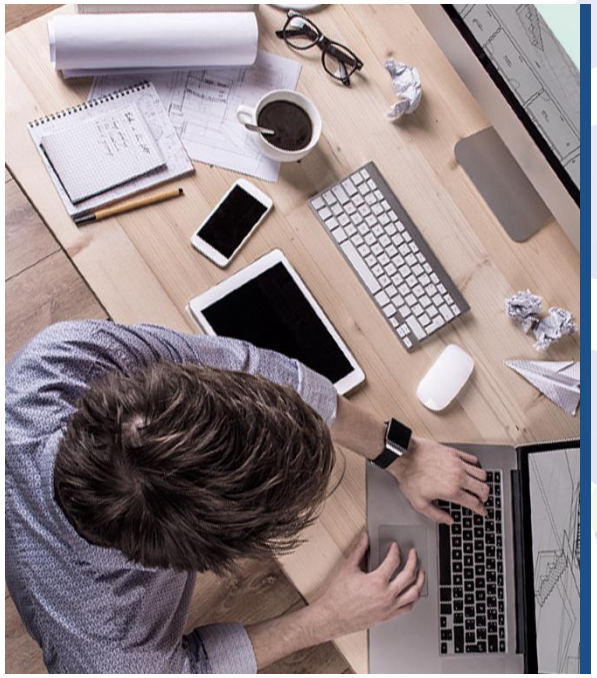
SANGFOR

SANGFOR_NGAF_V8.0.6_Professional

Attack Protection 2



1. Common Web Application Attack
2. SQL Injection
3. Whitelist

1. Common Web Application Attack

SANGFOR
深信服科技

Common Web Application Attack

The OWASP Top 10 is a powerful awareness document for web application security. It represents a broad consensus about the most critical security risks to web applications.

From 2007–2017, the Injection and XSS attack is always at top 3 attack.

OWASP Top 10 – 2013 (Previous)	OWASP Top 10 – 2017 (New)
A1 – Injection	A1 – Injection
A2 – Broken Authentication and Session Management	A2 – Broken Authentication and Session Management
A3 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References - Merged with A7	A4 – Broken Access Control (Original category in 2003/2004)
A5 – Security Misconfiguration	A5 – Security Misconfiguration
A6 – Sensitive Data Exposure	A6 – Sensitive Data Exposure
A7 – Missing Function Level Access Control - Merged with A4	A7 – Insufficient Attack Protection (NEW)
A8 – Cross-Site Request Forgery (CSRF)	A8 – Cross-Site Request Forgery (CSRF)
A9 – Using Components with Known Vulnerabilities	A9 – Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards - Dropped	A10 – Underprotected APIs (NEW)

Common Web Application Attack

Web application protection, mainly used to protect the web server from attack. The common attack is as below:

1. SQL Injection
2. XSS Attack
3. Trojan
4. Website Scan
5. WebShell
6. CSRF
7. OS Command Injection
8. File Inclusion
9. Path Traversal
10. Information Disclosure
11. Web Site Vulnerabilities

So on…

2. SQL Injection

SANGFOR
深信服科技

SQL Injection

SQL Injection refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server

SQL injection is actually in the web page to perform some SQL statements to operate the database, for its attack characteristics have a preliminary understanding, to further understanding, need to figure out the following questions:

1. Where does the attack data appear (where to submit, how to submit)
2. What is the SQL injection attack (what content is considered to be SQL injection attack)

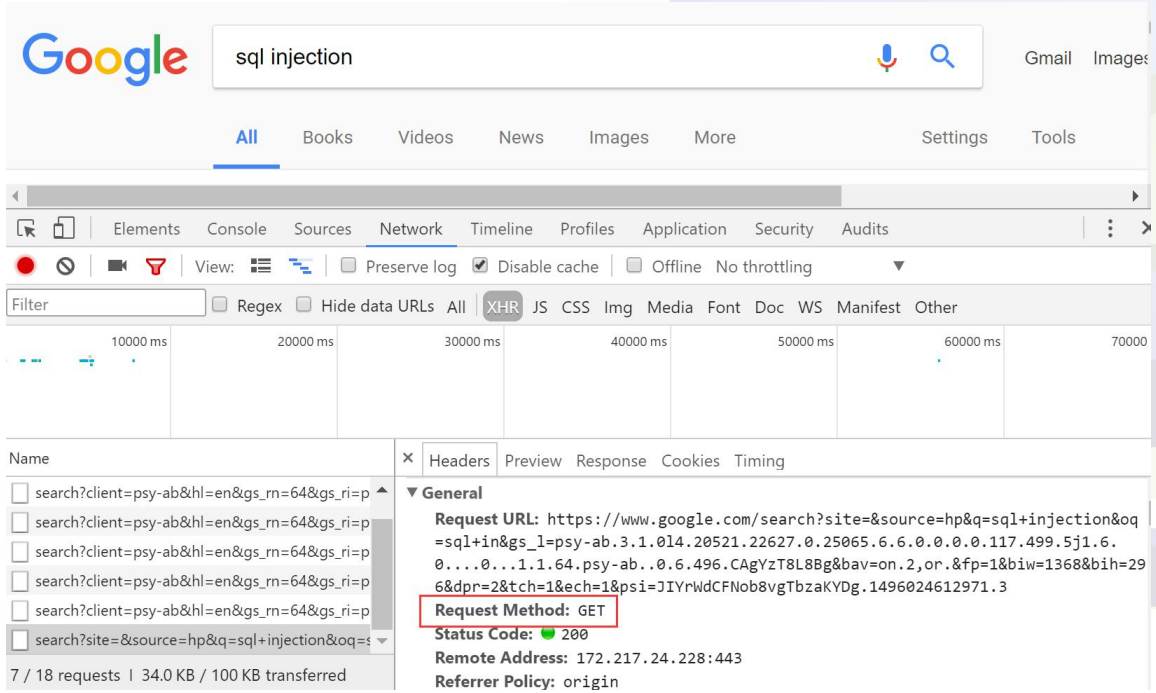
SQL Injection

Where does the attack data appear?

