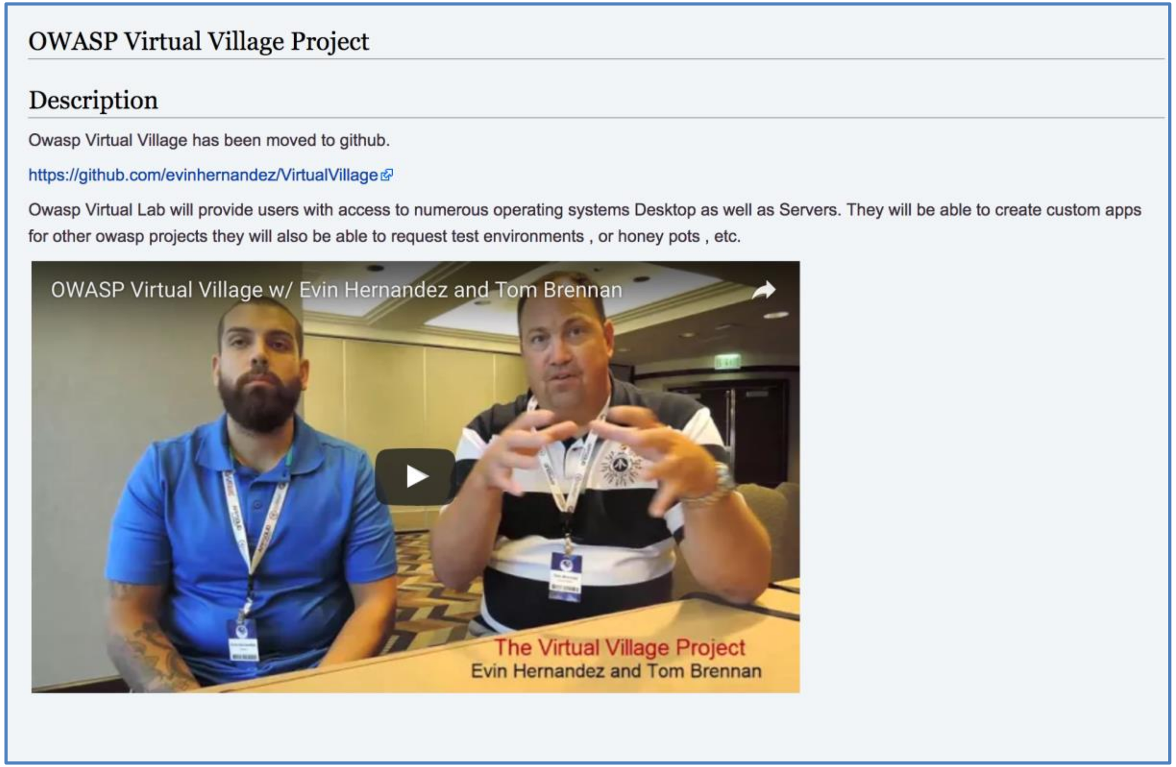
Nanne Baars (Xebia) - Java/backend lead & architect

Jason White (AsTech) – UI lead, & architect

“Capture the Flag Star”

Special thanks & credit to Mark Miller and Gary Robinson

Thanks to OWASP Virtual Village



OWASP Virtual Village Project

Description

Owasp Virtual Village has been moved to github.

https://github.com/evinhernandez/VirtualVillage

Owasp Virtual Lab will provide users with access to numerous operating systems Desktop as well as Servers. They will be able to create custom apps for other owasp projects they will also be able to request test environments , or honey pots , etc.

OWASP Virtual Village w/ Evin Hernandez and Tom Brennan
The Virtual Village Project
Evin Hernandez and Tom Brennan

Intended Audience

Capture the Flag

Capture the Flag

Traditionally, red vs blue

Both have flags

Both attack and defend

Capture the Flag

Also, ‘Jeopardy’ style (what we’ll be doing today)

WebGoat Background

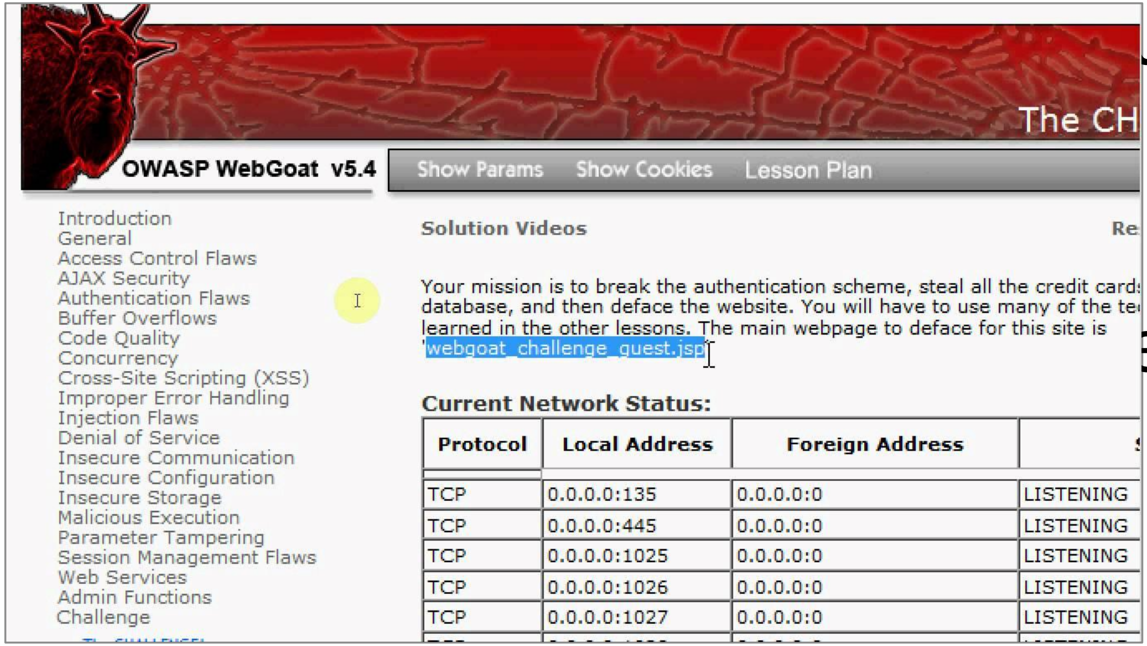
Originally a ‘gimmick’ … now a number of other OWASP ‘goats’ out there.

Transitioned through technologies, leadership and contributors over the years

WebGoat Background

umber of other

es, leadership



Your mission is to break the authentication scheme, steal all the credit card database, and then deface the website. You will have to use many of the te learned in the other lessons. The main webpage to deface for this site is 'webgoat_challenge_guest.jsp'

Current Network Status:

Protocol	Local Address	Foreign Address	
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1025	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1026	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1027	0.0.0.0:0	LISTENING

WebGoat Background

By 7.x, up to 50+ Security topics and developer labs, some redundant

Used by a number of vendors as a demo/baseline app to test for vulnerabilities

WebGoat Background

By 7.x, up to 50+ Security to developer labs, some redun

Used by a number of vendo demo/baseline app to test f

Other OWASP ‘Goats’

Node.js Goat (now JuiceShop too)