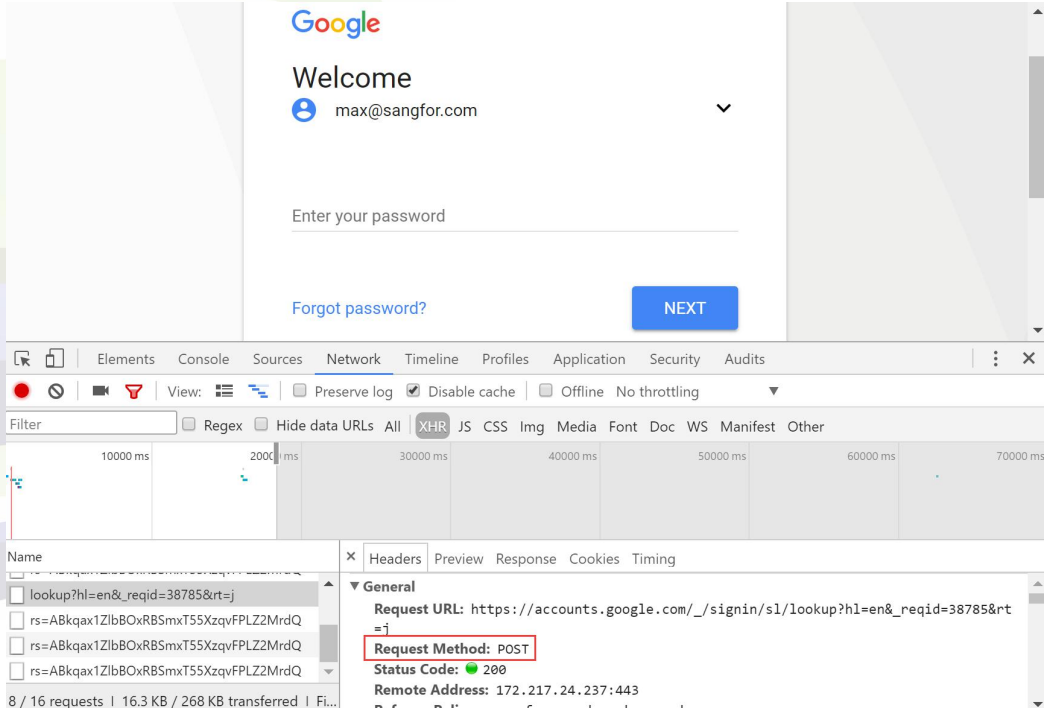
Two commonly used methods for a request-response between a client and server are: GET and POST.

- **GET** - Requests data from a specified resource
- **POST** - Submits data to be processed to a specified resource

GET



POST



SQL Injection

What is the SQL injection attack

SQL injection attacks can be classified according to their characteristics are weak features, strong features, injection tool features.

Weak attack: like “select * from test”, in this SQL statement, there are two key words: “select” and “from” perform a query, the risk is relatively low and strong attack;

Strong attack: such as “insert into test values (Max, 123)”, There are three SQL keywords: “insert”, “into”, “values” in this statement, and this statement may cause the user to add Max to the test table. This statement is considered dangerous. ;

Strong attack generally has the following characteristics:
1. contains three or more SQL keywords, and these three keywords together can become a legitimate SQL statement.
2. contains any SQL keyword conjunctions, these conjunctions include “union”, “;”, “and”, “or”, etc., and take the commonly used sql injection method to use these conjunctions, such as the existence of the packet “and 1 = 1” will be considered Strong features.

Injection tool attack: the use of a number of professional SQL injection tool to attack, these tools are attacks with fixed data flow characteristics.

SQL Injection

SQL injection test methods, generally can be divided into two types:

1. In the customer's real environment for scanning analysis to find the injection point and invasion,
   The first approach requires the tester to have a high level of technical analysis and may affect the customer's actual business, the test success rate is low, but also the most convincing.

2. Build a virtual environment and a demonstration.
   The second method is simple and easy to demonstrate, and can demonstrate the actual attack effect, the test success rate is higher, mainly play a demonstration effect.

SQL Injection

Take the virtual environment test as an example:

1. Build a test environment;
2. Get ready for testing tools or manually attack;
3. Configure NGAF WAF policy;
4. Check the NGAF WAF log.