droidGoat

iGoat

WebGoat.Net

Rails Goat

WebGoat PHP

Security Shepherd

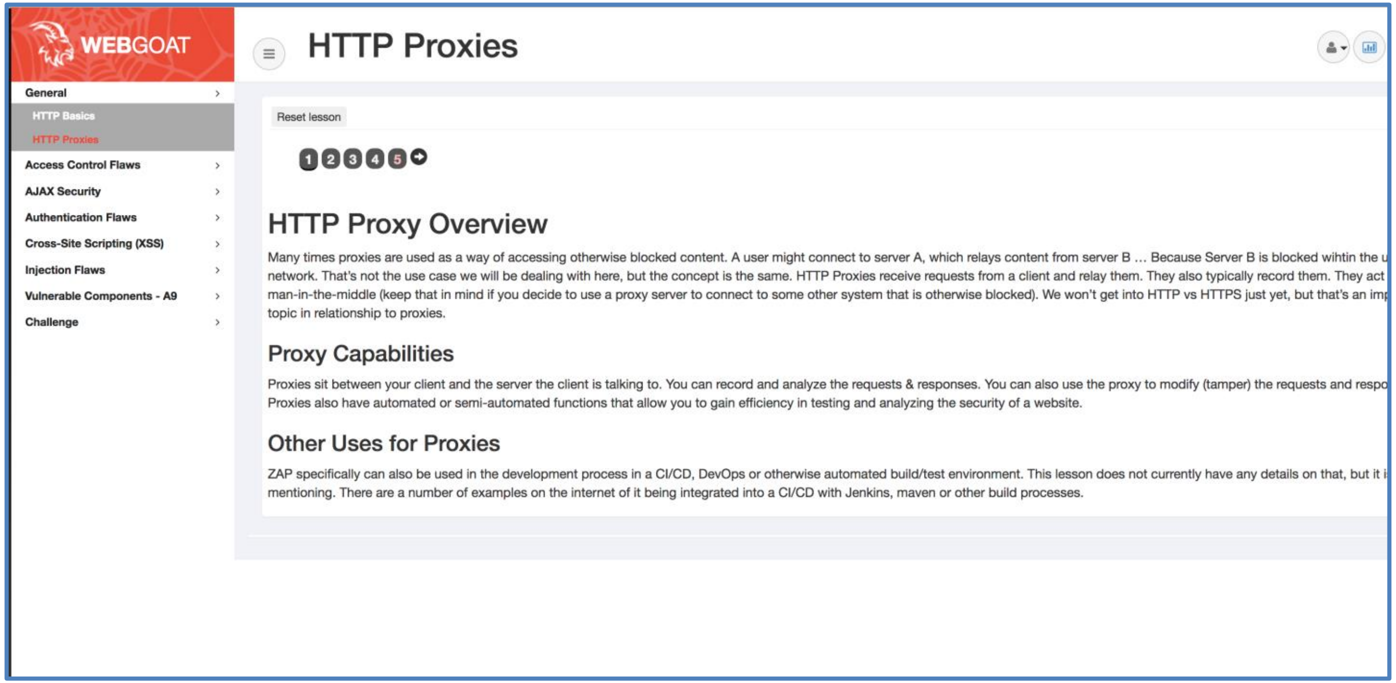
Fast Forward to 2017

6.x & 7.x mainly re-plumbing, general modernization

8.0 - New focus on content and ’assignments’ (or challenges)

Not just about vulnerabilities, but about secure coding too

WebGoat - Now



HTTP Proxies

HTTP Proxy Overview

Many times proxies are used as a way of accessing otherwise blocked content. A user might connect to server A, which relays content from server B … Because Server B is blocked wihtin the u network. That's not the use case we will be dealing with here, but the concept is the same. HTTP Proxies receive requests from a client and relay them. They also typically record them. They act man-in-the-middle (keep that in mind if you decide to use a proxy server to connect to some other system that is otherwise blocked). We won't get into HTTP vs HTTPS just yet, but that's an imp topic in relationship to proxies.

Proxy Capabilities

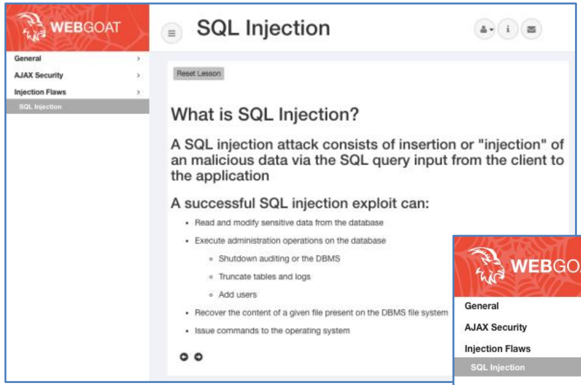
Proxies sit between your client and the server the client is talking to. You can record and analyze the requests & responses. You can also use the proxy to modify (tamper) the requests and respo Proxies also have automated or semi-automated functions that allow you to gain efficiency in testing and analyzing the security of a website.