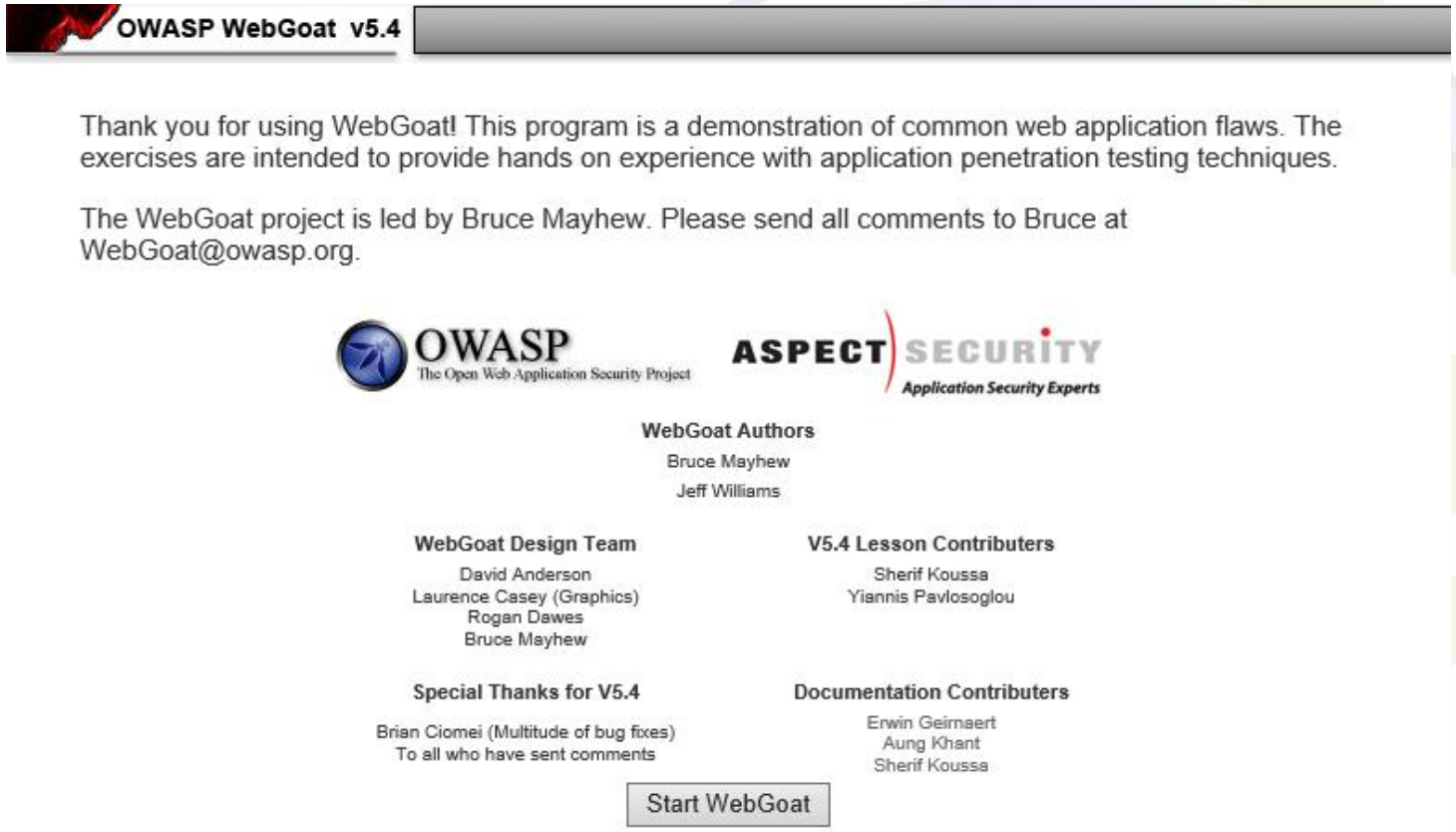
SQL Injection

Test diagram:

Configure the basic network settings.

SQL Injection

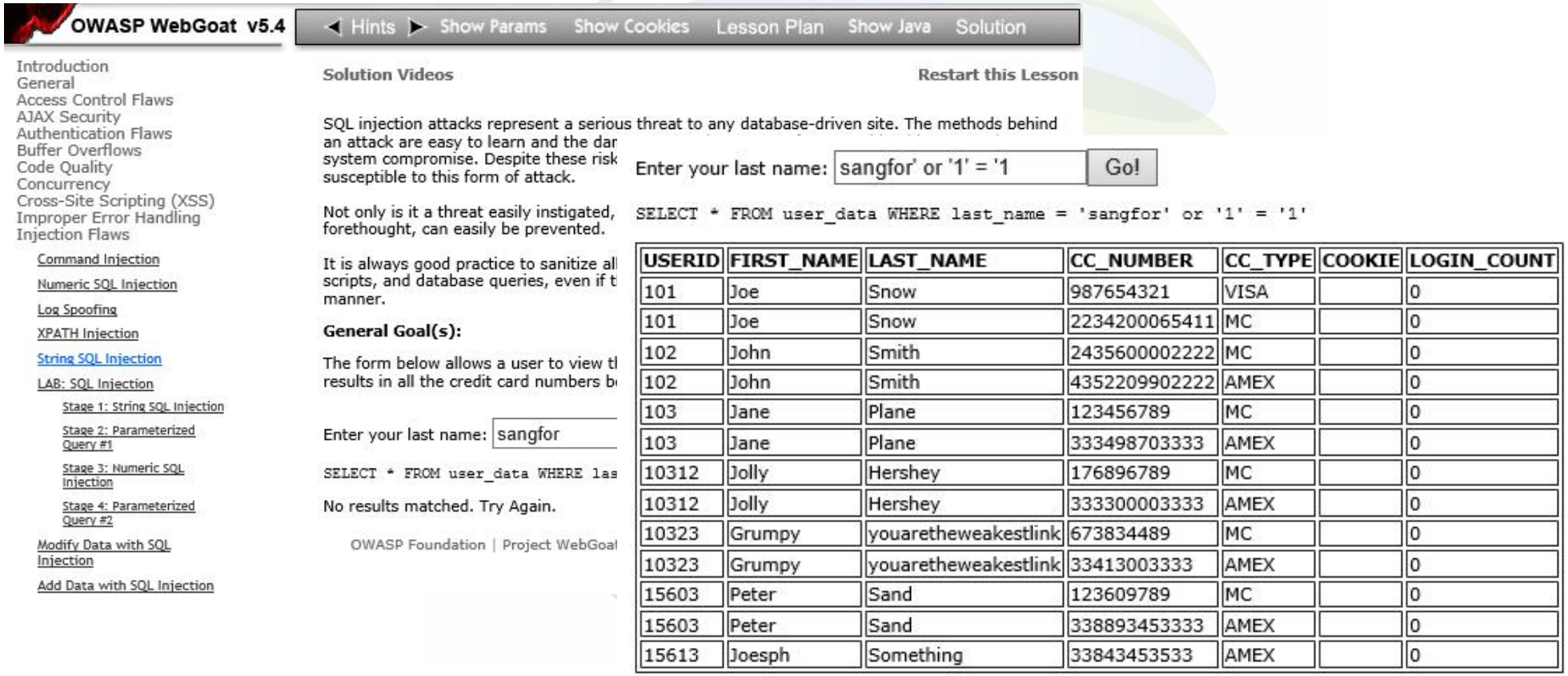
We use the WebGoat as the attack object.



You can learn more about WebGoat from https://www.owasp.org/index.php/Category:OWASP_WebGoat_Project

SQL Injection

String SQL injection attack without WAF



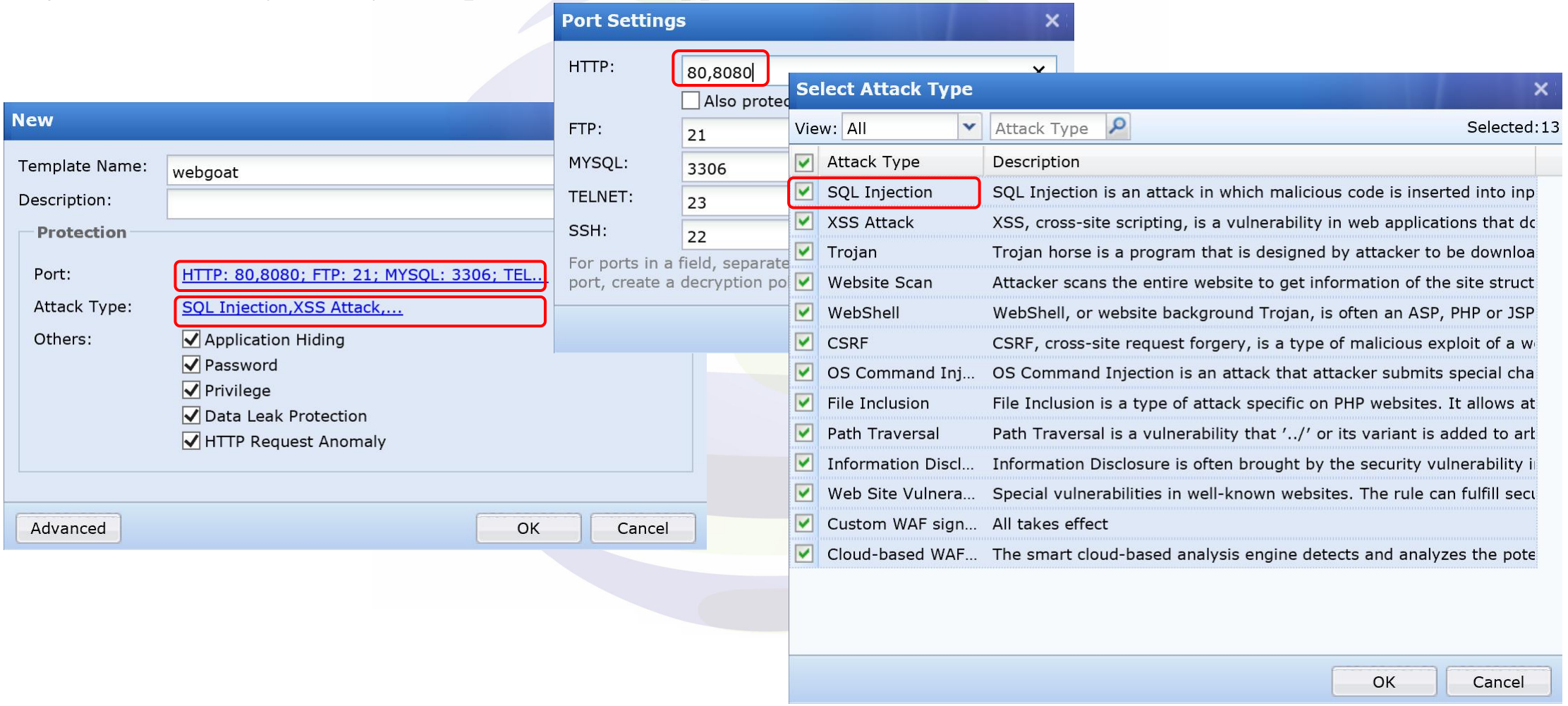
USERID	FIRST_NAME	LAST_NAME	CC_NUMBER	CC_TYPE	COOKIE	LOGIN_COUNT
101	Joe	Snow	987654321	VISA		0
101	Joe	Snow	2234200065411	MC		0
102	John	Smith	2435600002222	MC		0
102	John	Smith	4352209902222	AMEX		0
103	Jane	Plane	123456789	MC		0
103	Jane	Plane	333498703333	AMEX		0
10312	Jolly	Hershey	176896789	MC		0
10312	Jolly	Hershey	333300003333	AMEX		0
10323	Grumpy	youaretheweakestlink	673834489	MC		0
10323	Grumpy	youaretheweakestlink	33413003333	AMEX		0
15603	Peter	Sand	123609789	MC		0
15603	Peter	Sand	338893453333	AMEX		0
15613	Joesph	Something	33843453533	AMEX		0

All data is exposed.