Other Uses for Proxies

ZAP specifically can also be used in the development process in a CI/CD, DevOps or otherwise automated build/test environment. This lesson does not currently have any details on that, but it i mentioning. There are a number of examples on the internet of it being integrated into a CI/CD with Jenkins, maven or other build processes.

WebGoat 8 - A Training Platform

Instruction, Exploits & Best Practices



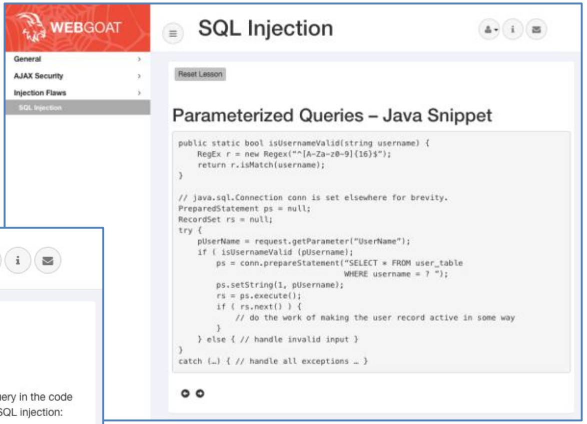
SQL Injection

What is SQL Injection?

A SQL injection attack consists of insertion or "injection" of an malicious data via the SQL query input from the client to the application

A successful SQL injection exploit can:

- Read and modify sensitive data from the database
- Execute administration operations on the database
  - Shutdown auditing or the DBMS
  - Truncate tables and logs
  - Add users
- Recover the content of a given file present on the DBMS file system
- Issue commands to the operating system

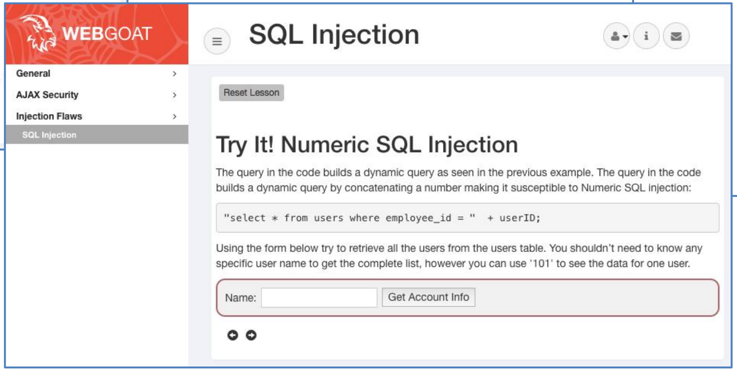


SQL Injection

Parameterized Queries – Java Snippet

```
public static bool isUsernameValid(string username) {
    RegEx r = new Regex("^[A-Za-z0-9]{16}$");
    return r.isMatch(username);
}

// java.sql.Connection conn is set elsewhere for brevity.
PreparedStatement ps = null;
RecordSet rs = null;
try {
    pUserName = request.getParameter("UserName");
    if ( isUsernameValid (pUsername);
        ps = conn.prepareStatement("SELECT * FROM user_table
                                    WHERE username = ? ");
        ps.setString(1, pUsername);
        rs = ps.execute();
        if ( rs.next() ) {
            // do the work of making the user record active in some way
        }
    } else { // handle invalid input }
}
catch (…) { // handle all exceptions … }
```



SQL Injection

Try It! Numeric SQL Injection

The query in the code builds a dynamic query as seen in the previous example. The query in the code builds a dynamic query by concatenating a number making it susceptible to Numeric SQL injection:

```
"select * from users where employee_id = "  + userID;
```

Using the form below try to retrieve all the users from the users table. You shouldn't need to know any specific user name to get the complete list, however you can use '101' to see the data for one user.