SQL Injection

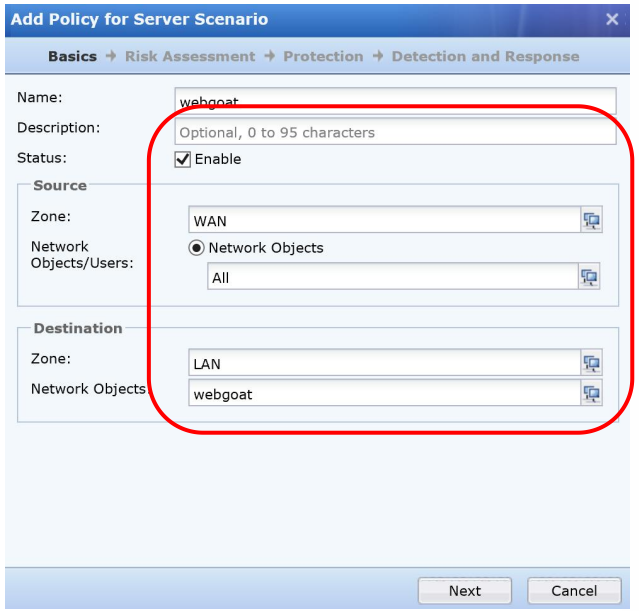
Create a template.

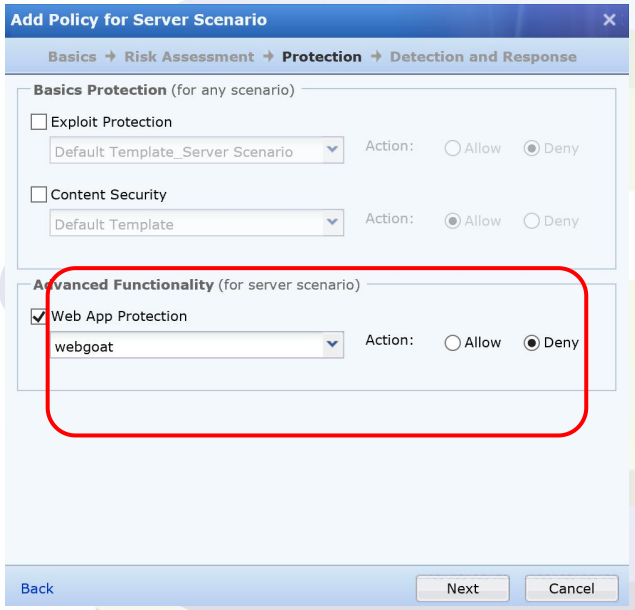
Objects > Security Policy Template > Web App Protection