Back to Today’s CtF

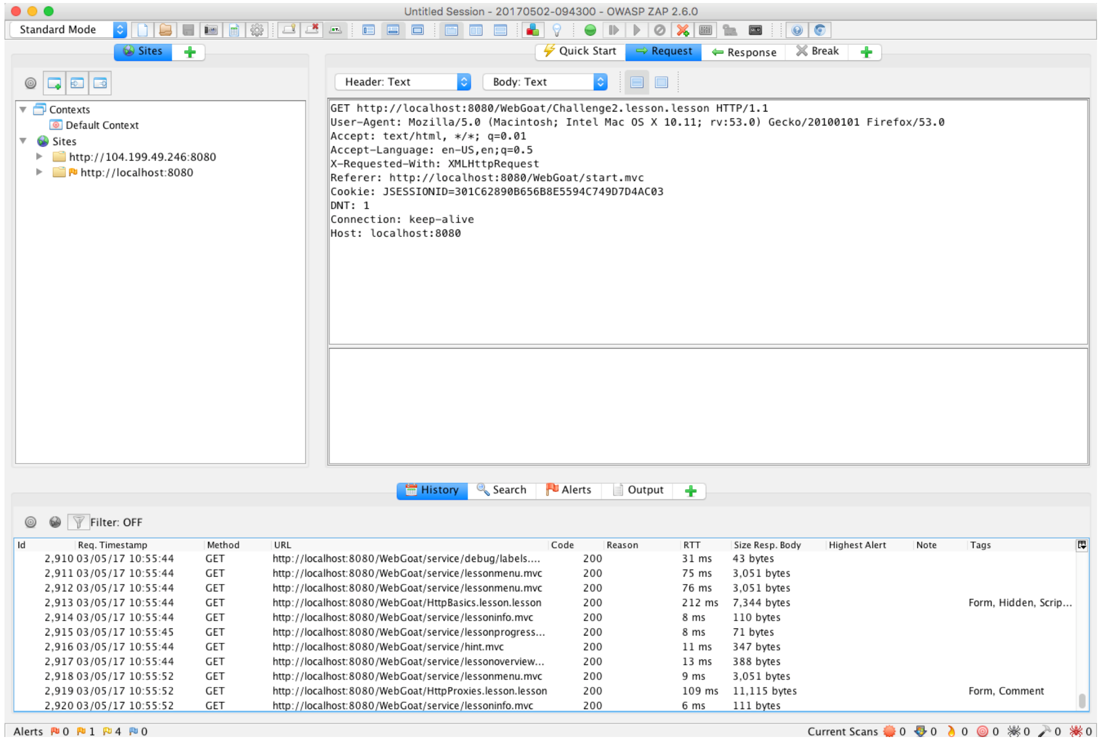
Today will be Jeopardy style, using WebGoat

AppSec Issues, also [mostly] covered in lessons in WebGoat

Tracked on a ‘scoreboard’

Doable with a proxy and a browser

Speaking of a proxy



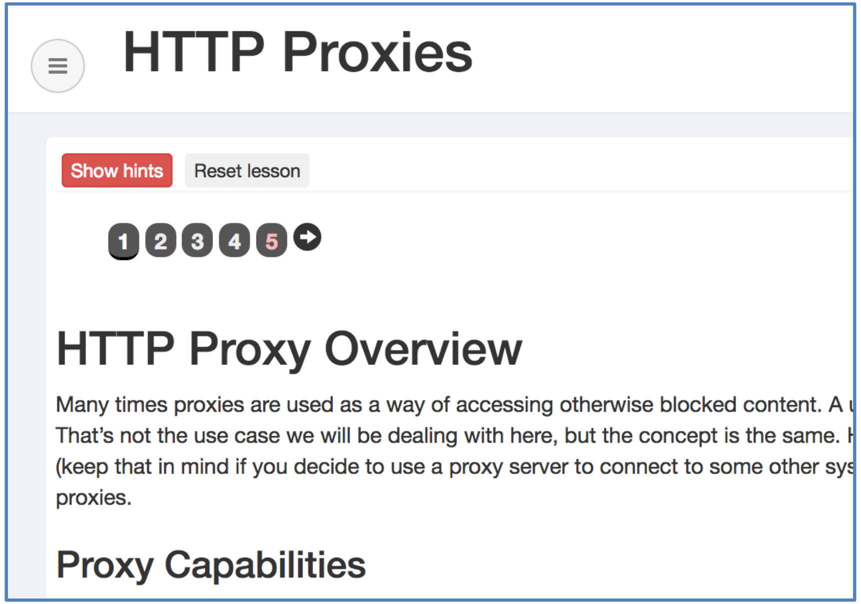
```
GET http://localhost:8080/WebGoat/Challenge2.lesson.lesson HTTP/1.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11; rv:53.0) Gecko/20100101 Firefox/53.0
Accept: text/html, */*; q=0.01
Accept-Language: en-US,en;q=0.5
X-Requested-With: XMLHttpRequest
Referer: http://localhost:8080/WebGoat/start.mvc
Cookie: JSESSIONID=301C62890B656B8E5594C749D7D4AC03
DNT: 1
Connection: keep-alive
Host: localhost:8080
```

Id	Req. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Body	Highest Alert	Note	Tags
2,910	03/05/17 10:55:44	GET	http://localhost:8080/WebGoat/service/debug/labels....	200		31 ms	43 bytes			
2,911	03/05/17 10:55:44	GET	http://localhost:8080/WebGoat/service/lessonmenu.mvc	200		75 ms	3,051 bytes			
2,912	03/05/17 10:55:44	GET	http://localhost:8080/WebGoat/service/lessonmenu.mvc	200		76 ms	3,051 bytes			
2,913	03/05/17 10:55:44	GET	http://localhost:8080/WebGoat/HttpBasics.lesson.lesson	200		212 ms	7,344 bytes			Form, Hidden, Scrip...
2,914	03/05/17 10:55:44	GET	http://localhost:8080/WebGoat/service/lessoninfo.mvc	200		8 ms	110 bytes			
2,915	03/05/17 10:55:45	GET	http://localhost:8080/WebGoat/service/lessonprogress...	200		8 ms	71 bytes			
2,916	03/05/17 10:55:44	GET	http://localhost:8080/WebGoat/service/hint.mvc	200		11 ms	347 bytes			
2,917	03/05/17 10:55:44	GET	http://localhost:8080/WebGoat/service/lessonoverview...	200		13 ms	388 bytes			
2,918	03/05/17 10:55:52	GET	http://localhost:8080/WebGoat/service/lessonmenu.mvc	200		9 ms	3,051 bytes			
2,919	03/05/17 10:55:52	GET	http://localhost:8080/WebGoat/HttpProxies.lesson.lesson	200		109 ms	11,115 bytes			Form, Comment
2,920	03/05/17 10:55:52	GET	http://localhost:8080/WebGoat/service/lessoninfo.mvc	200		6 ms	111 bytes			

Alerts 0 1 4 0 Current Scans 0 0 0 0 0 0 0

Using an Intercept Proxy

http://173.228.153.243:8080/WebGoat/



HTTP Proxies

HTTP Proxy Overview

Many times proxies are used as a way of accessing otherwise blocked content. A
That's not the use case we will be dealing with here, but the concept is the same.
(keep that in mind if you decide to use a proxy server to connect to some other sys
proxies.

Proxy Capabilities

<OWASP ZAP Demo />

Let’s Practice Some

Recommended Lessons

1. Client-side Filtering
2. XXE
3. SQL Injection

<Capture the Flags />

Post-Mortem

What did you learn today?

Questions?

Suggestions, Feedback?

WebGoat

https://github.com/WebGoat/WebGoat

@OWASP_WebGoat

Jason

jason.white@owasp.org

@misfir3

OWASP Slack (@misfir3)

Nanne

Nanne.baars@owasp.org

OWASP Slack @nbaars