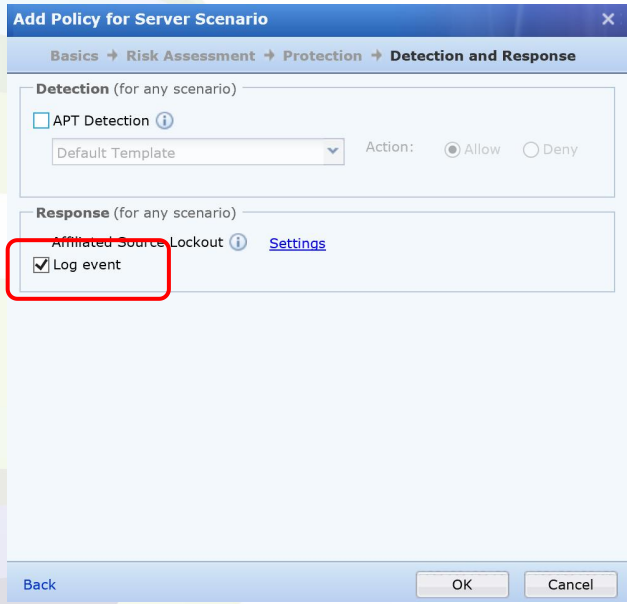


SQL Injection

Create a policy of Server Scenario.
Policies >Network Security > Policies

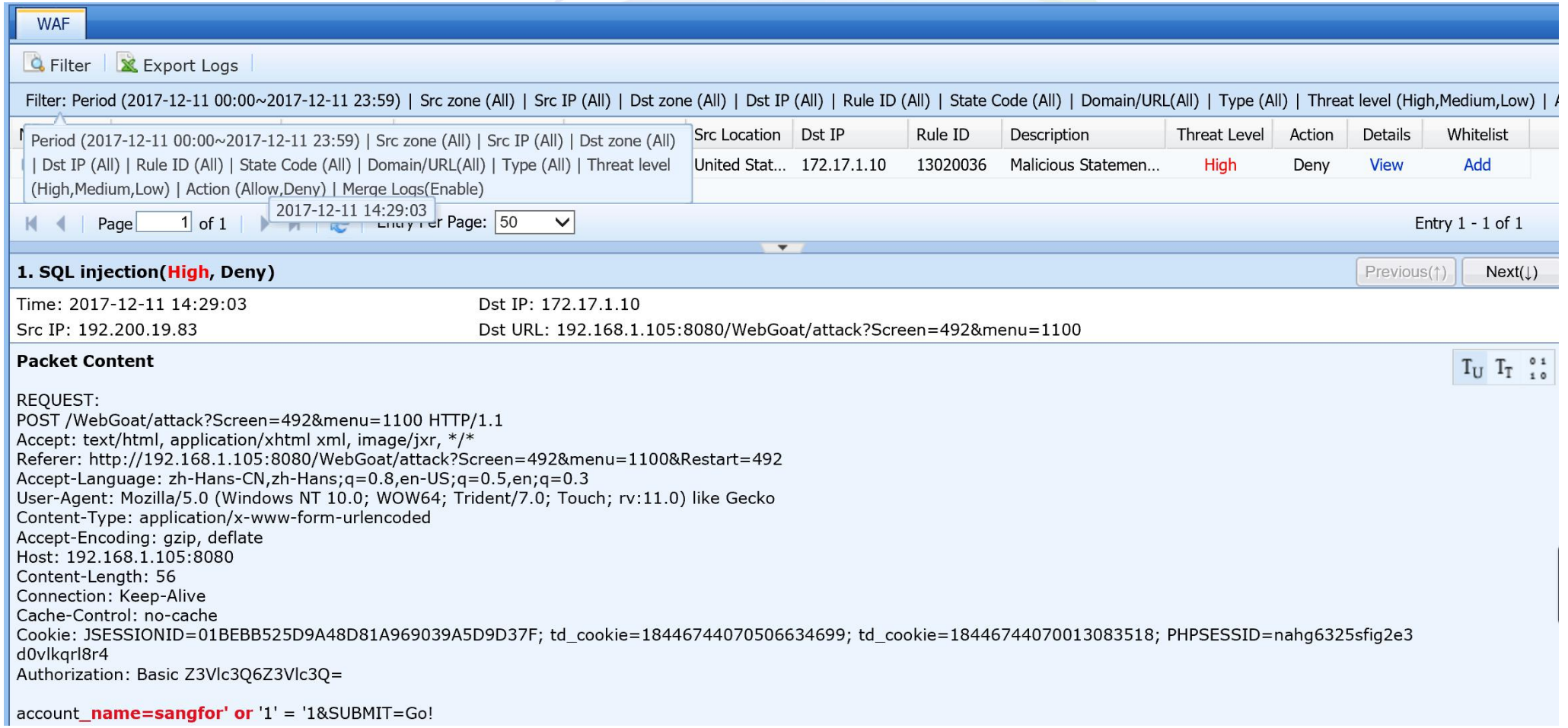






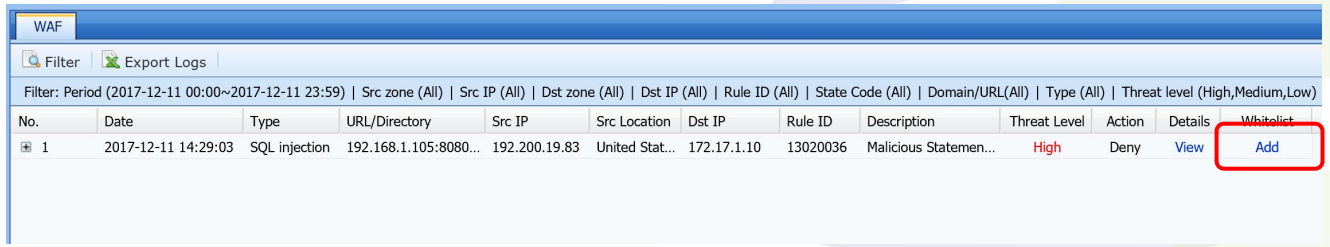
SQL Injection

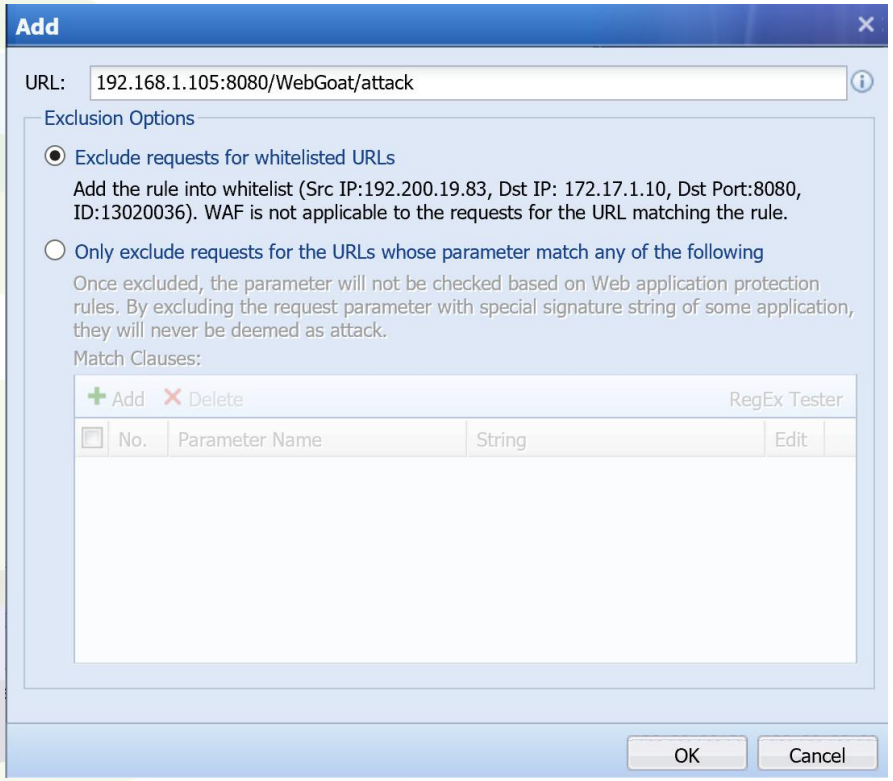
If we input the sangfor' or '1' = '1, NGAF will detect it and block it and we can check the log in report center.



SQL Injection

How to add whitelist if there is a misjudgment?



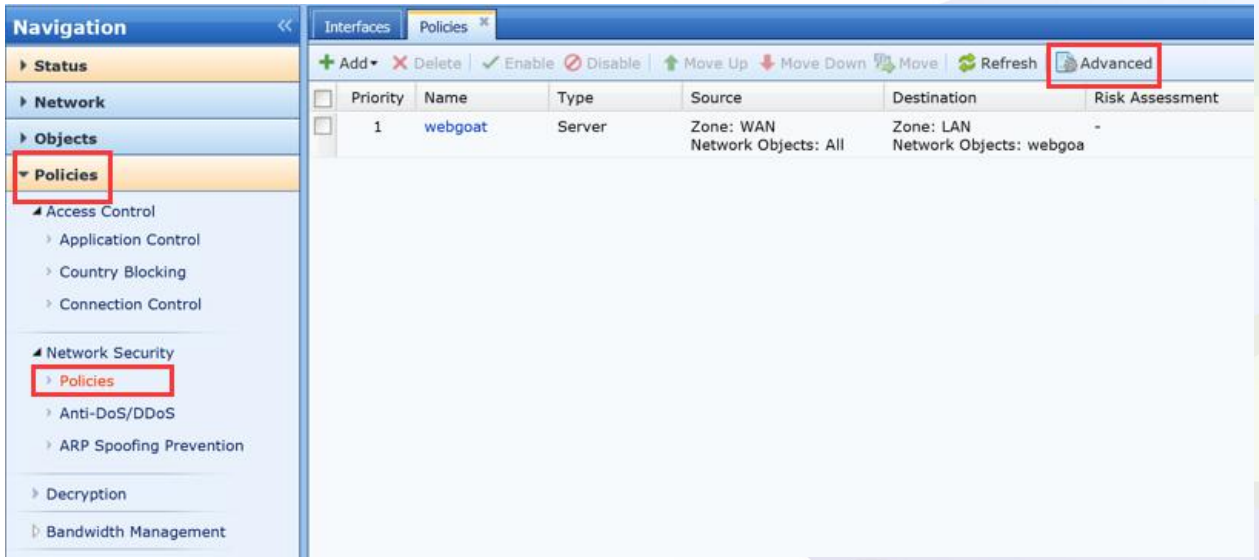


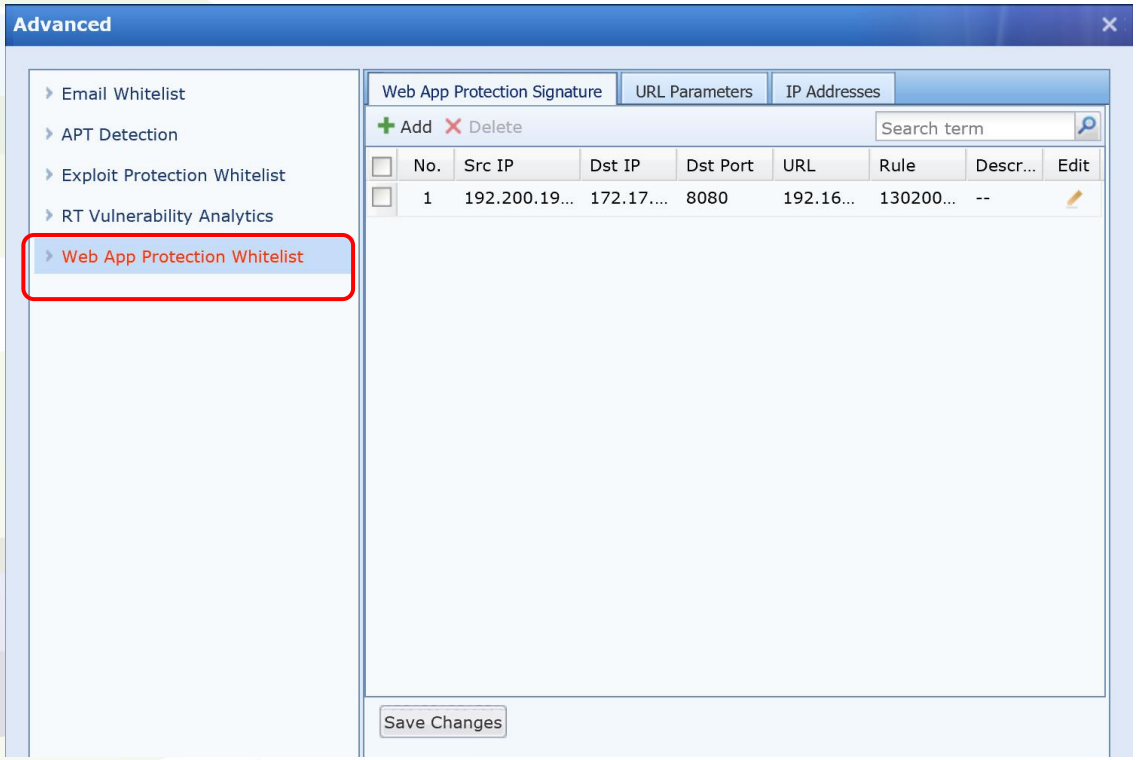
3. Whitelist

SANGFOR
深信服科技

Whitelist

We can check the whitelist added.

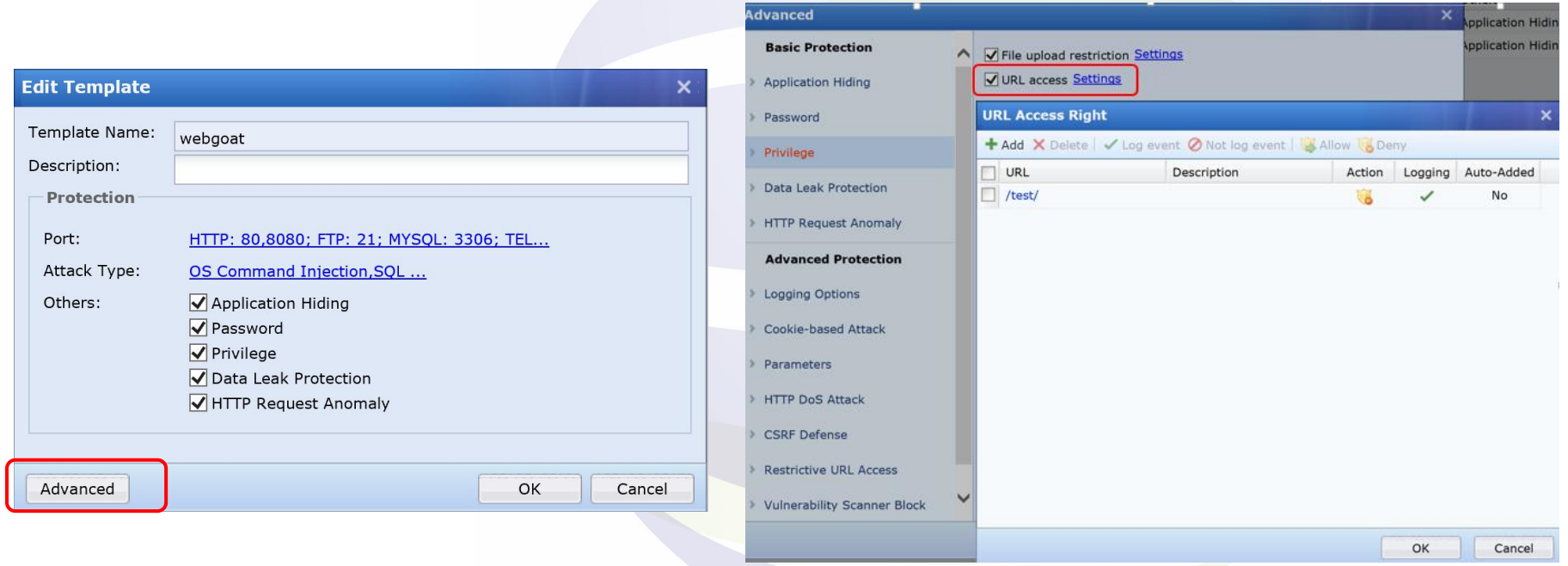




We can add manually here by these 3 ways.

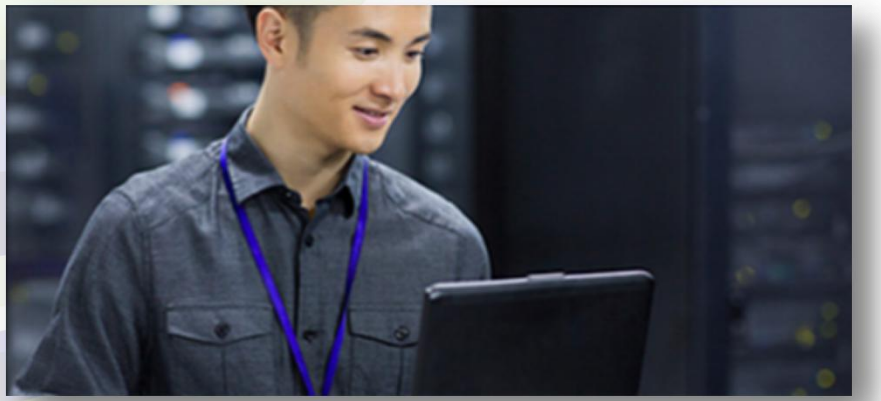
Whitelist

We also can add the URL to **URL access**, NGAF will not detect the URL added as allow and log the logs in the report center as **URL access**.



Thank you !

tech.support@sangfor.com
community.sangfor.com



Sangfor Technologies (Headquarters)
Block A1, Nanshan iPark, No.1001
Xueyuan Road, Nanshan District,
Shenzhen, Guangdong Province,
P. R. China (518055)